UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

MAYO 2023 – SEPTIEMBRE 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCION DEL TITULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS COMPARATIVO ENTRE LOS MÉTODOS DE AUTENTICACIÓN UNIFACTORIAL Y MULTIFACTORIAL.

ESTUDIANTE:

JONATHAN DAVID VALVERDE CASTRO

TUTOR:

ING. ENRIQUE DELGADO CUADRO

AÑO 2023

ÍNDICE

PLANTEAMIENTO DEL PROBLEMA

En la era digital actual, la seguridad de la información es de suma importancia. La autenticación es un componente fundamental para garantizar que solo los usuarios autorizados puedan acceder a sistemas, aplicaciones y datos confidenciales. En este contexto, los métodos de autenticación de factor único y multifactor son dos enfoques básicos que buscan equilibrar la seguridad y la facilidad de uso de la autenticación del usuario.

La autenticación de un solo factor se basa en proporcionar una sola prueba para verificar la identidad de un usuario, como una contraseña o una huella digital. La autenticación de múltiples factores, por otro lado, consta de múltiples elementos de prueba, como algo que el usuario sabe (contraseña), algo que el usuario tiene (token de seguridad) y quién es el usuario (huella digital o reconocimiento facial).

Un enfoque de un solo factor se basa en el uso de un solo factor para autenticar a un usuario, mientras que un enfoque de múltiples factores usa múltiples factores para una mayor seguridad. En la industria, manufactura, procesos de atención al cliente, y otras actividades, porque una persona se desarrolla día a día.

La autenticación de un solo factor se basa en un solo elemento para verificar la identidad de un usuario, generalmente una contraseña o PIN. La autenticación multifactor, por otro lado, requiere que los usuarios proporcionen múltiples elementos para verificar su identidad, como una contraseña, tarjeta de acceso, huella digital, token de seguridad o una combinación de autenticación biométrica.

El debate sobre cuál de estos enfoques puede proporcionar mayor seguridad y al mismo tiempo ser más fácil de usar sigue siendo una cuestión central en ciberseguridad.

Para encontrar una posible solución, se debe plantear la siguiente pregunta ¿Cuáles son las principales diferencias entre los métodos de autenticación unifactorial y multifactorial en términos de seguridad, facilidad de uso e implementación y cómo influyen estas diferencias a la toma de decisiones para garantizar la protección de los sistemas de información y comunicación en el contexto de innovación y emprendimiento?

El objetivo de esta investigación es responder a esta pregunta fundamental y proporcionar una base sólida para tomar decisiones informadas al elegir métodos de autenticación, promoviendo así la seguridad, la innovación y el espíritu empresarial en un entorno tecnológico cambiante.

JUSTIFICACIÓN

En los últimos años, ha habido un aumento significativo en los ciberataques y las violaciones de seguridad. Los métodos de autenticación tradicionales, como las contraseñas, han demostrado ser vulnerables a técnicas de hacking y ataques de fuerza bruta. La autenticación multifactorial ofrece una capa adicional de seguridad al requerir múltiples factores para verificar la identidad, lo que dificulta los intentos de suplantación de identidad.

La seguridad en línea se ha convertido en un tema fundamental en la sociedad actual debido a la cantidad cada vez mayor de datos confidenciales y transacciones que tienen lugar en el entorno digital. La autenticación, que verifica la identidad de los usuarios que acceden a un sistema o servicio, desempeña un papel fundamental en la protección de la información confidencial y la prevención del acceso no autorizado. En este contexto, han surgido debates sobre la efectividad y aplicabilidad de los métodos de autenticación de un solo factor y de múltiples factores.

El propósito de este análisis comparativo es explorar y evaluar las ventajas y desventajas de los métodos de autenticación de un solo factor y de múltiples factores en términos de seguridad, facilidad de uso y accesibilidad.

OBJETIVOS

OBJETIVO GENERAL:

- Analizar los métodos de autenticación unifactorial y multifactorial en entornos de acceso a sistemas y protección de datos.

OBJETIVOS ESPECÍFICOS:

- Fundamentar teóricamente el contexto de la autenticación unifactorial y multifactorial.
- Identificar el entorno a sistemas y protección de datos.
- Determinar las ventajas y desventajas de los métodos de autenticación unifactorial y multifactorial en entorno de acceso a sistemas.

LÍNEAS DE INVESTIGACIÓN

Cabe destacar que la línea de investigación aplicada en este caso de estudio es Sistemas de información y comunicación, emprendimiento e innovación, donde la elección correcta entre autenticación unifactorial y multifactorial influye en la creación y gestión de soluciones tecnológicas innovadoras y seguras.

Mientras que la sublínea de investigación es Redes y tecnologías inteligentes de software y hardware, de manera que, se evaluara cómo los métodos de autenticación unifactorial y multifactorial pueden mejorar fortalecer en la prevención de amenazas cibernéticas y aumentar la confianza en estas tecnologías.

MARCO CONCEPTUAL

CIBERSEGURIDAD EN ENTORNOS TECNOLÓGICOS AVANZADOS

La ciberseguridad se enfoca en salvaguardar los recursos digitales, como redes, hardware, software y los datos procesados, almacenados o transmitidos a través de redes interconectadas. Se refiere a un conjunto de estrategias, sistemas de gestión y medidas destinadas a resguardar la información digital y los dispositivos que la manipulan de eventos malicioso o accidentales. (Ortega Candel, 2021)

Aquí obtenemos algunos conceptos clave relacionados con la ciberseguridad en estos entornos:

- **Amenazas Avanzadas Persistentes (APT):** Estos son ataques cibernéticos altamente elaborados y prolongados que suelen recibir respaldo de identidades estatales o grupos organizados. Su objetivo es infiltrarse y operar en redes avanzadas durante un largo periodo sin ser detectados.
- **Inteligencia de Amenazas:** Se refiere a la recopilación y análisis de datos relacionados con amenazas cibernéticas con el propósito de identificar patrones, tendencias y actividades maliciosas que puedan afectar un entorno tecnológico avanzado.
- **Seguridad Perimetral:** Este término abarca un conjunto de medidas y controles diseñados para proteger el perímetro de una red avanzada, incluyendo la implementación de firewalls, sistemas de detección y prevención de instrucciones (IDS/IPS), y sistemas de defensas contra malware.
- **Seguridad de Confianza Cero:** Zero trust es un enfoque se seguridad que opera bajo la premisa de no confiar en ningún usuario o dispositivo, incluso si se encuentran dentro de

la red. Constantemente verifica la autenticidad y autorización de elementos en un entorno tecnológico avanzado.

- **Criptografía Cuántica:** La criptografía cuántica es una técnica de cifrado que emplea principios de la mecánica cuántica para garantizar la seguridad de la comunicación y el almacenamiento de datos en entornos avanzados, resistiendo a los ataques de computadoras cuánticas.
- **Seguridad en la Nube:** Esto implica la aplicación de medidas de seguridad específicas para proteger los datos y servicios alojados en entornos de computación en la nube. Incluye la autenticación, el cifrado y el control de acceso.
- **Gestión de identidad y Acceso (IAM):** La IAM involucra la administración de la identidad y los permisos de acceso de usuario y dispositivos en un entorno avanzado, asegurando que únicamente las personas autorizadas tengan acceso a recursos críticos.
- **Resiliencia Cibernética:** La resiliencia cibernética se refiere a la capacidad de un entorno tecnológico avanzado para resistir y recuperarse de ataques cibernéticos, minimizando su impacto y garantizando la continuidad de las operaciones.
- **Seguridad en Dispositivos loT:** Aquí se trata de proteger dispositivos de internet de las Cosas (loT) en entornos avanzados, que a menudo comprenden dispositivos interconectados que podrían ser vulnerables a ataques.
- **Evaluación de Vulnerabilidad:** La evaluación de vulnerabilidades implica la identificación y la mitigación proactiva de debilidades y brechas de seguridad en sistemas y aplicaciones avanzadas, antes de que puedan ser explotadas por amenazas cibernéticas.

- **Educación en ciberseguridad:** Esto implica proporcionar formación y aumentar la concienciación entre los usuarios y el personal en un entorno tecnológico avanzado, para que estén alerta y sean capaces de identificar y evitar posibles amenazas cibernéticas.
- **Seguridad en el Desarrollo de Software:** Aquí nos referimos a la incorporación de prácticas de seguridad desde las primeras etapas del desarrollo de software, con el fin de garantizar que las aplicaciones sean resistentes a ataques.

USABILIDAD Y ACEPTACIÓN DE MÉTODOS DE AUTENTICACIÓN

La autenticación es la primera medida de seguridad que un usuario experimental al utilizar una aplicación web, Sin embargo, los desarrolladores a menudo se centran más en la funcionalidad y la seguridad, dejando de lado la facilidad de uso. En este contexto, han surgido requisitos más estrictos para las contraseñas, como la necesidad de incluir mayúsculas, minúsculas, números y caracteres especiales, que los usuarios deben de recordar en cada inicio de sesión. Esto ha llevado a que muchos opten por utilizar la misma contraseña en varios sitios web, lo que representa un riesgo significativo en la gestión de contraseñas. (Pailiacho Mena & Omar S., 2021)

DEFINICIÓN DE AUTENTICACIÓN:

Mientras que el siguiente autor define lo siguiente Autenticación es un término que se refiere al proceso de demostrar que ciertos hechos o ciertos documentos son genuinos. En informática, el término suele asociarse con la prueba de la identidad de un usuario. Normalmente, un usuario demuestra su identidad proporcionando sus credenciales, es decir, información acordada y compartida entre el usuario y el sistema. (Duarte C. , 2018)

Desde mi perspectiva sobre el tema, la autenticación es un proceso que permite indicar a un usuario o entidad, asegurando que quienes dicen acceder a un sistema, servicio o recurso son realmente quienes dicen ser. Utilice diferentes métodos y factores como contraseñas, huellas dactilares, tarjetas inteligentes o reconocimiento facial para mantener la información segura y privada y evitar el acceso no autorizado. La autenticación juega un papel vital en la protección de datos, previniendo posibles ataques o intrusiones y protegiendo la integridad y confidencialidad de los recursos protegidos.

AUTENTICACIÓN UNIFACTORIAL:

La autenticación unifactorial es el tipo más básico de autenticación, donde se verifica la identidad del usuario utilizando un solo factor. Los principales factores utilizados en la autenticación.

¿POR QUÉ ES IMPORTANTE LA AUTENTICACIÓN MULTIFACTOR?

Según (Viscarra, 2019)Los ataques de fuerza bruta también son una amenaza real, ya que los delincuentes pueden usar herramientas automatizadas de descifrado de contraseñas para adivinar varias combinaciones de nombres de usuario y contraseñas hasta que encuentren la secuencia correcta. Aunque bloquear una cuenta después de una cierta cantidad de intentos de inicio de sesión incorrectos puede ayudar a proteger una organización, los piratas informáticos tienen muchos otros métodos para acceder al sistema. Esta es la razón por la que la autenticación multifactor es tan importante, ya que puede ayudar a reducir los riesgos de seguridad.

¿En qué medida la autenticación multifactorial mejora la seguridad en comparación con la autenticación unifactorial?

Según (Duarte D. , 2021)Una solución de autenticación multifactor como Powertech Multi-Factor Authentication proporciona a los administradores control sobre las distintas formas en las que se puede realizar la autenticación y qué métodos pueden utilizarse. A medida que las necesidades de Seguridad de su organización evolucionan, los administradores pueden potenciar la inversión existente de Powertech Multi-Factor Authentication para mejorar la protección de datos.

El siguiente autor define lo siguiente:

La autenticación multifactor es un método de verificación que se utiliza para verificar su identidad basándose en diferentes métodos para confirmar que realmente es usted quien solicita acceso a una cuenta; la autenticación multifactor también se utiliza para proteger dispositivos como teléfonos inteligentes, computadoras portátiles y más. (Parraga, 2022)

ECONOMÍA DE LA SEGURIDAD CIBERNÉTICA

América latina, que se ha rezagado significativamente en comparación con los países occidentales en la adopción de tecnologías de la información, transformación digital y digitalización, también enfrenta problemas relacionados con la ciberseguridad. En los últimos cinco años, la región ha experimentado un aumento del 40% en la cantidad de ataques cibernéticos, lo que equivale a más de 700 millones de ataques al año. Los ataques cibernéticos dirigidos a las instituciones financieras en América Latina han aumentado en un 50%. Anualmente, los ciberdelitos causan daños por un valor de aproximadamente US$90 mil millones a los países de América Latina. (Yu. Kosévich, 2019)

Los tres países que registran la mayor cantidad de delitos cibernéticos son: Brasil, que recibe el 55% de todos los ataques cometidos en la región; México, que es blanco del 17% de los ataques; y Colombia, que representa el 9% de los ataques. En una investigación conjunta realizada en 2016 por la Organización de Estados Americanos (OEA) y el banco Interamericano de Desarrollo (BID), se señala que 16 de los 32 países de América Latina y el Caribe carecen por completo de capacidad para enfrentar los ataques cibernéticos.

BIOMETRÍA Y RECONOCIMIENTO FACIAL EN AUTENTICACIÓN

Los registros biométricos estáticos se generan al procesar datos utilizando métodos automáticos que examinan las características de ADN humano para verificar la identidad de una persona en particular. Este enfoque se concentra en analizar las características que son compartidas y únicas, lo que permite lograr una mayor exactitud en la coincidencia. (Gutiérrez Yánez , 2022)

Los datos personales son manejados siguiendo ciertos principios, que incluyen obtener el consentimiento, definir un propósito específico, permitir el acceso a la persona propietaria de los datos y establecer restricciones en la transferencia. Es importante considerar que, al almacenar esta información, debe hacerse de manera que ninguna tercera persona pueda identificar fácilmente a quien pertenecen los datos mediante métodos razonables, ya que, en caso contrario, los datos perderían su calidad de ser considerados como datos personales.

¿Cuál es la percepción de los usuarios sobre la conveniencia y seguridad de estos métodos de autenticación?

Los usuarios necesitan una autenticación de dos factores para proteger sus cuentas de manera más confiable: si bien cada método de autenticación individual es vulnerable, el uso de

dos (o más) métodos de autenticación juntos hace que el secuestro de cuentas sea mucho más difícil. (Kaspersky, 2023)

ESTUDIOS DE CASO EN EMPRENDIMIENTO TECNOLÓGICO

El emprendimiento tecnológico ha sido abordado desde diversas perspectivas. Algunos lo ven como un generador de innovación dentro de las empresas que se centran en la fabricación. Otros lo definen como un estilo de liderazgo que implica identificar oportunidades comerciales en tecnologías de alto potencial, lo que facilita la acumulación de recurso como talento y capital, y un rápido crecimiento mediante habilidades de toma de decisiones. En este sentido, es común que emprendedores con un sólido crecimiento tecnológico establezcan empresas orientadas hacia la investigación y el desarrollo (I&D) y la innovación. Este proceso también conlleva ciertos riesgos, ya que los emprendedores tecnológicos poseen conocimientos técnicos, pero a menudo carecen de la experiencia necesaria para garantizar el éxito de la empresa en el mercado. (Espinosa Nuñez & Pérez Hernández, 2021)

IMPACTO DE LA LEGISLACIÓN Y REGULACIÓN

La identificación personal se refiere a la relación entre la identidad de un individuo y su persona, manifestada a través de procesos de verificación, autenticación y reconocimiento. Tradicionalmente, los medios empleados para la identificación han sido los “tokens”, es decir, objetos que la persona posee y utiliza para autenticarse, tales como el pasaporte o la cedula de identificación. Asimismo, está el “conocimiento”, que comprende aquello que la persona sabe y emplea, como códigos, contraseñas y números de identificación personal (PIN). No obstante, la utilización de estos medios ha dado lugar a graves problemas, como el robo, extravío, olvido o suplantación, lo que compromete la seguridad personal de manera considerable. (Quintanilla Mendoza, 2020)

Esto abarca la información empleada en procedimientos de autenticación, como contraseñas y datos biométricos. Algunos de los efectos incluyen:

Requisitos de seguridad: Las regulaciones frecuentemente demandan que las organizaciones implementen medidas de seguridad robustas para resguardar los datos personales. Esto puede influir en la selección de métodos de autenticación más avanzados y seguros.

Consentimiento informado: Las leyes de protección de datos pueden requerir que los usuarios otorguen un consentimiento explícito para el procesamiento de sus datos, incluyendo la forma en que se autentican.

Mantenimiento de registros: Puede ser obligatorio para las organizaciones mantener registros de las actividades de autenticación para cumplir con los requisitos de auditoría establecidos por las regulaciones.

Derecho a la portabilidad de datos: Los usuarios pueden tener el derecho de trasladar o duplicar sus datos personales de un entorno a otro, lo que puede influir en la manera en que se administran los métodos de autenticación.

Principio de minimización de datos: Las regulaciones a menudo enfatizan la importancia de recopilar solo la cantidad mínima necesaria de datos. Esto puede tener un impacto en la elección de métodos de autenticación que requieren una mínima cantidad de información personal.

Notificación de violaciones de datos: En caso de una violación de datos, las regulaciones pueden exigir que las organizaciones informen a las autoridades y a los individuos afectados.

TENDENCIAS EMERGENTES EN AUTENTICACIÓN

Este método emplea una forma de autenticación basada en el uso de una clave compuesta por palabras o información específica. Su propósito es habilitar el uso de palabras como parte del proceso de autenticación de un individuo. En lugar de depender de caracteres individuales, se forma una contraseña a partir de una secuencia de palabras. En este contexto, los componentes de la contraseña son palabras en lugar de caracteres individuales. Se ha seleccionado un subconjunto de palabras del idioma español para cumplir con dos objetivos clave: 1) Incrementar la seguridad al evitar que cualquier palabra del español sea considerada como una entrada válida y 2) Prevenir la confusión entre palabras homófonas, es decir, palabras que se pronuncian de manera similar, pero tienen significados diferentes. Para lograr este segundo objetivo, se han elegido palabras con pronunciaciones distintas entre sí. El primer objetivo ha posibilitado la implementación del método con una clave física, consistente en que el usuario deberá poseer una tarjeta impresa con un listado de las palabras autorizadas que representan las posibles entradas al sistema, así como información relevante para los demás métodos de autenticación que serán utilizados. (Pastor, 2020)

SEGURIDAD EN REDES INTELIGENTES Y IOT

En los últimos años, el Internet de las Cosas (IoT) ha sido gradualmente integrado en la economía, creando un variado mercado de soluciones y comodidades tanto para la industria como para el ámbito doméstico. Las aplicaciones de IoT abarcan desde hogares inteligentes hasta sistemas de medición avanzada, monitoreo en fábricas, agricultura y edificaciones inteligentes, entre otros. Aunque tecnologías inalámbricas como Bluetooth, WiFi y ZigBee inicialmente satisfacían las necesidades de comunicación para IoT, su alcance limitado a corta distancia restringía las capacidades del sistema. Para superar estas limitaciones, se han implementado redes

de área amplia y baja potencia (LPWAN, por sus siglas en inglés), que proporcionan conectividad a larga distancia, abarcando varios kilómetros. LPWAN facilita el intercambio de mensajes pequeños entre dispositivos IoT a grandes distancias, con un consumo de energía extremadamente bajo, lo que permite el funcionamiento de los dispositivos durante varios años con baterías pequeñas. Por estas razones, LPWAN ha sido ampliamente adoptado en el ámbito industrial debido a sus diversas aplicaciones. (González González, Arévalo Tapias, & Hernández Gutiérrez, 2019)

EDUCACIÓN Y CONCIENCIACIÓN EN SEGURIDAD CIBERNÉTICA

En el presente, se ha constatado que las compañías que dedican recursos a la ciberseguridad son considerablemente más exitosas en la prevención de ataques, hasta en un factor de 200 veces. Tanto en entornos educativos como empresariales, es imperativo no subestimar la relevancia de la seguridad informática, dado que cada año, la frecuencia de estos ataques va en aumento de manera significativa. (Salazar Mata, Cruz Navarro, Balderas Sánchez, & Díaz Uribe, 2021)

AMENAZAS DE CIBERSEGURIDAD

Según (Acosta, 2022) En la era digital en la que vivimos, es fundamental comprender los peligros a los que nos enfrentamos en línea. Una amenaza de ciberseguridad es un ataque o acto malicioso diseñado para dañar, robar información o interrumpir nuestros sistemas y dispositivos conectados. En este módulo, veremos algunas de las amenazas más comunes, como el phishing, el malware y el robo de identidad. Aprenderemos a reconocer estas amenazas y tomaremos medidas para protegernos y mantenernos seguros en el mundo digital.

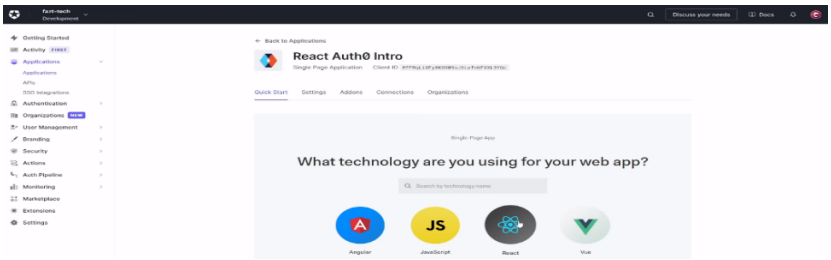
DESARROLLO DE SOLUCIONES DE AUTENTICACIÓN PERSONALIZADAS

Después de llevar a cabo una fase de investigación y comparación, se opta por seleccionar OpenAM como el pilar fundamental del sistema. Esta aplicación ofrece una gestión de identidad integral y la capacidad de implementar un inicio de sesión único. También permite la integración de módulos de autenticación personalizados además de los predeterminados. Tras evaluar diversas técnicas de inteligencia artificial, se determina que las más exhaustivas y compatibles son proporcionadas por Behaviosec. Esta plataforma tiene la capacidad de entrenar perfiles de comportamiento de usuarios y, al iniciar sesión, evaluar el nivel de riesgo asociado a esa acción. Esta tecnología se fundamenta en comportamientos como la velocidad y presión al escribir o al usar el ratón, y tiene la capacidad de actualizar los perfiles de comportamiento en caso de cambios significativos en los mismos. (Aguado Perulero, 2022)

PROCESO DEL USO DE LA PLATAFORMA REACT AUTH0

En las siguientes imágenes se puede observar el proceso del uso de la plataforma React Auth0, la cual permite administrar la identidad de nuestros usuarios de forma efectiva y con mucho control.

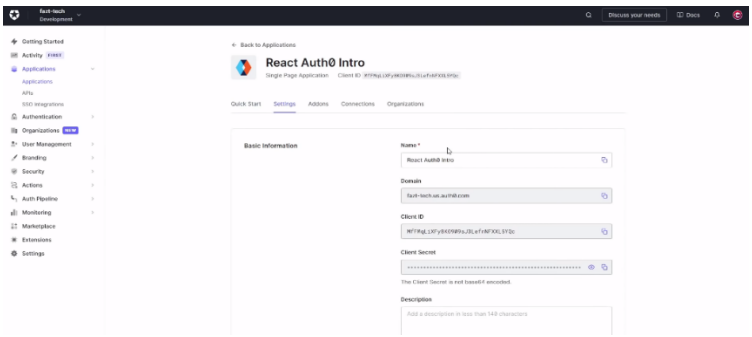
Ilustración 1. Se empezará a crear toda una interfaz en donde va a dar como primera opción si se quiere integrar este proyecto en este caso se escoge React.



Elaborado por: *Jonathan Valverde Castro*

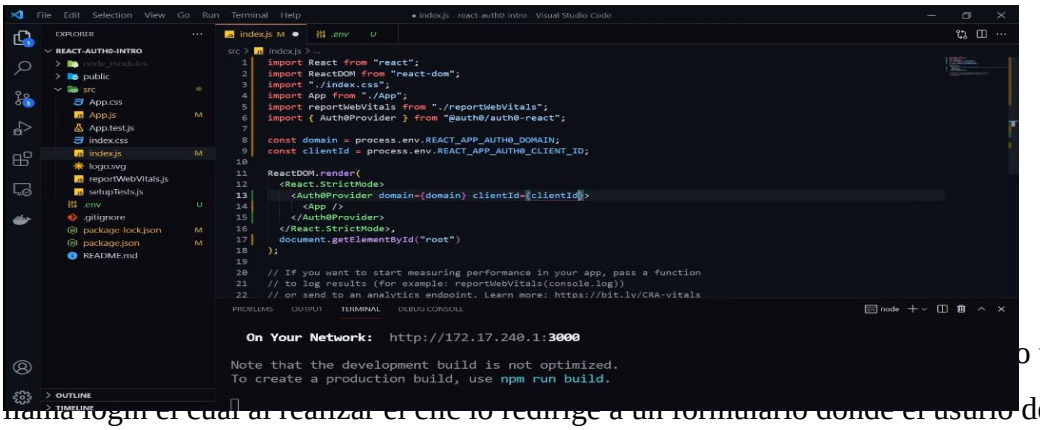
Ilustración 2. Como se puede observar esta opción sirve para realizar las configuraciones del proyecto el cual está separado en varios campos como: El Domain, es decir cuando se dese

autenticar el usuario, se abrirá una nueva URL en este dominio y al final permitirá mostrar el usuario y un Login. El client ID, su función es pedir autorización de pedir información al usuario.

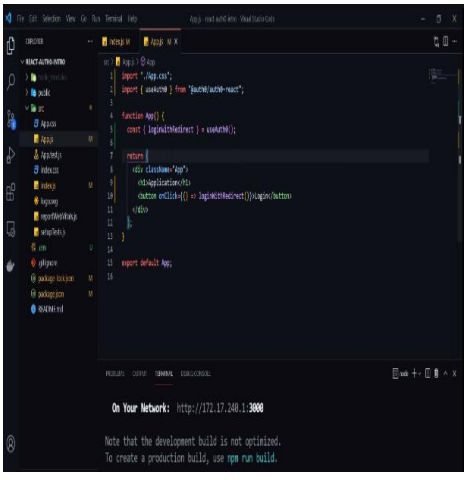


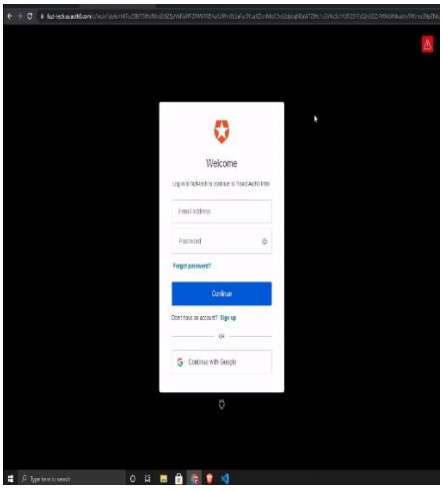
Elaborado por: *Jonathan Valverde Castro.*

Ilustración 3. Se creó un componente llamado Index.js en donde importaron varios variables que son importante para el uso de la aplicación de React. Además, se programa el domain y el client esto sirve para que una vez logeado se vuelva a redireccionar.



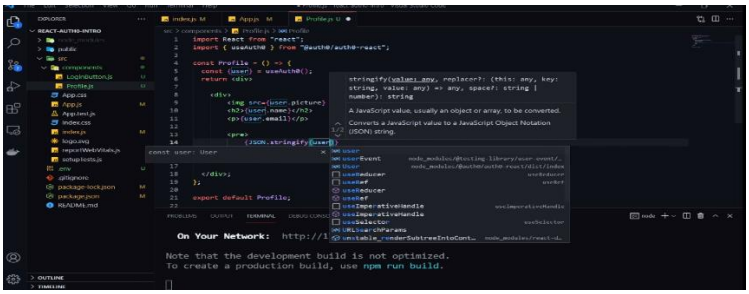
llamá login el cual al realizar el clic lo redirige a un formulario donde el usuario debe ingresar los datos concretos para poder ingresar.





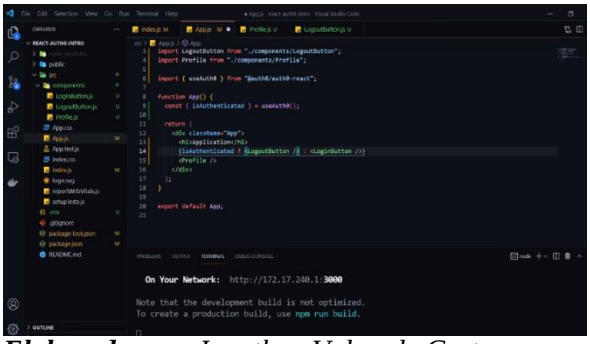
Elaborado por: Jonathan Valverde Castro

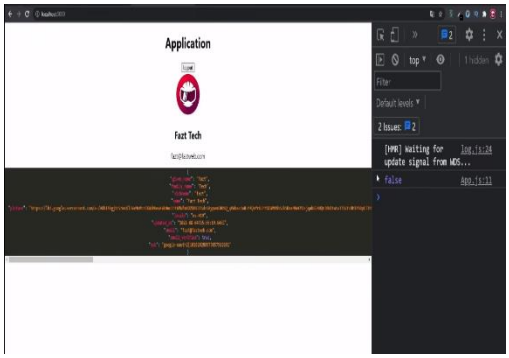
Ilustración 5. Se creó un componente llamado Profile.js aquí se programa para que pinte y muestre el nombre, la imagen, el correo del usuario



Elaborado por: *Jonathan Valverde Castro*

Ilustración 6. Se creó una propiedad la cual es la isAuthenticated la cual da ciertos requerimientos al momento de logearse el usuario y asi poder continuar con la autenticación y asi poder entrar dentro de la aplicación.





Elaborado por: *Jonathan Valverde Castro*

MARCO METODOLÓGICO

Este estudio proporciona una revisión exhaustiva de la literatura y de investigaciones previas sobre autenticación de unifactorial y multifactorial. Se recopila información sobre las características, ventajas, desventajas y casos de uso de ambos métodos. Esta revisión de la bibliográfica proporciona una base sólida para comprender el contexto y los fundamentos teóricos de la autenticación.

El propósito de este trabajo es analizar y comparar métodos de autenticación simple y multifactor en entornos de uso de sistemas y protección de datos. Para obtener resultados

concretos y confiables se utiliza la plataforma Auth0, la cual se caracteriza por su eficiencia y confiabilidad en la gestión de autenticación y seguridad de los sistemas de información.

La plataforma Auth0 facilita la recopilación de datos sobre la implementación y efectividad de los métodos de autenticación. Se definen instancias específicas para cada organización seleccionada, lo que permite obtener información detallada y precisa sobre la actividad de autenticación.

Los datos recogidos a través de la plataforma Auth0 se analizan cuantitativa y cualitativamente. Esto permite evaluar el rendimiento de los métodos de autenticación en cada caso específico y proporciona un punto de referencia sólido.

RESULTADOS

Los resultados obtenidos muestran el proceso detallado de implementación y configuración de la plataforma React Auth0 para una gestión efectiva de la identidad de los usuarios. Este enfoque proporciona un control detallado sobre la autenticación en aplicaciones React.

El proceso de implementación involucró la creación de una interfaz de usuario desde cero, que brindó a los usuarios la opción de integrar el proyecto en React. Además, se realizaron

configuraciones clave, como la especificación del dominio y el cliente ID. Estos parámetros son esenciales para autenticar a los usuarios y solicitar autorización para acceder a sus datos.

La configuración del dominio y el ID del cliente se llevó a cabo para garantizar la autenticación efectiva y la autorización de acceso a la información del usuario. El dominio permitió la autenticación del usuario en una URL específica, mientras que el cliente ID se utilizó para solicitar permisos de acceso.

Se creó una interfaz de usuario amigable y funcional en la que se destacan botones y formularios. Estos elementos permitieron a los usuarios interactuar de manera sencilla con la aplicación y proporcionaron una experiencia de usuario positiva.

A través de la plataforma React Auth0, se logró una gestión eficaz de la identidad del usuario. Se implementó un componente de perfil que mostraba información importante, como el nombre, la imagen y el correo del usuario. La propiedad isAuthenticated desempeñó un papel crucial, permitiendo condicionales que determinaron el acceso a diversas partes de la aplicación según el estado de autenticación. Cuando estaba cargando, se permitía el acceso, mientras que un estado falso denegaba la autenticación y el acceso al componente del usuario.

DICUSIÓN DE RESULTADOS

Los resultados confirman que la plataforma React Auth0 es muy eficaz para la gestión de identidades de usuarios en aplicaciones React. Esto proporciona un control preciso sobre el proceso de autenticación, que es fundamental para la seguridad y el acceso a los datos del usuario.

A continuación, proporciono un cuadro comparativo detallado de la autenticación de unifactorial y multifactorial, especialmente en relación con la plataforma Auth0:

Tabla 1 Cuadro comparativo específico para la autenticación unifactorial y multifactorial.

Características	Autenticación Unifactorial	Autenticación Multifactorial
Factores de Autenticación	Un solo factor, por ejemplo contraseña.	Dos o más factores, estas pueden ser una combinación de contraseñas, autenticación biométrica, etc.
Nivel de Seguridad	Menor en comparación con multifactorial	Mayor debido a la necesidad de superar múltiples barreras.
Facilidad de Integración	Más rápida y sencilla de implementar	Requiere configuración adicional y puede llevar más tiempo configurarlo
Facilidad de Uso	Más fácil para los usuarios, ya que implica un solo paso	Puede resultar más difícil debido a varios factores, pero proporciona un nivel adicional de protección.
Tipos de Factores	Contraseñas, PINs, autenticación social, ya sea Facebook o google	Contraseñas, tokens móviles, autenticación biométrica, notificaciones push, etc.
Resistencia a Ataques	Es más vulnerable a ataques como fuerza bruta o ataques de diccionario.	Más resistente a este tipo de ataques porque aunque se obtengan las credenciales, se requiere otro factor para acceder.
Costo	Generalmente más económica de implementar	Puede requerir inversión en tecnología adicional, como tokens de hardware o software de autenticación adicional.
Configuración de reglas	Puede requerir menos configuración de reglas de autenticación.	Puede implicar configuraciones más extensas para manejar múltiples factores.
Cumplimiento normativo	Cumple con los requisitos mínimos en la mayoría de los casos	Puede requerir el cumplimiento de regulaciones y estándares de seguridad más estrictos.
Personalización de Experiencia	Puede ser menos adaptable en comparación con varios factores.	Permite una mejor personalización de la experiencia de autenticación, incluidos pasos de verificación adicionales.

Elaborado por: *Jonathan Valverde Castro.*

Se proporciona una descripción detallada de las principales diferencias entre los dos métodos de autenticación.

AUTENTICACIÓN UNIFACTORIAL:

Seguridad es menos crítica: La autenticación de un factor puede ser suficiente para aplicaciones donde la seguridad no es una prioridad máxima. Ejemplo, en programas de noticias.

Acceso rápido y fácil: Es adecuado para sistemas que requieren un proceso de inicio de sesión rápido y sencillo sin pasos de verificación adicionales

Experiencia del usuario: En situaciones donde el objetivo principal es brindar una experiencia de usuario fluida y sin esfuerzo, esta puede ser la mejor opción.

AUTENTICACIÓN MULTIFACTORIAL:

Alto nivel de seguridad: Los sistemas que manejan información confidencial, como información bancaria o médica, deben implementar autenticación multifactor para una protección adicional.

Acceso a información sensible o privada: Las aplicaciones que contienen información confidencial o privada, como cuentas bancarias, información de tarjetas de crédito o información médica, deben utilizar autenticación multifactor.

Transacciones de financieras sensibles: En aplicaciones de banca online, servicios de pago o plataformas de compras online, la autenticación multifactor es esencial para proteger las transacciones financieras.

Empresas y organizaciones: Para empresas u organizaciones que necesitan proteger el acceso a sistemas internos, bases de datos de clientes o sistemas administrativos, la autenticación multifactor es fundamental.

CONCLUSIONES

Mediante la presente investigación que se tuvo a lo largo del proyecto llegamos a la siguiente conclusión:

Al estudiar los antecedentes y las bases teóricas de la autenticación de un solo factor y de múltiples factores, hemos desarrollado una comprensión sólida de los principios y conceptos subyacentes de estos métodos de autenticación. Exploramos la historia, los

mecanismos y las tecnologías de la autenticación de un solo factor y de múltiples factores, proporcionando una base sólida para nuestro análisis comparativo.

Al identificar los contextos en lo que se utilizan estos métodos de autenticación, reconocemos la complejidad de los sistemas de información y comunicación, la diversidad de entornos comerciales y el impacto de las regulaciones de protección de datos en la elección de los métodos de autenticación. Comprender este contexto es fundamental para tomar decisiones informadas sobre cómo implementar métodos de autenticación de manera efectiva y segura.

El análisis exhaustivo de las ventajas y desventajas de los métodos de autenticación de un solo factor y de múltiples factores para el acceso al sistema revela varias consideraciones importantes. Además, la autenticación de un solo factor ofrece simplicidad y facilidad de uso, también tiene vulnerabilidades importantes, como la vulnerabilidad a ataques de fuerza bruta. Por otro lado, la autenticación multifactor proporciona un nivel adicional de seguridad, pero puede requerir recursos adicionales y ser menos conveniente para los usuarios.

RECOMENDACIONES

En entornos críticos para la seguridad, como el acceso a datos confidenciales o sistemas críticos, se debe considerar seriamente la implementación de la autenticación multifactor. Esto proporciona protección adicional contra amenazas cibernéticas.

Las normas de privacidad y protección de datos tienen un impacto significativo en la elección del método de autenticación. Se recomienda a las organizaciones que conozcan las leyes

y regulaciones aplicables en su jurisdicción y ajusten sus políticas de autenticación en consecuencia.

Se identificó que los principales pros y contras de la autenticación de un solo factor y de múltiples factores, se recomienda encarecidamente que las organizaciones y las personas realicen una evaluación exhaustiva basada en el contexto antes de decidir qué método de autenticación implementar. La elección entre estos enfoques debe ser una decisión informada que refleje las necesidades y riesgos específicos de cada entorno.

REFERENCIAS

Acosta, J. (2022). *www.genetec.com*. Obtenido de www.genetec.com: https://www.genetec.com/es/blog/ciberseguridad/como-funciona-la-autenticacion#:~:text=Cuando%20se%20trata%20de%20tu,tu%20sistema%20cuando%20inician%20sesi%C3%B3n.

Aguado Perulero, I. (Julio de 2022). *uc3m.* Obtenido de -archivo.uc3m.es: https://docs.google.com/viewerng/viewer?url=https://e-archivo.uc3m.es/bitstream/handle/10016/36205/TFG_Ivan_Aguado_Perulero.pdf

Duarte, C. (2018). *auth0.com*. Obtenido de auth0.com: https://auth0.com/es/intro-to-iam/what-is-authentication

Duarte, D. (24 de 08 de 2021). *www.fortra.com*. Obtenido de www.fortra.com: https://www.fortra.com/es/blog/cual-es-la-diferencia-entre-autenticacion-de-doble-factor-y-multifactor

Espinosa Nuñez, S. M., & Pérez Hernández, M. d. (2021). Estudio comparativo del emprendimiento tecnológico en aplicaciones móviles en Japón, Corea y México. *Revista gestión de las personas y tecnología*.
https://www.scielo.cl/scielo.php?pid=S0718-56932021000100094&script=sci_arttext&tlng=pt

González González, C. A., Arévalo Tapias, F., & Hernández Gutiérrez, J. (2019). Análisis de seguridad en redes LPWAN para dispositivos IoT. *Revista Vínculos*.
http://revistas.udistrital.edu.co:8080/index.php/vinculos/article/view/15712/15352

Gutiérrez Yánez , A. E. (7 de marzo de 2022). *dspace.ups.edu.ec.* Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/22173/1/UPS%20-%20TTS659.pdf

Kaspersky. (2023). *www.linkedin.com*. Obtenido de https://www.linkedin.com/pulse/tipos-de-autenticaci%C3%B3n-dos-factores-ventajas-y-desventajas/?originalSubdomain=es

Ortega Candel, J. M. (2021). *CIBERSEGURIDAD. Manual práctico.* Ediciones Paraninfo.
https://books.google.es/books?hl=es&lr=&id=QsROEAAAQBAJ&oi=fnd&pg=PR5&dq=que+es+Ciberseguridad+en+Entornos+Tecnol%C3%B3gicos+Avanzados&ots=3siol-AmTc&sig=4vcIUT1zp0bT0greMPGqasnXlAg#v=onepage&q&f=false

Pailiacho Mena, V., & Omar S., G. (2021). Métodos de Autenticación en Aplicaciones Web bajo un Enfoque de Usabilidad: Una Revisión Sistemática de Literatura. *risti*, 469.
https://www.researchgate.net/profile/Omar-S-Gomez/publication/353541241_Metodos_de_Autenticacion_en_Aplicaciones_Web_bajo_un_Enfoque_de_Usabilidad_Una_Revision_Sistematica_de_Literatura/links/610211331ca20f6f86e6088c/Metodos-de-Autenticacion-en-Aplicaciones-Web-bajo-un-Enfoque-de-Usabilidad-Una-Revision-Sistematica-de-Literatura.pdf

Parraga, C. (5 de 10 de 2022). *easydmarc.com/*. Obtenido de easydmarc.com/: https://easydmarc.com/blog/es/que-es-la-autenticacion-multifactor-y-por-que-es-tan-necesaria/

Pastor, D. (2020). RSA SecurID Access, la transformación de la seguridad del acceso. *Dialnet*.
https://dialnet.unirioja.es/servlet/articulo?codigo=7864700

Quintanilla Mendoza, G. (2020). Legislación, riesgos y retos de los sistemas biométricos. *scielo*.
https://www.scielo.cl/scielo.php?pid=S0719-25842020000100063&script=sci_arttext#aff1

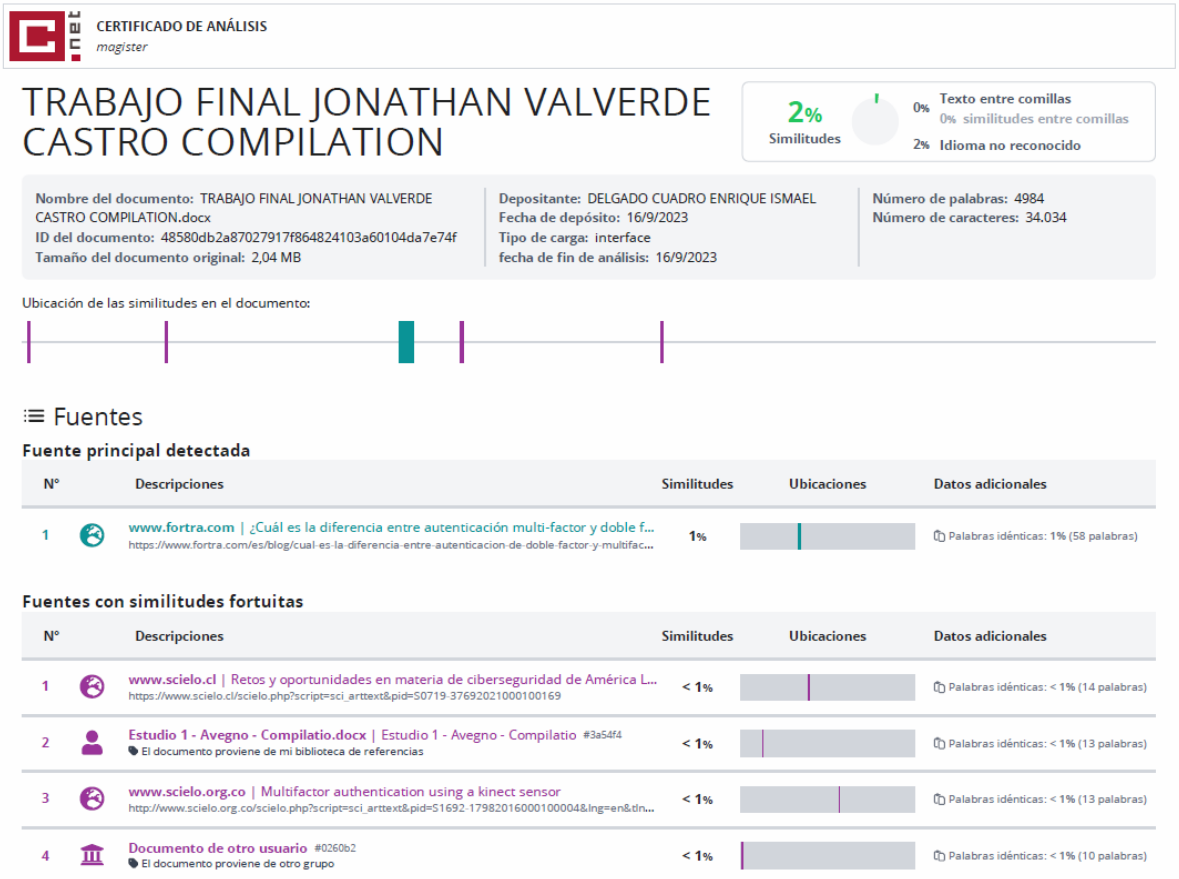
Salazar Mata, J. M., Cruz Navarro, C., Balderas Sánchez, A. V., & Díaz Uribe, H. F. (2021). La seguridad informática en las instituciones de educación superior. *Dialnet*.
https://dialnet.unirioja.es/servlet/articulo?codigo=8524233

Viscarra, M. (2019). *www.computerweekly*. Obtenido de www.computerweekly: https://www.computerweekly.com/es/definicion/Autenticacion-multifactor-o-MFA

Yu. Kosévich, E. (18 de Noviembre de 2019). *researchgate.* Obtenido de https://www.researchgate.net/profile/Ekaterina-

Kosevich/publication/340419950_Cyber_Security_Strategies_of_Latin_America_Countries/links/5eac0008a6fdcc70509e07c7/Cyber-Security-Strategies-of-Latin-America-Countries.pdf

ANEXOS



CERTIFICADO DE ANÁLISIS
magister

TRABAJO FINAL JONATHAN VALVERDE CASTRO COMPILATION

2% Similitudes

0% Texto entre comillas
0% similitudes entre comillas
2% Idioma no reconocido

Nombre del documento: TRABAJO FINAL JONATHAN VALVERDE CASTRO COMPILATION.docx
ID del documento: 48580db2a87027917f864824103a60104da7e74f
Tamaño del documento original: 2,04 MB

Depositante: DELGADO CUADRO ENRIQUE ISMAEL
Fecha de depósito: 16/9/2023
Tipo de carga: interface
fecha de fin de análisis: 16/9/2023

Número de palabras: 4984
Número de caracteres: 34.034

Ubicación de las similitudes en el documento:

Fuentes

Fuente principal detectada

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	www.fortra.com | ¿Cuál es la diferencia entre autenticación multi-factor y doble f... https://www.fortra.com/es/blog/cual-es-la-diferencia-entre-autenticacion-de-doble-factor-y-multifac...	1%		Palabras idénticas: 1% (58 palabras)

Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	www.scielo.cl | Retos y oportunidades en materia de ciberseguridad de América L... https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-37692021000100169	< 1%		Palabras idénticas: < 1% (14 palabras)
2	Estudio 1 - Avegno - Compilatio.docx | Estudio 1 - Avegno - Compilatio #3a54f4 El documento proviene de mi biblioteca de referencias	< 1%		Palabras idénticas: < 1% (13 palabras)
3	www.scielo.org.co | Multifactor authentication using a kinect sensor http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1692-17982016000100004&lng=en&tln...	< 1%		Palabras idénticas: < 1% (13 palabras)
4	Documento de otro usuario #0260b2 El documento proviene de otro grupo	< 1%		Palabras idénticas: < 1% (10 palabras)