Dom. Cien., ISSN: 2477-8818
Vol. 8, núm. 3. Especial Agosto, 2022, pp. 503-523

DOI: http://dx.doi.org/10.23857/dc.v8i3

Ciencias Técnicas y Aplicadas
Artículo de Investigación

Seguridad informática aplicando la Autentificación por Doble factor para la plataforma HomeOfi

Computer security applying Double Factor Authentication for the HomeOfi platform

Computer security applying Double Factor Authentication for the HomeOfi platform

Lady Espinoza Tinoco [I]
lespinoza@unach.edu.ec
https://orcid.org/0000-0001-6569-3686

Byron Barriga Rivera [II]
byronbarriga96@gmail.com@espoch.edu.ec
https://orcid.org/0000-0003-2594-7164

Josué Izurieta Navarrete [III]
josue.izurieta6@gmail.com
https://orcid.org/0000-0003-4471-2766

Cristian Hugo Morales Alarcón [IV]
cmorales@unach.edu.ec
https://orcid.org/0000-0002-0197-0581

Correspondencia: lespinoza@unach.edu.ec

*Recibido: 29 de junio del 2022 *Aceptado: 12 de julio de 2022 * Publicado: 16 de agosto de 2022

I. Magíster en Informática Educativa, Ingeniera en Sistemas Informáticos, Universidad Nacional de Chimborazo, Riobamba, Ecuador.
II. Ingeniero en Sistemas y Computación, Plasticaucho Industrial S.A, Ambato, Ecuador
III. Ingeniero en Sistemas y Computación. Universidad Nacional de Chimborazo, Riobamba, Ecuador.
IV. Magíster en Gestión de Sistemas de Información e Inteligencia de Negocios, Ingeniero en Sistemas y Computación. Universidad Nacional de Chimborazo, Riobamba, Ecuador.

Resumen

HomeOfi es una plataforma informática que permite la interconexión entre profesionales que desean ofertar sus servicios por medio de tele consultas o venta de productos digitales, la misma posee información y datos de usuarios incluida su información bancaria, por lo que necesita considerar una estructura robusta de seguridad informática. El objetivo de esta investigación fue aplicar la Autentificación por Doble Factor para la plataforma informática HomeOfi, con el propósito de gestionar y validar la información de los usuarios, detectar y neutralizar ataques informáticos y garantizar el acceso exclusivo de sus usuarios autorizados. Para la validación de esta implementación se utilizó el método Delphi bajo las métricas de seguridad de la norma ISO 25010, para realizar este procesos se utilizaron dos ciclos, el primero sin la implementación de la Autentificación por Doble factor y el segundo con la implementación, dando como resultado en la primera interacción un cumplimento del 83% en general y en la segunda cumpliendo con un 100% de todas las métricas, mejorando así la seguridad informática de la empresa HomeOffice S.A.S.

Palabras Claves: Ataques Informáticos; Autentificación por Doble factor; Norma ISO 25010; Seguridad Informática.

Abstract

HomeOfi is a computer platform that allows interconnection between professionals who wish to offer their services through teleconsultations or the sale of digital products, it has user information and data, including their bank information, so it needs to consider a robust security structure. computing. The objective of this research was to apply Double Factor Authentication to the HomeOfi computing platform, with the purpose of managing and validating user information, detecting and neutralizing computer attacks and guaranteeing exclusive access to authorized users. For the validation of this implementation, the Delphi method was used under the security metrics of the ISO 25010 standard, to carry out this process two cycles were used, the first without the implementation of Double Factor Authentication and the second with the implementation, giving as a result, in the first interaction, a compliance of 83% in general and in the second, complying with 100% of all the metrics, thus improving the computer security of the company HomeOffice S.A.S.

Keywords: Computer Attacks; Double Factor Authentication; ISO 25010 standard; Informatic security.

Resumo

A HomeOfi é uma plataforma informática que permite a interligação entre profissionais que pretendem oferecer os seus serviços através de teleconsultas ou venda de produtos digitais, possui informações e dados dos utilizadores, incluindo os seus dados bancários, pelo que necessita de considerar uma estrutura de segurança robusta. O objetivo desta pesquisa foi aplicar a Autenticação de Fator Duplo à plataforma computacional HomeOfi, com a finalidade de gerenciar e validar as informações dos usuários, detectar e neutralizar ataques informáticos e garantir acesso exclusivo aos usuários autorizados. Para a validação desta implementação foi utilizado o método Delphi sob as métricas de segurança da ISO 25010, para realizar este processo foram utilizados dois ciclos, o primeiro sem a implementação da Autenticação de Fator Duplo e o segundo com a implementação, dando como resultado , na primeira interação, uma conformidade de 83% em geral e na segunda, cumprindo 100% de todas as métricas, melhorando assim a segurança informática da empresa HomeOffice S.A.S.

Palavras-chave: Ataques de computador; Autenticação de Fator Duplo; norma ISO 25010; Segurança informática.

Introducción

La tecnología ha cambiado y es parte fundamental de la vida cotidiana de las personas, esta es utilizada para actividades de comunicación, entretenimiento, educativas, de comercio entre otras, las plataformas digitales guardan una gran cantidad de información personal de sus usuarios. Debido a esto las empresas e instituciones han optado por un enfoque prioritario de la seguridad de software.

En la última década el desarrollo de sistemas informáticos y en especial los sistemas web se han convertido en una base del desarrollo tecnológico, los usuarios confían sus datos, información personal e incluso bancaria a un gran número de plataformas digitales, por lo que la información que se encuentra en internet debe siempre contar con importantes estándares de seguridad (Lagreca, 2017).

Los ataques informáticos aprovechan alguna debilidad o vulnerabilidad en el software, hardware e incluso en el personal involucrado en el ambiente informático, con el fin de obtener un beneficio, en su mayoría de índole económico (Mieres, 2009). Estos ataques causan daño directo a la seguridad de los sistemas informáticos, que luego repercute directamente a la información de la organización, además de producir daño monetario (Cañón, 2015).

La seguridad en sistemas informáticos se presenta como un conjunto de reglas y procesos que ayudan a proteger la integridad, confidencialidad y disponibilidad de la información. Por otra parte, permite asegurar que los recursos de un sistema de información de una organización sean utilizados de manera correcta y por el personal autorizado (Tirado, Ramos, Álvarez, & Carreño, 2017). También trata de reducir los riesgos de acceso y utilización de ciertos sistemas de manera no autorizada y malintencionada. Su objetivo principal es precautelar por la integridad de los recursos informáticos de gran valor para una organización. Con las buenas prácticas de seguridad informática ayuda a la organización a proteger sus recursos tangibles e intangibles (Gil & Gil, 2017).

Uno de los objetivos de la seguridad informática es optimizar los riesgos sobre los recursos informáticos y con esto aportar con el funcionamiento normal de las operaciones de la empresa, dejando en segundo plano la administración de riesgos informáticos, otro objetivo de la seguridad informática consiste en asegurar que los documentos cumplan con una alta confiabilidad, con características importantes las cuales son: permanecía, accesibilidad, disponibilidad, confidencialidad, autenticidad y aceptabilidad (Quiroz-Zambrano & Macías-Valencia, 2017). Se debe tener en cuenta que la seguridad informática es un proceso en constante cambio, que necesita actualizar métodos, herramientas, procedimientos y técnicas que ayuden a contrarrestar los ataques informáticos que van apareciendo día con día (Suárez & Ávila, 2015). Se han creado varias técnicas para mejorar los métodos de autentificación en sistemas informáticos (Singh, 2017).

Las brechas de seguridad (el crimen digital y el fraude en internet), han dado origen a varios métodos de seguridad en torno al ingreso a los sistemas informáticos, siendo el más utilizado la autenticación por Doble factor (2FA) (Alzahrani, 2018). Este proceso de seguridad sirve para que el usuario confirme su identidad mediante dos factores de autenticación diferentes (clave estática y clave dinámica) (Waheed, Ali Shah, & Khan, 2016).

La autenticación de dos factores es usada como un protocolo para prevenir muchos ataques. Esta autentificación se basa en la suposición de varios factores de identidad. Se puede dar una serie de contraseñas temporales llamadas *One Time Password (OTP*) que solo se pueden utilizar una vez. Cuando se aplica ese código o contraseña temporal, la plataforma inicia el proceso y verificación del token. Para realizar el inicio de cualquier operación el token debe estar registrado con anterioridad (Waheed, Ali Shah, & Khan, 2016). Según Alzahrani, (2018) puede haber dos factores de autenticación que son muy seguros. Un dispositivo móvil de verificación se puede utilizar junto con la contraseña en lugar de usar tarjetas, fichas, etc.

En Arabia Saudita se realizaron investigaciones acerca de los mejores métodos de autentificación para acceso de sistemas informáticos demostrando que la Autentificación por Doble factor es uno de los métodos más usados en sistemas bancarios junto a la autentificación biométrica, la seguridad en la banca digital es considerada la más importante entre sistemas que requieren la autentificación de sus usuarios, siendo la base para cualquier sistema que requiera mejorar su seguridad (Alzahrani, 2018). Además, China y Estados Unidos son países que más utilizan la autentificación de usuarios, a tal punto en que todos sus sistemas cuentan con diferentes formas de Autentificación por Doble factor, siendo los biométricos los más usados en China y los basados en *OTP* por Arabia (Kuang & Xu, 2020). Según estudios realizados en Perú se analizaron las políticas de seguridad que deben ser cumplidas tomando en cuenta los sistemas informáticos, el comportamiento humano, conociendo que la información es el mayor bien a proteger (Altamirano & Bayona, 2017).

En el Ecuador existen estudios referentes a la problemática de ciberdefensa y ciberseguridad según los estudios de (Vargas, Reyes, & Recalde, 2007) argumentan que unos de los motivos que causa el problema en ciberseguridad es el aumento de servicios y productos por internet (transacciones, banca online, pago del agua, luz etc.).

La empresa HomeOffice S.A.S, ha creado HomeOfi que es una plataforma informática que permite la interconexión entre profesionales que desean ofertar sus servicios por medio de tele consultas o venta de productos digitales (Homeofi, 2020). En sus métodos de pago permite las opciones de pagos o transferencias bancarias, por lo que al trabajar con entidades bancarias requiere una mayor seguridad en todos sus procesos informáticos incluyendo un método de seguridad al ingreso del sistema, con el fin de validar el acceso exclusivo a los usuarios y personal autorizado dentro del sistema.

Es así que, para la protección de la plataforma digital, la cual usa constantemente la autenticación de usuarios para múltiples procesos, como el ingreso de información o la compra de productos, la gestión de sus administradores, validación de datos y pagos, es fundamental la implementación de estrategias de seguridad que permitan la protección de datos. Es por esto que la presente investigación busca aplicar la Autentificación por Doble factor para la plataforma informática HomeOfi de la empresa HomeOffice S.A.S, además del diseño de un módulo de seguridad contra ataques Informáticos validando estas implementaciones mediante el estándar de calidad ISO 25010.

Metodología

El desarrollo de la investigación presenta un enfoque mixto. Cualitativa debido que se proporcionó una descripción correspondiente al cumplimiento de las métricas de seguridad de la norma ISO 25010 y cuantitativa porque se aplica la tabulación de datos para la evaluación de las métricas de seguridad y se realiza un análisis basado en números. También se realizó una recopilación bibliográfica de información y datos relacionados en artículos científicos, tesis, páginas web y guías oficiales, conceptos referentes al tema de investigación.

La implementación de Autentificación por Doble factor y el módulo de seguridad se desarrolló bajo los lenguajes de programación PHP y JavaScript, bajo el patrón de diseño Modelo Vista Controlador (MVC), la Autentificación por Doble factor se realizó en el ingreso del sistema mediante el uso del algoritmo Time-based One-time Password (TOTP) implementado en la aplicación Google Authenticator. Se utilizó la arquitectura Cliente – Servidor, para desarrollar la aplicación web permitiendo realizar validaciones por lado del cliente y del servidor, para el desarrollo de software se utilizó el Modelo Cascada que consiste en 5 fases las cuales son: Análisis, Diseño, Desarrollo, Evaluación y Mantenimiento en este caso se desarrolló hasta la fase de Evaluación.

Para la evaluación de resultados se aplicó el método Delphi, se realizó un proceso de selección de 5 evaluadores, también conocidos como expertos, quienes fueron los encargados de medir la calidad de la seguridad del software, mediante las métricas establecidas en el estándar de calidad ISO 25010. Para garantizar la selección de los expertos se consideró criterios de formación académica tanto internos de la empresa HomeOffice S.A.S., como externos a la empresa. Los 3 expertos de la empresa HomeOffice S.A.S., del departamento de desarrollo y 2 expertos de distintos establecimientos educativos de educación superior en el área de informática, dando un total de 5 expertos. Los mismos que mediante un cuestionario evaluaron la calidad de la seguridad.

Resultados y discusión

Proceso de Autentificación por Doble factor

Mediante el análisis teórico se determinó que existen varios métodos y factores para la implementación en el proceso de Autentificación por Doble factor (2FA), los cuales pueden variar según las necesidades de cada sistema de seguridad. En la tabla 1 se muestra cada uno de los métodos de autentificación y en qué acción específica fue implementada, además del recurso necesario para la implementación en cada acción.

Tabla 1. Factores y métodos de autenticidad implementados

Factor	Método de autentificación	Acción	Recurso
Captcha	Click Pattern	Registro de un nuevo cliente	Google Captcha
Mail	Doble factor	Activación de cuenta de cliente	Gmail
Captcha	Click Pattern / Doble factor	Inicio de sesión	Google Captcha
QR	Doble factor	Inicio de sesión	Autenticador de Google (App Móvil)
Contraseña	Convencional	Inicio de sesión	Base de datos

Elaborado por: los autores

Desarrollo del módulo de seguridad contra ataques informáticos

Para el desarrollo del módulo de seguridad se implementó el Modelo Cascada que consiste en 5 fases las cuales son: análisis, diseño, desarrollo, evaluación y mantenimiento en este caso se desarrolló hasta la fase de evaluación.

Fase de análisis

Para este ciclo de la Ingeniería de Software se implementaron las siguientes etapas correspondientes a la fase de análisis, los cuales se mencionan a continuación:

*Roles de usuarios. S*e definieron un total de 3 roles para el sistema en general y el módulo de seguridad, los cuales son: cliente, administrador y superadministrador.

Requerimientos funcionales. Los requerimientos de funcionalidad fueron detallados en base a las necesidades de cada uno de los roles de los usuarios, se establece en general que el cliente tiene acceso solamente a su información personal, mientras que el administrador tiene acceso al historial e información del cliente y el superadministrador tiene el acceso al historial tanto de administradores y clientes, además acceso a los ataques detectados y neutralizados del sistema.

Requerimientos no Funcionales. se tomaron en cuenta las siguientes métricas: eficiencia, usabilidad, funcionalidad, compatibilidad, fiabilidad y seguridad, este último siendo de vital importancia para el desarrollo de la presente investigación.

Fase de diseño

Para este ciclo de la Ingeniería de Software se implementaron las siguientes etapas correspondientes a la fase de diseño, los cuales son necesarias para la construcción del módulo de seguridad:

Arquitectura de software. Se ocupo el patrón MVC para el desarrollo arquitectónico del módulo de seguridad, debido a la facilidad de implementación en el sistema general.

Modelo entidad relación. Se utilizó el modelo entidad relación para evidenciar las atributos y relaciones de cada una de las entidades del módulo de seguridad, además sirvió como base para la construcción de los siguientes modelos y la base de datos final.

Modelo relacional. Se utilizó el modelo relacional para la definición de datos y estructura normalizada del modelo entidad relación.

Diagrama de casos de uso. El modelo de caso de uso se ocupó para indicar las acciones de cada uno de los usuarios en base a sus roles y requisitos funcionales ya definidos, el cual sirvió para el modelado de la base de datos.

Modelo de base de datos. Se realizó un modelo final de base de datos tomando en cuenta todos los modelos y diagramas antes mencionados para el desarrollo del módulo de seguridad.

Diccionario de datos. En esta etapa se detalló cada uno de los datos utilizados para la creación de tablas, los mismos que sirvieron para la correcta construcción de la base de datos.

Actividades para el desarrollo del módulo de seguridad

- Elaboración de la estructura de las carpetas del módulo de seguridad.
- Elaboración del archivo Index.php.
- Creación del archivo de conexión.
- Creación de las clases modelos del módulo de seguridad.
- Creación de las vistas de las vistas principales del módulo de seguridad.
- Creación de las vistas de usuarios anónimos.
- Creación del controlador de usuario anónimo.
- Creación de las vistas del usuario cliente.
- Creación del controlador del cliente.

- Creación de las vistas del usuario administrador.
- Creación del controlador del administrador.
- Creación de las vistas del usuario superadministrador.
- Creación del controlador del administrador.
- Creación del archivo HTTACCESS.

Fase de Evaluación

Para la evaluación del módulo de seguridad se realizaron encuestas y entrevistas acerca de la funcionalidad con las que cuenta el módulo de seguridad hacia el personal de desarrollo de la empresa HomeOffice S.A.S, además de la evaluación de los requerimientos no funcionales sin tomar en cuenta la seguridad.

Integración del proceso de Autentificación por Doble factor al módulo de seguridad

Para el proceso de integración de la autentificación al módulo de seguridad se utilizó el código QR y la aplicación Google Authenticator, generando un código de 6 dígitos con una duración de 30 segundos y un máximo de disponibilidad de 60 segundos, integrado entre el proceso de autentificación de usuario y el ingreso a su respectivo panel, generando por cada usuario un código y mostrando su nombre en la aplicación.

Evaluación de la seguridad del módulo informático

Finalmente, mediante el método Delphi se procedió a la evaluación del módulo de seguridad para la cual se realizaron dos encuestas para la toma de información. Las cuales mediante técnicas de análisis e interpretación de datos permitió evaluar la calidad de la seguridad del módulo de informático bajo las métricas recomendadas por el estándar de calidad ISO/IEC 25010 (ISO25000, 2015), el cual tiene el objetivo de evaluar y determinar la excelencia del software, este modelo de evaluación posee 8 características principales, cada una con sus respectivas métricas. En la tabla 2 se resume cada una de las características y subcaracterísticas de la norma ISO 25010.

Descripción de los Criterios de Evaluación

Para el análisis de los resultados se establecieron una serie de criterios de evaluación basados en las subcategorías de la métrica de seguridad correspondiente a la norma ISO 25010 y el trabajo elaborado por (Calabrese & Pesado, 2017). En la tabla 2, se establece cada criterio en base a las preguntas establecidas en el cuestionario de evaluación, obteniendo la fórmula y la equivalencia de cada uno de los valores representados.

Tabla 2. Descripción de criterios de evaluación

ID	Nombre	Descripción
C-1	Conexiones seguras	Se considera una conexión segura si cuenta con certificado HTTPS y si no redirige hacia sitios inseguros
C-2	Control de acceso	El sistema debe ser capaz de contralar el acceso a funcionalidades, base de datos, código de la aplicados, servidores solo a personal autorizado
C-3	Encriptación de datos	Por lo menos debe existir algún dato importe encriptado dentro de la base de datos
C-4	Contraseña de bajo nivel	La contraseña se considera de bajo nivel si posee menos de 7 caracteres, no posee letras mayúsculas y minúsculas, no posee letras y números
	Contraseña de nivel medio	La contraseña se considera de nivel medio si posee al menos 7 caracteres o letras y mayúsculas y minúsculas o letras y números
	Contraseña de alto nivel	La contraseña se considera de alto nivel si posee al menos 7 y menos de 15 caracteres, con letras minúsculas y mayúsculas y números
I-5	Prevención de Accesos	El sistema debe ser capaz de prevenir el acceso a base de datos, acceso de código, funcionalidades especificas a personal no autorizado, además que no se permitan inyecciones de Javascript y/o de SQL
I-6	Prevención de modificaciones	Se debe establecer que no se altere el código del sistema sin una autorización establecida

ID	Nombre	Descripción
I-7	Confirmación de datos	Se debe efectuar una revalidación de los datos del registro por medio de un mail
NR-8	Operaciones realizadas	Se debe contar con un historial de antecedentes de acciones realizadas e informar del inicio de sesión por mail, además de poseer un cierre forzado en el caso de un determinado tiempo de no uso del sistema o luego de finalizar la sesión
NR-9	Mecanismo de Cifrado	Se debe implementar métodos de encriptación sea por algoritmos o mecanismos criptográficos
NR-10	Verificación de acciones	Se debe requerir una validación de los datos antes de realizar una determinada acción
R-11	Registro de acciones y datos	Se debe tener un expediente de las acciones realizadas, un registro por hora y fecha o capturar el direccionamiento IP desde que se ingresa al sistema
R-12	Detección de posibles ataques	Se debe llevar un registro de los posibles ataques realizados, detectándolos y neutralizándolos y guardando los datos causantes de los mismos
A-13	Comprobación de identidad	El sistema debe ejecutar una verificación de identidad mediante cualquiera de los siguientes métodos: datos biométricos, Captchas, QR.
A- 14	Comprobaciones adicionales	Se debe contar con un sistema de autentificación en dos pasos, aplicaciones externas de autentificación o se debe recurrir a una clave de segundo nivel para el ingreso

ID	Nombre	Descripción
		al sistema o confirmación del registro mediante un mail

Elaborado por: los autores

Resultados

Primer ciclo de evaluación

En este primer ciclo de evaluación se tomó el módulo de seguridad sin la implementación de la Autentificación por Doble factor, en el cual no se implementó ningún factor de autentificación externa al propio módulo desarrollado. En la tabla 3 se describen los resultados de la evaluación del primer ciclo.

Tabla 3. Resultados de la evaluación del primer ciclo

ID	Nombre	Primer evaluador	Segundo evaluador	Tercer evaluador	Cuarto evaluador	Quinto evaluador
C-1	Conexiones seguras	0	0	1	0	0
C-2	Control de acceso	1	1	1	1	1
C-3	Encriptación de datos	1	1	1	1	1
C-4	Contraseña de alto nivel	1	1	1	1	1
I-5	Prevención de Accesos	1	1	1	1	1
I-6	Prevención de modificaciones	1	1	1	1	1
I-7	confirmación de datos	1	1	1	1	1

ID	Nombre	Primer evaluador	Segundo evaluador	Tercer evaluador	Cuarto evaluador	Quinto evaluador
NR-8	Operaciones realizadas	1	1	1	1	1
NR-9	Mecanismo de Cifrado	1	1	1	1	1
NR-10	Verificación de acciones	1	0	1	1	0
R-11	Registro de acciones y datos	1	1	1	1	1
R-12	Detección de posibles ataques	1	1	1	1	1
A-13	Comprobación de identidad	0	0	0	0	0
A-14	Comprobaciones adicionales	1	1	1	1	1

Elaborado por: los autores

En la tabla 4 se evidencia el cumplimento de cada una de las métricas de seguridad en el primer ciclo de evaluación, en el que se muestra que apenas dos métricas son cumplidas a cabalidad. En la métrica de confidencialidad existe un cumplimento del 75%, siendo el 25% de no cumplimiento debido a la falta de seguridad en el redireccionamiento de sitos seguros, en la métrica de no repudio existe una discrepancia entre los evaluadores, siendo el 33% de cumplimento en esta métrica, dado a la falta de verificación de los datos al realizar una acción. Finalmente, en la métrica de autenticidad existe apenas un 50% de cumplimento de la métrica debido a que no existe ningún tipo de autentificación externa por parte del módulo informático.

Tabla 4. Cumplimiento de las métricas de seguridad primera evaluación

Métrica	Porcentaje de cumplimiento de cada métrica				
	Primer evaluador	Segundo evaluador	Tercer evaluador	Cuarto evaluador	Quinto evaluador
Confidencialidad	75%	75%	100%	75%	75%
Integridad	100%	100%	100%	100%	100%
No Repudio	100%	67%	100%	100%	67%
Responsabilidad	100%	100%	100%	100%	100%
Autenticidad	50%	50%	50%	50%	50%

Elaborado por: los autores

Segundo ciclo de evaluación

En este segundo ciclo de evaluación se tomó el módulo de seguridad con la implementación de la Autentificación por Doble factor, además de mejorar el cumplimiento de varias métricas vistas en el anterior ciclo de evaluación.

Tabla 5. Criterios de evaluación del segundo ciclo de evaluación

ID	Nombre	Primer evaluador	Segundo evaluador	Tercer evaluador	Cuarto evaluador	Quinto evaluador
C-1	Conexiones seguras	1	1	1	1	1
C-2	Control de acceso	1	1	1	1	1
C-3	Encriptación de datos	1	1	1	1	1
C-4	Contraseña de alto nivel	1	1	1	1	1
I-5	Prevención de Accesos	1	1	1	1	1

ID	Nombre	Primer evaluador	Segundo evaluador	Tercer evaluador	Cuarto evaluador	Quinto evaluador
I-6	Prevención de modificaciones	1	1	1	1	1
I-7	Confirmación de datos	1	1	1	1	1
NR-8	Operaciones realizadas	1	1	1	1	1
NR-9	Mecanismo de Cifrado	1	1	1	1	1
NR-10	Verificación de acciones	1	1	1	1	1
R-11	Registro de acciones y datos	1	1	1	1	1
R-12	Detección de posibles ataques	1	1	1	1	1
A-13	Comprobación de identidad	1	1	1	1	1
A-14	Comprobaciones adicionales	1	1	1	1	1

Elaborado por: los autores

En la tabla 6 se evidencia el cumplimento total de cada una de las métricas recomendadas por la norma ISO 25010, según los resultados obtenidos, la implementación de factores de autentificación externas mejora en el cumplimento de todas las métricas, la métrica de autenticidad es la más afectada pasando de un 50% a 100%, esto debido a la implementación de la Autentificación por Doble Factor.

Tabla 6. Cumplimiento de las métricas de seguridad segunda evaluación

Métrica	Porcentaje de cumplimiento de cada métrica				
	Primer evaluador	Segundo evaluador	Tercer evaluador	Cuarto evaluador	Quinto evaluador
Confidencialidad	100%	100%	100%	100%	100%
Integridad	100%	100%	100%	100%	100%
No Repudio	100%	100%	100%	100%	100%
Responsabilidad	100%	100%	100%	100%	100%
Autenticidad	100%	100%	100%	100%	100%

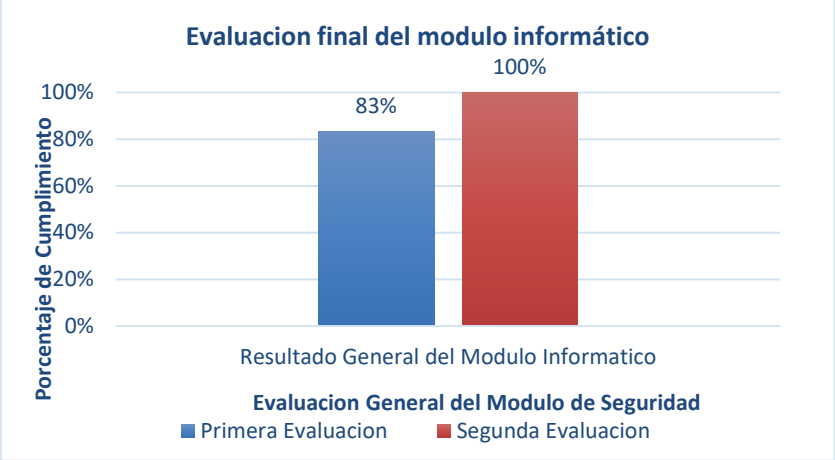
Elaborado por: los autores

Resultado final del módulo de seguridad

En el gráfico 1, se muestra la diferencia que existe entre los dos ciclos de evaluación, demostrando que en la primera evaluación existe un cumplimento del 83% y luego de la implementación del doble factor, un cumplimiento del 100%. Entre estos dos ciclos existe una diferencia del 17%, dicha diferencia en términos generales no es muy notoria, pero al revisar cada una de las métricas, se muestra que la implementación de métodos de autentificación externas mejora la seguridad de todas las métricas y en especial la métrica de Autenticidad.

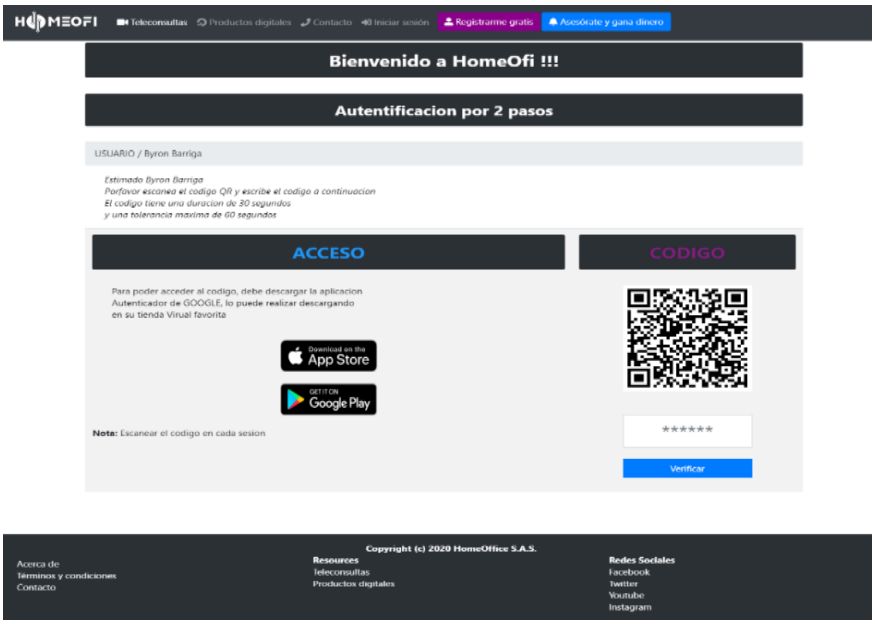
En la figura 1 y 2 se puede observar las vistas de la Autentificación por Doble factor, la primera en la cual se encuentra el código QR y en la segunda la confirmación de la autentificación del cliente a través de Google Authenticator.

Gráfico 1. Análisis general del módulo de seguridad informática



Elaborado por: los autores

Figura 1. Vista Autentificación por Doble Factor para el cliente



Elaborado por: los autores

Figura 2. Código de la App Google Authenticator del cliente

Elaborado por: los autores

Conclusiones

Los sistemas informáticos, se encuentran en constante vulnerabilidad debido al incremento de ciberdelincuentes, métodos de robo de contraseñas y de suplantación de identidad, además de las múltiples formas de realizar un ataque informático directo al sistema. Todo sistema informático debe ser capaz de neutralizar y detectar ataques, implementando en sus sistemas varios métodos de autentificación, tanto externos como internos, además de un historial de cada acción realizadas por sus múltiples usuarios y finalmente debe tener algoritmos de encriptación y cifrado de datos. Para la Autentificación por Doble factor existen varios métodos para implementarlos en módulos de seguridad, entre ellos está la implementación de captchas, contraseña convencional, y código QR, los cuales son los más utilizados, debido a su facilidad de implementación, costo muy bajo y facilidad de uso tanto para el usuario como para el sistema. Para mejorar la seguridad Informática de la plataforma informática HomeOfi se implementó un módulo de seguridad el cual permite llevar un registro de usuarios con sus respectivos datos y roles, permitiendo acceder a las distintas funcionalidades del mismo, además, cada usuario posee un historial de las acciones realizadas junto con un bloqueo en el caso de no cumplir las condiciones correctas al momento de ingresar y actualizar su información. El ingreso del sistema cuenta con una Autentificación por Doble factor, la primera cuenta con una contraseña y un captcha, mientras que el segundo cuenta con un código QR y la aplicación Google Authenticator. Finalmente se da una comprobación de inicio de sesión por medio de un mensaje de

correo electrónico al usuario. El módulo de seguridad posee un historial con los datos más relevantes de los ataques informáticos que detectó y neutralizó.

Para la evaluación del módulo de seguridad informática se utilizó las métricas de la categoría de seguridad recomendada por la Norma ISO 25010, de acuerdo al criterio para el análisis de la seguridad se establece que solamente cuando este cumplidas todas las métricas al 100 % se definirá al módulo de seguridad como seguro. A través del análisis de seguridad por medio del método Delphi permitió evaluar el módulo de seguridad en dos ciclos, el primero sin contar con la Autentificación por Doble factor obteniendo un porcentaje de aceptación del 83% en general, mientras que en el segundo ciclo se implementó la Autentificación por Doble factor dando como resultado un porcentaje de aceptación del 100%, evidenciado que la misma mejora la seguridad informática del sistema HomeOfi.

Estas implementaciones técnicas permiten mantener a los sistemas informáticos más seguros, sin embargo, las plataformas siguen siendo vulnerables a ataques, tanto internos como externos, por esta razón es necesario un adecuado monitoreo evaluación constante y actualización tecnológica, además, de educación a los usuarios con la finalidad que los mismos puedan proteger sus datos confidenciales.

Referencias

1. Altamirano, J., & Bayona, S. (2017). Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento. Revista lbérica de Sistemas y Tecnologías de Información, 25, 134. https://doi.org/10.17013/risti.25.112-134
2. Alzahrani, A. (2018). Useable Authentication Mechanisms for Secure Online Banking. International Journal of Scientific Research in Computer Science, Engineering and Information Technology.
3. Cañón, Lady. (2015). Ataques informáticos, Ethical Hacking y conciencia de seguridad informática en niños. Universidad Piloto de Colombia. Recuperado de https://core.ac.uk/download/pdf/226151976.pdf
4. Gil, V., & Gil, J. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. Scientia et Technica, 22(2), 193–197. https://doi.org/10.22517/23447214.11371
5. Homeofi. (2020). Quienes Somos. Recuperado de https://homeofi.com/acerca-de
6. ISO25000. (2015). Norma ISO/IEC 25010. Recuperado de https://iso25000.com/index.php/normas-iso-25000/iso-25010?limit=3&limitstart=0

7. Kuang, G., & Xu, H. (2020). Realization of Identity Card and Face Recognition Two-Factor Authentication System Based on Wechat. Advances in Intelligent Systems and Computing, 1017, 929–936. Springer Verlag. https://doi.org/10.1007/978-3-030-25128-4_114/COVER
8. Lagreca, N. (2017). Modelo de auditoria para servicios telemáticos de la universidad Simón Bolívar. Télématique, 16(2), 79–95. Recuperado de https://www.redalyc.org/pdf/784/78457361005.pdf
9. Mieres, J. (2009). Ataques informáticos Debilidades de seguridad comúnmente explotadas | Mario Mamani - Academia.edu. Recuperado el 25 de julio de 2022, de https://www.academia.edu/8522766/Ataques_informáticos_Debilidades_de_seguridad_comúnmente_explotadas
10. Quiroz-Zambrano, S., & Macías-Valencia, D. (2017). Seguridad en informática: consideraciones . Dominio de las Ciencias, 3(5), 676–688. Recuperado de https://dominiodelasciencias.com/ojs/index.php/es/article/view/663/pdf
11. Singh, S. (2017). Multi-factor Authentication and their Approaches. International Research Journal of Management, 4(3), 68–81. Recuperado de https://sloap.org/journals/index.php/irjmis/article/view/468
12. Suárez, D., & Ávila, A. (2015). Una forma de interpretar la seguridad informática . Journal of Engineering and Technology, 4(2). Recuperado de http://179.1.108.245/index.php/jet/article/view/1015
13. Tirado, N., Ramos, D., Álvarez, E., & Carreño, S. (2017). Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas. Revista, 4(10), 462–473. Recuperado de https://core.ac.uk/download/pdf/236644851.pdf
14. Vargas, R., Reyes, R., & Recalde, L. (2007). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO. Revista Latinoamericana de Estudios de Seguridad, (20), 31–45. https://doi.org/10.17141/URVIO.20.2017.2571
15. Waheed, A., Ali Shah, M., & Khan, A. (2016). Secure login protocols: An analysis on modern attacks and solutions. 22nd International Conference on Automation and Computing, ICAC 2016: Tackling the New Challenges in Automation and Computing, 535–541. https://doi.org/10.1109/ICONAC.2016.7604975