Innovación y Software
ISSN: 2708-0927
ISSN: 2708-0935
facin.innosoft@ulasalle.edu.pe
Universidad La Salle
Perú

Reyes Riveros, Anderson Jhanyx; Mendoza de los Santos, Alberto; Salinas Meza, Jhon Erick
Modelo de Autentificación de Doble Factor
Innovación y Software, vol. 4, núm. 1, 2023, Marzo-Agosto, pp. 82-95
Universidad La Salle
Perú

Revista Innovación y Software
Vol. 4, No. 1, Mes Marzo-Agosto, 2023
ISSN: 2708-0935
Pág. 82-95
https://revistas.ulasalle.edu.pe/innosoft

Tipo de artículo: Artículos originales
Temática: Desarrollo de aplicaciones informáticas
Recibido: 15/11/2022 | Aceptado: 27/12/2022 | Publicado: 30/03/2023

Identificadores persistentes:
ARK: ark:/42411/s11/a81
PURL: 42411/s11/a81

Modelo de Autentificación de Doble Factor

Two-Factor Authentication Model

Anderson Jhanyx Reyes Riveros [1][0000-0002-7324-5055]*, Jhon Erick Salinas Meza [2][0000-0003-1715-2716], Alberto Carlos Mendoza de los Santos 3[0000-0002-0469-915X]

[1] Universidad Nacional de Trujillo. ajreyesr@unitru.edu.pe
[2] Universidad Nacional de Trujillo. jsalinas@unitru.edu.pe
[3] Universidad Nacional de Trujillo. amendozad@unitru.edu.pe

* Autor para correspondencia: ajreyesr@unitru.edu.pe

Resumen

El presente artículo tiene como objetivo principal el desarrollo de un modelo que permita la autentificación de un usuario para el control de accesos mediante el modelo de Autentificación de doble factor. Para el desarrollo de dicho modelo presentamos un esquema seguro de autentificación de dos factores(TFA) basado en la posesión por el usuario de una contraseña y un dispositivo con capacidad criptográfica. La seguridad de este modelo es de extremo a extremo en el sentido de que el que quiera acceder de una manera fraudulenta se le va a complicar y asi garantizar la seguridad del usuario de dicho sistema, se tuvo como algoritmo Redes criptográficas, el cual es un modelo de doble autentificación. Así mismo se utilizó el lenguaje de programación cakephp 4.0, además de utilizar el programa visual studio code para poder realizar los algoritmos requeridos para que funciones el modelo de doble autentificación.

Palabras clave: Control de acceso, Autenticación de dos factores, Criptografía.

Abstract

The main objective of this paper is the development of a model that allows the authentication of a user for access control using the Two-Factor Authentication model. For the development of such a model we present a secure two-factor authentication (TFA) scheme based on the user's possession of a password and a cryptographically capable device. The security of this model is end-to-end in the sense that whoever wants to access in a fraudulent way is going to find it difficult and thus guarantee the security of the user of the system, the algorithm used was Cryptographic Networks, which is a double authentication model. Also the programming language cakephp 4.0 was used, in addition to using the visual studio code program to perform the algorithms required for the double authentication model to work.

Keywords: *Access Control, Two-factor Authentication, Cryptography.*

Revista Innovación y Software
Vol. 4, No. 1, Mes Marzo-Agosto, 2023
ISSN: 2708-0935
Pág. 82-95
https://revistas.ulasalle.edu.pe/innosoft

Introducción

Actualmente las contraseñas son el mecanismo dominante de autentificación digital y por ende van a proteger una gran cantidad de información importante. Sin embargo, las contraseñas son vulnerables ataques en línea y fuera de línea. Un adversario de la red puede probar las contraseñas adivinadas en interacciones en línea con el servidor, mientras que un atacante que compromete los datos de autenticación almacenados por el servidor (es decir, una base de datos de contraseñas) puede organizar un ataque de diccionario fuera de línea comparando la información de autenticación de cada usuario con un diccionario de posibles contraseñas. Los ataques de diccionario fuera de línea son una amenaza importante, experimentada rutinariamente por las ventas comerciales, y conducen al compromiso de miles de millones de cuentas de usuario [13], por lo cual requiere de un sistema de autenticación para restringir el acceso de los usuarios a cierta información almacenada en computadores.

Dentro de los diferentes tipos de autenticación se encuentra la autenticación donde los usuarios autorizados pueden acceder a los datos almacenados en la nube, según el esquema del mecanismo de autenticación para sistemas de banca por Internet en la nube con autenticación multifactorial. Los usuarios se autentican utilizando una combinación de factores como su nombre de usuario, contraseña, número aleatorio y huella dactilar biométrica. -La huella biométrica del usuario se utiliza para cifrar el número aleatorio [6]. Sin embargo, en este proceso, el número arbitrario cifrado se envía al número de teléfono registrado a través de un entorno abierto y vulnerable, lo que da lugar a diversos ataques. Además, para validar las muestras biométricas de huellas dactilares se necesita una potencia de computación adicional. Una base conceptual para la técnica 2FA (verificación de dos factores) mezcla elementos de verificación de contraseñas (basada en el conocimiento) y biométrica (dinámica de pulsación de teclas) [7]. Una solución de autenticación multifactorial (MFA) basada en el polinomio de Lagrange invertido, como expansión de la función de compartición de secretos de Shamir, aborda las situaciones de verificación de la identidad incluso si algunas de las partes están desalineadas o ausentes. También ayuda en la calificación de los elementos que faltan sin revelar información sensible al validador; por lo tanto, cuando un usuario pierde o sigue olvidando sus claves 2F, una asignación apropiada está lista para ayudar con la autenticación mediante el envío de una información privada al usuario [17]. Para completar los pasos de la MFA, la solución propuesta se concibe explícitamente, por lo que su gestión para 2FA y SFA no es aclamada. Añadir un factor de tiempo aleatorio no es capaz de proporcionar un nivel útil de protección de datos biométricos, ya que el espía podría ser capaz de recuperar instantáneamente el secreto del factor.

En este artículo se tratará de abordar un modelo de autenticación de contraseña de dos factores (TFA), en la que el usuario U se autentica ante el servidor S "demostrando la posesión" de un dispositivo personal auxiliar D (por ejemplo, un smartphone o un token USB) además de conocer su contraseña, constituye una defensa común contra los ataques de contraseña en línea, así como una segunda línea de defensa en caso de fuga de contraseñas. Un esquema TFA que utiliza un dispositivo que no está directamente conectado al terminal cliente C de U suele funcionar de la siguiente manera: D muestra un breve PIN secreto de un solo uso, recibido de S (por ejemplo, mediante un mensaje SMS) o calculado por D basándose en una clave compartida con S, y el usuario teclea manualmente el PIN en el cliente C además de su contraseña. Ejemplos de sistemas basados en PINs de un solo uso incluyen PINs basados en SMS, TOTP [10], HOTP [14], Google Authenticator [4], FIDO U2F [2], y esquemas en la literatura como [3].

Materiales y métodos o Metodología computacional

Estado del arte:

Propuesta de esquema seguro de autenticación multifactor en la nube. Nuestro sistema propuesto tiene una estructura modular que permite analizar cada riesgo y su respuesta por separado. -is facilita la gestión del sistema en la nube y permite a los administradores y usuarios integrar soluciones especializadas para combatir los riesgos. El sistema en nube tiene dos tipos de entidades: el servidor en nube y el usuario en nube. El procedimiento de autenticación propuesto consta de las dos fases siguientes: fase de registro y fase de inicio de sesión

A. Fase de registro.

Esta fase consta además de tres pasos. Los usuarios de la nube se registran en el servidor de la nube para utilizar los servicios prestados por el servidor de la nube con los tres pasos principales siguientes:

Primer paso. En el primer paso, el usuario de la nube se registra con su ID de usuario, ID de correo electrónico y número de móvil; el servidor valida y verifica toda la información proporcionada y envía el correo electrónico y el número de móvil OTP para validar al cliente.

(1) Cliente: el cliente envía su nombre de usuario, correo electrónico y número de móvil al servidor en la nube.

(2) Servidor: el servidor almacena la información recibida y envía la OTP por correo electrónico y SMS al cliente.

(3) Cliente: el cliente almacena y recibe la OTP por correo electrónico y SMS del servidor.

Segundo paso. En el segundo paso, el cliente introduce las OTP válidas y recibe la clave del servidor para seguir comunicándose de forma segura con el servidor y otra información útil como la contraseña.

(1) Cliente: el cliente introduce la OTP por correo electrónico y la OTP por SMS en el servidor en la nube.

(2) Servidor: el servidor verifica la OTP enviada y genera el par de claves EC.

(3) Servidor: el servidor envía la clave pública EC generada al cliente para una comunicación segura.

(4) Cliente: el cliente recibe la clave pública EC del servidor.

Tercer paso. En el tercer paso, el cliente elige la contraseña, el tipo de servicio y la duración del servicio y envía toda la información de forma segura utilizando la clave compartida del servidor con las siguientes medidas de seguridad avanzadas:

(1) El cliente genera y guarda la contraseña segura salada utilizando PBDKF2, como se muestra en la Figura 1. Enccs_pk {H(UserID) ||H(SecureSaltedPassword) || nonceX}

(2) Servidor: el servidor recibe la contraseña segura y los datos de suscripción, servicio y duración.

A continuación, el servidor almacena toda la información relativa a la identificación del usuario en la base de datos del servidor de forma segura y genera un certificado en la nube que contiene la identificación del usuario, la suscripción y la duración, que se enviará al usuario en formato cifrado. Servidor: el servidor cifra el certificado de suscripción utilizando su clave privada.

B. Inicio de sesión y autenticación tiene las siguientes dos capas o autenticación de dos factores para verificar la identidad del usuario

Autenticación de primer factor en la nube. Durante la primera fase, el usuario solicita el primer factor de autenticación. -e solicitud es recibida y procesada por la plataforma en nube. -La plataforma en nube consta de un servidor de base de datos y un servidor web. -El servidor de la base de datos autentica las credenciales electrónicas comparándolas con los registros ya registrados y, tras la autenticación, se envía una confirmación al servidor en la nube para comunicar al usuario que la autenticación se ha realizado correctamente. Aquí, el usuario de la nube proporciona el ID de usuario y la contraseña al servidor de la nube. EncMsg1 Enccs_pk {H(UserID) ||H (Password)}

(i) El servidor en nube recibe el mensaje cifrado (EncMsg1) y primero lo descifra y luego verifica la firma digital del usuario.

(ii) (ii) Si se verifica el paso anterior, el servidor en nube envía la OTP al correo electrónico registrado (OTP1) y al móvil (OTP2) y espera al segundo paso de autenticación.

Autenticación de segundo factor en la nube. Una vez verificado con éxito el 1FA, se pide al usuario que verifique el segundo factor a través de una aplicación autenticadora. Al recibir la solicitud, el servidor en la nube reverifica el primer factor y envía la confirmación o el rechazo a la nube para que la procese. Tras la reverificación satisfactoria del 1FA, la nube envía la solicitud para verificar el segundo factor y envía una solicitud OTP al usuario para verificar el dispositivo. Tras una autenticación correcta, se concede al usuario acceso a la nube. El usuario de la nube pasa por un procedimiento de autenticación multifactor en el que, en el primer proceso, envía de forma segura las credenciales tradicionales, como el ID de usuario y una palabra clave con sal fuerte, al servidor de la nube para que se verifiquen[7]; si se verifican, el servidor pide al usuario que envíe otro factor de autenticación, que es el certificado ya proporcionado por el servidor de la nube como su certificado de identidad y la OTP en el correo electrónico y el móvil. -De este modo, se envían los tres elementos siguientes:

(1) certificado en la nube;

(2) OTP en el correo electrónico;

(3) OTP en el móvil. (Figura 4) EncMsg2 Enccs_pk { H(CloudCertificate) ||H (OTP2) || H (OTP2) || nonceY}

(i) Si se verifican los tres factores anteriores, el usuario estará autenticado y podrá utilizar los servicios en la nube.

Fundamentación Teórica

Autentificación de Doble Factor

La autenticación de dos factores proporciona una capa secundaria de seguridad que hace que sea más difícil para los piratas informáticos acceder a los dispositivos y las cuentas en línea de una persona para robar información personal. Con la autenticación de dos factores habilitada, incluso si el pirata informático conoce la contraseña de su víctima, la autenticación seguirá fallando y evitará el acceso no autorizado. Además, también proporciona a las organizaciones un nivel adicional de control de acceso a sistemas sensibles y datos y cuentas en línea, protegiendo esos datos de ser comprometidos por piratas informáticos armados con contraseñas de usuario robadas.[24]

Inteligencia Artificial

La inteligencia artificial (IA) es un conjunto de algoritmos (reglas que definen con precisión un conjunto de operaciones) que permiten realizar cálculos para percibir, razonar y actuar. La IA es usada para llevar a cabo la realización de múltiples tareas, pero puede usarse para brindar mejoras a la inteligencia humana.[8]

Machine learning

Machine learning es definido como aprendizaje automático, y su uso está enfocado en el análisis masivo de datos [19]. Dentro de sus algoritmos más usados tenemos: SVM, BOSQUE ALEATORIO, Árbol de decisiones KNN y Adaboost clasificadores [20].

Deep Learning

Definido como aprendizaje profundo, ofrece una estrategia de optimización global. Dentro de sus usos tenemos: Procesamiento de información, reducción de ruido en imágenes [22], procesamiento del lenguaje natural [21]
Además, el aprendizaje profundo es una rama derivada del aprendizaje automático (Machine learning) [23].

Seguridad de la información

Es la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información almacenada en un sistema informático, contra cualquier tipo de amenaza, minimizando los riesgos tanto físicos como físicos. lógica, a la que está expuesto.[18]

Control de Accesos

Es implementado como un método de seguridad para delimitar un conjunto de usuarios autorizados para acceder a una determinada información [20].

Herramientas y elementos

Visual Studio Code Visual Studio Code es definido como una plataforma de código abierto, un editor de código de multiplataforma que pertenece a Microsoft y proporciona todos los componentes necesarios de un IDE como: IntelliSense, depuración, control de versiones, creación de plantillas y API de extensiones que brindan muchas facilidades a los desarrolladores.[11]

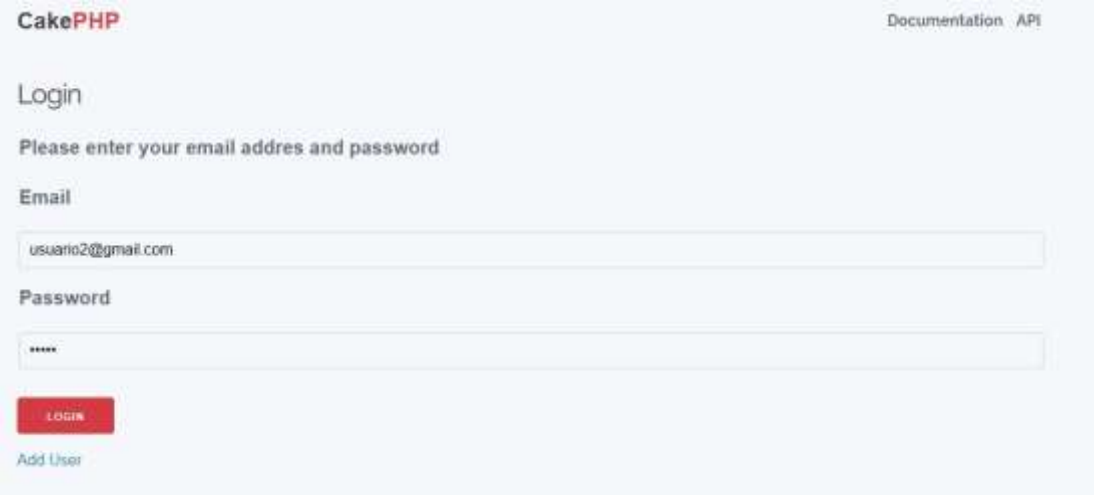
Cakephp 4.0 Proporciona una estructura organizativa básica que cubre los nombres de las clases, archivos, tablas de base de datos y otras convenciones más. Aunque lleva algo de tiempo aprender las convenciones, siguiéndolas CakePHP

evitará que tengas que hacer configuraciones innecesarias y hará que la estructura de la aplicación sea uniforme y que el trabajo con varios proyectos sea sencillo. El capítulo de convenciones muestra las que son utilizadas en CakePHP.**[**12]

Encuesta nos ayudara a poder sacar resultados con los usuarios que se comprometieron a testear este modelo y poder analizar si es eficiente su aplicación en varios sistemas o en la nube, además si es rentable, para las empresas corporativas.

Uso del modelo de doble factor

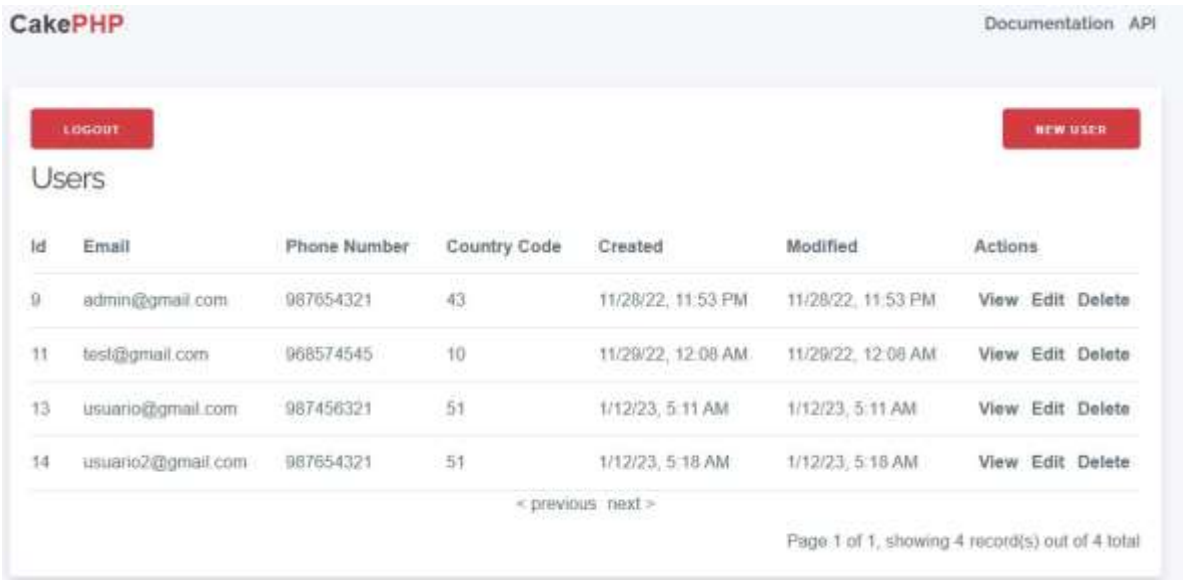
Ingresamos nuestro usuario para poder acceder al sistema



Cuando digitamos correctamente los datos del usuario el siguiente paso es digitar el token o código enviado un numero móvil para poder validar o también podrías escanear el qr con nuestro móvil vinculado, es decir tratar de usar el modelo de doble autentificación.

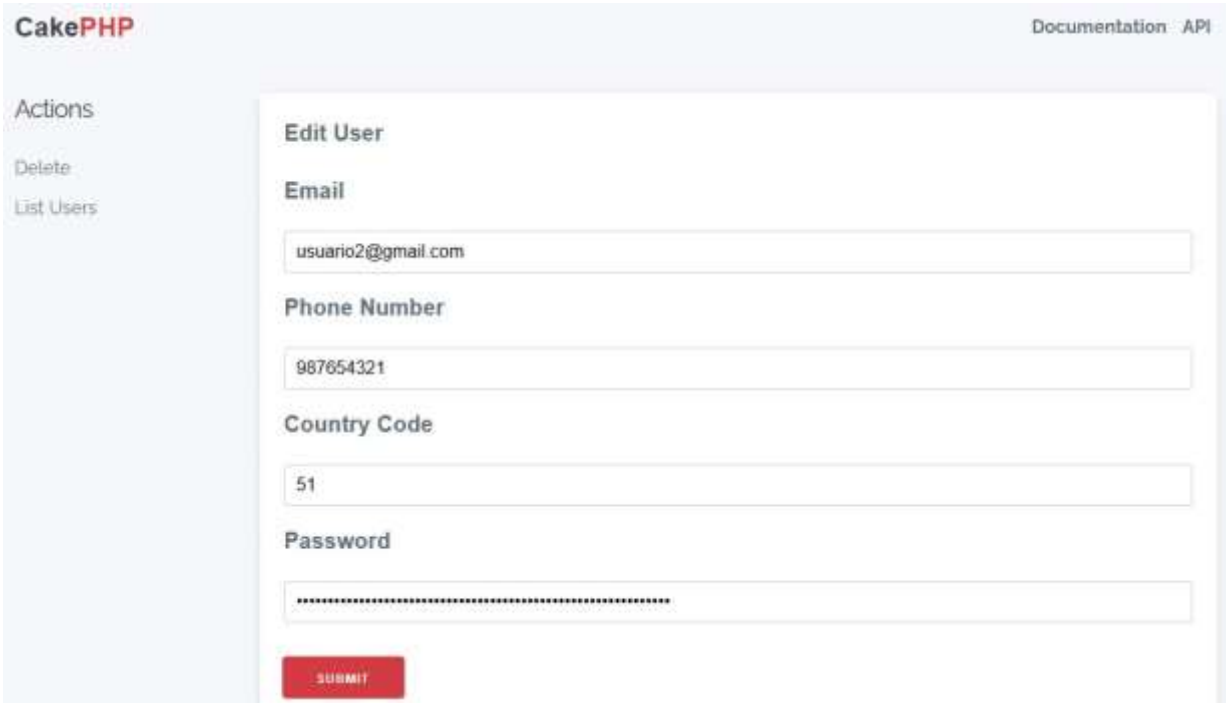
Revista Innovación y Software
Vol. 4, No. 1, Mes Marzo-Agosto, 2023
ISSN: 2708-0935
Pág. 82-95
https://revistas.ulasalle.edu.pe/innosoft

Aquí vemos los usuarios vinculados a dicho sistema, la cuales podrán usar el método de doble autentificación.



Además, el usuario podrá editar sus datos y en especial su número móvil, la cual es usada para usar el modelo de doble autenticación, esto es algo fundamental, mas cuando uno es propenso a perder el móvil o que será robado.

Revista Innovación y Software
Vol. 4, No. 1, Mes Marzo-Agosto, 2023
ISSN: 2708-0935
Pág. 82-95
https://revistas.ulasalle.edu.pe/innosoft



Resultados y discusión

¿Le ha resultado útil la autenticación doble factor? (protección doble).

Entre los encuestados respondieron sobre la pregunta de le ha resultado útil la autenticación doble factor, en un 77-1% afirman que les pareció útil y en un 29-9%, que no están útil. En concreto, el 51.6% de la muestra señalaba la seguridad como su razón principal. Esto puede deberse a que la mayor parte de los encuestados no están muy familiarizados con la doble autenticación.

Utiliza un sistema de seguridad en computadora de escritorio (PC).

En la utilización de un sistema de seguridad en computadora de escritorio (PC), los encuestados respondieron en un 48.6% que, si utilizan, en un 11.8% que no utilizan y en un 39-3%, que no tienen PC. Según Arellano y Peralta (2014), un 42,7% de las empresas que utiliza Internet no cuenta ni utiliza instalaciones o procedimientos internos de seguridad, coincidiendo aproximadamente con los porcentajes encontrados en el trabajo.

Utiliza un sistema de seguridad en Smartphone (Android, IOs).

En la utilización de un sistema de seguridad en smartphone (Android, IOs), respondieron los encuestados en un 54.9% que, si utilizan, en un 27-2% que no utilizan y en un 17-6%, que no tienen Smartphone. En relación a la pregunta no se encontró investigaciones realizadas.

Sabe lo que es el Phishing.

La respuesta de los encuestados sobre si sabe lo que es el Phishing, solo en un 19-1% conocen y en un 80.9% que no conocen. En un 46% de los encuestados afirmó haber recibido un mensaje fraudulento que afirmaba provenir de servicios de correo electrónico como Yahoo!, Microsoft y Gmail. Las siguen las redes sociales con un 45%, los bancos 44% y tiendas en línea 37%.

Sabe la diferencia entre hacker y cracker.

Los encuestados respondieron sobre la pregunta, si sabe la diferencia entre hacker y cracker, en un 59-4% no conocen y en un 40.6% que conoce.

Con qué frecuencia realiza usted copias de seguridad.

La respuesta de los encuestados sobre con qué frecuencia realiza usted copias de seguridad, en un 33-5% hace copias Anualmente, en un 15-3% hace copias Diariamente, en un 26.3% hace copias Mensualmente, en un 14.2% hace copias Semanalmente y en un 10.4% hace copias Trimestralmente.

Sabe lo que es una Dirección IP

La respuesta de los encuestados sobre si sabe lo que es una dirección IP, en un 37-7% no conocen y en un 62.3% que si conocen.

Sabe lo que es una dirección MAC.

Los encuestados respondieron sobre la pregunta, si sabe lo que es una dirección MAC, en un 77-4% no sabe y en un 22.6% que si saben lo que es una dirección MAC.

Sabe lo que significa el protocolo https.

La respuesta de los encuestados sobre si Sabe lo que significa el protocolo https, mencionan que en un 52.5% no sabe y en un 47-5% que sabe lo que significa el protocolo https.

¿Sabe lo que es una VPN?

Entre los que saben lo que es una VPN, están en un 39-7% y entre los que no saben están en un 60.3%.

Cómo considera la seguridad para hacer pagos a través de Internet.

Entre los encuestados que respondieron con respecto a cómo considera usted la seguridad para hacer pagos a través de Internet, se observa que, el 3-8% indica que es muy seguro, el 19-9% menciona que es nada seguro, el 47.1% indica que es poco seguro y el 28.9% indica que es seguro.

Utiliza autentificador de seguridad

Entre los encuestados que respondieron con respecto a utiliza autentificador de seguridad, se observa que, el 3-5% indica que es sí, el 93-95% menciona que no, ya que o desconocen su uso o no tienen tiempo que perder.

Conclusiones

Entre los encuestados respondieron sobre la pregunta de le ha resultado útil la autenticación doble factor, en un 77-1 % afirman que les ha resultado util; En la utilización de un sistema de seguridad en computadora de escritorio (PC), los encuestados respondieron en un 48.6% que si utilizan.

En la utilización de un sistema de seguridad en smartphone (Android, IOs), en un 54.9% que si utilizan.

La respuesta de los encuestados sobre si sabe lo que es el Phishing, solo en un 19-1% conocen.

Los encuestados respondieron sobre la pregunta, si sabe la diferencia entre hacker y cracker, en un 40.6% que conoce.

La respuesta de los encuestados sobre con qué frecuencia realiza usted copias de seguridad, en un 33-5% hace copias Anualmente, los demás en menor porcentaje.

La respuesta de los encuestados sobre si sabe lo que es una dirección IP, en un 62.3% que conocen.

La respuesta de los encuestados sobre si Sabe lo que significa el protocolo https, mencionan que en un 47-5% que sabe lo que significa el protocolo https.

Entre los encuestados que respondieron con respecto a cómo considera usted la seguridad para hacer pagos a través de Internet, el 47-1 % indica que es poco seguro, entre los de más porcentaje.

El Género Masculino obtuvo 8.0% de conocimiento de seguridad informática.

Los promedios de Ocupación con referente a la seguridad informática. El conocimiento de seguridad informática en la ocupación el que más porcentaje obtuvo es la ocupación Profesional independiente con 46%.
El Género Masculino alcanzó 2 % que utiliza autentificador de seguridad. Y de estos el 70-75% son población laboral activa.

Referencias

[1] "Facial Expression Recognition Using Machine Learning Techniques", *International Journal of Advance Engineering and Research Development*, vol. 1, n.º 06, junio de 2020. Accedido el 17 de noviembre de 2022. [En línea]. Disponible: https://doi.org/10.21090/ijaerd.010633

[2] FIDO Universal 2nd Factor. https://www.yubico.com/

[3] Shirvanian, M., Jarecki, S., Saxena, N., Nathan, N.: Two-factor authentication resilient to server compromise using mix-bandwidth devices. In: Network & Distributed System Security Symposium (2014)

[4] Google Authenticator Android app. https://goo.gl/Q4LU7k

[5] "OpenCV: OpenCV modules". OpenCV documentation index. https://docs.opencv.org/4.x/ (accedido el 17 de noviembre de 2022).

[6] S. Nagaraju and L. Parthiban, “Trusted framework for onlinebanking in public cloud using multi-factor authentication and privacy protection gateway,” Journal of Cloud Computing, vol. 4, no. 1, pp. 1–23, 2015.

[7] M. Olalere, M. Taufik Abdullah, R. Mahmod, and A. Abdullah, “Bring your own device: security challenges and A theoretical framework for two-factor Authentication,” Inaternational Journal of Computer Networks and Communications Security, vol. 4, no. 1, pp. 21–32, 2016, http://www.ijcncs.org.

[8] O. Niel y P. Bastard, "Artificial Intelligence in Nephrology: Core Concepts, Clinical Applications, and Perspectives", *American Journal of Kidney Diseases*, vol. 74, n.º 6, pp. 803–810, diciembre de 2019. Accedido el 17 de noviembre de 2022. [En línea]. Disponible: https://doi.org/10.1053/j.ajkd.2019.05.020

[9] T. Walsh, "The troubling future for facial recognition software", *Communications of the ACM*, vol. 65, n.º 3, pp. 35–36, marzo de 2022. Accedido el 15 de noviembre de 2022. [En línea]. Disponible: https://doi.org/10.1145/3474096

[10] TOTP: Time-Based One-Time Password Algorithm. https://goo.gl/9Ba5hv

[11] S. Latifi, Ed., *17th International Conference on Information Technology–New Generations (ITNG 2020)*. Cham: Springer International Publishing, 2020. Accedido el 17 de noviembre de 2022. [En línea]. Disponible: https://doi.org/10.1007/978-3-030-43020-7

[12] S. K. Shammi, S. Sultana, M. S. Islam y A. Chakrabarty, "Low Latency Image Processing of Transportation System Using Parallel Processing co-incident Multithreading (PPcM)", en *2018 Joint 7th International Conference on Informatics, Electronics & Vision (ICIEV) and 2018 2nd International Conference on Imaging, Vision & Pattern Recognition (icIVPR)*, Kitakyushu, Japan, 25–29 de junio de 2018. IEEE, 2018. Accedido el 17 de noviembre de 2022. [En línea]. Disponible: https://doi.org/10.1109/iciev.2018.8640957

[13] Kaur, S., Kaur, G., & Shabaz, M. (2022). A Secure Two-Factor Authentication Framework in Cloud Computing. *Security and Communication Networks, 2022*. https://doi.org/10.1155/2022/7540891

[14] RFC 4226 HOTP: An HMAC-based One-Time Password Algorithm (2005). https://goo.gl/wxHBvT

[15] I. Sluganovic, M. Roeschlin, K. B. Rasmussen y I. Martinovic, "Analysis of Reflexive Eye Movements for Fast Replay-Resistant Biometric Authentication", *ACM Transactions on Privacy and Security*, vol. 22, n.º 1, pp. 1–30, enero de 2019. Accedido el 17 de noviembre de 2022. [En línea]. Disponible: https://doi.org/10.1145/3281745

[16] L. Monastyrskii, V. Lozynskii, Y. Boyko y B. Sokolovskii, "Fingerprint recognition in inexpensive biometric system", *Electronics and Information Technologies*, vol. 9, 2018. Accedido el 17 de noviembre de 2022. [En línea]. Disponible: https://doi.org/10.30970/eli.9.120

[17] A. Ometov, S. Bezzateev, N. Makitalo, S. Andreev, ¨T. Mikkonen, and Y. Koucheryavy, “Multi-factor authentication: a survey,” Cryptography, vol. 2, no. 1, pp. 1–31, 2018

[18] H. AYDIN, "The Importance of Cyber Security in Management Information Systems (MIS)", *Bilgisayar Bilimleri ve Teknolojileri Dergisi*, octubre de 2022. Accedido el 17 de noviembre de 2022. [En línea]. Disponible: https://doi.org/10.54047/bibted.1138252

[19] M. Meroni, F. Waldner, L. Seguini, H. Kerdiles y F. Rembold, "Yield forecasting with machine learning and small data: What gains for grains?", *Agricultural and Forest Meteorology*, vol. 308-309, p. 108555, octubre de 2021. Accedido el 17 de noviembre de 2022. [En línea]. Disponible: https://doi.org/10.1016/j.agrformet.2021.108555

[20] M. S. Bouzakraoui, A. Sadiq y A. Y. Alaoui, "Customer Satisfaction Recognition Based on Facial Expression and Machine Learning Techniques", *Advances in Science, Technology and Engineering Systems Journal*, vol. 5, n.º 4, p. 594, agosto de 2020. Accedido el 17 de noviembre de 2022. [En línea]. Disponible: https://doi.org/10.25046/aj050470

[21] A. Bazaga, N. Gunwant y G. Micklem, "Translating synthetic natural language to database queries with a polyglot deep learning framework", *Scientific Reports*, vol. 11, n.º 1, septiembre de 2021. Accedido el 17 de noviembre de 2022. [En línea]. Disponible: https://doi.org/10.1038/s41598-021-98019-3

[22] B. Liu *et al.*, "Unsupervised Deep Learning for Random Noise Attenuation of Seismic Data", *IEEE Geoscience and Remote Sensing Letters*, pp. 1–5, 2021. Accedido el 17 de noviembre de 2022. [En línea]. Disponible: https://doi.org/10.1109/lgrs.2021.3057631

[23] J. Han, E. Shihab, Z. Wan, S. Deng y X. Xia, "What do Programmers Discuss about Deep Learning Frameworks", *Empirical Software Engineering*, vol. 25, n.º 4, pp. 2694–2747, abril de 2020. Accedido el 17 de noviembre de 2022. [En línea]. Disponible: https://doi.org/10.1007/s10664-020-09819-6

[24] Kaur, S., Kaur, G., & Shabaz, M. (2022). A Secure Two-Factor Authentication Framework in Cloud Computing. *Security and Communication Networks, 2022*. https://doi.org/10.1155/2022/7540891

Roles de Autoría

Rene Aquino Arcata: Investigación, Metodología, Redacción - borrador original. **Ronald Zenón Cuevas Machaca:** Conceptualización, Investigación, Metodología, Redacción - borrador original. **Gustavo Adolfo Villarroel Laura:** Investigación, Metodología, Redacción - borrador original.