PORTAL ACADÉMICO SEGURO CON AUTENTICACIÓN MULTIFACTOR (MFA).

CARLOS DANIEL ALVAREZ QINTERO - 1099734902
RUSBELL OVEYMAR ENDES - 1116868419
WILSON PARADA GELVEZ - 1094275964

UNIVERSIDAD DE PAMPLONA
PROGRAMA DE INGENIERIA DE SISTEMAS
SGURIDAD INFORMATICA
2025-2

PORTAL ACADÉMICO SEGURO CON AUTENTICACIÓN MULTIFACTOR (MFA).

DESCRIPCIÓN.

El presente proyecto tiene como finalidad fundamental el diseño e implementación de un portal académico web que incorpore un mecanismo de autenticación multifactor (MFA), con el propósito de fortalecer significativamente la seguridad en el acceso y gestión de información crítica perteneciente a estudiantes, docentes y personal administrativo. En un contexto donde las instituciones educativas dependen cada vez más de plataformas digitales para sus procesos académicos y administrativos, consideramos esencial integrar medidas de seguridad avanzadas que garanticen la protección de los datos y reduzcan de manera considerable la superficie de ataque.

De esta manera, se propone un sistema basado en dos factores de autenticación: en primer lugar, una contraseña segura que representa "algo que el usuario sabe" y en segundo lugar, un código temporal OTP ("One-Time Password") que representa "algo que el usuario tiene". Este enfoque dual permite mitigar de forma efectiva riesgos como el acceso no autorizado, el robo de credenciales y la suplantación de identidad, fortaleciendo así los principios fundamentales de la seguridad informática: la confidencialidad, la integridad y la disponibilidad de la información académica.

El sistema será desarrollado bajo una arquitectura cliente-servidor. El frontend estará compuesto por una interfaz web implementada con tecnologías modernas como HTML, CSS y JavaScript mediante el framework React, lo que permite una experiencia de usuario fluida, dinámica y segura. Paralelamente, se integrará un backend desarrollado en Node.js que gestionará procesos críticos como la validación de credenciales, la generación y verificación de códigos OTP, así como la administración de sesiones seguras mediante JWT u otros mecanismos equivalentes. Toda la información será almacenada en una base de datos relacional, como MySQL o PostgreSQL, garantizando una estructura sólida, escalable y confiable para la gestión de usuarios, roles y registros de acceso.

Este proyecto, en su conjunto, simulará el flujo real de un sistema institucional académico, replicando procesos como el inicio de sesión, la verificación de identidad mediante MFA y el acceso autorizado a módulos específicos del portal. Con ello, buscamos demostrar de manera práctica y fundamentada cómo la autenticación multifactor mejora la seguridad de los sistemas actuales sin comprometer la experiencia del usuario final.

ANÁLISIS DEL ENTORNO O CASO DE USO DONDE SE APLICARÁ MFA.

En la actualidad, la mayoría de instituciones educativas, tanto públicas como privadas, han adoptado plataformas digitales orientadas a facilitar la gestión académica y administrativa,

abarcando servicios como portales de calificaciones, sistemas de matrícula en línea, consulta de asistencia, repositorios de materiales educativos, comunicación interna, entre otros. Todos estos servicios requieren, de manera inevitable, procesos de autenticación para verificar la identidad del usuario antes de concederle acceso a información personal o institucional.

No obstante, estas plataformas suelen basarse exclusivamente en sistemas de autenticación de un solo factor, principalmente el uso de nombres de usuario y contraseñas. Si bien este enfoque ha sido la norma durante muchos años, concluimos que resulta insuficiente frente a las amenazas cibernéticas actuales, las cuales han incrementado tanto en frecuencia como en complejidad. Amenazas como el phishing, el keylogging, los ataques de fuerza bruta y la reutilización de contraseñas en múltiples servicios representan un riesgo real y creciente para cualquier sistema que no esté preparado adecuadamente.

Considerando todo lo anterior, opinamos que un portal académico es un entorno ideal para aplicar mecanismos de autenticación multifactor, debido al alto valor y sensibilidad de la información que maneja. Entre los datos que se gestionan en estas plataformas se encuentran:

- Calificaciones, evaluaciones y progreso académico.
- Datos personales de estudiantes, docentes y personal administrativo.
- Información vinculada a matrículas, horarios, asistencia y registros administrativos.
- Historiales académicos y documentos oficiales.

Por lo tanto, concluimos que garantizar la protección de esta información no solo es un requerimiento técnico, sino también una responsabilidad institucional. La implementación de MFA no solo incrementa la seguridad, sino que además permite evidenciar la aplicabilidad real de estándares avanzados de autenticación utilizados comúnmente en sectores financieros, gubernamentales o empresariales, trasladándolos a un entorno educativo que cada vez depende más de herramientas tecnológicas.

El sistema propuesto reproducirá el flujo típico de acceso a un portal universitario, demostrando cómo la integración del segundo factor de autenticación puede reducir la probabilidad de ataques exitosos sin afectar negativamente la experiencia del usuario. Por el contrario, se busca que los usuarios perciban una plataforma más confiable, robusta y alineada con las mejores prácticas de seguridad informática.

PROBLEMA DE SEGURIDAD IDENTIFICADO.

El problema principal identificado radica en la vulnerabilidad inherente de los sistemas que dependen únicamente de métodos de autenticación basados en un solo factor. Este esquema tradicional, centrado exclusivamente en el uso de contraseñas, presenta múltiples debilidades que se vuelven críticas en entornos donde se maneja información sensible.

Actualmente, muchos portales académicos permiten el ingreso únicamente con un nombre de usuario y una contraseña, lo que facilita que un atacante pueda obtener acceso mediante diversas técnicas maliciosas. Entre los riesgos más comunes se encuentran:

- **Robo o filtración de contraseñas:** debido a bases de datos expuestas, contraseñas débiles o reutilizadas en otros servicios externos.
- **Ataques de phishing:** donde los usuarios, mediante engaños, revelan sus credenciales creyendo que ingresan a sitios legítimos.
- **Ataques de fuerza bruta o diccionario:** los atacantes prueban múltiples combinaciones de contraseñas hasta encontrar una válida.
- **Acceso interno indebido:** un individuo con credenciales válidas puede consultar, modificar o extraer información sin autorización.

En consecuencia, concluimos que la autenticación de un solo factor representa un riesgo elevado tanto para los usuarios como para la integridad de la institución. Por este motivo, resulta imprescindible adoptar mecanismos como MFA, los cuales añaden una segunda capa de seguridad que dificulta considerablemente cualquier intento de intrusión. Incluso si un atacante logra obtener la contraseña del usuario, sin el segundo factor (el código OTP temporal), será incapaz de acceder al sistema.

Opino que la implementación de MFA constituye una mejora sustancial en los procesos de autenticación, ya que refuerza los mecanismos tradicionales y garantiza un nivel de protección más adecuado para los sistemas actuales. De esta manera, se promueve un entorno digital más seguro, confiable y alineado con las mejores prácticas de ciberseguridad.

OBJETIVOS DEL PROYECTO.

Objetivo general

Diseñar e implementar un sistema de autenticación multifactor en un portal académico web que fortalezca la seguridad del acceso a la información institucional, integrando contraseñas y códigos OTP para garantizar la protección de las credenciales de los usuarios y reducir los riesgos asociados a accesos no autorizados.

Objetivos específicos

- Analizar de manera exhaustiva el entorno académico y los riesgos inherentes al uso de métodos tradicionales de autenticación de un solo factor.
- Diseñar una arquitectura web segura, escalable y eficiente que incorpore mecanismos de MFA empleando herramientas modernas, confiables y compatibles con los estándares actuales.
- Implementar un flujo completo de autenticación basado en contraseña y OTP generado a través de correo electrónico o aplicaciones de autenticación como Google Authenticator.
- Validar la efectividad del sistema mediante pruebas de seguridad, pruebas de usabilidad y evaluaciones que garanticen su correcto funcionamiento.
- Documentar minuciosamente el proceso de diseño, desarrollo e implementación de la solución MFA, resaltando sus ventajas, limitaciones y oportunidades de mejora.

ALCANCE Y LIMITACIONES DEL PROYECTO.

Alcance del proyecto

El presente proyecto contempla el diseño e implementación de un portal académico que incorpore un sistema de autenticación multifactor (MFA), con el fin de fortalecer los mecanismos de seguridad empleados durante el proceso de acceso a información institucional. De esta manera, el alcance del proyecto se concentra en desarrollar únicamente las funciones esenciales que permitan demostrar el funcionamiento práctico del MFA y su impacto en la protección de los datos académicos. Por consiguiente, se busca construir un prototipo funcional que replique el flujo típico de autenticación utilizado en plataformas universitarias reales.

Dentro del alcance de esta primera versión del sistema se incluye:

- **Inicio de sesión mediante usuario y contraseña**, utilizando técnicas seguras de almacenamiento de credenciales, como el uso de hash criptográfico.
- **Verificación de identidad mediante un código OTP temporal**, generado para el usuario y validado antes de permitir su acceso al portal.
- **Acceso a un panel básico según el rol del usuario**, ya sea estudiante, docente o administrador. Aunque estas interfaces serán representativas, se desarrollarán de manera sencilla con el propósito de demostrar el correcto funcionamiento del proceso de autenticación multifactor.
- **Registro de logs de acceso**, donde se almacenarán los intentos de inicio de sesión, verificaciones MFA, accesos exitosos y accesos fallidos, lo que permitirá evaluar el comportamiento del sistema y fortalecer las prácticas de auditoría.

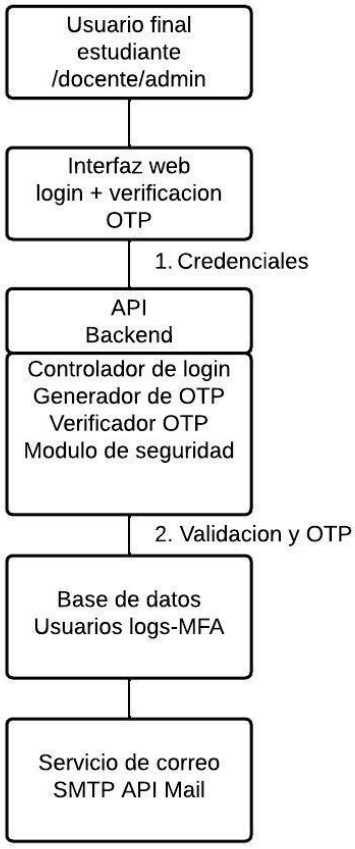
Sin embargo, es importante aclarar que existen elementos que se encuentran fuera del alcance del proyecto, debido principalmente a la naturaleza académica del trabajo y al tiempo limitado para su ejecución. En este sentido, no se desarrollarán:

- **Sistemas completos de matrícula, horarios o gestión académica**, ya que estos requieren arquitecturas más extensas y procesos administrativos complejos.
- **Integraciones con sistemas reales de instituciones educativas**, puesto que este prototipo no está orientado a producción, sino a la demostración conceptual y técnica del MFA.
- **Mecanismos avanzados de recuperación de contraseña**, tales como envío de OTP por SMS, integración con proveedores externos o validación multidominio. Estas funciones serán consideradas fuera del alcance para mantener el enfoque principal del proyecto.

Consideramos que delimitar claramente el alcance permite concentrar los esfuerzos en el objetivo fundamental: evidenciar cómo la implementación de autenticación multifactor mejora la seguridad de un portal académico sin afectar negativamente la experiencia del usuario.

DIAGRAMA DE ARQUITECTURA PROPUESTA

Capa	Componente	Descripción
Cliente (Frontend)	**Portal web React**	Permite a estudiantes, docentes y administradores iniciar sesión, ingresar credenciales, y luego el código OTP.
	Módulo MFA (interfaz)	Muestra el campo para ingresar el código OTP temporal.
Servidor (Backend API)	**Controlador de Autenticación**	Recibe las credenciales, valida usuario y contraseña, genera y envía el OTP (por correo o app).
	Módulo de verificación OTP	Verifica el código temporal ingresado por el usuario.
	Servicio de envío OTP	Envía el OTP mediante **correo electrónico** o **aplicación de autenticación (Google Authenticator, Authy, etc.)**.
	Módulo de seguridad (JWT / sesiones)	Gestiona tokens de sesión y seguridad posterior al login.
Base de Datos	**Usuarios**	Guarda datos del usuario, roles (docente, estudiante, admin), hash de contraseña, clave secreta MFA.
	Logs de acceso	Registra intentos de autenticación y verificaciones MFA.



HERRAMIENTAS TECNOLOGICAS

1. Backend: Node.js + Express

El backend se implementará utilizando **Node.js**, un entorno de ejecución basado en JavaScript orientado a la creación de aplicaciones web rápidas y escalables. Sobre este entorno se empleará el framework **Express**, que permite construir APIs REST de manera estructurada y modular.
Estas herramientas facilitan la implementación de la lógica del sistema, incluyendo:

- Validación de credenciales.
- Generación y verificación de códigos OTP (TOTP).
- Gestión de sesiones o tokens JWT.
- Comunicación segura con la base de datos.

2. Frontend: React (HTML, CSS y JavaScript)

La interfaz del portal académico se construirá utilizando **React**, una biblioteca de JavaScript orientada al desarrollo de interfaces dinámicas y eficientes.

React permite:

- Crear componentes reutilizables (login, ingreso de OTP, panel de usuario).
- Mejorar la experiencia del usuario mediante renderizado rápido.
- Facilitar la comunicación con el backend mediante peticiones asincrónicas (fetch/Axios).

El frontend utiliza tecnologías estándar como **HTML, CSS y JavaScript**, complementadas con el enfoque modular de React para garantizar una interfaz moderna y fácil de mantener.

3. Base de datos: MySQL

Para el almacenamiento de la información del sistema se empleará **MySQL**, una base de datos relacional ampliamente utilizada en aplicaciones web.

Almacena:

- Información de usuarios (rol, correo, estado).
- Hash de contraseñas.
- Clave secreta utilizada para generar OTP en el MFA.
- Registros de auditoría (intentos de acceso, uso de OTP, fechas, etc.)

MySQL garantiza integridad en los datos y permite consultas estructuradas mediante SQL, lo cual es ideal para sistemas académicos que manejan usuarios y privilegios.

4. Seguridad y autenticación

El sistema incorpora herramientas específicas para reforzar la seguridad:

- **bcrypt**: para cifrar las contraseñas antes de guardarlas en la base de datos.
- **JWT (JSON Web Tokens)**: para manejar la sesión del usuario una vez completado el MFA.
- **speakeasy (o equivalente)**: para generar y validar códigos OTP basados en tiempo (TOTP), compatibles con aplicaciones como Google Authenticator.
- **nodemailer** (si usas OTP por correo): para enviar códigos temporales de forma segura.

Estas herramientas conforman la columna vertebral del mecanismo de autenticación multifactor.

CRONOGRAMA Y ROLES

Semana	Actividades Principales	ROL
Semana 1	• Levantamiento de requerimientos • Diseño de arquitectura (frontend, backend y base de datos) • Modelado del flujo MFA • Diseño del modelo de datos	**Todo el equipo** (trabajo conjunto)
Semana 2	**Frontend:** Diseño UI/UX, maquetación, pantallas de login y OTP **Backend:** Configuración del servidor, rutas básicas, conexión BD **Pruebas/Documentación:** Preparación de casos de prueba, revisión del diseño	**Frontend**, **Backend**, **Tester/Documentador**
Semana 3	**Frontend:** Integración de formularios con API (login) **Backend:** Implementación lógica de autenticación (contraseña), bcrypt **Backend:** Implementación MFA (generación OTP por correo/TOTP) **Pruebas:** Pruebas funcionales iniciales del flujo login	**Frontend**, **Backend**, **Tester**
Semana 4	**Integración completa:** Frontend ↔ Backend ↔ Base de datos • Validación y verificación OTP • Rutas protegidas con JWT • Ajustes de UI y usabilidad	**Frontend**, **Backend**, **Tester**
Semana 5	**Tester:** Pruebas funcionales y de seguridad (fuerza bruta, OTP incorrecto, sesiones) **Correcciones finales:** Backend y Frontend solucionan errores detectados	**Tester**, **Frontend**, **Backend**

	Documentación final: Informe, diagramas y sustentación	

ROLES

Desarrollador Backend	Rusbell	API REST, autenticación, generación OTP, BD, seguridad
Desarrollador Frontend	Daniel	React, UI/UX, integración con API, vistas de login/OTP
Tester y Documentador	Wilson	Pruebas funcionales y de seguridad, informe, casos de uso