MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LAINFORMACIÓN

Diseño de un esquema de seguridad para la autenticación de teléfonos inteligentes Android en aplicaciones web corporativas, que utilizan un servicio de directorio.

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por la estudiante:
Shirley Patricia PINOS ROMERO

Bajo la dirección de:
Christian Mauricio MERCHAN MILLER

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador
Septiembre del 2018

Diseño de un esquema de seguridad para la autenticación de teléfonos inteligentes Android en aplicaciones web corporativas, que utilizan un servicio de directorio.

Design of a security scheme for the authentication of Android smartphones in corporate web applications, which use a directory service.

Shirley Patricia PINOS ROMERO[1]
Christian Mauricio MERCHAN MILLER[2]

Resumen

La información es uno de los bienes intangibles más importantes de las organizaciones, la estrategia actual está orientada a la prevención y detección temprana de amenazas y vulnerabilidades sobre este recurso; el presente trabajo desarrolla un esquema de seguridad para acceder de manera controlada al aplicativo web organizacional desde teléfonos inteligentes que operan con el sistema operativo Android; este mecanismo de seguridad propone el uso de un nuevo modelo de autenticación que captura el número IMEI como identificador único del dispositivo, este atributo se añade a la tradicional solicitud de usuario y contraseña para el acceso a los aplicativos web, en efecto, la información se autentica al validarla con los datos del usuario almacenados previamente en el Directorio Activo de la organización, utilizando un servidor web como intermediario y un servidor proxy en el área perimetral de la red. Los resultados obtenidos con la herramienta para pruebas de seguridad y penetración ZAP y la metodología OWASP, demostraron que el modelo de seguridad propuesto contribuye a minimizar los riesgos por A2: 2017-Autenticación rota y A5: 2017-Control de acceso roto de acuerdo a OWASP Top 10-2017 en la intranet organizacional; estos resultados experimentales indican que el modelo de seguridad para autentificar usuarios en una red organizacional, es capaz de soportar una variedad de ataques de tipo Spoofing-Looping, fuerza bruta o de diccionario, haciéndola más eficiente y menos vulnerable a ataques de adivinanza.

Palabras clave: | Autenticación, IMEI, Directorio Activo, Aplicación Web, Metodología OWASP.

Abstract

Information is one of the most important intangible assets of organizations, the current strategy is oriented to the prevention and early detection of threats and vulnerabilities on this resource, the present work develops a security scheme to access in a controlled way the organizational web application from smartphones that operate with the Android operating system; this security mechanism proposes the use of a new authentication model that captures the IMEI number as the unique identifier of the device, this attribute is added to the traditional user request and password for access to the web applications, in effect, the information is authenticates with the user's data previously stored in the Active Directory of the organization, using a web server as an intermediary and a proxy server in the perimeter of the network. The results obtained with the tool for ZAP penetration and security tests and the OWASP methodology, demonstrated that the proposed security model contributes to minimize the risks by A2: 2017-Broken authentication and A5: 2017-Broken access control according to OWASP Top 10-2017 in the organizational intranet; These experimental results indicate that the security model for authenticating users in an organizational network is capable of supporting a variety of Spoofing-Looping, brute force or dictionary attacks, making it more efficient and less vulnerable to guessin attacks.

Key words | Authentication, IMEI, Active Directory, Web Application, OWASP Methodology

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail spinos@uees.edu.ec
[2] Docente de la Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail cmmerchan@uees.edu.ec

INTRODUCCIÓN

La generalización del uso de dispositivos móviles, tanto en el caso de organizaciones como en clientes particulares, junto con la necesidad de estar siempre conectados e informados, ha impulsado no solo el desarrollo aplicaciones web, sino también la mejora en sus prestaciones (Solutions, 2012). En este contexto, las organizaciones están enfocadas en mantenerse a la vanguardia, presentando una imagen de innovación, a través del desarrollo de aplicaciones móviles que facilitan las gestiones en sus procesos y que mantienen a sus integrantes conectados.

Es así que, desde el año 2009, el concepto "Traiga su Propio Dispositivo" o BYOD (Por sus siglas en inglés) ha revolucionado muchas industrias. Esta investigación afirma que, mientras el 44% de las organizaciones encuestadas estaban permitiendo a los empleados trabajar con sus propios dispositivos, otro 18% estaba planeando hacerlo en los próximos 12 meses; tendencia que ha ayudado a las empresas a reducir los costos de hardware y servicios (Tech Pro, 2015).

En este mismo tema, otro informe afirma que el 50% de las grandes empresas desarrolladoras de aplicaciones móviles no destina ningún presupuesto a la seguridad y casi el 40% de ellas no están tomando las precauciones pertinentes para proteger las aplicaciones móviles que desarrollan para sus usuarios. Así mismo, describen que aunque la mayoría de los empleados hace uso intensivo de las aplicaciones, más de la mitad (un 55%) afirma que su organización no cuenta con una política que defina cómo debería ser su uso en el móvil en el lugar de trabajo, y del mismo modo, el 55% de las organizaciones dice que los empleados están autorizados a utilizar y descargar aplicaciones empresariales en los dispositivos personales (IBM, 2015).

En efecto, la subsidiaria de Hewlett Packard Enterprise, presenta un reporte de las vulnerabilidades más comunes detectadas en las aplicaciones de teléfonos inteligentes, donde señala que aproximadamente el 88% de las aplicaciones móviles inspeccionadas en este estudio presentaban vulnerabilidades, entre las que se destacan con el 22% el control de accesos a los aplicativos, errores de autentificación y violaciones a la privacidad (TechBeacon, 2016).

De modo que, hoy en día se considera importante reforzar los sistemas de autenticación, debido a que generalmente los usuarios estándar emplean claves de acceso fáciles de recordar, como el mismo nombre de usuario y empleo de la misma contraseña para diferentes servicios, comprometiendo a la seguridad de la información, desde la fase de la autenticación (Carullo, Ferrucci, & Sarro, 2012).

En este contexto, se presentan numerosos problemas con la implementación de las políticas de seguridad física y lógica, relacionados con la transmisión de datos y su vulneración, ya que los dispositivos móviles acceden a las aplicaciones web corporativas desde diferentes ubicaciones geográficas (Saurabh, Sampalli, & ye, 2016). Por consiguiente, reforzar la autenticación es un paso primario para salvaguardar la integridad y confidencialidad de una infraestructura que solo puede mantenerse mediante la identificación adecuada de los usuarios finales. Los controles de autenticación y autorización ayudan a proteger a la organización del acceso no aprobado desde dispositivos móviles a información privilegiada (UShafique, y otros, 2017).

Y aunque los usuarios esperan que los servicios modernos de Internet integren en su contenido la protección de sus sistemas informáticos locales, sin problemas y sin esfuerzo en las aplicaciones, por ahora, la implementación de seguridades adicionales, será necesaria para reducir entidades potencialmente malintencionadas (Wurzinger, Platzer, Ludl, Kirda, & Kruegel, 2009).

De ahí que, esta investigación se enmarca particularmente en fortalecer los controles de seguridad para el acceso de los usuarios a los aplicativos web organizacionales, que evidentemente en el análisis que se realizó a la problemática actual, arrojó pocos resultados en el mercado de aplicaciones que expongan un modelo de seguridad basado en la interacción con el directorio activo organizacional, utilizando métodos alternativos de inicio de sesión y la participación directa de los administradores para lograr un entorno controlado.

Marforio, Nikolaos, Soriente, Kostiainen, & Apkun (2014) sostienen además, que la tendencia actual de las organizaciones es emplear un segundo factor de seguridad como mecanismo de acceso para la autentificación de teléfonos móviles, situación que se ha vuelto común especialmente en las entidades de servicios que están adoptando métodos alternativos para el inicio de sesión en sus aplicativos como son: el uso de códigos de verificación automática, cartilla de coordenadas, tokens y el uso de identificadores únicos, a fin de verificar la identidad del usuario autorizado.

Para concluir, el argumento central del presente trabajo consiste en reforzar el modelo tradicional de autenticación que conecta al dispositivo móvil inteligente hacia el servidor web organizacional, para esto se propone incrementar el nivel de seguridad en la zona perimetral y en su mecanismo de acceso, validando el usuario, la contraseña y el IMEI como código único del empleado, contra la información que reposa en el Directorio Activo ubicado dentro del dominio de la organización teniendo como intermediario al servidor web y al servidor proxy inverso. Con este proceso se plantea presentar un mecanismo de autenticación eficiente, el cual ha sido evaluado con la herramienta para pruebas de seguridad y penetración ZAP (Zed Attack Proxy) y con el apartado de análisis de riesgos Top 10-2017 de la metodología OWASP (Proyecto abierto de seguridad de aplicaciones web) para reducir o mitigar el riesgo que supone intentos de acceso no autorizados tipo Spoofing-Looping, fuerza bruta o ataques de diccionario.

MARCO TEÓRICO

Esquema de Seguridad en la Red

Domingo (2014) señala que las aplicaciones son una fuente de vulnerabilidad para los sistemas de información, sin embargo, afirma que la seguridad perimetral contribuye a disminuir los riesgos. Existen diferentes aplicaciones que pueden añadir nuevas capas de seguridad a los dispositivos móviles, ya sea con métodos de autenticación adicionales más restrictivos, sistemas de copia de seguridad, cifrado de los datos, aplicaciones antivirus o cortafuegos que pueden utilizarse para crear un sistema de seguridad robusto.

Las herramientas de seguridad interactúan con otros mecanismos, como cortafuegos, herramientas de monitoreo, herramientas evasivas, entre otras para lograr cerrar más, los posibles accesos no autorizados

Mejía & Ramírez (2016) señalan que los controles de seguridad son medios de protección frente amenazas, que reducen la frecuencia de los ataques y limitan el daño causado por éstos. Una vez definidas las tecnologías a utilizar, se proponen los controles de seguridad específicos que se necesitarán.

Aplicación web

De acuerdo a Vora (2009), una aplicación web es un software o programa codificado en un lenguaje compatible con el navegador, como JavaScript o HTML, el cual esta habitualmente orientado a un modelo de servicio.

Fuchs, Hofkirchner, Schafranek, Raffl & Sandoval (2010), afirman que las aplicaciones web se establecieron con el objetivo de acceder a la información desde cualquier lugar, en donde la navegación e intercambio de datos

generalmente inicia con la autenticación del usuario en forma de lenguaje de hipertexto.

Seguridades de Aplicaciones web

Huang (2015) manifiesta que la seguridad de las aplicaciones web sigue siendo un obstáculo importante para la aceptación universal de los aplicativos en la web para muchos tipos de transacciones en línea, especialmente dado que el reciente aumento pronunciado de vulnerabilidades explotables remotamente se ha atribuido a errores de las aplicaciones. Recientemente, las herramientas de verificación formal también han demostrado su éxito en el descubrimiento de vulnerabilidades en los programas.

Además, Parravisini (2011) expresa que los problemas de seguridad en la aplicaciones web constituyen un capitulo extenso de estudio, debido a que las seguridades no se referencian a una tecnología o a un lenguaje en particular, sino que afectan a todos los programas que se desarrollen, es por ese motivo que, para garantizar la disminución de los agujeros de seguridad, y que el riesgo se mantenga en un nivel aceptable, se debe comprender de manera abstracta el uso de herramientas y metodologías que orienten a las mejores prácticas a los desarrolladores y al personal de seguridad organizacional.

Riesgos de seguridad en aplicaciones web

La norma ISO 27001 (2013) define como riesgo a la posibilidad en que una amenaza concreta pueda explotar una vulnerabilidad, para causar una pérdida o daño en un activo de información.

Hiard (2016) señala que, cuando más tarde se detecte el riesgo, más difícilmente reversibles serán las consecuencias; el análisis de riesgo permite detectar los peligros inherentes y controlarlos a lo largo del ciclo de vida.

Metodología OWASP

OWASP (2018) se describe como una comunidad abierta, dedicada al análisis de las seguridades en aplicaciones web y su entorno, proporcionando directrices para un software seguro y además determina mediante estándares, estudios, buenas prácticas, etc., las causas hacen a un software inseguro.

El marco de referencia proporcionado por OWASP es usado incluso por estándares internacionales de seguridad informática, tales como: COBIT, ITIL e ISO-27001. OWASP Top 10-2017, además de identificar los riesgos, enseña como remediar dichas vulnerabilidades con ejemplos y buenas prácticas. Los atacantes pueden, potencialmente, utilizar diferentes rutas a través de su aplicación para perjudicar su negocio u organización, cada uno de estos caminos representa un riesgo que puede o no ser suficientemente grave como para merecer atención. En la Figura 1, se observa un esquema que representa el ciclo del ataque, que inicia por la búsqueda de las herramientas que ayuden a encontrar la debilidad en la seguridad, la validación de los controles y finalmente el impacto que sufre el negocio, por el daño o eliminación de sus activos intangibles.

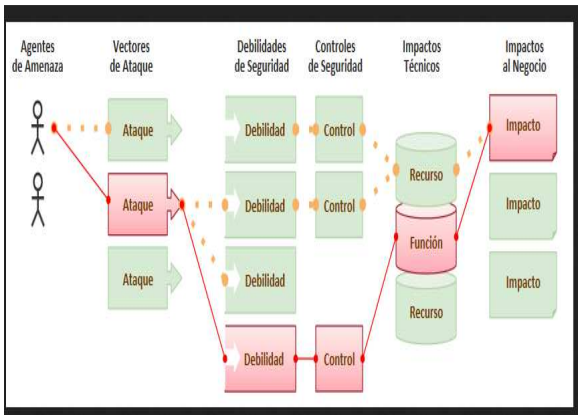

Figura 1. Esquema de amenaza, controles e impacto técnico del negocio. (Foundation, 2017)

Riesgos según la Metodología OWASP Top10-2017

El OWASP Top 10 se enfoca en identificar los riesgos más críticos para un amplio tipo de organizaciones. Para cada uno de estos

riesgos, se proporciona información genérica sobre la probabilidad y el impacto técnico.

La Metodología de Evaluación de Riesgo OWASP (2018) presenta numerosos factores para ayudar a calcular el riesgo de una vulnerabilidad identificada. Sin embargo, el Top 10 debe basarse en generalidades en lugar de vulnerabilidades específicas en aplicaciones y APIs reales, como se resumen en la Figura 2. El propietario o administrador del sistema está mejor capacitado para juzgar la importancia de las aplicaciones, de los datos, de conocer sus amenazas, cómo ha sido construido y cómo está siendo operado el sistema.

Figura 2. Riesgos OWAST Top 10-2017 (Foundation, 2017)

Herramienta de detección de vulnerabilidades ZAP

OWASP (2018) define a Zed Attack Proxy (ZAP) como una herramienta intuitiva que puede detectar vulnerabilidades de seguridad y penetración como: Inyección SQL, Cross Site Scripting, inclusión de archivos, gestión de sesiones, configuraciones de servicios débiles, Spoofing-Looping, fuerza bruta, entre otros y está alineada con el proyecto OWASP Top 10-2017.

Directorio Activo

De acuerdo a OpenLDAP (2012), el Directorio Activo, es una base de datos especializada y específicamente diseñada para funciones básicas de búsqueda y de actualización. Los directorios tienden a contener información descriptiva, basada en atributos y soportan un sofisticado filtrado.

Desmond, Richards, Allen, & Alistair (2009) afirman que, el directorio activo es un repositorio común para obtener información de objetos que residen en la red. Por defecto, el esquema del directorio Activo soporta muchos atributos por cada clase de objetos que pueden ser almacenados.

Microsoft (2008) establece que un esquema es la estructura subyacente que proporciona el formato para un servicio de directorio. El esquema de directorio activo define las clases y atributos de objeto que se usan en los Servicios de dominio. El esquema principal proporciona definiciones para muchas clases conocidas como: usuario, computador y unidad organizacional, y además atributos como números de teléfono o Identificadores únicos.

De ahí que, Aguilar, Pérez, & Cornejo (2011) indican que el Protocolo Ligero de acceso a aplicaciones (LDAP), corre sobre la pila TCP/IP y que sus aplicaciones son independientes de la plataforma que los hospeda. LDAP ha ganado auge como método de acceso a directorio en la intranet corporativa por su capacidad de implementar permisos hacia los archivos o recursos. Las herramientas OpenLDAP y de directorio activo utilizan los servicios de LDPA, lo que permite que cuenten con la capacidad de crear un árbol de directorios manteniendo la integridad de los archivos. No obstante, para cumplir con la administración de estos servicios,

se requiere de conocimientos sobre temas como: LDAP, Kerberos, DNS y políticas de grupo. Además se ofrece el mecanismo que presenta más flexibilización para el desarrollo de las aplicaciones, cuando un nuevo atributo es adicionado en el árbol, se lo realiza como una instancia del esquema ClassSchemaObject del Directorio Activo.

Teléfonos inteligentes

Maaniitty (2011) señala que los teléfonos inteligentes son herramientas utilizadas por los usuarios, que se encuentran definidos por sus características, su utilidad, por el propósito requerido y por la capacidad de su interfaz. Por otro lado, de acuerdo a Kamel, Wheeler, Tavares, & Jones (2011) manifiestan que estos teléfonos son dispositivos que ofrecen no solo las instalaciones estándar, como la comunicación de voz y texto, sino también una avanzada capacidad de cómputo y comunicación.

Identificadores Únicos para los teléfonos Inteligentes

Android (2017) afirma que el sistema operativo de sus equipos, ofrece una variedad de Identificadores (ID) con diferentes características de comportamiento, dependiendo del funcionamiento de las características que se requieran. La exclusividad establece las probabilidades de que no existan identificadores idénticos en el ámbito asociado. En el nivel más alto, un identificador exclusivo global nunca experimentará una colisión, ni siquiera en otros dispositivos o aplicaciones. Los ID de instancia ofrecen mejores propiedades de privacidad en comparación con los ID de hardware para el ámbito del dispositivo que no admiten restablecimiento, debido a que el identificador es único a nivel global, y puede usarse para identificar una instancia de APP específica.

Mientras que, Moreno (2015) señala que el IMEI es un identificador único ubicado en cada terminal. Cada móvil tiene su IMEI diferente, este número es muy importante ya que se encarga de identificar al terminal en la red.

Electronic Frontier Foundation (2015) se refiere al número de Identidad de Suscriptor Móvil Internacional IMSI, que identifica la tarjeta SIM de un suscriptor particular, se utiliza principalmente como un número de identificación para cada dispositivo Android. El IMSI asocia un teléfono único a su portador.

Como estos identificadores existen otros códigos únicos en los dispositivos inteligentes que se pueden considerar para identificarlos individualmente.

Teléfonos con sistema operativo Android

Amaro (2012) que el sistema operativo móvil de los teléfonos inteligentes Android, están basados en el kernel de Linux, con una interfaz de programación Java desarrollado por la Open Handset Alliance, la cual es liderada por Google. Android permite programar aplicaciones en una variación de la máquina virtual de Java llamada Android Runtime. El sistema operativo proporciona todas las interfaces necesarias para el desarrollo de programas, a través de un lenguaje muy popular, como es Java y su framework de aplicaciones, que permite el remplazo y la reutilización de los componentes.

APIs para Android

Para Jason (2013) una interfaz de aplicaciones de programación (API), incluye un conjunto de métodos para acceder a datos en otro sistema cerrado. Los APIs dan a los programadores y desarrolladores las herramientas necesarias para construir software con datos y servicios de fuentes externas.

De acuerdo a Patiño-Díaz (2013) la plataforma de Android proporciona un framework API, que las aplicaciones pueden utilizar para interactuar con este Sistema Operativo.

Autenticación

Según Niño (2011), la autenticación es el método que se utiliza para añadir usuarios al

sistema, normalmente la forma de autenticarse puede ser interna o externa. La forma interna seria desde el propio sistema de gestión de archivos de la web, y la externa utilizando un sistema de control de archivos como el directorio activo u otro sistema. En la Figura 3, se verifica las fases de seguridad en la aplicación.

Figura 3. Fase de Autenticación en el esquema de seguridad para la detección, prevención y detección de fallos de seguridad en las aplicaciones web de la organización (OWASP, 2018)

De acuerdo a OWASP (2017), la Autenticación debe garantizar que una aplicación verificada cumpla con los siguientes requisitos de alto nivel:

- Verificar la identidad digital del emisor de una comunicación.
- Asegurar que solo aquellos autorizados puedan autenticarse y las credenciales sean transportadas de manera segura.

Autenticación de Teléfonos Inteligentes

Vapen & Shahmehri (2011) definen que las soluciones de autenticación para teléfonos inteligentes difieren significativamente entre sí, y que hay muchas opciones para asegurar la transferencia de datos y la comunicación, puede ser difícil determinar los niveles de seguridad como una solución. También es difícil de representar una nueva solución de autenticación con un nivel de seguridad especificado, ya que las opciones de entrada y comunicación dependen de la situación específica.

Por su parte, Domingo (2014) indica que el sistema de intercambio de claves no implica el envío de claves en claro, pero requiere que la clave secreta compartida se haya proporcionado por un canal seguro con anterioridad al proceso de autenticación. Por defecto, los Smartphone se venden como mínimo con una medida de autenticación como es el código PIN, que se tiene que introducir al iniciar el dispositivo. Pero, una vez el dispositivo está encendido, no es común para los usuarios utilizar más métodos de autenticación, lo que lo hace muy vulnerable. Por ello, se han desarrollado aplicaciones que aseguran la autenticación durante la utilización del dispositivo.

Es así que, Vongsingthon & Boonkrong (2014) señalan que los métodos de autenticación basados en tokens o identificadores se deben utilizar regularmente. Existen varios enfoques para el uso de tokens de hardware y software. Basado en hardware puede ir desde tarjetas de proximidad sin contacto a tarjetas inteligentes de contacto regulares dentro del propio teléfono móvil, mientras que el software puede presentarse en forma de contraseña única, código QR, identificadores únicos etc. El software de autenticación puede tener algunas ventajas sobre el hardware, a través de una rápida y fácil finalización del procedimiento de autenticación.

Carullo, Ferrucci & Sarro (2012) señalan como una opción óptima, que los datos de la sesión se transfieran desde el teléfono inteligente al servidor de autenticación, a través de códigos únicos de identificación.

Para autenticar al usuario que accederá al servicio web, se requiere un teléfono inteligente con una tarjeta SIM. El proveedor de identidad utilizará un servidor LDAP para almacenar los códigos únicos (IMEI o el IMSI) del usuario, que son identificadores asociados con el teléfono móvil y la tarjeta SIM; de esta forma se garantiza un nivel alto de seguridad, ya que el

atacante debe burlar la autenticación normal y además derribar el código único del móvil para la suplantación.

Developer Android (2017) afirma que para codificar y recuperar la identificación única asociada a un dispositivo, se utiliza el método getDeviceId() como se muestra en la Figura 4; la función de obtención de código único del dispositivo, puede llamarse desde otros lenguaje de programación que utilicen el mismo esquema de seguridad, para fortalecer el proceso de autenticación de usuarios.

```
Private String obtenerImei(Context c) {
  String Imei=null
  TelephonyManager telephonyManager =
(TelephonyManager)
c.getSystemService(Context.TELEPHONY_SERV
ICE);
Imei=telephonyManager.getDeviceId();
}
```

Figura 4. Ejemplo de código fuente para capturar el número IMEI del teléfono Android.

METODOLOGIA

El enfoque de la Investigación es Cualitativo, debido a que la información que se presenta en este trabajo produce datos descriptivos y flexibles con respecto al método que se investiga. El esquema de seguridad de red sobre Teléfonos Inteligentes Android, presenta un proceso de desarrollo que se basa en la lógica y el proceso inductivo e interpretativo, basado en la revisión documental, para fundamentar las teorías de la autenticación en la seguridad móvil para el acceso a las aplicaciones web y su entorno.

Este modelo va dirigido a compañías que desean mantener el control de acceso de los colaboradores hacia los servidores de aplicaciones web ubicados en su dominio. Los colaboradores se conectan a las aplicaciones organizacionales a través de teléfonos inteligentes que cuentan con un módulo de identificación de abonado, con acceso a internet y que en su arquitectura física cuente con una sola ranura, además se requiere contar con 3 servidores para filtrar las solicitudes de los usuarios en el proceso de autenticación que se propone, sin embargo, el modelo de seguridad en la red puede ajustarse de acuerdo a las limitantes que presente el negocio, siempre que exista un análisis para el uso de controles de acceso alternativos.

Para validar el cumplimiento del objetivo general de estudio, en lo que respecta al peso de las vulnerabilidades y amenazas con mayor impacto, se utilizan los resultados recabados por la fundación OWAST a 46 organizaciones participantes y 76 miembros colaboradores, en un estudio realizado en el año 2017 (Foundation, 2017); además, para efectos de completar el modelo de análisis, se realiza una entrevista a un grupo de especialistas de gestión y seguridad informática para determinar el valor de los factores amenazas e impacto que usa el modelo OWASP en el negocio , debido a estos valores son propios de cada organización.

El proceso que se propone consta de 3 fases, la primera fase es la que está soportada por herramientas de seguridad lógica ubicadas en el área perimetral de la red, la cual se plantea como sugerencia para complementar el trabajo propuesto, la segunda y tercera fase esta soportada por herramientas de software aplicados en el esquema de seguridad para reforzar la fase de autenticación que se valida al acceder a los servidores de aplicaciones ubicados dentro de un dominio de la organización. En la Figura 5 se presenta el modelo tradicional de seguridad comparado con el modelo propuesto.

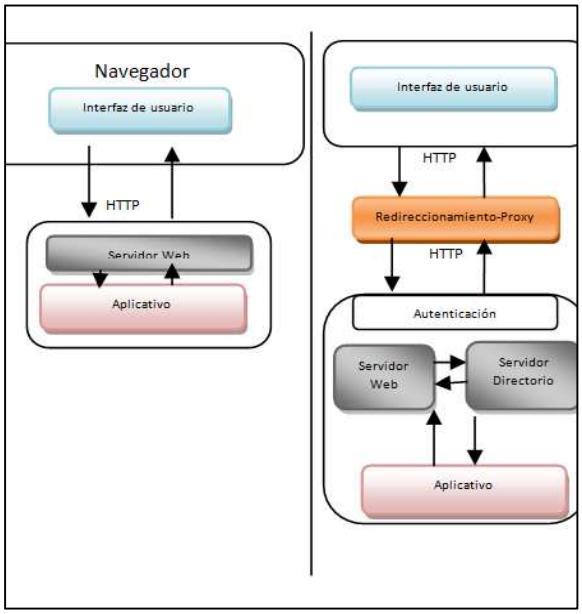

Figura 5. Comparación del modelo clásico de acceso a un Aplicativo web móvil y de la nueva propuesta de acceso.

Para empezar el desarrollo, en la primera fase el diseño de seguridad de la zona segura, ubicada entre la red interna de una organización y la red externa, se configura un Servidor Proxy inverso que enmascarará las direcciones de los sitios destino y direcciona los requerimientos de los usuarios; se deja abierta la posibilidad de implementar otras herramientas como el Firewall para complementar la seguridad en la red, lo cual debe sujetarse a más análisis para medir otras variables importantes en los controles de acceso, como son los tiempos de respuesta que se obtienen al incorporar otros filtros de seguridad versus el nivel de seguridad que se desea alcanzar.

En la Figura 6, se observa que el servidor proxy inverso recibe el link hacia donde se direcciona la petición del usuario, y este a su vez, encamina el requerimiento hacia el servidor donde se valida la autenticación del cliente. Después, el servidor web le envía la respuesta al proxy, este a su vez, enmascara la página de respuesta que envía al cliente (IBM, 2017).Para el ejemplo de uso, se configura Apache HTTP Server, el cual procesa las solicitudes editando el archivo httpd.conf.

```
LoadModule proxy_module modules/mod_proxy.so

LoadModule proxy_ajp module modules/mod_proxy_ajp.so

LoadModule proxy_http_module modules/mod_proxy_http.so

LoadModule ssl_module modules/mod_ssl.so

#URL enmascarada, imeiuees.000webhostapp.com/php-logiimei/index.php

#URL original: https://imeiuees.000webhostapp.com/php-loginimei/index.php

Name Virtual Host *.80

<Name Virtual Host *.80>

ServiceName imeiuees.000webhostapp.com/php-logiimei/index.php

Proxy Preserve Host On

Proxy Requests Off

Proxy Pass "/web/" "https://imeiuees.000webhostapp.com/php-
loginimei/index.php/"

Proxy Pass Reverse "/web/" "https://imeiuees.000webhostapp.com/php-
loginimei/index.php/"

</VirtualHost>
```

Figura 6. Configuración básica del Servidor Proxy Inverso.

En la segunda fase, se ha añadido en el Directorio de Servicio Activo Windows Server, el nuevo atributo (IMEI) obtenido del teléfono inteligente, el cual no se encuentra en las opciones configuradas por defecto en el Sistema Operativo estándar. El atributo añadido será validado junto con el usuario y la clave, en un intercambio de datos entre el Directorio Activo y el Webservice que interpreta las solicitudes de los usuarios en el módulo de autenticación.

Para el ejemplo de este proceso, se utiliza el Servicio de Directorio de Windows Server para añadir un atributo; se inicia añadiendo una DLL al servidor mediante el comando “REGSVR32.EXE SCHMMGMT.DELL”, luego se abre la Raíz de la consola y se añade el “Esquema de Directorio Activo”. Previamente debemos obtener un ID único proporcionado por el repositorio de Microsoft, esto permitirá que se agregue el nuevo atributo en el esquema. Posterior a esto, se abre la carpeta “Clases” de Directorio Activo la subcarpeta “Atributos”, dentro de sus propiedades se procede a agregar el nuevo campo (WindowServer, 2014).

En la Figura 7, se observa la opción para añadir el atributo IMEI al Directorio Activo.

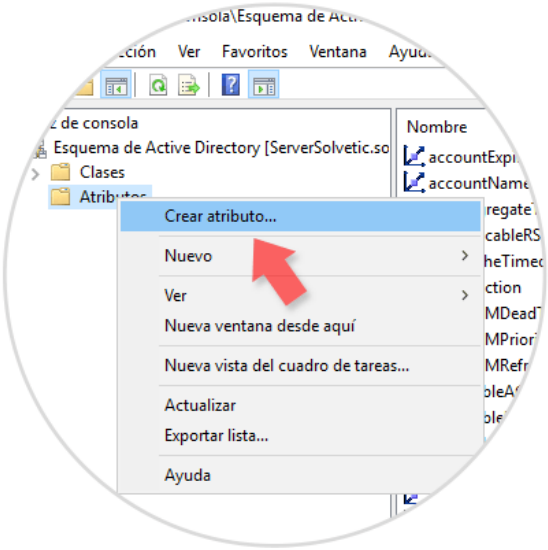

Figura 7. Creación de un nuevo atributo en el Directorio Activo (WindowServer, 2014).

Por consiguiente, la organización será la responsable de incluir en sus políticas de seguridad el registro del número IMEI de los usuarios como política, para que se valide el esquema de autenticación mediante el servicio de directorio.

Se debe considerar en este punto, que para validar el código único EMEI se requiere que esté habilitado el servidor Protocolo Ligero/Simplificado de Acceso a Directorios.

En la tercera fase, se presenta el modelo de autenticación para teléfonos inteligentes Android, es donde radica la parte medular del proceso. El usuario accede desde su teléfono al sitio web de la empresa, a través de una interfaz básica, que solicita usuario y clave, ya que el IMEI es capturado internamente. Se valida esta información contra el almacén de datos que reposa en el servidor de directorio (LDAP), todo dependerá de los controles que la organización considere necesarios implementar. En la Figura 8, se muestra un ejemplo de la interfaz de acceso del usuario.

Figura 8. Modelo de Interfaz de acceso al aplicativo web.

En este tema, el módulo de autenticación se construye bajo la modalidad Android Library Project que permite construir con código fuente empaquetado, y que será compartido con la aplicación móvil que requiera contar con este tipo de seguridad o mediante un mecanismo centralizado de validación.

Además, el Módulo Autenticación, es la clase principal y el núcleo del proceso, tiene como principales operaciones: realizar la validación de los datos del usuario, crear la estructura del mensaje, transformar el mensaje para su transporte, notificar eventos, y otorgar o denegar acceso al usuario (Benavides, 2016).

No obstante, podemos decir que, para que el modelo de autenticación tenga validados los controles de acceso al aplicativo, se deberá desarrollar las clases que deben intervenir en el flujo, así como operaciones locales para la validación de datos, mensajes de respuesta, notificación de eventos, entre otros.

En resumen, la arquitectura de seguridad de red autentica el acceso, utilizando el módulo de validación que se encuentra en el servidor web, este a su vez interactúa con el servidor de directorio para permitir o denegar la solicitud de acceso y así evitar exponer el servidor de directorio directamente, esquema que se muestra en la Figura 9.

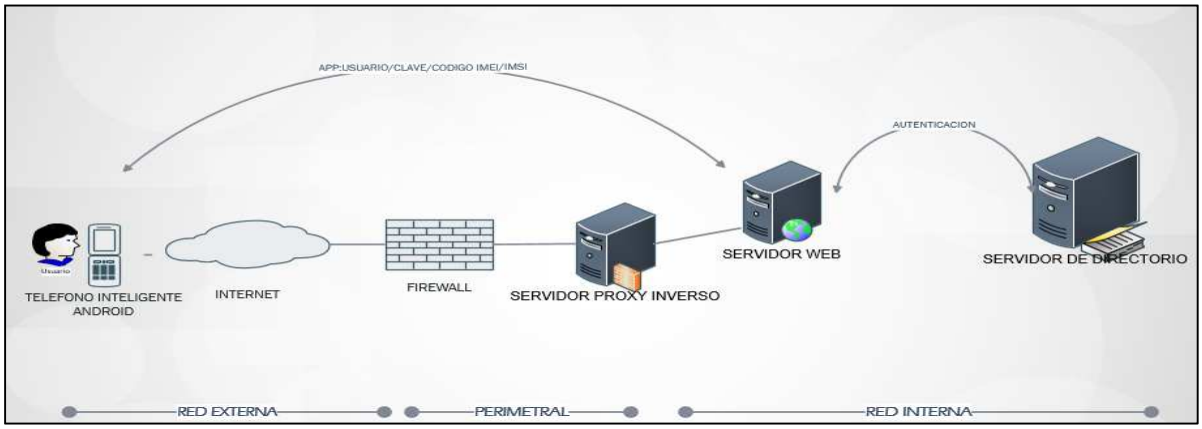

Figura 9. Esquema de seguridad de Red para Teléfonos Inteligentes Android

Evaluación del esquema de seguridad para la autenticación del usuario

Para evaluar la propuesta de este trabajo se realiza un análisis de seguridad, que mostrará el proceso para deducir el porcentaje de vulnerabilidad que se presenta al implementar el esquema planteado de la fase 1,2 y 3. La valoración se realiza desde las directrices que proporciona la Metodología OWASP, de código abierto que se encuentra enfocada en la Seguridad en aplicaciones web, basada en estándares y buenas prácticas, para que las organizaciones desarrollen, adquieran y mantengan aplicaciones y APIs confiables (OWASP, 2014).

En efecto, se utiliza un esquema de trabajo para las pruebas y validaciones en un entorno creado para este fin. Así mismo, una investigación se puede realizar mediante la realización de diferentes tipos de estudios, como son encuestas, estudios de campo, experimentos, simulación del modelo por computadora, etc. (Carpendales, Kerren, Stasko, Fekete, & North, 2008). Por este motivo, se ha considerado crear un ambiente simulado del esquema propuesto, para validar las vulnerabilidades presentes en la perdida de autentificación en el ámbito de aplicaciones web, mediante herramientas de código abierto como Owasp-Zap, y para su análisis se utilizará el apartado de seguridad web OWASP Top 10-2017, que nos guía en la identificación de amenazas y la categorización del riesgo para determinar el nivel de impacto que representa el proceso de autenticación.

Bajo este esquema, se inicia el proceso verificando que el Directorio activo organizacional registre los datos del usuario, la clave y el número IMEI autorizado para el acceso remoto. Además, se establece que el servidor web, el servidor de la base de datos y del aplicativo se están ejecutando dentro del mismo dominio de la organización. Cuando un móvil registrado envía la solicitud de autenticación del usuario, clave e IMEI al servidor web, se valida y se genera la respuesta de autenticación exitosa al dispositivo móvil, esta ruta puede verse comprometida por algún elemento no autorizado. La simulación proporciona una forma de crear un entorno con los servidores y el teléfono inteligente, donde el iniciador se configura como dispositivo móvil trazando una trama que llega hasta el servidor del aplicativo.

Finalmente, se presentará una matriz de riesgo para determinar si se propone un procedimiento seguro para minimizar vulnerabilidades de autentificación y protección de datos sensibles, estimando de manera clara el riesgo al cual está sometida la organización, y que en resumen es la información más valiosa para mantener la

confidencialidad, integridad y disponibilidad de la información.

La metodología para la evaluación que se ejecutará se detalla a continuación:

1. Definición
   - Se evaluará la página web creada en el ambiente simulado.
   - Definir la herramienta de software para la detección o escaneo de vulnerabilidades en la aplicación web elegida, para este caso será Zed Attack Proxy (ZAP).
   - Creación de un usuario y clave temporal para acceder al aplicativo.
   - Detección de vulnerabilidades de autenticación de la aplicación web organizacional, enmarcados en el apartado OWASP Top 10-2017.
   - La detección de las vulnerabilidades será realizada desde un equipo que se encuentre fuera del dominio de la empresa.

2) Análisis de riesgos según la Metodología de Evaluación de Riesgos OWASP (OWASP, 2018):
   - Identificación del riesgo.
   - Estimación de la probabilidad.
   - Estimación del impacto.
   - Determinación de la severidad del riesgo.
   - Priorizar los planes de acción.

3) Medidas preventivas y correctivas a implementarse:
   - Recomendar el establecimiento de procedimientos y buenas prácticas para mitigar los riesgos encontrados.

Para empezar, instalamos y configuramos la herramienta ZAP 2.7.0, para analizar la dirección web del aplicativo, con la finalidad de encontrar la mayor cantidad de vulnerabilidades que se puedan descubrir a lo largo del esquema. El aplicativo analiza y generada las alertas encontradas, el color amarillo indica un nivel de riesgo bajo, las alertas de color naranja indican un riesgo medio y las alertas de color rojo indican un nivel de riesgo de criticidad alto.

El escaneo activo también muestra el nivel de criticidad bajo, medio y alto; Al presentarse un escaneo general a la dirección web, se considera para el análisis de riesgos, todas las vulnerabilidades de acceso al aplicativo, sin embargo, en el análisis de resultados se hará énfasis en las vulnerabilidades detectadas por fallas de autenticación en el caso de encontrarlas; las vulnerabilidades por autenticación más comunes.

Se realiza el escaneo y en la Tabla 1 se detallan las vulnerabilidades encontradas por ZAP

Tabla 1
Vulnerabilidades encontradas en el escaneo de la herramienta ZAP

Nivel de Riesgo	Alertas detectadas
Alto	0
Medio	4
Bajo	1

Nota. El número de alertas descritas, corresponde a la cantidad de agentes detectados por cada nivel de riesgo.

Los reportes que genera esta herramienta permite determinar la clasificación del apartado OWASP Top 10 2017, basado en su numeración (Jesper, 2016). En la Figura 10 se muestra el resultado del escaneo realizado al esquema de autentificación.

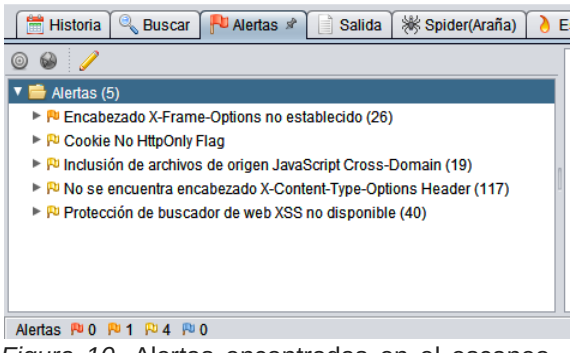

Figura 10. Alertas encontradas en el escaneo de la herramienta ZAP.

Luego, se describen los resultados obtenidos al relacionar las vulnerabilidades detectadas con la clasificación OWASP Top 10-2017, como se representa en la Tabla 2.

Tabla 2
Vulnerabilidades clasificadas con OWASP Top 10-2017

Vulnerabilidad	OWASP Top 10 2017
Encabezado X-Frame-Option no establecido.	A6: Configuración de seguridad Incorrecta.
Cookie No HttpOnly Frag.	A6: Configuración de seguridad Incorrecta.
Inclusión de archivos de origen JavaScript-Cross Domain.	A7: Cross Site Scripting(XSS)
No se encuentra encabezado X-Content-Type-Options Header	A6: Configuración de seguridad Incorrecta.
Protección de buscador web XSS no disponible.	A7: Secuencia de comandos en sitios cruzados (XSS).

Nota. Vulnerabilidades detectadas por la herramienta ZAP en el esquema de seguridad propuesto, y su clasificación de acuerdo a la Metodología OWASP.

Diseño de la matriz de riesgos - análisis de probabilidad

Se analiza el nivel de riesgo que representa para la organización, las vulnerabilidades detectadas. La metodología de análisis de riesgos de OWASP consiste en estimar la probabilidad de ocurrencia y estimar el impacto técnico sobre una vulnerabilidad (OWASP, 2018).

Para determinar la Probabilidad de Ocurrencia, se examinan 2 factores: el agente causante de la amenaza y agente causante de la vulnerabilidad. Los factores están asociados a un grado de probabilidad entre 0 y 9 que servirán posteriormente para estimar la probabilidad general, Tabla 3.

Tabla 3
Grado de probabilidad de ocurrencia - OWASP Top 10-2017

PROBABILIDAD DE OCURRENCIA	
0 >=3	BAJA
3>=6	MEDIA
6>=9	ALTA

Nota. Recuperado de "OWASP Risk Rating Methodology", de OWASP, F., (7 de agosto, 2018). Recuperado de https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Es así que, un agente Amenaza se relaciona al grupo de ataques que realizan las personas con conocimiento de información sensible, dentro del grupo de trabajo o desde el internet, y se clasifica de acuerdo a la Tabla 4.

Tabla 4
Factores de Agente Amenaza

Habilidades Técnicas	Motivación	Oportunidad	Tamaño
Sin conocimiento técnicos **(1)**	Baja motivación /Sin recompensa **(1)**	Acceso total **(1)**	Desarrolladores / Administradores de sistemas **(2)**
Cierto conocimiento técnico **(3)**	Posible recompensa **(4)**	Acceso especial **(4)**	Usuarios de la intranet **(4)**
Usuario avanzado en computación **(5)**	Alta recompensa **(9)**	Acceso parcial **(6)**	Socios **(5)**
Usuario con conocimiento en redes y programación **(6)**		Sin acceso **(9)**	Usuarios autenticados **(6)**
Conocimiento de intrusiones de seguridad **(9)**			Usuarios anónimos de internet **(9)**

Nota. Recuperado de "OWASP Risk Rating Methodology", de OWASP, F., (7 de agosto, 2018). Recuperado de https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Riesgo	Agentes de Amenaza	Vectores de Ataque	Debilidades de Seguridad		Impacto		Puntuación
		Explotabilidad	Prevalencia	Detectabilidad	Técnico	Negocio	
A1: 2017- Inyección	Específico de la Aplicación	FACIL: 3	COMUN: 2	FACIL: 3	GRAVE: 3	Específico de la Aplicación	8,0
A2: 2017 - Pérdida de Autenticación	Específico de la Aplicación	FACIL: 3	COMUN: 2	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	7,0
A3: 2017 - Exposición de Datos Sensibles	Específico de la Aplicación	PROMEDIO: 2	DIFUNDIDO: 3	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	7,0
A4: 2017 - Entidad Externa de XML (XXE)	Específico de la Aplicación	PROMEDIO: 2	COMUN: 2	FACIL: 3	GRAVE: 3	Específico de la Aplicación	7,0
A5: 2017 - Pérdida de Control de Acceso	Específico de la Aplicación	PROMEDIO: 2	COMUN: 2	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	6,0
A6: 2017 - Configuración de Seguridad Incorrecta	Específico de la Aplicación	FACIL: 3	DIFUNDIDO: 3	FACIL: 3	MODERADO: 2	Específico de la Aplicación	6,0
A7: 2017 - Secuencia de Comandos en Sitios Cruzados (XSS)	Específico de la Aplicación	FACIL: 3	DIFUNDIDO: 3	FACIL: 3	MODERADO: 2	Específico de la Aplicación	6,0
A8: 2017 - Deserialización Insegura	Específico de la Aplicación	DIFICIL: 1	COMUN: 2	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	5,0
A9: 2017 - Componentes con Vulnerabilidades Conocidas	Específico de la Aplicación	PROMEDIO: 2	DIFUNDIDO: 3	PROMEDIO: 2	MODERADO: 2	Específico de la Aplicación	4,7
A10: 2017 - Registro y Monitoreo Insuficientes	Específico de la Aplicación	PROMEDIO: 2	DIFUNDIDO: 3	DIFICIL: 1	MODERADO: 2	Específico de la Aplicación	4,0

Figura 11. Definición del peso de los factores de vulnerabilidad de la Metodología OWASP.

Esta metodología incluye tres factores de probabilidad para cada vulnerabilidad (prevalencia, posibilidad de detección y facilidad de explotación) y un factor de impacto técnico. La escala de riesgos para cada factor utiliza el rango de 1 (bajo) a 3 (alto). La prevalencia de una vulnerabilidad ha sido calculada con el promedio de los datos agregados, para elaborar el Top 10 de probabilidad de existencia según la prevalencia. Esta información es posteriormente combinada con los dos factores de probabilidad (posibilidad de detección y facilidad de explotación) para calcular la tasa de probabilidad de cada vulnerabilidad. Esta tasa se multiplica por el impacto técnico promedio estimado de cada elemento, para finalmente elaborar la clasificación de riesgo total para cada elemento del Top 10 (cuanto mayor sea el resultado, mayor será el riesgo). La detectabilidad, la facilidad de explotación y el impacto se calcularon analizando las vulnerabilidades reportadas y asociadas a las 10 categorías principales.

Para determinar el peso asignado a cada factor, la fundación OWAST ha recabado información de 46 organizaciones participantes y 76 de sus miembros, en un estudio realizado en el año 2017 (Foundation, 2017), además, para la información que no consta en el levantamiento de datos para el cálculo del Agente Amenazas y del Impacto del Negocio se realiza una entrevista a un grupo de especialistas de gestión y seguridad informática para determinar el valor de los factores amenazas e impacto que usa el modelo OWASP en el negocio, debido a que estos valores son propios de cada organización. Cualquiera de los valores estimados podrían afectar significativamente la probabilidad total. La clasificación para considerar el promedio del Agente Amenazas y el impacto real sobre el negocio, está relacionado directamente con los resultados que arroje cada organización, la que deberá decidir cuánto riesgo de seguridad en las aplicaciones y APIs está dispuesta a asumir dada su cultura, su industria y el entorno regulatorio.

Ahora bien, se ha calculado el promedio de los datos agregados para elaborar la tabla probabilidad de existencia y finalmente elaborar

la clasificación de riesgo total para los 5 agentes calculados del Top 10 (cuanto mayor sea el resultado, mayor será el riesgo). La detectabilidad, la facilidad de explotación y el impacto se calcularon analizando las Vulnerabilidades y amenazas comunes reportados y asociados a las 10 categorías principales (Foundation, 2017).

Avanzando con el desarrollo, se presenta la tabla con los pesos asignados a las amenazas, estos valores se suman dando el peso total a cada vulnerabilidad detectada.

Tabla 5

Análisis de factores agentes de amenazas del negocio

	Habilidades Técnicas	Motivación	Oportunidad	Tamaño	Total
Encabezado X-Frame-Option no establecido.	3	4	4	4	3,75
Cookie No HttpOnly Frag.	6	1	6	4	3,75
Inclusión de archivos de origen JavaScript-Cross Domain.	6	1	6	4	4,25
No se encuentra encabezado X-Content-Type-Options Header	6	1	6	4	4,25
Protección de buscador web XSS no disponible.	6	4	6	4	5

Además, se presenta el cálculo de las vulnerabilidades definidas previamente por OWASP, estos valores se promedian por los factores de vulnerabilidad y se multiplica por el Impacto técnico promedio de cada elemento, definiéndose los resultados de la Tabla 6.

Tabla 6

Análisis de factores agentes de vulnerabilidad

	Explotabilidad	Prevalencia	Detectabilidad	Técnico Moderado	Total
Encabezado X-Frame-Option no establecido.	FACIL 3	DIFUNDIDO 3	FACIL 3	MODERADO 2	6,0
Cookie No HttpOnly Frag.	FACIL 3	DIFUNDIDO 3	FACIL 3	MODERADO 2	6,0
Inclusión de archivos de origen JavaScript-Cross Domain.	FACIL 3	DIFUNDIDO 3	FACIL 3	MODERADO 2	6,0
No se encuentra encabezado X-Content-Type-Options Header	FACIL 3	DIFUNDIDO 3	FACIL 3	MODERADO 2	6,0
Protección de buscador web XSS no disponible.	FACIL 3	DIFUNDIDO 3	FACIL 3	MODERADO 2	6,0

Nota. Adaptado de "OWASP Top 10 - 2017", de OWASP, F., (2017). Recuperado de https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

En resumen, para el cálculo se suman los pesos de las amenazas, como el de las vulnerabilidades detectadas, y se los divide para el total de agentes validados. El valor calculado es considerado para determinar el nivel de probabilidad general, dicho valor puede fluctuar entre bajo, medio y alto, como se muestra en la Tabla7.

Tabla 7
Resultados de los factores agentes de amenazas y vulnerabilidad

	TOTAL FACTORES AMENAZAS	TOTAL DE VULNERABILIDAD	TOTAL DE FACTORES	CANTIDAD DE FACTORES PROMEDIO
Encabezado X-Frame-Option no establecido.	3,75	6	9,75	4,8
Cookie No HttpOnly Frag.	3,75	6	9,75	4,8
Inclusión de archivos de origen JavaScript-Cross Domain.	4,25	6	10,25	5,1
No se encuentra encabezado X-Content-Type-Options Header	4,25	6	10,25	5,1
Protección de buscador web XSS no disponible.	5	6	11	5,5

Nota. Adaptado de "OWASP Top 10 - 2017", de OWASP, F., (2017). Recuperado de https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Matriz de Riesgo-análisis de impacto

En el orden del proceso, luego del cálculo de la probabilidad general, se debe realizar la matriz de impacto que conllevaría la explotación de la vulnerabilidad encontrada (OWASP, 2018).

Para determinar este impacto, se evalúa el impacto técnico relacionado con la aplicación, además se debe calcular el impacto en el negocio para mitigar los riesgos que se presenten.

Los factores relacionados con el impacto técnico están alineados con los pilares de la seguridad informática (la confidencialidad, la integridad y la disponibilidad) lo cual permite determinar la dimensión del impacto en las aplicaciones si la vulnerabilidad es explotada.

Por otra parte, los factores relacionados al impacto del negocio, dependen de la apreciación de la cada organización y están definidos para su clasificación de acuerdo a la Tabla 8.

Tabla 8
Factores de impacto del negocio

Daño Económico	**Daño de Imagen**	**Incumplimiento**	**Violación a la Privacidad**
Menor al costo de arreglar la vulnerabilidad **(1)**	Daño mínimo **(1)**	Mínimo **(2)**	Una persona**(1)**
Leve efecto en el beneficio anual **(3)**	Pérdida de cuentas principales **(3)**	Medio **(5)**	Cientos de personas **(5)**
Efecto significativo en el beneficio anual **(7)**	Pérdida de credibilidad a gran escala **(6)**	Alto **(8)**	Miles de personas **(7)**
Bancarrota **(9)**	Daño total de la imagen **(9)**		Millones de personas**(9**)

Nota. Recuperado de "OWASP Risk Rating Methodology", de OWASP, F., (7 de agosto, 2018). Recuperado de https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Es así que, se evalúa los factores del impacto técnico para reflejar el grado de impacto tendrá este factor sobre el proceso, Tabla 9.

Tabla 9
Análisis factores de impacto técnico

Vulnerabilidad	Promedio
Encabezado X-Frame-Option no establecido.	MODERADO 2
Cookie No HttpOnly Frag.	MODERADO 2
Inclusión de archivos de origen JavaScript-Cross Domain.	MODERADO 2
No se encuentra encabezado X-Content-Type-Options Header	MODERADO 2
Protección de buscador web XSS no disponible.	MODERADO 2

Nota. Recuperado de "OWASP Risk Rating Methodology", de OWASP, F., (7 de agosto, 2018). Recuperado de https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

A continuación, al igual que el caso anterior los pesos de cada vulnerabilidad se suman dando un total para el grupo de factores relacionados

con el impacto en el negocio, como se demuestra en la Tabla 10.

Tabla 10
Evaluación Factores de Impacto del Negocio

Perdida de:	Daño económico	Daño de Imagen	Incumplimientos	Validación de privacidad	Total
Encabezado X-Frame-Option no establecido.	1	1	2	3	1,75
Cookie No HttpOnly Frag.	1	1	2	3	1,75
Inclusión de archivos de origen JavaScript-Cross Domain.	1	1	5	3	2,5
No se encuentra encabezado X-Content-Type-Options Header	1	1	5	3	2,5
Protección de buscador web XSS no disponible.	1	1	2	3	1,75

Nota. Recuperado de "OWASP Risk Rating Methodology", de OWASP, F., (7 de agosto, 2018). Recuperado de https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

ANÁLISIS DE RESULTADOS

El proceso ejecutado permite identificar el riesgo que debe ser observado y mitigado con mayor urgencia, la metodología de análisis de riesgo indica las coordenadas para hallar la severidad del riesgo asociado según sus niveles de probabilidad y de impacto global (OWASP, 2018).

Ahora bien, después de realizado los cálculos se encuentra que las 5 vulnerabilidades asociadas a los riesgos están valoradas con un nivel de impacto global medio, según el apartado OWASP Top 10 2017.

- Encabezado X-Frame-Option no establecido. A6: Configuración de seguridad Incorrecta.
- Cookie No HttpOnly Frag. A6: Configuración de seguridad Incorrecta.
- Inclusión de archivos de origen JavaScript-Cross Domain. A7: Cross Site Scripting(XSS)
- No se encuentra encabezado X-Content-Type-Options Header A6: Configuración de seguridad Incorrecta.
- Protección de buscador web XSS no disponible. A7: Cross Site Scripting(XSS)

Información que se refleja en la matriz de resultados identificados en la Tabla 11, en donde se conglomeran los resultados del ciclo de análisis efectuado a las vulnerabilidades detectadas; es así que se promedian las probabilidades obtenidas como resultado del impacto técnico, del impacto del negocio, de las vulnerabilidades y de las amenazas, obteniendo los resultados de la severidad del riesgo, a fin de que sea atendido de acuerdo al nivel alcanzado.

Tabla 11
Determinación de severidad del riesgo en la organización

	Nivel de Probabilidad e Impacto técnico	Nivel de Impacto del negocio	Severidad del Riesgo
Encabezado X-Frame-Option no establecido.	6.0 MEDIO	1,75 BAJO	3,88 MEDIO
Cookie No HttpOnly Frag.	6,0 MEDIO	1,75 BAJO	3,88 MEDIO
Inclusión de archivos de origen JavaScript-Cross Domain.	6,0 MEDIO	2,5 BAJO	4,25 MEDIO
No se encuentra encabezado X-Content-Type-Options Header	6,0 MEDIO	2,5 BAJO	4,25 MEDIO
Protección de buscador web XSS no disponible.	6,0 MEDIO	1,75 BAJO	3,88 MEDIO

Nota. Calculo final para medir la severidad del riesgo y el nivel de impacto que representa.

Las soluciones implementadas para estas aplicaciones están categorizadas de acuerdo al apartado OWASP Top 10-2017, esto quiere decir que, la planificación de soluciones estará orientada según el ranking del riesgo asociado a la vulnerabilidad, tomando como prioridad las aplicaciones con un nivel de riesgo medio y alto,

consideradas importantes para la institución en el caso de que estas presenten riesgos para la plataforma.

En la Tabla 12 se proporciona los lineamientos para la mitigación del riesgo asociado a las vulnerabilidades detectadas, y que no fueron filtradas por el esquema de seguridad implementado, considerando que no existe una técnica que se haya implementado hasta el momento, con la cual se mitigue completamente al riesgo.

Tabla 12

Remediación para mitigar las vulnerabilidades detectadas, según la metodología OWASP.

Vulnerabilidad	Ranking OWASP Top 10 2013	Severidad del riesgo
Encabezado X-Frame-Option no establecido.- Cookie No HttpOnly Frag.No se encuentra encabezado X-Content-Type-Options Header	A6: Configuración de seguridad incorrecta.	MEDIO
Remediación: Proceso de fortalecimiento reproducible que agilice y facilite la implementación de otro entorno asegurado. Los entornos de desarrollo, de control de calidad (QA) y de Producción deben configurarse de manera idéntica y con diferentes credenciales para cada entorno. • Siga un proceso para revisar y actualizar las configuraciones apropiadas de acuerdo a las advertencias de seguridad y siga un proceso de gestión de parches. En particular, revise los permisos de almacenamiento en la nube (por ejemplo, los permisos de buckets S3). Utilice un proceso automatizado para verificar la efectividad de los ajustes y configuraciones en todos los ambientes		
Inclusión de archivos de origen JavaScript-Cross Domain.- Protección de buscador web XSS no disponible.	A7: Cross Site Scripting(XSS)	MEDIO
Remediación: Prevenir XSS requiere mantener los datos no confiables separados del contenido activo del navegador. • Utilizar frameworks seguros que, por diseño, automáticamente codifican el contenido para prevenir XSS, como en Ruby 3.0 o React JS. • Codificar los datos de requerimientos HTTP no confiables en los campos de salida HTML (cuerpo, atributos, JavaScript, CSS, o URL) resuelve los XSS Reflejado y XSS Almacenado. La hoja de trucos OWASP para evitar XSS tiene detalles de las técnicas de codificación de datos requeridas. • Habilitar una Política de Seguridad de Contenido (CSP) es una defensa profunda para la mitigación de vulnerabilidades XSS, asumiendo que no hay otras vulnerabilidades que permitan colocar código malicioso vía inclusión de archivos locales, bibliotecas vulnerables en fuentes conocidas almacenadas en Redes de Distribución de Contenidos (CDN) o localmente.		

Nota. Adaptado de "OWASP Risk Rating Methodology", de OWASP, F., (7 de agosto, 2018). Recuperado de https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

La matriz de riesgo elaborada a partir de los datos recabados por el escáner de vulnerabilidades y validados de acuerdo a la recolección de datos, permitió detectar en el esquema simulado, las vulnerabilidades existentes, de manera que se las pueda identificar y tratar correctamente, siguiendo las recomendaciones que la misma metodología propone para minimizar el riesgo.

Es así que, la existencia de ciertas deficiencias de controles de seguridad en la codificación se mostraron en el análisis ZAP, los mismas que no fueron consideradas en su totalidad al crear el ambiente simulado, debido a que esta propuesta está enfocada en disminuir las vulnerabilidades causadas por falencias en el canal que valida el acceso a los aplicativos web, y no en las otras fases de aplicación de seguridad.

Sin embargo, las vulnerabilidades detectadas por ZAP no comprometen directamente los problemas típicos de autenticación que se propone mitigar con la propuesta de trabajo, estos son: los controles A2: 2017-Autenticación rota y de A5: 2017-Control de acceso roto de acuerdo a OWASP Top 10-2017, lo que significa que la arquitectura propuesta es efectiva, y arroja resultados alentadores al mitigar los riegos que conlleva la autenticación controlada desde teléfonos inteligentes a aplicaciones organizacionales.

En otras palabras, el resultado de aumentar un nivel adicional de seguridad a través de un control de acceso particular del dispositivo móvil, ayuda a prevenir ataques de tipo spoofing, fuerza bruta o de diccionario. El modelo obliga al atacante a realizar mínimo 2 tipos diferentes de ataques de acceso, el primero para descubrir el usuario y contraseña con que se autentica el usuario del aplicativo, y el otro ataque dirigido a descubrir cuál es el número IMEI registrado en el dispositivo móvil Android autorizado, lo que contribuye a disminuir el riesgo con respecto al objetivo de ataque.

En el mismo tema y para finalizar, no se puede dejar de mencionar la importancia de contar con una seguridad perimetral robusta, que busque minimizar los accesos no autorizados, es así que el modelo propuesto sugiere que la autenticación del usuario lo realice un servidor web de validación intermedia y de un servidor proxy inverso, para proteger al servidor de directorios de una exposición directa de su información, descrita en el control A3: Exposición de datos sensibles; control que también fue superado en el análisis de vulnerabilidades del scanner ZAP.

CONCLUSIONES

Con el propósito de abordar las deficiencias actuales de la autenticación existente en los controles de acceso y de reforzar el sistema de seguridad de los teléfonos inteligentes Android, se propone el uso de un esquema de seguridad para una autenticación flexible y segura de los usuarios registrados en el dominio organizacional. Para esto, se captura el número único IMEI del dispositivo desde el cual se desea acceder a la información de la red corporativa, a este dato se suma la validación tradicional del usuario y la contraseña del empleado, enviando así 3 parámetros para validarlos contra el servidor web centralizado; el servidor WEB intercambia datos con el servidor que almacena los atributos del usuario en el Directorio Activo del dominio, lo que sirve para autorizar el acceso a los recursos de la organización de manera controlada y segura.

Es así que, en este trabajo se evaluó la probabilidad de ocurrencia y se estimó el impacto técnico del modelo de seguridad propuesto, calculando la prevalencia, posibilidad de detección y facilidad de explotación en los factores de análisis de la metodología OWASP.

La matriz de riesgo elaborada a partir de los datos recabados por el escáner de vulnerabilidades especializado ZAP, detectó las siguientes vulnerabilidades en el diseño del sistema: Encabezado X-Frame-Option no establecido, Cookie No HttpOnly Frag, Inclusión de archivos de origen JavaScript-Cross Domain, No se encuentra encabezado X-Content-Type-Options Header y Protección de buscador web XSS no disponible. En efecto, la matriz general de riesgos arrojó como resultado, que el diseño de seguridad de todo el esquema se encontraba en el nivel medio de riesgo en la escala OWASP; esta información resultó en primera instancia del análisis general que se realiza al modelo propuesto, en todas las fases del diseño de seguridad (autorización, validación data, manejo de excepciones y auditoria); estas fases no fueron reforzadas con otros controles de seguridad por la extensión del estudio.

El enfoque de este artículo esta direccionado exclusivamente a la fase de autenticación. Es así que, se determinó en el resultado del análisis de esta fase , que las vulnerabilidades

detectadas por el escáner ZAP, no están relacionadas con los controles de autenticación de los usuarios como son: los controles A2: 2017-Autenticación rota y A5: 2017-Control de acceso roto de acuerdo a OWASP Top 10-2017, lo que significa que la arquitectura propuesta es efectiva, y arroja resultados alentadores para mitigar los riegos que conlleva la autenticación controlada multifactor (MFA) desde teléfonos inteligentes Android, haciéndolo menos vulnerable a la variedad de ataques directos de acceso tipo Spoofing-Looping, fuerza bruta o de diccionario a los que se sometió el modelo,

Para trabajos futuros, se considera evaluar la usabilidad de nuestro sistema en varios escenarios, para formular métricas de varios tipos de ataques, que incluyen los que no fueron contemplados en este estudio, como son ataques de intercepción de claves tipo Hombre en el Medio e IP Splicing-Hijacking; los resultados de este trabajo futuro nos permitirán evaluar el rendimiento de esta solución y controlar mejor los aspectos de seguridad y usabilidad en la implementación.

Finalmente, se puede señalar que si bien los resultados iniciales son los esperados, no se debe enfocar la seguridad únicamente en la autenticación de los usuarios autorizados, sino también se debe recordar que este proceso es solo una parte de la amplia estrategia de defensa en profundidad que debe ser considerado por las organizaciones enfocadas en resguardar sus activos.

Referencias Bibliográficas

Aguilar, Alejandro; Pérez, Juan; Cornejo, Luis. (2011). Implementación de un sistema de Autenticación usando LDAP para control de acceso a la RED. México D.F., México.

Amaro, J. (2012). *El gran libro de programación avanzada con Android.* Granada: Marcombo S.A.

Android. (2017). *Prácticas recomendadas para identificadores únicos*. Recuperado el 09 de 2017, de Android.com: https://developer.android.com/training/articles/user-data-ids.html?hl=es-419

Android, D. (2017). *Sugerencias de Seguridad.* Recuperado el 28 de 09 de 2017, de https://developer.android.com/training/articles/security-tips.html

Benavides, L. (11 de 2016). *IMPLEMENTACIÓN DE MÓDULO DE AUTENTICACIÓN PARA APLICACIONES MÓVILES CORPORATIVAS QUE UTILICEN UN SISTEMA DE SERVICIO DE DIRECTORIO.* Recuperado el 2017, de http://www.dspace.espol.edu.ec/xmlui/handle/123456789/36463

Carpendales, Kerren, Stasko, Fekete, & North. (2008). Evaluating Information Visualizations. In: Information Visualization. *Computer Science, 4950*, 19-45.

Carullo, G., Ferrucci, F., & Sarro, F. (2012). *Towards Improving Usability of Authentication Systems Using Smartphones for Logical and Physical Resource Access in a Single Sign-On Environment.* Berlin, Heidelberg: Springer-Verlag.

Desmond, Brian; Richards, Joe; Allen, Robbie; Alistair, Lowe-Norris. (2009). *Active Directory: Designing, Deploying, and Running Active Directory* (4ta ed.). (J. O. Ruma, Ed.) California, Sebastopol, Estados Unidos: Reilly Media.

Domingo, M. (2014). Seguridad en dispositivos móviles. Cataluña.

Foundation, O. (2017). *OWASP Top 10 - 2017.*Recuperado el 09 de 2018, de https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Frontier, E. (2015). *The Problem with Mobile Phones.*Recuperado el 2017, de https://ssd.eff.org/en/module/problem-mobile-phones

Fuchs, C., Hofkirchner, W., Schafranek, M., Raffl, C., & Sandoval, M. (2010). "Theoretical Foundations of the Web: Cognition. *Future internet* (doi:10.3390/fi2010041), 41-59.

Hiard, V. (2016). *Gestión de un proyecto web Planificación, dirección y buenas prácticas.*Barcelona: ENI.

Huang, Y.-W. (2015). WEB APPLICATION SECURITY-PAST, PRESENT, AND FUTURE. *COMPUTER SECURITY IN THE 21 CENTURY* , 183-227.

IBM. (2017). *Configuración de Apache HTTP como un proxy inverso para Rational DOORS Web Access.* Recuperado el 23 de 09 de 2017, de IBM KNOWLEDGE CENTER: https://www.ibm.com/support/knowledgecenter/es/SSYQBZ_9.6.0/com.ibm.rational.dwa.install.doc/topics/t_config_rev_proxy_apache.html

IBM, P. I. (2015). *El 50% de los desarrolladores de aplicaciones móviles no invierte en seguridad.* Recuperado el 25 de 06 de 2017, de https://www-03.ibm.com/press/es/es/pressrelease/46400.wss

ISO. (2013). *Normativa ISO 27001*. Recuperado el 2018, de https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Jason, M. (2013). *Web Service APIs and Libraries.*Ohio, Estados Unidos: American Library Association.

Jesper, J. (06 de 2016). *OWASP to WASC to CWE Mapping*. Obtenido de https://docs.google.com/viewer?url=http%3A%2F%2Fwww.criticalwatch.com%2Fassets%2Fc-Owasp-to-Wasc-to-CWE-Mapping-Tech-Paper-0710131.pdf

Kamel, Maged; Wheeler, Steve; Tavares, Carlos; Jones, Ray. (2011). How smartphones are changing the face of mobile and participatory healthcare: an overview, with example from eCAALYX. *BioMedical Engineering OnLine* (https://doi.org/10.1186/1475-925X-10-24).

Maaniitty, Jussi. (2011). Intelligent Mobile User Interface. Tampere, Finlandia.

Marforio, C., Nikolaos, K., Soriente, C., Kostiainen, K., & apkun, S. C. (2014). Smartphones as Practical and Secure Location,Verification Tokens for Payments. *Internet Society* .

Mejia, J., & Ramirez, H. (2016). Estableciendo controles y perímetro de seguridad para una página web de un CSIRT. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Información* (1646-9895).

Microsoft. (2008). Ampliación del esquema de Active Directory. *TechNet Magazine* .

Moreno, C. (2015). *Campaña de Benhmarking.* Obtenido de

http://bibing.us.es/proyectos/abreproy/11909/fichero/Volumen+1%252F2.pdf

Niño, J. (2011). *Gestión de archivos web (Aplicaciones web).*Editex.

OpenLDAP. (2012). OpenLDAP Software 2.4 Administrator's Guide. Michigan.

OWASP. (17 de 08 de 2018). *About The Open Web Application Security Project*. Obtenido de https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project

OWASP. (5 de 12 de 2017). *ASVS V2 Authentication*. Obtenido de https://www.owasp.org/index.php/ASVS_V2_Authentication

OWASP. (7 de 08 de 2018). *OWASP Risk Rating Methodology*. Obtenido de https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

OWASP. (14 de 06 de 2018). *OWASP Zed Attack Proxy Project*. Obtenido de https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

OWASP. (11 de 11 de 2014). *Sobre OWASP*. Recuperado el 2018, de https://www.owasp.org/index.php/Sobre_OWASP

Parravicini, L. (2011). *Programación web segura.* (J. Horiguela, Ed.) Luis Parravicini.

Patiño-Diaz, Angel. (2013). Aplicación móvil en Android para la gestión de entrenos de Deportistas. Valencia, España.

Research, T. P. (2015). *Wearables, BYOD and IoT: Current and future plans in the enterprise.*Recuperado el 25 de 08 de 2017, de http://www.techproresearch.com/downloads/wearables-byod-and-iot-current-and-future-plans-in-the-enterprise/

Saurabh, D., Sampalli, S., & ye, Q. (2016). MDA: message digest-based authentication for mobile cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications* (DOI 10.1186/s13677-016-0068-6), 5-18.

Solutions, M. (2012). *La nube: oportunidades y retos para los integrantes de la cadena de valor.* Recuperado el 26 de 08 de 2017, de https://www.managementsolutions.com/sites/default/files/publicaciones/esp/La-nube.pdf

TechBeacon. (2016). *State of app security 2016: Most common vulnerabilities, top trends.*Recuperado el 08 de 2017, de https://techbeacon.com/state-app-security-2016-most-common-vulnerabilities-top-trends

UShafique, U., Sher, A., Ullah, R., Khan, H., Zeb, A., Ullah, R., y otros. (2017). Modern Authentication Techniques in Smart Phones:Security and Usability Perspective. *International Journal of Advanced Computer Science and Applications, 8* (1).

Vapen, Anna; Shahmehri, Nahid. (2011). Security Levels for Web Authentication Using Mobile Phones. Linkoping, Sweden.

Vongsingthong, S., & Boonkrong, S. (2 de Junio de 2014). A Survey on Smartphone

Authentication. *Walailak J Sci & Tech* , 1-19.

Vora, P. (2009). *Web Application Design Patterns.*Burlington, Estados Unidos: Morgan Kaufmann.

WindowServer. (10 de 2014). *Active Directory: Agregar Atributos Personalizados*. Recuperado el 09 de 2017, de WordPress.com: https://windowserver.wordpress.com/2014/10/09/active-directory-agregar-atributos-personalizados/

Wurzinger, P., Platzer, C., Ludl, C., Kirda, E., & Kruegel, C. (2009). Mitigating XSS attacks using a reverse proxy. *Researchgate* (10.1109/IWSESS.2009.5068456).