Evaluación de la Seguridad Digital de los estudiantes de la UTP sede de Veraguas, análisis del uso de autenticación multifactor y verificación de vulneraciones en correos electrónicos

Evaluation of the Digital Security of the students of the UTP Veraguas branch, analysis of the use of multifactor authentication and verification of email vulnerabilities.

Prof. Horacio Sandoval,
[1]Licenciatura en Ciberseguridad,
[2]Facultad de Ingeniería en Sistemas Computacionales, Centro Regional de Veraguas, Universidad Tecnológica de Panamá

Resumen Este estudio evalúa la seguridad digital de los estudiantes de la UTP, campus Veraguas, analizando el uso de autenticación multifactor (MFA) y la exposición a brechas de seguridad en correos electrónicos. Los resultados muestran una falta de concienciación y prácticas seguras, aumentando el riesgo de ataques como phishing y robo de credenciales.
Se identificó que el desconocimiento es el principal obstáculo para adoptar MFA, junto con el uso frecuente de contraseñas débiles y reutilizadas. Se recomienda fortalecer la educación en ciberseguridad mediante capacitaciones, verificación de credenciales y gestores de contraseñas para mejorar la protección digital en la comunidad estudiantil.

Palabras clave Autenticación Multifactor (MFA), Ciberseguridad, Concienciación, Verificación, ISO/IEC 27001.

Abstract This study assesses the digital security of UTP students, Veraguas campus, focusing on multi-factor authentication (MFA) usage and email security breaches. Findings reveal a lack of awareness and safe practices, increasing risks of phishing and credential theft.
The main barrier to MFA adoption is lack of knowledge, along with frequent use of weak and reused passwords. Strengthening cybersecurity education through training, credential verification, and password managers is recommended to enhance digital protection among students.

Keywords Multifactor Authentication (MFA), Cybersecurity, Awareness, Verification, ISO/IEC 27001.

I. Introducción

En un mundo cada vez más digitalizado, la seguridad de la información se ha convertido en un pilar fundamental para garantizar la integridad y privacidad de los datos personales y académicos. Las instituciones educativas, al ser custodias de grandes volúmenes de información sensible, enfrentan desafíos significativos en la protección de sus sistemas y usuarios. En este contexto, la autenticación multifactor (MFA) y la verificación de vulneraciones en correos electrónicos han surgido como herramientas esenciales para mitigar riesgos cibernéticos. Sin embargo, la adopción de estas medidas por parte de los estudiantes universitarios sigue siendo un tema poco explorado, especialmente en entornos académicos específicos como la Universidad Tecnológica de Panamá (UTP), sede de Veraguas. Este estudio se enfoca en analizar el nivel de seguridad digital de los estudiantes de la UTP sede de Veraguas, con un énfasis particular en el uso de autenticación multifactor y la verificación de vulneraciones en correos electrónicos. La investigación busca responder preguntas clave, como: ¿Qué porcentaje de estudiantes utiliza MFA? ¿Con qué frecuencia verifican si sus correos han sido comprometidos en filtraciones de datos? ¿Cuáles son las principales barreras que impiden la adopción de estas medidas de seguridad? Estas preguntas son relevantes no solo para comprender el comportamiento de los estudiantes frente a las amenazas cibernéticas, sino también para proponer estrategias que fortalezcan la cultura de ciberseguridad en el entorno universitario. El trabajo se desarrollará en la Facultad de Ingeniería en Sistemas Computacionales (FISC) de la UTP sede de Veraguas, un escenario ideal debido a la alta

interacción de sus estudiantes con tecnologías digitales y herramientas de seguridad informática. Mediante un enfoque metodológico que combina encuestas y entrevistas, se buscará obtener datos cuantitativos y cualitativos que permitan una comprensión integral del problema. Los resultados de esta investigación no solo contribuirán a identificar brechas en las prácticas de seguridad digital de los estudiantes, sino que también servirán como Página 8 de 49 base para el diseño de programas de capacitación y políticas institucionales que promuevan una mayor concienciación en ciberseguridad. En un futuro donde las amenazas cibernéticas seguirán evolucionando, es imperativo que las instituciones educativas y sus comunidades adopten medidas proactivas para proteger la información. Este estudio representa un paso importante en esa dirección, al proporcionar insights valiosos sobre el comportamiento de los estudiantes frente a las herramientas de seguridad digital y al proponer soluciones concretas para reducir su exposición a riesgos cibernéticos.

II. Antecedentes

El sector educativo es uno de los más afectados por ataques de ransomware y phishing, según **Cybersecurity Ventures (2024)**, debido a la falta de conciencia sobre seguridad y la interconexión de sistemas. La **autenticación multifactor (MFA)** se ha demostrado eficaz en la prevención de accesos indebidos, reduciendo en un **99%** la probabilidad de comprometer cuentas, según el **Microsoft Security Report (2023)**. Sin embargo, muchos estudiantes no la utilizan en sus cuentas académicas y personales.

Asimismo, la **verificación de vulneraciones en correos electrónicos** es crucial para detectar filtraciones de datos. Herramientas como **Have I Been Pwned** han mostrado que millones de correos académicos han sido expuestos, poniendo en riesgo información sensible. A pesar de ello, un estudio de **Educause (2023)** indica que solo el **45%** de los estudiantes en universidades tecnológicas usa MFA y menos del **30%** verifica si su correo ha sido comprometido.

Este estudio busca evaluar la seguridad digital de los estudiantes de la UTP, analizando el uso de MFA y la exposición a vulneraciones en correos electrónicos. Los resultados permitirán identificar brechas de seguridad y proponer estrategias para mejorar la protección de datos en el ámbito académico.

II. Identificación del Problema

La seguridad digital de los estudiantes de la UTP sede Veraguas enfrenta riesgos debido a la baja adopción de medidas como la **autenticación multifactor (MFA)** y la falta de monitoreo de credenciales expuestas en filtraciones de datos. Muchos estudiantes utilizan **contraseñas débiles o reutilizadas**, lo que los hace vulnerables a ataques como **phishing** y **credential stuffing**.

A pesar de que el uso de MFA reduce significativamente el riesgo de acceso no autorizado, se desconoce su nivel de adopción entre los estudiantes. Además, la exposición de correos en filtraciones masivas aumenta la posibilidad de ataques dirigidos si no se toman medidas correctivas.

Esta investigación busca evaluar la seguridad digital en la comunidad estudiantil, analizando la implementación de MFA y la exposición a brechas de datos. Con los hallazgos, se podrán proponer estrategias para fortalecer la protección de la información personal y académica. Ante la evolución de las amenazas cibernéticas y el uso de inteligencia artificial en ataques, es crucial fomentar la concienciación y formación en ciberseguridad para mitigar riesgos futuros.

III. Delimitaciones

Este estudio se llevará a cabo en la **Universidad Tecnológica de Panamá (UTP), sede Veraguas**, abarcando a estudiantes de **todas las facultades** con el objetivo de evaluar el nivel de seguridad digital en una muestra más amplia de la comunidad universitaria.

La investigación analizará las prácticas de seguridad digital en distintos grupos académicos, sin limitarse únicamente a la **Facultad de Ingeniería en Sistemas Computacionales (FISC)**. No se evaluará la infraestructura de seguridad informática de la universidad ni sus sistemas administrativos o de red.

El estudio se desarrollará durante el **año 2025**, cubriendo un ciclo académico completo. Se empleará un **enfoque mixto (cuantitativo y cualitativo)**, basado en **encuestas dirigidas a estudiantes de diferentes facultades**, **entrevistas con profesores y expertos en ciberseguridad**, y **análisis de datos sobre la adopción de medidas de protección digital**. No se realizarán pruebas técnicas, ya que el objetivo principal es medir la **conciencia y el uso de estrategias de seguridad digital** entre los estudiantes de la UTP.

IV. Diseño del proyecto

a) Herramientas y tecnologías que utilizar:

Have I Been Pwned (HIBP) es una herramienta en línea gratuita desarrollada por Troy Hunt que permite a los usuarios verificar si sus credenciales han sido comprometidas en filtraciones de datos. La plataforma recopila información de bases de datos expuestas en brechas de seguridad y permite a los usuarios ingresar su correo electrónico o número de teléfono para comprobar si han sido afectados.

Además, HIBP ofrece un servicio de notificación que alerta a los usuarios cuando sus credenciales aparecen en nuevas filtraciones, ayudando a mejorar la seguridad digital al fomentar el uso de contraseñas seguras y la autenticación multifactor. También proporciona una API que permite a empresas y desarrolladores integrar la funcionalidad en sus propios sistemas para proteger mejor sus cuentas y credenciales.

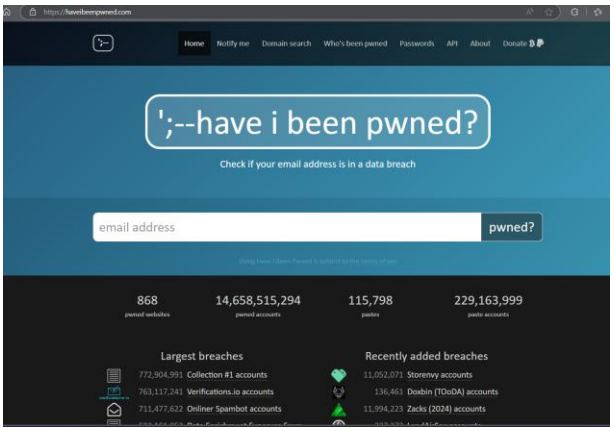

Figura 1 Página web de HIBP

Holehe es una herramienta de OSINT (Open Source Intelligence) que permite verificar en qué plataformas en línea está registrado un correo electrónico. Su principal utilidad radica en la ciberseguridad y la investigación digital, ya que ayuda a los analistas a determinar si una dirección de correo electrónico ha sido utilizada para crear cuentas en diversos servicios, como redes sociales, foros o plataformas de comercio electrónico.

Holehe funciona enviando solicitudes a diferentes sitios web y analizando las respuestas para identificar si el correo electrónico está asociado a una cuenta existente. Esta herramienta es especialmente útil en auditorías de seguridad, investigaciones forenses digitales y pruebas de penetración, ya que puede proporcionar información valiosa sobre la presencia de un usuario en distintos servicios en línea.

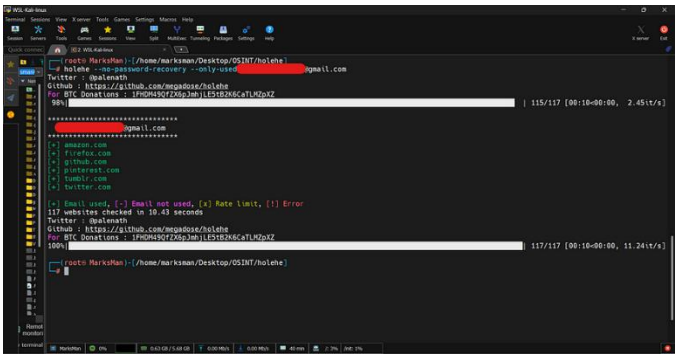

Figura 2 Ejecución de Holehe en Kali

Microsoft Authenticator es una aplicación de autenticación multifactor (MFA) desarrollada por Microsoft que permite a los usuarios aumentar la seguridad de sus cuentas mediante verificaciones adicionales más allá de la contraseña. La aplicación es compatible con cuentas de Microsoft y otros servicios en línea que admitan MFA, proporcionando métodos de autenticación como códigos temporales (TOTP), notificaciones push y verificación biométrica.

Esta herramienta es ampliamente utilizada en entornos empresariales y personales para proteger cuentas contra accesos no autorizados. Permite iniciar sesión sin necesidad de una contraseña mediante la autenticación sin contraseña (passwordless), donde el usuario aprueba el acceso desde su dispositivo móvil. Microsoft Authenticator está disponible para dispositivos iOS y Android, facilitando la autenticación segura en aplicaciones y servicios en la nube.

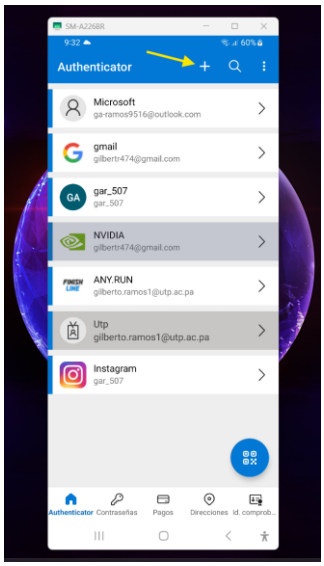

Figura 3 Uso del Authenticator

b) Encuesta sobre seguridad digital en la UTP sede de Veraguas

Evaluar el nivel de conciencia y adopción de medidas de seguridad digital entre los estudiantes de la UTP sede de Veraguas, con énfasis en el uso de autenticación multifactor (MFA) y la verificación de vulneraciones en correos electrónicos, para identificar brechas en su protección digital y proponer estrategias de mejora.

3. **¿Con qué frecuencia utiliza plataformas digitales para actividades académicas?**
   - ( ) Todos los días
   - ( ) Varias veces a la semana
   - ( ) Casi nunca
   - ( ) Nunca

Sección 1: Autenticación Multifactor (MFA)

4. **¿Sabes qué es la autenticación multifactor (MFA)?**
   - ( ) Sí, y la utilizo en mis cuentas
   - ( ) Sí, pero no la utilizo
   - ( ) No estoy seguro(a)
   - ( ) No, nunca, no sé qué es (Si selecciono esta respuesta pasa a sección 2)

5. **¿Tiene actividad la autenticación multifactor en tu correo institucional o cuentas académicas?**
   - ( ) Sí, en todas mis cuentas
   - ( ) No, no sé dónde se hace
   - ( ) No, pero me gustaría activarla
   - ( ) Nunca

Figura 4 Algunas preguntas de la encuesta

c) Resultados de la Instrumentación

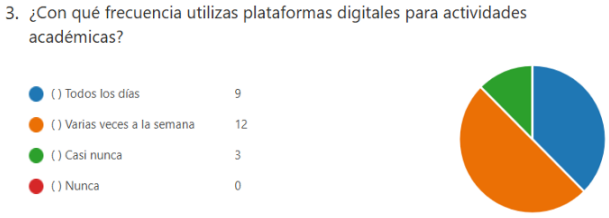

Figura 5 Resultado de la 3 pregunta

Análisis: La mayoría de los encuestados (9 personas) usa plataformas digitales para actividades académicas todos los días, mientras que 12 lo hacen varias veces a la semana, lo que indica una alta dependencia de herramientas digitales en el entorno educativo. Solo 3 personas reportan usarlas casi nunca, y nadie afirmó no usarlas. Esto sugiere que la digitalización es clave en la educación, con la mayoría de los estudiantes utilizando frecuentemente estas plataformas para su aprendizaje.

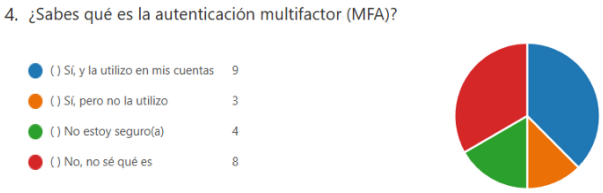

Figura 6 Resultado de la 4 pregunta

Análisis: La gráfica muestra que 9 encuestados conocen y utilizan la autenticación multifactor (MFA), mientras que 3 la conocen, pero no la usan. Sin embargo, un número significativo de participantes (8 personas) no sabe qué es MFA, y 4 no están seguros. Esto indica una brecha en la concienciación sobre seguridad digital, ya que casi la mitad de los encuestados (12 personas) no la usa o no la conoce. Se recomienda reforzar la educación sobre MFA para aumentar su adopción y mejorar la seguridad en las cuentas digitales.

Figura 7 Resultado de la 5 pregunta

Análisis: La mayoría de los encuestados (13 personas) no tienen activada la autenticación multifactor (MFA) en sus cuentas académicas, pero están interesados en activarla. Solo 9 personas la han implementado, mientras que 2 nunca la han activado ni muestran interés en hacerlo. Este resultado indica una oportunidad para promover la adopción de MFA mediante campañas de concienciación y capacitación, ya que un alto porcentaje de los encuestados está dispuesto a mejorar la seguridad de sus cuentas.

V. Resultado general de las gráficas

Los resultados muestran fallas en el conocimiento y aplicación de medidas de seguridad digital. La UTP tiene la oportunidad de fortalecer la ciberseguridad entre sus estudiantes mediante capacitaciones, promoviendo MFA, buenas prácticas en

contraseñas y gestión de filtraciones de datos. A continuación, realizo un resumen conciso de los resultados.

• **Uso de plataformas digitales:** La mayoría utiliza herramientas digitales para actividades académicas, lo que resalta la importancia de su seguridad.

• **Conocimiento sobre MFA:** Aunque algunos estudiantes conocen la autenticación multifactor, muchos no saben activarla o desconocen su utilidad, lo que limita su adopción.

• **Activación de MFA:** A pesar de que algunos la usan, una gran cantidad de encuestados aún no la activa, a pesar de su interés en hacerlo.

• **Razones para no usar MFA:** La falta de conocimiento es el principal obstáculo para su implementación.

• **Reacción ante una filtración de datos:** La mayoría cambiaría su contraseña, pero pocos activarían MFA, lo que indica desconocimiento sobre de seguridad más robustas.

• **Reutilización de contraseñas:** Un número considerable de encuestados reutiliza sus contraseñas, lo que representa un riesgo significativo de seguridad.

• **Frecuencia de cambio de contraseñas:** La mayoría solo cambia sus credenciales si sospecha un compromiso, mientras que otros nunca lo hacen.

• **Almacenamiento de contraseñas:** Aunque varios usan gestores de contraseñas, una parte aún opta por escribirlas en papel, lo que representa un riesgo.

• **Interés en capacitación**: La gran mayoría está interesada en recibir formación en seguridad digital, lo que indica una oportunidad clave para la UTP en mejorar la concienciación y prácticas seguras.

VI. Conclusiones

El estudio sobre la seguridad digital de los estudiantes de la UTP sede de Veraguas ha evidenciado brechas significativas en la adopción de medidas de protección, especiales una gran parte de los estudiantes aún no implementa estrategias de seguridad adecuadas, lo que los deja vulnerables ante ataques como phishing y robo de credenciales.

Los resultados obtenidos muestran que la principal barrera para la adopción de MFA es el desconocimiento sobre su importancia y configuración, mientras que la falta de hábito preventivo en el cambio de contraseñas y la reutilización de credenciales aumentan las probabilidades de compromisos de seguridad. Además, aunque existe un alto interés en recibir capacitación en ciberseguridad, aún hay una baja aplicación de herramientas como Have I Been Pwned para la verificación de filtraciones.

Este análisis resalta la necesidad de implementar programas de concienciación en seguridad digital dentro del entorno universitario. Se recomienda a la UTP fortalecer su infraestructura educativa con talleres prácticos, material informativo y el fomento del uso de MFA como una medida esencial de protección. Asimismo, la integración de herramientas de verificación de credenciales y el uso de gestores de contraseñas ayudarían a reducir las vulnerabilidades existentes.

Dado el contexto de transformación digital en la educación, es fundamental que los estudiantes adopten una cultura de autoprotección digital. El éxito de estas estrategias dependerá del compromiso institucional y de la responsabilidad individual de los estudiantes para aplicar buenas prácticas de seguridad informática

REFERENCIAS

[1] Cybersecurity Ventures, “Informe sobre delitos cibernéticos: el impacto de las amenazas cibernéticas en el sector educativo,” 2024. [En línea]. Disponible https://cybersecurityventures.com. [Accedido: 20-feb-2025].

[2] Educause, “Concientización y mejores prácticas en materia de ciberseguridad en la educación superior,” 2023. [En línea]. Disponible en: https://www.educause.edu. [Accedido: 20-feb 2025].

[3] Instituto Nacional de Estándares y Tecnología (NIST), “Framework para la mejora de la ciberseguridad de infraestructuras críticas,” 2023. [En línea]. Disponible en: https://www.nist.gov. [Accedido: 20-feb-2025].

[4] Organización Internacional de Normalización (ISO), ISO/IEC 27001:2022 - Sistemas de Gestión de Seguridad de la Información, 2022. [En línea]. https://www.iso.org. [Accedido: 20-feb-2025].

[5] Microsoft, “Informe de seguridad de Microsoft: mejora de la seguridad mediante la autenticación multifactor (MFA),” 2023. [En línea]. Disponible en: https://www.microsoft.com. [Accedido: 20-feb-2025].

[6] Have I Been Pwned, “Plataforma de verificación de filtraciones de datos y credenciales comprometidas,” 2025. [En línea]. Disponible en: https://haveibeenpwned.com. [Accedido: 20-feb-2025].

[7] Megadose, “Holehe: Herramienta OSINT para verificar la reutilización de correos electrónicos en distintos servicios,” 2025. [En línea]. Disponible en: https://github.com/megadose/holehe. [Accedido: 20-feb-2025].