Asesorías y Tutorías para la Investigación Científica en la Educación Puig-Salabarría S.C.
José María Pino Suárez 400-2 esq a Lerdo de Tejada. Toluca, Estado de México. 7223898475
RFC: ATI120618V12

Revista Dilemas Contemporáneos: Educación, Política y Valores.
http://www.dilemascontemporaneoseducacionpoliticayvalores.com/
Año: VIII Número: Edición Especial. Artículo no.:17 Período: Julio, 2021

TÍTULO: Política para la creación de contraseñas usando números en dialectos mexicanos en instituciones educativas.

AUTORES:

1. Dr. Rolando Salazar Hernández.
2. Dr. Adán López Mendoza.

RESUMEN: Existen algunas formas de autenticarse en los sistemas computacionales locales o remotos, ya bien sean portales web o aplicaciones. La mayoría de estas aplicaciones se autentica a través de las credenciales de los usuarios, una cuenta y una contraseña. Se ha demostrado a través de la literatura consultada que muchos usuarios utilizan contraseñas débiles formadas por palabras que se pueden encontrar en diccionarios de palabras de diferentes idiomas. En el presente artículo presentamos una técnica que permita robustecer las contraseñas de usuario a través del uso de los números de tres dialectos mexicanos sin tener que memorizar la contraseña sino utilizar una aplicación portable o la interpolación e intercalación de palabras.

PALABRAS CLAVES: autenticación, contraseña, robustecer, dialectos.

TITLE: Policy for creating passwords using numbers in Mexican dialects in educational institutions.

AUTHORS:

1. Dr. Rolando Salazar Hernández.
2. Dr. Adán López Mendoza.

ABSTRACT: There are some ways to authenticate to local or remote computer systems, whether they are web portals or applications. Most of these applications authenticate through user credentials, an account, and a password. It has been shown through the consulted literature that many users use weak passwords made up of words that can be found in dictionaries of words from different languages. In this article we present a technique that allows us to strengthen user passwords through the use of the numbers of three Mexican dialects without having to memorize the password but instead using a portable application or the interpolation and interleaving of words.

KEY WORDS: authentication, password, robust, dialects.

INTRODUCCIÓN.

Existen diferentes maneras de autenticar a los usuarios de los sistemas informáticos, ya bien sean locales o remotos, a través de huella dactilar, patrones de dibujo, contraseña numérica, imagen del rostro, pero la manera más común de autenticar a los usuarios es a través de una contraseña que está formada por un conjunto de letras, números y en algunos casos símbolos.

En años recientes cuando se crean credenciales de usuario, lo conveniente es formar contraseñas robustas que incluyan números, letras y símbolos especiales ($, %, &, ¡!, etc.) que algunas veces resulta imposible de memorizar y que muchas veces el usuario no la recuerda y tiene que recuperar a través de técnicas para ello. Morris y Thompson describen un esquema para la seguridad de las contraseñas en sistemas UNIX desde el año 1979, donde proponen password seguras para evitar que personas no autorizadas accedan a los sistemas (Morris & Thompson, 1979).

Yan y otros en 2004, realizan un estudio donde prueban con un estudio empírico las deficiencias en el uso de las contraseñas y presentan un método del uso de la mnemotecnia como una estrategia para la memorización de las contraseñas; los autores mencionan que muchas de las deficiencias en las contraseñas se deben a las limitaciones de memorización y que algunos no son capaces de recordar

las contraseñas aun acabadas de crear y realizan una investigación cuantitativa para probar que las contraseñas se pueden romper con longitudes de 6 caracteres fácilmente (Yan, Alan, Anderson, & Grant, 2004).

En el año 1996, Jablon propone un método para robustecer las contraseñas cortas; este método llamado SPEKE, utiliza la criptografía y el modelado matemático para hacer más fuerte la contraseña y que no se pueda encontrar en los diccionarios de palabra, es comparado con otro método llamado DH-EKE, aunque genera palabras muy robustas son difíciles de memorizar para una gran mayoría de personas (Jablon, 1996).

Weir y otros realizan pruebas métricas con un conjunto de 32 millones de contraseñas a fin de determinar su efectividad usando la entropía, en sus resultados experimentales demuestran con pruebas de metodologías de ataque a contraseñas que puedan ser vulnerables y proponen políticas de seguridad en las contraseñas que no permitan contraseñas débiles, realizan pruebas con diferentes escenarios y combinaciones como letras mayúsculas, minúsculas, caracteres especiales en diferentes posiciones de las contraseñas y obtienen estadísticas de ellas (Weir, Aggarwal, Collins, y Stern, 2010).

En el año 2010, Shay y otros realizaron un estudio a través del cuestionamiento de 470 usuarios de la Universidad de Carnegie Mellon, donde encontraron lo siguiente en la composición de las contraseñas, 163 personas que representan 34.9% utilizan una palabra basada en un nombre como contraseña. Solo 79 personas el 16.8% utilizan la combinación de nombres, números y símbolos para formar su contraseña. Los demás utilizan su fecha de cumpleaños, su domicilio, su número telefónico pero no la combinación de estos, lo que es fácil encontrar en un diccionario de palabras de los diferentes idiomas y estos con un programa de fuerza bruta puede revelar la contraseña y tener accesos no autorizados a los sistemas (Shay et al., 2010).

Una buena guía para el establecimiento de políticas de contraseñas es el que muestra el Instituto Nacional de Estándares y Tecnologías (NIST National Institute Standard and Technology). Este instituto propone en un documento 800-63B requisitos para los secretos memorizados por ejemplo contraseñas y números de identificación personal. En el documento hace una recomendación de una longitud mínima de 8 caracteres y de diferentes tipos alfabético, numérico y caracteres especiales "NIST".

El modelo de referencia de seguridad CIA (Confidencialidad, Autenticación y Disponibilidad, CIA por sus siglas en inglés) es muy utilizado para establecer las políticas de seguridad informática en todas las organizaciones. La autenticación es una primera línea de defensa ante los ataques de personas no autorizadas accedan a los sistemas computacionales. En este sentido, existen técnicas que permitan facilitar la memorización de las contraseñas dándole fortaleza a esas contraseñas, Cherdmuangpak y otros han propuesto un trabajo de investigación utilizando imágenes reemplazando los caracteres que se usan en las contraseñas, han demostrado que su técnica es efectiva para jóvenes de secundaria y previenen algunos ataques con el uso de la técnica que proponen (Cherdmuangpak, Anusas-Amonkul, & Limthanmaphon, 2017).

Existen algunos otros trabajos de investigación que utilizan técnicas contraseñas gráficas, porque los usuarios pueden recordar con más facilidad una imagen que un texto. Otros trabajos proponen el realizar un dibujo como contraseña, el uso de esta técnica puede producir problemas porque no se pueden solapar los vértices o las aristas en un trazo (Blonder, 1996; Chakrabarti, Landon, & Singhal, 2007).

Existen algunas otras técnicas que se basan en imágenes del rostro humano, dibujos animados y los autores de las técnicas afirman que puede ser más eficaz que se cree la propia contraseña con estas técnicas que las que se puedan generar por los sistemas informáticos (Gurav, Gawade, Rane, y Khochare, 2014).

Otras técnicas de autenticación utilizan dos vías, utilizan la contraseña capturada en texto y la huella digital, el rostro, el iris del ojo o algún patrón dibujado, y en algunos casos un mensaje de texto por la telefonía móvil, argumentando que este proceso de autenticación es más seguro que el uso de una sola contraseña (Khanaa, Thooyamani, y Udayakumar, 2014); sin embargo, estas técnicas se vuelven complicadas de implementar en cualquier entorno debido a los dispositivos hardware informáticos que utilizan para capturar la huella, el iris, o el patrón de dibujo, son costosos y algunos poco portables.

Alodhyani y otros realizaron un estudio mixto del uso de los gestores de contraseñas en donde encontraron como principal factor de no usar estos administradores de contraseñas como la desconfianza y la transparencia en el uso de ellas, y encontraron que algunos administradores tienen problemas con las interfaces y las funciones que utilizan (Alodhyani, Theodorakopoulos, y Reinecke, 2020).

Maqbali y Mitchel presentan un esquema generador de contraseñas llamado AutoPass, basado en cliente-servidor, donde con una entrada mínima el usuario puede generar o regenerar una contraseña robusta utilizando funciones compendio como hash-256, aunque cumple con los requisitos para generar una contraseña del mundo real, necesita un servidor y una pasarela para generar la contraseña, lo que supone un inconveniente al momento de su implementación (Maqbali y Mitchell, 2017).

Glory y otros han desarrollado un generador de contraseñas basado en un único algoritmo que utiliza palabras y números que proveen los usuarios y que no representan un reto de recordar esa contraseña generada, han probado su efectividad a través de ataques de fuerza bruta donde presentan resultados satisfactorios (Glory, Ul Aftab, Tremblay-Savard, y Mohammed, 2019).

DESARROLLO.

En el presente trabajo, hemos desarrollado un generador de contraseñas utilizando los números de tres dialectos mexicanos (Otomí, Náhuatl y Maya) para darle mayor robustez a las contraseñas, en una aplicación que permita la generación sin necesidad de memorizar la contraseña generada. A continuación, presentamos el desarrollo e implementación de la propuesta.

Algoritmo.

En el algoritmo primero tomamos como entrada un texto que el usuario elija, es un texto que el fácilmente puede memorizar como un nombre, una dirección, un número telefónico o la combinación entre ellos, una vez se tiene el texto proponemos una conversión en 2 pasos, el primer paso es convertir las 5 letras vocales en números arábigos; por ejemplo (a=4, e=3, i=1, o=5, u=6), para en un segundo paso convertir esos números arábigos por números en el dialecto de su elección; se ha seleccionado el 5 y 6 debido a que en algunos dialectos no se cuenta con un número cero para ser utilizado y el 6 se selecciona por ser el consecutivo. Continuando con la técnica, los siguientes pasos serían seleccionar un dialecto de los tres posibles, el otomí, el maya o el náhuatl y reemplazar los números arábigos por los números en el dialecto elegido. A continuación, se describe el algoritmo que se utilizó para realizar la técnica antes descrita.

Algoritmo generador de contraseña.

Requisitos.

Texto sin límite de caracteres, sin espacios, incluya números, letras o caracteres especiales.

1. Inicio.
2. Cadena1 <- texto plano.
3. N <- número de caracteres.
4. Mientras cadena1 < N.
5. Hacer.

a. alfabeto1 <-{a, e, i, o, u}
b. alfabeto2 <-{4, 3, 1, 5, 6}
c. cadena2 <-reemplaza.cadena1(alfabero1,alfabeto2)
d. alfabeto-maya <-{kan, óox, jun, jo'o, waak}
e. alfabeto-otomí <-{goho, hñu, n'a, kütá, r'ato}
f. alfabeto-náhuatl <-{nähui, ëyi, cë, mäcuïlli, chicuacë}
g. selecciona dialecto
h. cadenafinal <-reemplaza.cadena2(alfabeto seleccionado)

6. N <- N -1
7. Fin.

A continuación, en la Figura 1, se ilustra un ejemplo con un texto plano con la palabra "rolando" en la aplicación del algoritmo utilizando el dialecto otomí, quedando como resultado "ryoncelnahuindyonce", donde se puede observar que la longitud de la contraseña se ha incrementado de 7 a 19 caracteres, quedando de longitud aceptable para la mayoría de las aplicaciones que necesitan autenticación.

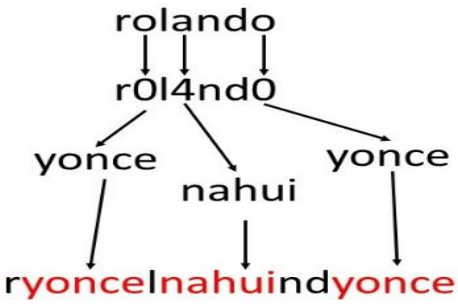

Figura 1. Ejemplo del algoritmo usando dialecto otomí

Fuente: Elaboración propia.

Se ha seleccionado el lenguaje de marcación de hipertexto, así como las hojas en cascada, el lenguaje javascript y el framework json para el desarrollo de una aplicación que se implementará como una extensión del navegador Google Chrome®; esto debido a que se tiene la idea que se use para la autenticación de los portales y aplicaciones web que son de uso más común en la actualidad.

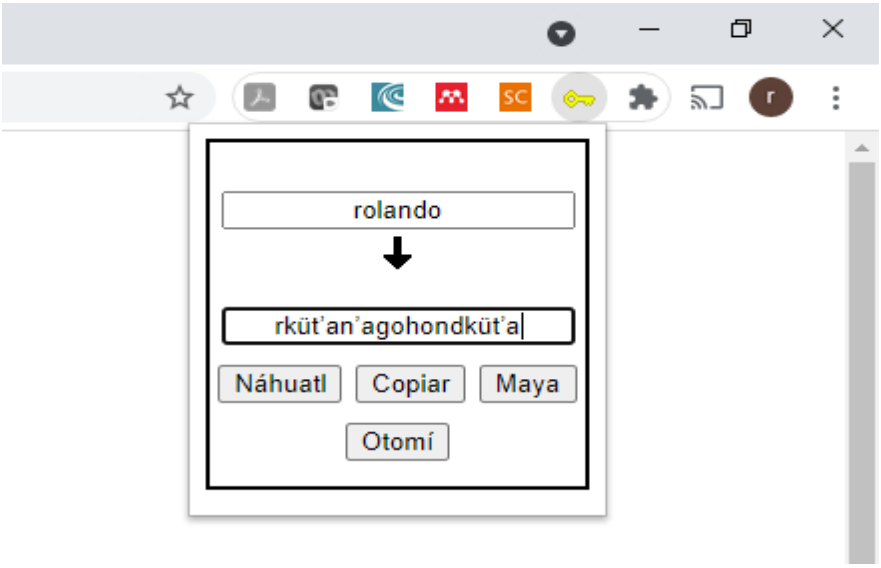

Figura 2 Aplicación desarrollada como extensión de Google Chrome.

Fuente: Elaboración propia.

La aplicación de extensión de Google Chrome® se puede observar en la Figura 2, donde en un cuadro de texto se introduce la palabra que puede ser alfanumérica que incluya minúsculas, mayúsculas y caracteres especiales. Esa palabra puede ser común y fácil de memorizar para el usuario. Se selecciona el botón con el dialecto a convertir, y en el siguiente cuadro de texto se obtendrá la contraseña, se le ha colocado un botón de copiar que permitirá tener la contraseña en una memoria temporal para que el usuario pueda disponer de ella en la aplicación que le solicite la contraseña.

Resultados.

A manera de ejemplo, se han generado tres contraseñas a partir de nombres de personas, utilizando la técnica propuesta para los tres dialectos y los resultados se pueden observar, donde se ha incrementado considerablemente su longitud e inclusive incluye caracteres especiales en algunos casos.

Tabla 1. Palabra y sus equivalencias en dialectos después de aplicar el algoritmo.

palabra	Otomí	Maya	Náhuatl
rolando	rküt'an'agohondküt'a	rjo'ojunkanndjo'o	rmäcuïllicënähuindmäcuïlli
clarisa	clgohorn'asgoho	clkanrjunskan	Clnähuircësnähui
rodrigo	rküt'adrn'agküt'a	rjo'odrjungjo'o	Rmäcuïllidrcëgmäcuïlli

Fuente: Elaboración propia.

Figura 3. Resultado de evaluación en passwordmeter de una contraseña usando la técnica. Fuente: Elaboración propia.

Continuando con la experimentación con pruebas de laboratorio, se han utilizado portales web que verifican la seguridad de contraseñas, midiendo entre otros parámetros la robustez y la capacidad de craqueo (craking del idioma inglés).

Los verificadores de contraseñas utilizados fueron The Password Meter, Kapersky Lab., Password Checker Online y Strength Test. Cada uno de ellos tienen diferentes salidas de resultados, pero en todos ellos se ha demostrado que las contraseñas utilizando la técnica propuesta han superado las pruebas de fortaleza y de resistencia al pirateo. En la Figura 3 se muestra el resultado de la evaluación usando el portal The Password Meter, en donde los indicadores marcan 4 valores excepcionales, 9 suficientes, 2 precauciones y 1 error.

CONCLUSIONES.

En el presente trabajo existen dos aportes importantes: primero, se mejora el fortalecimiento de las contraseñas usadas como medio de autenticación en los sistemas de computadora con el uso de la técnica antes descrita. Segundo, se desarrolla una extensión de Google Chrome para instalar en las computadoras de la institución educativa y que permita el uso de ella a los estudiantes, docentes y personal administrativo.

Con el uso de la aplicación de la técnica propuesta, la convertirá en una contraseña robusta; actualmente no contamos con resultados de la aplicación de la técnica en institución educativa a nivel superior. Para futuros trabajos se realizará el análisis cuantitativo del uso de la técnica y de la aplicación extensión de Google Chrome, donde se pueda medir el uso de la herramienta y la efectividad.

REFERENCIAS BIBLIOGRÁFICAS.

1. Alodhyani, F., Theodorakopoulos, G., & Reinecke, P. (2020). Password managers—it’s all about trust and transparency. *Future Internet*, *12*(11), 1–50. https://doi.org/10.3390/fi12110189

2. Blonder, G. E. (1996). Graphical Password. United States of America.
3. Chakrabarti, S., Landon, G. V., & Singhal, M. (2007). Graphical passwords: Drawing a secret with rotation as a new degree of freedom. *Proceedings of the 4th IASTED Asian Conference on Communication Systems and Networks, AsiaCSN 2007*, 114–120.
4. Cherdmuangpak, N., Anusas-Amonkul, T., & Limthanmaphon, B. (2017). Two factor image-based password authentication for junior high school students. *Proceedings of the 2017 14th International Joint Conference on Computer Science and Software Engineering, JCSSE 2017*, 12–17. https://doi.org/10.1109/JCSSE.2017.8025913
5. Glory, F. Z., Ul Aftab, A., Tremblay-Savard, O., & Mohammed, N. (2019). Strong Password Generation Based on User Inputs. *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2019*, 416–423. https://doi.org/10.1109/IEMCON.2019.8936178
6. Gurav, S. M., Gawade, L. S., Rane, P. K., & Khochare, N. R. (2014). Graphical password authentication: Cloud securing scheme. *Proceedings - International Conference on Electronic Systems, Signal Processing, and Computing Technologies, ICESC 2014*, 479–483. https://doi.org/10.1109/ICESC.2014.90
7. Jablon, D. P. (1996). Strong Password-Only Authenticated Key Exchange, 5–26.
8. Khanaa, V., Thooyamani, K. P., & Udayakumar, R. (2014). Two factor authentication using mobile phones. *World Applied Sciences Journal*, *29*(14), 208–213. https://doi.org/10.5829/idosi.wasj.2014.29.csea.2268
9. Maqbali, F. Al, & Mitchell, C. J. (2017). AutoPass: An automatic password generator. *Proceedings - International Carnahan Conference on Security Technology*, *2017-Octob*, 1–6. https://doi.org/10.1109/CCST.2017.8167791

10. Morris, R., & Thompson, K. (1979). Password Security: A Case History. *Communications of the ACM*, *22*(11), 594–597. https://doi.org/10.1145/359168.359172
11. Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., … Cranor, L. F. (2010). Encountering stronger password requirements: User attitudes and behaviors. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/1837110.1837113
12. Weir, M., Aggarwal, S., Collins, M., & Stern, H. (2010). Testing metrics for password creation policies by attacking large sets of revealed passwords. *Proceedings of the ACM Conference on Computer and Communications Security*, 162–175. https://doi.org/10.1145/1866307.1866327
13. Yan, J., Alan, B., Anderson, R., & Grant, A. (2004). Password memorability and security: Empirical results. *IEEE Security and Privacy*, *2*(5), 25–31. https://doi.org/10.1109/MSP.2004.81

DATOS DE LOS AUTORES.

1. **Rolando Salazar Hernández**. Doctor en Informática, Profesor de la Facultad de Comercio, Administración y Ciencias Sociales de la Universidad Autónoma de Tamaulipas. Nuevo Laredo, Tamaulipas, México. ORCID.ORG/0000-0001-5879-4083 Email: rsalazar@docentes.uat.edu.mx
2. **Adán López Mendoza**. Doctor en Educación Internacional, Profesor de la Facultad de Comercio, Administración y Ciencias Sociales de la Universidad Autónoma de Tamaulipas. Nuevo Laredo, Tamaulipas, México. ORCID.ORG/0000-0003-4801-640X Email: alopez@uat.edu.mx

RECIBIDO: 3 de junio del 2021. **APROBADO:** 21 de junio del 2021.