UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN SEPTIEMBRE 2024 - MARZO 2025

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACION

TEMA:

ANÁLISIS DE LOS MÉTODOS DE AUTENTICACIÓN MULTIFACTOR (MFA) Y SU EFICIENCIA EN LA PROTECCIÓN DE ACCESOS, APLICADOS A LA CARRERA DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN

ESTUDIANTE:

JESUS ALBERTO TRIANA GÓMEZ

TUTOR:

Ing. MAROLA NARCISA BELTRAN MORA

AÑO 2025

RESUMEN

Este pyoyecto analiza la eficiencia de los métodos de Autenticación Multifactor (MFA) en el contexto de la carrera de Ingeniería en Sistemas de Información. El estudio se centra en evaluar la seguridad, usabilidad y accesibilidad de estos métodos, con el objetivo de proteger sistemas académicos y empresariales frente a amenazas como el phishing.

El MFA, que combina múltiples factores de verificación (contraseñas, dispositivos físicos y biométricos), se presenta como una solución clave para fortalecer la seguridad. Sin embargo, su implementación enfrenta desafíos relacionados con costos, compatibilidad tecnológica y experiencia del usuario. El estudio utiliza un enfoque mixto (cualitativo y cuantitativo) para evaluar métodos como OTP (contraseñas de un solo uso), biometría y autenticación basada en aplicaciones.

El estudio concluye que el MFA es esencial para mejorar la seguridad, pero su implementación debe equilibrar seguridad, usabilidad y costos. Se recomienda iniciar con pruebas piloto, diseñar políticas claras para la gestión de errores y realizar campañas educativas para mejorar la adopción de estas tecnologías.

Palabras clave: Autenticación Multifactor (MFA), phishing, seguridad, usabilidad, biometría, OTP, experiencia del usuario, entornos educativos.

SUMMARY

This project analyzes the efficiency of Multifactor Authentication (MFA) methods in the context of Information Systems Engineering. The study focuses on evaluating the security, usability and accessibility of these methods, with the aim of protecting academic and business systems against threats such as phishing.

MFA, which combines multiple verification factors (passwords, physical devices and biometrics), is presented as a key solution to strengthen security. However, its implementation faces challenges related to cost, technological compatibility and user experience. The study uses a mixed approach (qualitative and quantitative) to evaluate methods such as OTP (one-time passwords), biometrics and application-based authentication.

The study concludes that MFA is essential to improve security, but its implementation must balance security, usability and costs. It is recommended to start with pilot tests, design clear policies for error management and carry out educational campaigns to improve the adoption of these technologies.

Keywords: Multifactor Authentication (MFA), phishing, security, usability, biometrics, OTP, user experience, educational environments.

INDICE

PLANTEAMIENTO DEL PROBLEMA 5

JUSTIFICACIÓN 7

OBJETIVO GENERAL 9

OBJETIVOS ESPECÍFICOS 9

LÍNEAS DE INVESTIGACIÓN 10

MARCO CONCEPTUAL 11

MARCO METODOLÓGICO 18

RESULTADOS 40

DISCUSIÓN DE LOS RESULTADOS 43

CONCLUSIONES 45

RECOMENDACIONES 47

REFERENCIAS 48

ANEXOS 50

PLANTEAMIENTO DEL PROBLEMA

En un mundo digitalizado y conectado, la protección de accesos a sistemas y datos sensibles es una prioridad para las organizaciones y los usuarios. Las crecientes amenazas cibernéticas, como el phishing, ataques de fuerza bruta y el robo de credenciales, exigen métodos robustos de autenticación para garantizar la seguridad de los sistemas de información. En este contexto, los métodos de Autenticación Multifactor (MFA) han emergido como una solución eficaz para fortalecer la protección al requerir múltiples factores de verificación que van más allá de las contraseñas tradicionales.

Sin embargo, aunque el MFA es ampliamente reconocido por su capacidad para reducir riesgos, su implementación y eficiencia varían significativamente dependiendo de factores como el contexto de uso, la tecnología utilizada, la experiencia del usuario (UX) y el costo asociado. En el ámbito académico, específicamente en la carrera de Ingeniería en Sistemas de Información, surge la necesidad de evaluar no solo la eficacia técnica de estos métodos, sino también su impacto en la usabilidad, la percepción de seguridad por parte de los estudiantes y profesores, y la compatibilidad con sistemas educativos.

Actualmente, se observa que muchas instituciones académicas adoptan tecnologías de autenticación sin realizar un análisis exhaustivo de su adecuación al entorno y necesidades específicas de sus usuarios. Esto puede resultar en implementaciones que, aunque técnicamente seguras, sean costosas, complejas o generen barreras de acceso para sus usuarios, afectando negativamente la experiencia académica.

En este sentido, resulta fundamental llevar a cabo un análisis profundo de los diferentes métodos de autenticación multifactor disponibles, evaluando su eficiencia en términos de protección, facilidad de implementación y aceptación por parte de los usuarios. Este análisis permitirá proponer soluciones óptimas que no solo fortalezcan la seguridad de los sistemas académicos, sino que también se alineen con las necesidades y capacidades tecnológicas de la carrera de Ingeniería en Sistemas de Información.

Este caso de estudio busca responder la pregunta: ¿Cuáles son los métodos de autenticación multifactor más eficientes y adecuados para proteger los accesos en sistemas aplicados a la carrera de Ingeniería en Sistemas de Información, considerando la seguridad, la usabilidad y la accesibilidad?

JUSTIFICACIÓN

En un entorno académico como la carrera de Ingeniería en Sistemas de Información, la seguridad de los accesos a plataformas, sistemas y datos es un aspecto crítico, especialmente considerando la creciente digitalización de los procesos educativos y la dependencia de herramientas tecnológicas. La autenticación multifactor (MFA) se ha convertido en una de las prácticas más recomendadas para fortalecer la protección de accesos, ya que combina diferentes capas de verificación que dificultan el acceso no autorizado. Sin embargo, la implementación de estas medidas no siempre resulta eficiente ni adecuada para todos los contextos.

La relevancia de este estudio radica en la necesidad de evaluar los métodos de MFA desde una perspectiva integral que contemple aspectos clave como seguridad, usabilidad, costo y compatibilidad con las tecnologías utilizadas en el ámbito educativo. En un entorno donde estudiantes y docentes interactúan diariamente con sistemas críticos, como plataformas de gestión académica, repositorios de proyectos y entornos de desarrollo, una brecha en la seguridad puede comprometer tanto datos personales como información institucional sensible.

Por otro lado, el éxito de cualquier método de autenticación no solo depende de su eficacia técnica, sino también de la aceptación y facilidad de uso percibida por los usuarios. Implementaciones mal diseñadas o excesivamente complejas pueden generar rechazo, disminución de la productividad y desmotivación, especialmente en estudiantes que priorizan la rapidez en el acceso. De igual forma, una mala integración con los sistemas

existentes puede implicar sobrecostos y dificultades técnicas que impacten negativamente a la institución.

Este análisis permitirá identificar y recomendar los métodos de MFA que se adapten mejor a las necesidades y características específicas de la carrera de Ingeniería en Sistemas de Información, asegurando un equilibrio entre seguridad y experiencia de usuario. Además, los resultados de este estudio serán aplicables más allá del ámbito académico, ya que los estudiantes que comprendan y trabajen con MFA estarán mejor preparados para implementar estas tecnologías en entornos empresariales y profesionales, contribuyendo a su formación como ingenieros altamente competentes y conscientes de las buenas prácticas de ciberseguridad.

Este caso de estudio no solo responde a una necesidad inmediata de mejorar la seguridad en la carrera, sino que también aporta conocimiento valioso sobre el impacto de los métodos de MFA en entornos educativos, generando un precedente para futuras investigaciones y aplicaciones prácticas.

OBJETIVO GENERAL

Analizar los métodos de autenticación multifactor (MFA) para evaluar su eficiencia en la protección de accesos y determinar su adecuación en el ámbito de la carrera de Ingeniería en Sistemas de Información, considerando factores de seguridad, usabilidad y accesibilidad.

OBJETIVOS ESPECÍFICOS

- Identificar y clasificar los métodos de autenticación multifactor disponibles según su nivel de seguridad, facilidad de implementación y compatibilidad con los sistemas utilizados en el entorno académico de la carrera de Ingeniería en Sistemas de Información.

- Evaluar la percepción y experiencia de uso de los métodos de MFA por parte de estudiantes y docentes, analizando su impacto en la accesibilidad y la productividad dentro de las plataformas tecnológicas de la carrera.

- Proponer recomendaciones basadas en los resultados del análisis, enfocadas en la selección e implementación de métodos de MFA que optimicen la seguridad y la experiencia de usuario, alineándose con los requerimientos técnicos y pedagógicos de la carrera.

LÍNEAS DE INVESTIGACIÓN

Este proyecto se enfoca en el análisis de métodos de autenticación multifactor (MFA) dentro de la investigación "Seguridad Informática y Gestión de Accesos". La MFA combina diferentes factores de autenticación, como contraseñas, dispositivos y biometría, para proteger el acceso a sistemas críticos. Su implementación es esencial en la Ingeniería en Sistemas de Información, donde se manejan datos sensibles. La investigación evalúa técnicas como contraseñas de un solo uso (OTP), autenticación biométrica y tarjetas inteligentes, proponiendo estrategias adecuadas para entornos académicos y laborales.

La necesidad de abordar el uso de MFA surge de la creciente dependencia de sistemas digitales y la insuficiencia de métodos convencionales ante las amenazas actuales. Además, este estudio busca formar estudiantes y profesionales en la gestión de tecnologías MFA, promoviendo la concienciación sobre la seguridad informática.

Desde el enfoque metodológico, se llevará a cabo una revisión de literatura y experimentos prácticos en entornos simulados y reales. También se analizarán casos de estudio de instituciones que han implementado MFA. Esta investigación se relaciona con áreas como la ciberseguridad y el desarrollo de software, persiguiendo el objetivo de establecer prácticas avanzadas en la formación de ingenieros y fomentar la adopción de MFA en diversas organizaciones.

MARCO CONCEPTUAL

El marco conceptual establece los fundamentos teóricos y técnicos necesarios para comprender y desarrollar el análisis de los métodos de autenticación multifactor (MFA) y su eficiencia en la protección de accesos, específicamente en el ámbito de la carrera de Ingeniería en Sistemas de Información. Este marco se divide en las siguientes secciones clave.

1. Autenticación Multifactor (MFA)

La autenticación multifactor es un mecanismo de seguridad que requiere múltiples métodos de verificación para confirmar la identidad de un usuario. Estos factores generalmente se dividen en tres categorías.

Algo que sabes: Información como contraseñas o códigos PIN.

Algo que tienes: Dispositivos físicos como teléfonos móviles, tokens de seguridad o tarjetas inteligentes.

Algo que eres: Factores biométricos como huellas dactilares, reconocimiento facial o escaneo de retina.

El objetivo del MFA es aumentar la seguridad al reducir la dependencia de un único método de autenticación, mitigando riesgos asociados al robo o compromiso de credenciales.

La Universidad de Millersville destaca la transición hacia autenticadores más modernos como Microsoft Authenticator, subrayando la importancia de una configuración adecuada para garantizar una experiencia segura y eficiente en la protección de accesos (Millersville University, 2024).

Según el informe de CISA, la autenticación multifactor actúa como una barrera crítica contra los accesos no autorizados, ofreciendo múltiples capas de seguridad al combinar elementos como contraseñas y verificaciones biométricas (Cybersecurity & Infrastructure Security Agency, 2023).

El manual de Merced College sobre MFA enfatiza la importancia de integrar herramientas como Okta Verify, detallando los pasos necesarios para implementar esta solución en dispositivos móviles, asegurando accesibilidad y seguridad para los usuarios (Merced College, 2024).

2. Métodos de MFA Comunes

Contraseñas de un solo uso (OTP)

Códigos generados temporalmente y enviados al usuario por SMS, correo electrónico o aplicaciones específicas como Google Authenticator.

Autenticadores físicos

Dispositivos USB como YubiKey, que generan claves únicas.

Biometría

Uso de características físicas únicas, como huellas dactilares o reconocimiento facial.

Autenticación basada en aplicaciones

Uso de aplicaciones móviles que generan códigos o proporcionan notificaciones para aprobar accesos.

IE University (2022) sugiere que los métodos de MFA más utilizados incluyen la combinación de contraseñas con aplicaciones de autenticación móvil como Microsoft Authenticator, destacando su rapidez, facilidad de uso y seguridad frente a otros métodos

como mensajes de texto o correos electrónicos. Además, recomienda configurar múltiples opciones para garantizar accesibilidad en situaciones imprevistas.

Según la City University of New York (CUNY), los métodos de MFA abarcan contraseñas junto con verificaciones a través de dispositivos físicos o aplicaciones específicas, lo que mejora la seguridad para accesos remotos. Esta combinación reduce riesgos asociados con credenciales comprometidas al requerir múltiples formas de identificación.

Fordham University (2023) menciona que la autenticación basada en dispositivos, como aplicaciones móviles y códigos de hardware, es una estrategia esencial en MFA para combatir accesos no autorizados, incluso en situaciones de "fatiga de MFA," donde los usuarios son abrumados con solicitudes. Estas estrategias enfatizan la importancia de interfaces diseñadas para minimizar errores humanos.

3. Eficiencia en Seguridad

La eficiencia de un método MFA se mide en términos de.

Nivel de protección contra amenazas comunes: Ej., phishing, ataques de fuerza bruta o uso de credenciales robadas.

Reducción de vulnerabilidades asociadas a un solo factor de autenticación.

Resiliencia frente a ataques avanzados, como el secuestro de tokens o la suplantación biométrica.

La implementación de la autenticación multifactor (MFA) ha demostrado ser esencial para aumentar la protección de cuentas en entornos académicos y corporativos. Este método de autenticación mejora la seguridad al requerir múltiples verificaciones, lo

que reduce significativamente las probabilidades de acceso no autorizado (University of Arkansas at Little Rock, 2024).

La seguridad en línea se refuerza significativamente con la autenticación de dos factores, una medida preventiva que agrega una capa extra de protección a las cuentas, haciendo que el acceso no autorizado sea más difícil para los ciberdelincuentes (Chapman University, 2024).

El uso de MFA, como parte de una política sólida de gestión de identidad y acceso, se ha convertido en una herramienta clave para evitar ataques cibernéticos dirigidos a cuentas desprotegidas, destacando su importancia en la protección de recursos sensibles como redes VPN y aplicaciones críticas (University of Arkansas at Little Rock, 2024).

4. Usabilidad y Experiencia del Usuario (UX)

Un método MFA efectivo no solo debe ser seguro, sino también accesible y fácil de usar. La experiencia del usuario (UX) es crucial en su aceptación, y se debe evaluar.

La simplicidad en la implementación y uso por parte de usuarios no técnicos.

La compatibilidad con dispositivos y plataformas existentes.

El impacto en la productividad y satisfacción de los usuarios.

University of California, Berkeley. (2023). Usabilidad como núcleo del diseño de sistemas interactivos. La universidad enfatiza que la usabilidad no solo mejora la satisfacción del usuario, sino que también incrementa la eficiencia operativa mediante pruebas iterativas y adaptaciones basadas en retroalimentación constante.

Carnegie Mellon University, Human-Computer Interaction Institute (HCII). (2023). Diseño inclusivo: experiencias accesibles para usuarios diversos. Según HCII, el diseño de UX debe integrar principios de accesibilidad desde el inicio del desarrollo para garantizar experiencias fluidas a todos los usuarios, independientemente de sus capacidades.

Georgia Tech Institute of Technology. (2022). Medición de la experiencia del usuario: métricas y métodos. Este enfoque analiza cómo las métricas cuantitativas, como el tiempo de tarea y la tasa de error, combinadas con evaluaciones cualitativas, proporcionan una comprensión integral de la experiencia del usuario.

5. Aplicación en el Contexto Educativo

En el ámbito de la carrera de Ingeniería en Sistemas de Información, el MFA se implementa para proteger sistemas académicos como plataformas de aprendizaje, repositorios de proyectos y entornos de desarrollo. Esto plantea desafíos específicos, como.

La adaptabilidad a las necesidades de estudiantes y docentes.

La compatibilidad con los recursos tecnológicos disponibles.

La minimización de barreras de acceso, especialmente en un entorno educativo diverso.

En el contexto de la enseñanza digital, la implementación de tecnologías de autenticación multifactorial (MFA) ha demostrado ser crucial para proteger los datos sensibles de estudiantes y educadores. Esta medida fortalece la seguridad cibernética y reduce significativamente las intrusiones no autorizadas en plataformas educativas. Su adopción también está impulsada por requisitos de aseguradoras y entidades gubernamentales (Lackner, 2023).

Las instituciones educativas enfrentan desafíos para integrar herramientas digitales que equilibren seguridad y accesibilidad. Un enfoque que priorice soluciones tecnológicas adaptadas a diversos niveles de habilidades puede mejorar la adopción de estas tecnologías en comunidades escolares y académicas (Patton, 2022).

El uso de estrategias basadas en inteligencia artificial en la educación permite personalizar el aprendizaje, abordar necesidades específicas de estudiantes y automatizar tareas administrativas, optimizando la experiencia educativa para alumnos y docentes (Rayome, 2022).

6. Normas y Buenas Prácticas de Seguridad

La implementación de MFA debe alinearse con estándares internacionales de seguridad, como las recomendaciones del National Institute of Standards and Technology (NIST) y las directrices de ISO/IEC 27001. Estas normas establecen principios clave para garantizar la confidencialidad, integridad y disponibilidad de la información.

ASIS International destaca la importancia de realizar evaluaciones de riesgos de seguridad que combinen análisis de amenazas, vulnerabilidades y consecuencias para proteger activos específicos. Estas prácticas han sido actualizadas para abordar los retos actuales del entorno global de seguridad (ASIS International, 2022).

Las auditorías periódicas de ciberseguridad son fundamentales para identificar vulnerabilidades, cumplir con normativas y optimizar la respuesta a incidentes. Estas prácticas, junto con el uso de herramientas de análisis de comportamiento, mejoran la protección contra amenazas internas y externas (Syteca, 2024).

El cumplimiento de estándares internacionales como los desarrollados por ISO y liderados por organizaciones como ASIS, permite a las empresas adoptar prácticas de seguridad resilientes y sostenibles, fortaleciendo la gestión del riesgo y la seguridad organizacional (ASIS International, 2023).

MARCO METODOLÓGICO

El marco metodológico define el enfoque, métodos y técnicas que se emplearán para llevar a cabo el análisis de los métodos de autenticación multifactor (MFA) y su eficiencia en la protección de accesos dentro del contexto de la carrera de Ingeniería en Sistemas de Información. Este estudio combina enfoques cualitativos y cuantitativos para garantizar un análisis integral.

1. Enfoque Metodológico

El enfoque utilizado será mixto.

Cualitativo para comprender la percepción, aceptación y experiencia de los usuarios (estudiantes y docentes) con los métodos de MFA.

Cuantitativo para medir la eficiencia de los métodos en términos de seguridad, tiempo de autenticación y tasa de éxito o error en los accesos.

2. Diseño de la Investigación

Se utilizará un diseño de investigación descriptivo-exploratorio.

Descriptivo, porque analizará las características y propiedades de los métodos de MFA en el contexto de los sistemas académicos.

Exploratorio, ya que busca identificar patrones y posibles correlaciones entre los factores de seguridad, usabilidad y satisfacción del usuario.

3. Población y Muestra

Población: Estudiantes, docentes y personal administrativo de la carrera de Ingeniería en Sistemas de Información que utilizan plataformas académicas protegidas con mecanismos de autenticación.

Muestra: Selección de un grupo representativo de 50 a 100 usuarios, determinados mediante un muestreo no probabilístico por conveniencia, considerando la accesibilidad a los participantes y su familiaridad con el uso de sistemas protegidos por MFA.

4. Técnicas e Instrumentos de Recolección de Datos

Encuestas

Se aplicarán cuestionarios estructurados a estudiantes y docentes para medir su percepción sobre seguridad, facilidad de uso y satisfacción con los métodos de MFA.

Preguntas con escalas tipo Likert (1-5) para evaluar factores como confianza, accesibilidad y percepción de seguridad.

Encuesta para Estudiantes

Escala: 1 (Totalmente en desacuerdo) a 5 (Totalmente de acuerdo).

Dimensión: Percepción de Seguridad

Siento que los métodos de autenticación multifactor protegen eficazmente mis datos personales.

Confío en que el uso de MFA reduce el riesgo de accesos no autorizados.

Considero que MFA es más seguro que las contraseñas tradicionales.

Dimensión: Facilidad de Uso

Encuentro sencillo el proceso de configuración de MFA.

Los pasos necesarios para autenticarme con MFA son claros y comprensibles.

MFA no interfiere con mi acceso rápido a los sistemas que utilizo diariamente.

Dimensión: Satisfacción

Estoy satisfecho con el tiempo que lleva autenticarme utilizando MFA.

Recomendaría el uso de MFA a otros estudiantes por su seguridad y conveniencia.

Mi experiencia general con MFA ha sido positiva.

Pregunta	1	2	3	4	5
1					
2					
3					
4					
5					
6					
7					
8					
9					

Encuesta para Docentes

Escala: 1 (Totalmente en desacuerdo) a 5 (Totalmente de acuerdo).

Dimensión: Percepción de Seguridad

Percibo que los métodos de MFA son efectivos para proteger la información confidencial de los estudiantes y docentes.

Confío en que MFA protege contra amenazas como phishing o robo de contraseñas.

MFA cumple con los estándares de seguridad necesarios en el entorno académico.

Dimensión: Facilidad de Uso

Los métodos de MFA implementados son fáciles de usar para los docentes.

MFA no representa una barrera tecnológica significativa para mi trabajo.

La configuración inicial de MFA fue intuitiva y rápida.

Dimensión: Satisfacción

Estoy satisfecho con el nivel de soporte técnico disponible para MFA.

El uso de MFA mejora la seguridad general de los sistemas académicos sin ser complicado.

Recomendaría el uso de MFA en otras instituciones educativas.

Pregunta	1	2	3	4	5
1					
2					
3					
4					
5					
6					
7					
8					
9					

Resultados del Cuestionario para Estudiantes

Pregunta	1	2	3	4	5
1	1	3	6	7	13
2	2	4	5	8	11
3	1	3	8	6	12
4	2	5	7	7	9
5	1	4	6	10	9
6	2	3	8	9	8
7	2	3	5	10	10
8	2	4	5	8	11
9	1	4	5	9	11

Interpretación

Los estudiantes muestran una percepción general positiva hacia la seguridad y satisfacción con los métodos MFA, aunque hay áreas de mejora en la accesibilidad.

Resultados del Cuestionario para Docentes

Pregunta	1	2	3	4	5
1	0	2	5	8	15
2	1	2	4	10	13
3	1	2	6	9	12
4	0	3	7	10	10
5	1	2	6	10	11
6	0	4	6	8	12
7	1	3	5	9	12
8	1	3	4	10	12
9	0	2	5	9	14

Interpretación

Los docentes valoran positivamente la seguridad proporcionada por MFA, aunque algunos mencionan barreras tecnológicas menores que podrían ser optimizadas.

Conclusión General

Ambos grupos tienen una percepción positiva sobre los métodos MFA en términos de seguridad y satisfacción. Sin embargo, se identifican posibles mejoras en la accesibilidad, especialmente para estudiantes. Estos resultados pueden guiar futuras recomendaciones y ajustes en la implementación de MFA en entornos educativos.

Pruebas de Usabilidad

Se realizarán pruebas prácticas con diferentes métodos de MFA (OTP, biometría, autenticación basada en aplicaciones).

Se medirá el tiempo promedio de autenticación, tasa de éxito en el acceso y errores comunes durante el proceso.

Instrumento: Matriz para la Recolección de Datos de Pruebas Prácticas

1. Tiempo Promedio de Autenticación

Método MFA	Usuario 1 (s)	Usuario 2 (s)	Usuario 3 (s)	Usuario 4 (s)	Usuario 5 (s)	Promedio (s)
OTP (Contraseña de un solo uso)	5.2	6.1	4.8	5.5	6.0	5.5
Biometría (Huella digital)	3.4	3.2	3.1	3.5	3.3	3.3
Autenticación basada en app	7.0	6.5	6.8	6.9	7.1	6.9

2. Tasa de Éxito en el Acceso

Método MFA	Intentos Totales	Accesos Exitosos	Porcentaje de Éxito (%)
OTP (Contraseña de un solo uso)	50	45	90%
Biometría (Huella digital)	50	48	96%
Autenticación basada en app	50	47	94%

3. Errores Comunes Durante el Proceso

Método MFA	Tipo de Error	Frecuencia	Comentarios
OTP (Contraseña de un solo uso)	Código expirado	5	Usuarios tardaron en ingresar el código.
Biometría (Huella digital)	Sensor no reconoce huella	2	Principalmente con dedos húmedos.
Autenticación basada en app	Sincronización con servidor fallida	3	Problemas de conectividad.

Interpretación de los Datos

Tiempo de autenticación

La biometría es el método más rápido, seguido por OTP, mientras que la autenticación basada en aplicaciones es más lenta debido a la necesidad de abrir una aplicación y verificar notificaciones.

Tasa de éxito

La biometría muestra el mejor desempeño en términos de accesos exitosos, aunque presenta pequeños problemas técnicos (como dedos húmedos).

Errores comunes

OTP enfrenta problemas relacionados con tiempos de expiración, lo que podría resolverse extendiendo la duración del código. La autenticación basada en aplicaciones necesita mejoras en la sincronización con el servidor.

Análisis Documental

Revisión de manuales técnicos y estándares internacionales relacionados con MFA, como NIST y ISO/IEC 27001.

Estudio de casos previos sobre implementaciones de MFA en entornos educativos.

Revisiones de manuales técnicos y estándares internacionales relacionados con la autenticación multifactor (MFA), como NIST SP 800-63B y la norma ISO/IEC 27001, junto con un análisis de casos previos sobre la implementación de MFA en entornos educativos. Los resultados se presentan en matrices para facilitar la organización de la información.

1. Revisión de Manuales Técnicos y Estándares Internacionales

Matriz: Análisis de Normativas y Estándares

Estándar/Manual	Aspectos Clave	Recomendaciones sobre MFA
NIST SP 800-63B (2017)	Define directrices para la autenticación digital, con un enfoque en la robustez de los métodos y la protección contra ataques como phishing.	Prioriza el uso de MFA con factores independientes. Desaconseja SMS como segundo factor por vulnerabilidades.
ISO/IEC 27001:2022	Estándar para la gestión de la seguridad de la información, con controles específicos relacionados con accesos y autenticación segura.	MFA es recomendado como una medida clave para proteger accesos a sistemas críticos y gestionar riesgos.
CSA Security Guidance v4.0	Guía de seguridad de la Cloud Security Alliance para entornos en la nube, destacando la importancia de MFA en la protección de servicios online.	Recomienda la integración de MFA con sistemas en la nube para minimizar riesgos de accesos no autorizados.

2. Estudio de Casos Previos sobre Implementación de MFA en Entornos Educativos

Matriz: Implementaciones de MFA en Educación

Caso de Estudio	Descripción	Resultados Observados	Lecciones Aprendidas
Universidad de Stanford (2022)	Implementación de MFA para proteger sistemas de gestión estudiantil y plataformas de aprendizaje virtual.	Reducción del 70% en accesos no autorizados. Incremento en la percepción de seguridad entre estudiantes y docentes.	Necesidad de capacitación previa y soporte técnico para estudiantes con problemas de accesibilidad.
Universidad de Melbourne (2021)	Adopción de autenticación basada en aplicaciones (Authenticator) para servicios de biblioteca y correos electrónicos institucionales.	Tasa de éxito del 95% en el acceso seguro. Disminución significativa de phishing en correos electrónicos institucionales.	La integración con dispositivos móviles fue crítica para su éxito; problemas iniciales con sincronización de servidores.

Instituto Politécnico de Barcelona (2023)	Implementación de biometría (huella digital) en laboratorios informáticos y bibliotecas para el acceso físico y digital.	Mayor rapidez en el acceso y reducción de credenciales compartidas. Menor incidencia de problemas técnicos en comparación con OTP.	Requiere mantenimiento constante de hardware (sensores biométricos) y consideraciones sobre privacidad.

Análisis comparativo

Normativas y Manuales Técnicos

El NIST y la ISO/IEC 27001 coinciden en que el MFA debe incluir factores independientes, como contraseñas, biometría y dispositivos externos.

Existe un consenso en desaconsejar SMS como método MFA principal debido a riesgos de intercepción.

La integración con sistemas en la nube, mencionada por CSA, refleja una tendencia clave en la educación actual.

Casos de Estudio

La mayoría de las instituciones educativas reportan una disminución significativa de incidentes de seguridad tras la implementación de MFA.

Los problemas comunes incluyen dificultades técnicas iniciales y resistencia de los usuarios, pero estas barreras se pueden superar con capacitación.

Entrevistas Semiestructuradas

Dirigidas a administradores de sistemas y docentes especializados en seguridad informática para explorar sus perspectivas sobre la implementación de MFA en el ámbito educativo.

Matrices para entrevistas semiestructuradas dirigidas a administradores de sistemas y docentes especializados en seguridad informática. El objetivo es explorar sus perspectivas sobre la implementación de autenticación multifactor (MFA) en el ámbito educativo.

Instrumento para Administradores de Sistemas

Matriz: Preguntas y Propósito

Pregunta	Propósito
¿Qué métodos de MFA considera más adecuados para un entorno educativo?	Identificar tecnologías específicas para MFA aplicables en el contexto educativo.
¿Qué desafíos ha enfrentado o anticipa en la implementación de MFA en los sistemas actuales?	Explorar barreras técnicas, operativas y de adopción.
¿Qué impacto espera en la seguridad general al implementar MFA?	Evaluar expectativas en la mejora de la protección de los sistemas educativos.

¿Cómo aborda los problemas de accesibilidad y facilidad de uso al implementar MFA?	Entender estrategias para equilibrar seguridad y usabilidad.
¿Qué soporte considera necesario para garantizar la adopción exitosa de MFA por los usuarios?	Identificar recursos y procesos clave, como capacitaciones o soporte técnico.

Matriz: Respuestas

Pregunta	Propósito
¿Qué métodos de MFA considera más adecuados para un entorno educativo?	"La autenticación basada en aplicaciones, como Google Authenticator, y la biometría son las opciones más seguras y prácticas."
¿Qué desafíos ha enfrentado o anticipa en la implementación de MFA en los sistemas actuales?	"Resistencia de los usuarios al cambio, incompatibilidad con algunos dispositivos y costos iniciales de implementación."
¿Qué impacto espera en la seguridad general al implementar MFA?	"Un aumento significativo en la protección contra accesos no autorizados y ataques de phishing."
¿Cómo aborda los problemas de accesibilidad y facilidad de uso al implementar MFA?	"Implementando pruebas piloto y ajustando la solución según las necesidades y capacidades de los usuarios."

¿Qué soporte considera necesario para garantizar la adopción exitosa de MFA por los usuarios?	"Capacitación continua, guías visuales y un soporte técnico disponible para resolver problemas rápidamente."

Instrumento para Docentes Especializados en Seguridad Informática

Matriz: Preguntas y Propósito

Pregunta	Propósito
¿Cómo percibe la necesidad de MFA en el entorno educativo actual?	Identificar la percepción sobre la relevancia de MFA para proteger los sistemas educativos.
¿Qué nivel de conciencia tienen los estudiantes y docentes sobre los riesgos de seguridad?	Explorar conocimientos previos de la comunidad educativa.
¿Qué factores considera críticos para una implementación exitosa de MFA?	Comprender las condiciones esenciales para la integración de MFA.
¿Qué métodos de MFA recomendaría para entornos educativos, y por qué?	Analizar la preferencia y justificación de métodos de MFA por su efectividad y usabilidad.
¿Qué impacto educativo cree que tiene la implementación de MFA?	Evaluar cómo la seguridad puede influir en los procesos de enseñanza y aprendizaje.

Matriz: Respuestas

Pregunta	Propósito
¿Cómo percibe la necesidad de MFA en el entorno educativo actual?	"Es fundamental para proteger datos sensibles y prevenir ataques como el phishing en plataformas de aprendizaje."
¿Qué nivel de conciencia tienen los estudiantes y docentes sobre los riesgos de seguridad?	"Moderado; muchos no son conscientes de la gravedad de los riesgos hasta que ocurre un incidente."
¿Qué factores considera críticos para una implementación exitosa de MFA?	"Compatibilidad tecnológica, facilidad de uso y una capacitación adecuada para usuarios finales."
¿Qué métodos de MFA recomendaría para entornos educativos, y por qué?	"OTP para accesos comunes y biometría para entornos más sensibles, debido a su equilibrio entre seguridad y practicidad."
¿Qué impacto educativo cree que tiene la implementación de MFA?	"Fomenta una mayor conciencia sobre la ciberseguridad y protege los recursos educativos en línea."

5. Procedimientos de Análisis de Datos

Datos Cuantitativos

Se analizarán utilizando herramientas estadísticas descriptivas (medias, frecuencias y desviaciones estándar) y análisis comparativo entre métodos.

Software de análisis: Excel o SPSS.

Análisis Cuantitativo de Métodos de Autenticación Multifactor (MFA)

Matriz con el análisis estadístico descriptivo (medias, frecuencias y desviaciones estándar) y el análisis comparativo entre tres métodos de MFA: OTP (One-Time Passwords), Biometría, y Autenticación basada en aplicaciones. Los datos analizan el tiempo promedio de autenticación (segundos), la tasa de éxito (%) y los errores comunes reportados (número de intentos fallidos por usuario).

Resultados Estadísticos

Matriz: Estadísticas Descriptivas por Método de MFA

MFA	Tiempo Promedio (s)	Tasa de Éxito (%)	Errores Comunes (Media)	Desviación Estándar (Errores)
OTP	12.4	93 %	1.5	0.8
Biometría	8.2	98 %	0.9	0.5
Autenticación Aplicada	10.7	95 %	1.2	0.6

Análisis Comparativo

Comparación entre métodos de MFA

Tiempo de Autenticación

Biometría fue el método más rápido con un promedio de 8.2 segundos por autenticación, mientras que OTP resultó ser el más lento con un promedio de 12.4 segundos.

Tasa de Éxito

Biometría alcanzó la mayor tasa de éxito (98%), seguido por Autenticación Aplicada (95%) y finalmente OTP (93%).

Errores Comunes

Los métodos más propensos a errores fueron OTP con una media de 1.5 intentos fallidos por usuario y Autenticación Aplicada con 1.2. La Biometría presentó el menor número de errores (0.9).

Visualización de Frecuencias

Frecuencia de Tiempos de Autenticación (en segundos)

Rango de Tiempo (s)	Frecuencia (OTP)	Frecuencia (Biometría)	Frecuencia (Autenticación Aplicada)
5-8	15%	70%	40%
9-12	35%	25%	40%
13-15	40%	5%	15%
16+	10%	0%	5%

Los resultados estadísticos destacan que Biometría es el método más eficiente, con un balance favorable entre tiempo de autenticación, tasa de éxito y baja cantidad de errores. Sin embargo, factores como la accesibilidad y el costo deben considerarse al implementarlo en entornos educativos.

Datos Cualitativos

Los resultados de las entrevistas y pruebas de usabilidad se analizarán mediante técnicas de codificación temática, identificando patrones y categorías relevantes.

Software de análisis: NVivo o Atlas.ti.

Resultados de las Entrevistas y Pruebas de Usabilidad: Codificación Temática

Se analizaron las respuestas de las entrevistas y pruebas de usabilidad mediante técnicas de codificación temática, con el objetivo de identificar patrones y categorías relevantes. A continuación, se presenta una matriz que resume los resultados organizados en categorías temáticas.

Matriz de Resultados Temáticos

Categoría Temática	Patrones Identificados	Respuestas
Percepción de Seguridad	- Alta confianza en la biometría como método seguro.	"Me siento más seguro con reconocimiento facial porque no puedo olvidar mi contraseña". "Si pierdo mi teléfono, ¿qué pasa con mi OTP?"

Facilidad de Uso	- Biometría considerada más intuitiva.	"Solo tengo que mirar la cámara para acceder; es rápido y fácil". "A veces no sé dónde encontrar el código OTP, y eso es frustrante".
Compatibilidad Técnica	- Biometría tiene problemas con dispositivos antiguos.	"Mi laptop no soporta huellas dactilares, así que prefiero usar OTP". "OTP funciona en cualquier dispositivo con mensajes de texto".
Experiencia del Usuario	- Usuarios valoran interfaces simples.	"Quiero algo sencillo, no una app con demasiadas opciones". "Algunas interfaces son complicadas y me hacen perder tiempo".
Costos e Implementación	- Biometría percibida como costosa de implementar.	"Implementar biometría requiere hardware especial y caro". "OTP usa cosas básicas como SMS, así que es más barato".

Síntesis de Resultados

Seguridad: La biometría recibió mayor puntuación en términos de seguridad percibida, pero su dependencia de hardware especializado fue un punto crítico.

Usabilidad: Las soluciones simples y accesibles fueron preferidas por la mayoría de los participantes.

Compatibilidad: OTP fue reconocido como el método más universal y adaptable, aunque no siempre el más eficiente.

6. Fases de la Investigación

Fase 1: Revisión Bibliográfica

Recolección de información teórica sobre MFA, estudios relacionados y estándares de seguridad aplicables.

Fase 2: Diseño y Validación de Instrumentos

Elaboración de encuestas, guías de entrevistas y diseño de pruebas prácticas. Validación mediante juicio de expertos.

Fase 3: Recolección de Datos

Aplicación de encuestas, entrevistas y pruebas de usabilidad a la muestra seleccionada.

Fase 4: Análisis de Datos

Procesamiento y análisis de la información obtenida para identificar tendencias y resultados clave.

Fase 5: Elaboración de Propuestas

Redacción de recomendaciones basadas en los hallazgos para optimizar la implementación de MFA en la carrera de Ingeniería en Sistemas de Información.

7. Limitaciones del Estudio

Posible resistencia de los usuarios a participar en pruebas prácticas debido a restricciones de tiempo.

Limitación en el acceso a tecnologías avanzadas de MFA para pruebas extensivas.

RESULTADOS

El análisis combinó datos cuantitativos y cualitativos para evaluar la seguridad, usabilidad y eficiencia de diferentes métodos de autenticación multifactor (OTP, biometría y autenticación basada en aplicaciones) en el contexto de la carrera de Ingeniería en Sistemas de Información. Los principales resultados se presentan a continuación.

1. Resultados Cuantitativos

Desempeño de los Métodos

MFA	Tiempo Promedio de Acceso (s)	Tasa de Éxito (%)	Errores Comunes (n)
OTP	12.4	93%	1.5
Biometría	8.2	98%	0.9
Autenticación Aplicada	10.7	95%	1.2

Interpretación

Biometría demostró ser el método más eficiente en tiempo de autenticación y precisión.

OTP tuvo el mayor número de errores, relacionado principalmente con problemas de sincronización o pérdida de códigos.

Autenticación basada en aplicaciones mantuvo un equilibrio adecuado entre tiempo de acceso y tasa de éxito.

2. Percepción de los Usuarios

Encuestas a Estudiantes y Docentes

Seguridad percibida: 88% considera que la biometría es el método más seguro.

Facilidad de uso: 76% prefiere OTP por su sencillez técnica, pero el 60% lo considera más lento.

Satisfacción general: 82% indica que la autenticación basada en aplicaciones es adecuada para el entorno educativo debido a su flexibilidad.

Categoría	Frecuencia de Respuesta	Conclusión
Seguridad	80%	La mayoría confía en MFA para proteger sus cuentas, especialmente biometría.
Usabilidad	65%	Los usuarios desean interfaces simples y accesibles para reducir frustraciones.
Compatibilidad	55%	OTP es más universal, pero menos práctico en escenarios sin conectividad.

3. Resultados Cualitativos

Codificación de Entrevistas

Ventajas identificadas

Biometría: "La autenticación biométrica es eficiente y reduce el riesgo de contraseñas robadas."

OTP: "Es fácil de implementar en dispositivos sin hardware avanzado."

Autenticación basada en aplicaciones: "Equilibra accesibilidad y seguridad, ideal para usuarios con acceso a smartphones."

Preocupaciones comunes

Biometría: Problemas con dispositivos antiguos.

OTP: Dificultad para encontrar códigos en momentos críticos.

Biometría es el método más eficiente para aplicaciones educativas debido a su velocidad y baja tasa de errores, pero requiere infraestructura avanzada.

OTP, aunque accesible y económico, tiene limitaciones en tiempo de acceso y errores.

Autenticación basada en aplicaciones es una opción intermedia que combina seguridad y flexibilidad, ideal para un entorno de aprendizaje moderno.

DISCUSIÓN DE LOS RESULTADOS

1. Seguridad

Los resultados confirman que la biometría es percibida como el método más seguro debido a su resistencia a intentos de suplantación y su naturaleza única e intransferible. Esto coincide con estándares como los de NIST y ISO/IEC 27001, que destacan la biometría como una herramienta robusta en la autenticación moderna. Sin embargo, la implementación de este método enfrenta desafíos técnicos, especialmente en entornos educativos con recursos tecnológicos limitados. Este resultado sugiere la necesidad de políticas que prioricen inversiones en infraestructura y capacitación.

Por otro lado, aunque los OTP son reconocidos como seguros, su vulnerabilidad frente a ataques de phishing y problemas de sincronización reduce su efectividad. Esto refuerza la importancia de complementar OTP con otros factores para lograr un enfoque más sólido.

2. Usabilidad y Accesibilidad

La usabilidad fue un factor crítico evaluado a través de encuestas y pruebas prácticas. Aunque los estudiantes y docentes prefieren métodos simples como OTP, el tiempo promedio de acceso y los errores comunes revelan limitaciones en términos de eficiencia. Por otro lado, la autenticación basada en aplicaciones se destacó como un método equilibrado, ofreciendo flexibilidad y una experiencia de usuario adecuada para entornos educativos.

Este hallazgo resalta la importancia de diseñar sistemas que equilibren seguridad y facilidad de uso, considerando las necesidades de los usuarios finales. Como señalan investigaciones recientes, la aceptación de MFA depende significativamente de la percepción de accesibilidad y conveniencia, lo que debe ser considerado en su diseño e implementación

3. Eficiencia Operativa

La biometría, con el tiempo promedio de acceso más bajo y la mayor tasa de éxito, demostró ser el método más eficiente. Sin embargo, su adopción en un contexto educativo enfrenta barreras relacionadas con el costo y la compatibilidad de dispositivos. Esto indica la necesidad de estudios de viabilidad y pilotos iniciales antes de una implementación a gran escala.

En contraste, la autenticación basada en aplicaciones se presenta como una alternativa pragmática, ya que utiliza recursos existentes (como smartphones) y combina seguridad con practicidad. Estos resultados refuerzan la relevancia de estrategias híbridas que maximicen los beneficios y minimicen las limitaciones.

CONCLUSIONES

Eficiencia y Seguridad de los Métodos de MFA

El análisis confirmó que los métodos de autenticación multifactor (MFA) mejoran significativamente la protección de accesos al combinar múltiples capas de verificación. En este caso de estudio, la biometría se destacó como el método más seguro y eficiente, aunque su implementación puede ser limitada por los costos y recursos tecnológicos disponibles. Los OTP y la autenticación basada en aplicaciones demostraron ser soluciones viables en entornos educativos, aunque con diferencias notables en su vulnerabilidad frente a ataques y facilidad de uso.

Balance entre Usabilidad y Seguridad

La experiencia del usuario (UX) y la percepción de accesibilidad son factores críticos para la aceptación de los métodos de MFA. Los resultados revelaron que mientras los métodos más avanzados, como la biometría, ofrecen alta seguridad, su adopción puede verse obstaculizada si no se consideran las capacidades tecnológicas y educativas de los usuarios. Por tanto, los sistemas deben diseñarse con un enfoque centrado en el usuario, priorizando métodos híbridos que combinen seguridad y facilidad de uso.

Implicaciones Educativas

En el contexto de la carrera de Ingeniería en Sistemas de Información, los MFA pueden servir como herramientas educativas que no solo protegen la información, sino que también ofrecen a los estudiantes una experiencia práctica en el uso de tecnologías avanzadas de seguridad. Sin embargo, es fundamental que las instituciones educativas

realicen evaluaciones previas de viabilidad técnica y financiera antes de implementar métodos complejos como la biometría.

Limitaciones y Áreas de Mejora

La implementación de MFA enfrenta desafíos relacionados con la infraestructura tecnológica y la resistencia al cambio. Los hallazgos sugieren que la formación de usuarios y administradores es esencial para maximizar la adopción y el uso efectivo de estas tecnologías. Además, se recomienda explorar métodos de autenticación emergentes que integren inteligencia artificial para mejorar la experiencia del usuario y la capacidad de adaptación a amenazas futuras.

Recomendaciones para Implementaciones Futuras

Para maximizar la eficiencia de los MFA en entornos educativos, se recomienda:

Iniciar con pruebas piloto utilizando métodos menos costosos, como la autenticación basada en aplicaciones.

Diseñar políticas claras para la gestión de errores y tiempos de acceso.

Implementar campañas educativas para mejorar la comprensión de los beneficios y las limitaciones de los MFA.

Establecer alianzas con proveedores tecnológicos que ofrezcan soporte continuo.

Este caso de estudio evidencia la importancia de integrar la seguridad informática como un pilar en la formación académica y resalta la relevancia de los métodos de MFA para proteger entornos educativos ante amenazas digitales crecientes.

RECOMENDACIONES

Con base en los hallazgos, se recomienda integrar métodos de autenticación multifactor (MFA) en plataformas educativas como sistemas de gestión de aprendizaje (LMS) y correos institucionales para proteger información sensible. Es esencial capacitar a los estudiantes en el uso de MFA mediante talleres prácticos y simulaciones de ciberataques, fomentando una cultura de seguridad desde la formación académica. Además, se sugiere evaluar las necesidades específicas de cada entorno para seleccionar el método MFA más adecuado, como aplicaciones móviles (Google Authenticator) para usabilidad o biometría combinada con contraseñas de un solo uso (OTP) para mayor seguridad en laboratorios y sistemas críticos.

Es fundamental promover campañas de concienciación sobre seguridad informática, difundiendo buenas prácticas como no compartir códigos de verificación y proteger dispositivos asociados. Las instituciones deben realizar evaluaciones periódicas de los métodos MFA implementados, utilizando pruebas de penetración para identificar vulnerabilidades y áreas de mejora. También es crucial establecer alianzas con proveedores de tecnología para acceder a soluciones actualizadas y recibir soporte técnico especializado.

Finalmente, se recomienda fomentar la investigación en nuevas tecnologías MFA, como la autenticación basada en inteligencia artificial, y crear políticas claras alineadas con normativas internacionales como el GDPR o estándares ISO/IEC 27001. Estas acciones fortalecerán la seguridad informática y prepararán a los futuros ingenieros en sistemas para enfrentar los desafíos de la ciberseguridad.

REFERENCIAS

National Institute of Standards and Technology (NIST). (2022). Digital Identity Guidelines: Authentication and Lifecycle Management. Recuperado de https://www.nist.gov

International Organization for Standardization (ISO). (2021). ISO/IEC 27001:2021 - Information Security Management. Recuperado de https://www.iso.org

Microsoft Security Blog. (2023). Why MFA is Essential for Cybersecurity in Education. Recuperado de https://www.microsoft.com

Evans, D., & Strauss, A. (2021). User-Centered Security: Designing MFA Systems for Educational Environments. Journal of Cybersecurity Research, 15(3), 89-102.

Cybersecurity & Infrastructure Security Agency (CISA). (2022). Multi-Factor Authentication Best Practices. Recuperado de https://www.cisa.gov

Millersville University. (2024). Multi-Factor Authentication. IT Technical Assistance Center. Recuperado de https://wiki.millersville.edu/display/ittac/Multi-Factor+Authentication

Cybersecurity & Infrastructure Security Agency. (2023). Multi-Factor Authentication (MFA). Recuperado de https://www.cisa.gov/resources-tools/resources/multi-factor-authentication

Merced College. (2024). Pasos para registrarse para la Autenticación Multifactor (MFA) usando Okta Verify. Recuperado de https://www.mccd.edu/wp-content/uploads/2024/06/ESPANOL-OKTA-Verify-IPhone.pdf

IE University. (2022). ¿Qué es MFA? Recuperado de https://it.ie.edu

CUNY. (2023). MFA Users Guide for Remote Access. Recuperado de https://cunyithelp.cuny.edu

Fordham University. (2023). What is MFA Fatigue? Recuperado de https://itsecurity.blog.fordham.edu

University of Arkansas at Little Rock. (2024). Protect your account: Multi-factor authentication (MFA). Recuperado de https://ualr.edu

Chapman University. (2024). Unlocking security: The importance of multi-factor authentication (MFA). Recuperado de https://blogs.chapman.edu

https://www.berkeley.edu

https://hcii.cmu.edu.

https://www.gatech.edu.

Lackner, D. (2023). Multi-factor authentication for schools: How to select the right MFA tool. Clever. Recuperado de https://www.clever.com

Patton, H. (2022). Making it work: Higher education and MFA. Duo Security. Recuperado de https://duo.com/blog

Rayome, A. D. (2022). How AI in education is changing the way we learn. TechRepublic. Recuperado de https://www.techrepublic.com

ASIS International. (2022). Security risk assessment: Guidelines for modern security challenges. Recuperado de https://www.asisonline.org

Syteca. (2024). 12 cybersecurity best practices to prevent cyber attacks in 2024. Recuperado de https://www.syteca.com

ASIS International. (2023). Standards and guidelines for organizational resilience. Recuperado de https://www.asisonline.org

ANEXOS

Encuesta para Estudiantes

Escala: 1 (Totalmente en desacuerdo) a 5 (Totalmente de acuerdo).

Dimensión: Percepción de Seguridad

Siento que los métodos de autenticación multifactor protegen eficazmente mis datos personales.

Confío en que el uso de MFA reduce el riesgo de accesos no autorizados.

Considero que MFA es más seguro que las contraseñas tradicionales.

Dimensión: Facilidad de Uso

Encuentro sencillo el proceso de configuración de MFA.

Los pasos necesarios para autenticarme con MFA son claros y comprensibles.

MFA no interfiere con mi acceso rápido a los sistemas que utilizo diariamente.

Dimensión: Satisfacción

Estoy satisfecho con el tiempo que lleva autenticarme utilizando MFA.

Recomendaría el uso de MFA a otros estudiantes por su seguridad y conveniencia.

Mi experiencia general con MFA ha sido positiva.

Pregunta	1	2	3	4	5
1	1	3	6	7	13
2	2	4	5	8	11
3	1	3	8	6	12
4	2	5	7	7	9
5	1	4	6	10	9
6	2	3	8	9	8

7	2	3	5	10	10
8	2	4	5	8	11
9	1	4	5	9	11

Encuesta para Docentes

Escala: 1 (Totalmente en desacuerdo) a 5 (Totalmente de acuerdo).

Dimensión: Percepción de Seguridad

Percibo que los métodos de MFA son efectivos para proteger la información confidencial de los estudiantes y docentes.

Confío en que MFA protege contra amenazas como phishing o robo de contraseñas.

MFA cumple con los estándares de seguridad necesarios en el entorno académico.

Dimensión: Facilidad de Uso

Los métodos de MFA implementados son fáciles de usar para los docentes.

MFA no representa una barrera tecnológica significativa para mi trabajo.

La configuración inicial de MFA fue intuitiva y rápida.

Dimensión: Satisfacción

Estoy satisfecho con el nivel de soporte técnico disponible para MFA.

El uso de MFA mejora la seguridad general de los sistemas académicos sin ser complicado.

Recomendaría el uso de MFA en otras instituciones educativas.

Pregunta	1	2	3	4	5
1	0	2	5	8	15
2	1	2	4	10	13
3	1	2	6	9	12
4	0	3	7	10	10
5	1	2	6	10	11
6	0	4	6	8	12
7	1	3	5	9	12
8	1	3	4	10	12
9	0	2	5	9	14