



UNIVERSIDAD TECNOLÓGICA DE TECAMACHALCO



TECNOLOGÍAS DE
LA INFORMACIÓN

ASIGNATURA

Dirección de Proyectos II

UNIDAD II

DOCENTE

ING. Juan Carlos Reyes Pedraza

PROPUESTA DE PROYECTO

Autenticación sin contraseña

INTEGRANTES

Citlalli Martínez Díaz
Marlem Rodríguez Torres
Wendy Viveros Bermúdez
José María Zambrano Zambrano

9ºA – RIC

CUATRIMESTRE

Mayo – Agosto 2024

FECHA: 23 de agosto 2024

Contenido

Descripción del proyecto	5
Documento de acreditación de la aceptación del producto	6
Descripción del Producto/Servicio/Resultado	6
Nombre del Producto/Servicio/Resultado:.....	6
Descripción:	6
Criterios de Aceptación	6
Resultados de las Pruebas.....	7
Pruebas Funcionales	7
Objetivo:	7
Detalles de las Pruebas:	7
Resultados:	8
Pruebas de Seguridad	8
Objetivo:	8
Detalles de las Pruebas:	8
Resultados:	8
Pruebas de Usuario	8
Objetivo:	8
Detalles de las Pruebas:	8
Resultados:	9
Pruebas de Integración.....	9
Objetivo:	9
Detalles de las Pruebas:	9
Resultados:	9
Conclusión de las Pruebas:	10

Documentación Entregada.....	10
Comentarios Adicionales del Cliente.....	10
Comentario 1	10
Comentario 2	10
Comentario 3	10
Declaración de Aceptación.....	11
Firmas de Aceptación	11
Reporte final del desempeño del proyecto	11
Análisis del Desempeño Pasado	11
Conclusión	12
Riesgos Identificados.....	12
Resultado:	12
Incidentes Recientes	13
Resultado:	13
Análisis del Presupuesto Ejercido.....	13
Detalles:	13
Análisis:.....	14
Cumplimiento del cronograma	14
Detalles:	14
Análisis:.....	14
Cumplimiento del Alcance Establecido	15
Detalles:	15
Análisis:.....	15
Lecciones aprendidas	15
Gerente del proyecto	15

Técnico en soporte	16
Desarrollo de Software	16
Especialista en seguridad	16
Acceso al repositorio del proyecto.....	16
Bitácoras individuales de trabajo.....	17

AUTENTICACIÓN SIN CONTRASEÑA

Descripción del proyecto

La Autenticación sin Contraseña es una metodología de seguridad que elimina las contraseñas tradicionales, utilizando métodos más seguros y convenientes para verificar la identidad del usuario. Este enfoque mejora significativamente la seguridad, reduciendo la vulnerabilidad a ataques como el phishing y el robo de credenciales, y mejora la experiencia del usuario.

el objetivo es desarrollar un sistema seguro y eficiente para la verificación de usuarios en una aplicación web. Para:

- Garantizar la seguridad y privacidad de los datos de los usuarios.
- Facilitar una experiencia de usuario intuitiva y eficiente.
- Proporcionar un sistema robusto que sea resistente a ataques comunes como la fuerza bruta, phishing y ataques de intermediario (MITM).

Este proyecto se desarrollará mediante el uso de la metodología Agile (Ágil) ya que es interactiva, enfocada en la colaboración, la flexibilidad y la entrega continua de valor, esta metodología es ideal debido a su capacidad para adaptarse rápidamente a cambios y nuevas tecnologías.

Para ello se utilizarán las siguientes tecnologías:

- **Backend:** se emplearán frameworks como Django(Python) o Node.js con Express para manejar las solicitudes del servidor, gestión de usuarios y la lógica de negocio.
- **Base de Datos:** se utilizarán base de datos relacionales como PostgreSQL, MySQL y MongoDB como sistema de gestión de las bases de datos para almacenar la información de los usuarios, incluyendo los hashes de las contraseñas.
- **Frontend:** se implementará con React o Angular para crear una interfaz de usuario interactiva y responsiva.
- **Seguridad:** uso de bibliotecas como bcrypt para el hashing de contraseñas, JWT para la gestión de tokens de sesión y Google Authenticator para la autenticación de dos factores.

Documento de acreditación de la aceptación del producto

Proyecto: Implementación de Autenticación sin Contraseña

Duración: 8 meses

Fecha de inicio: 09 de mayo de 2024

Fecha de Finalización: 13 de diciembre de 2024

Cliente: [Nombre del Cliente]

Gerente del Proyecto: Citlalli Martínez Díaz

Equipo de Proyecto: Marlem Rodríguez Torres – Técnico en soporte

Wendy Viveros Bermúdez – Desarrollo de Software

José María Zambrano Zambrano – Especialista en seguridad

Descripción del Producto/Servicio/Resultado

Nombre del Producto/Servicio/Resultado: Sistema de Autenticación sin Contraseña

Descripción:

El sistema de autenticación sin contraseña implementado permite a los usuarios acceder de manera segura a las plataformas de la organización sin necesidad de utilizar contraseñas tradicionales. En su lugar, se han integrado métodos de autenticación multifactor (MFA) utilizando biometría, tokens de seguridad y autenticación basada en dispositivos. El proyecto abarcó desde la planificación y diseño hasta el desarrollo, pruebas e implementación final del sistema.

Criterios de Aceptación

Los siguientes criterios fueron establecidos al inicio del proyecto para asegurar que el producto final cumpla con las expectativas:

1. **Funcionalidad Completa:** El sistema debe estar completamente funcional y ser capaz de autenticar a los usuarios sin contraseñas tradicionales en todas las plataformas designadas.
2. **Seguridad Mejorada:** La autenticación sin contraseña debe cumplir con los estándares de seguridad establecidos por la organización, incluyendo resistencia a ataques comunes como phishing y fuerza bruta.

3. **Experiencia del Usuario:** Los usuarios deben experimentar un proceso de autenticación fluido y rápido, mejorando su satisfacción en comparación con métodos de autenticación anteriores.
4. **Compatibilidad e Integración:** El sistema debe integrarse sin problemas con las aplicaciones existentes y ser compatible con todos los dispositivos soportados por la organización.
5. **Pruebas Exitosas:** El sistema debe haber pasado todas las fases de pruebas, incluyendo pruebas de usuario, pruebas de seguridad y pruebas de integración.
6. **Documentación Completa:** Toda la documentación técnica y de usuario debe estar completa y accesible.

Resultados de las Pruebas

Pruebas Funcionales

Objetivo: Verificar que todas las funcionalidades del sistema de autenticación sin contraseña operen según lo especificado en los requisitos del proyecto.

Detalles de las Pruebas:

- **Autenticación Multifactor (MFA):** Se probaron los métodos de autenticación multifactor, como biometría (huella digital y reconocimiento facial), tokens de seguridad y autenticación basada en dispositivos. Cada método fue probado en varios escenarios, incluyendo intentos de autenticación exitosa y fallida.
- **Gestión de Usuarios:** Se evaluaron las capacidades de gestión de usuarios, como el registro, recuperación de cuenta, y eliminación de usuarios. También se probaron las funciones de rol y permisos.
- **Compatibilidad con Aplicaciones:** Se verificó la integración del sistema con las aplicaciones críticas de la organización, asegurando que los usuarios puedan acceder sin contraseñas tradicionales.
- **Flujo de Trabajo:** Se revisaron los flujos de trabajo para asegurar que los procesos de autenticación no interfieran con las operaciones regulares de los usuarios.

Resultados:

- Todas las funcionalidades del sistema respondieron correctamente y cumplieron con las expectativas definidas en el documento de requisitos. No se encontraron fallos críticos ni interrupciones en los flujos de trabajo.

Pruebas de Seguridad

Objetivo: Asegurar que el sistema de autenticación sin contraseña sea resistente a amenazas de seguridad, protegiendo la información y el acceso de los usuarios.

Detalles de las Pruebas:

- **Pruebas de Penetración:** Se llevaron a cabo simulaciones de ataques cibernéticos comunes, como intentos de suplantación de identidad (phishing), ataques de fuerza bruta, y explotación de vulnerabilidades en la autenticación multifactor.
- **Evaluación de Criptografía:** Se revisaron los algoritmos criptográficos utilizados en el sistema, asegurando que cumplan con los estándares de la industria para la protección de datos sensibles.
- **Pruebas de Sesión:** Se verificó la seguridad de las sesiones de usuario, incluyendo la gestión de tokens, la expiración de sesiones, y la protección contra la captura de sesiones.

Resultados:

- El sistema demostró ser altamente seguro, resistiendo con éxito todos los ataques simulados. No se identificaron vulnerabilidades significativas, y las medidas de seguridad criptográficas fueron evaluadas como robustas.

Pruebas de Usuario

Objetivo: Evaluar la experiencia del usuario final al interactuar con el sistema de autenticación sin contraseña, asegurando facilidad de uso y satisfacción.

Detalles de las Pruebas:

- **Pruebas de Usabilidad:** Se realizaron pruebas de usabilidad con un grupo diverso de usuarios finales, evaluando la facilidad con la que pudieron utilizar los diferentes métodos de autenticación y navegar por la interfaz del sistema.

- **Pruebas de Accesibilidad:** Se incluyeron pruebas para asegurar que el sistema sea accesible para usuarios con discapacidades, evaluando la compatibilidad con lectores de pantalla y otros dispositivos de asistencia.
- **Encuestas de Satisfacción:** Después de las pruebas, se realizaron encuestas para medir la satisfacción general de los usuarios con el nuevo sistema, comparándolo con el método de autenticación anterior.

Resultados:

- La mayoría de los usuarios informaron una experiencia positiva, destacando la simplicidad y rapidez del proceso de autenticación. Los usuarios con discapacidades también pudieron utilizar el sistema sin problemas, cumpliendo con los estándares de accesibilidad.

Pruebas de Integración

Objetivo: Garantizar que el sistema de autenticación sin contraseña se integre perfectamente con la infraestructura existente y no interfiera con otras aplicaciones y servicios.

Detalles de las Pruebas:

- **Integración con Aplicaciones Existentes:** Se probó la compatibilidad e integración del sistema con aplicaciones críticas de la organización, como sistemas de gestión de contenido (CMS), plataformas de colaboración, y servicios en la nube.
- **Interoperabilidad con Dispositivos:** Se verificó que el sistema funcione en todos los dispositivos soportados, incluyendo computadoras de escritorio, laptops, tabletas y teléfonos inteligentes.
- **Pruebas de Carga:** Se realizaron pruebas de carga para evaluar el desempeño del sistema bajo condiciones de uso intensivo, asegurando que pueda manejar un gran número de autenticaciones simultáneas.

Resultados:

- El sistema se integró sin problemas con todas las aplicaciones y dispositivos probados. Las pruebas de carga demostraron que el sistema puede soportar un uso intensivo sin degradación significativa en el rendimiento.

Conclusión de las Pruebas: Todas las pruebas se completaron exitosamente, y el sistema cumple con los criterios de aceptación definidos.

Documentación Entregada

- Manual de Usuario
- Guía de Integración
- Documentación Técnica
- Plan de Continuidad y Soporte

Comentarios Adicionales del Cliente

Comentario 1

- "El sistema de autenticación sin contraseña ha superado nuestras expectativas en términos de seguridad y facilidad de uso. La implementación fue manejada de manera profesional, con mínima interrupción para nuestros usuarios. Apreciamos especialmente la rápida respuesta del equipo a nuestras preguntas durante las fases de prueba. Estamos satisfechos con el resultado y confiamos en que este sistema mejorará significativamente la seguridad de nuestra organización."

Comentario 2

- El proceso de implementación fue generalmente exitoso, aunque tuvimos algunos desafíos iniciales relacionados con la compatibilidad en dispositivos más antiguos. Sin embargo, el equipo abordó estos problemas rápidamente, lo que permitió cumplir con el cronograma establecido. En general, estamos contentos con el sistema y esperamos trabajar juntos en futuras actualizaciones."

Comentario 3



- El proyecto fue ejecutado con un alto nivel de profesionalismo y atención al detalle. El equipo fue muy receptivo a nuestros comentarios y ajustó el enfoque según nuestras necesidades. Nos impresionó especialmente la

calidad de la documentación proporcionada, que será muy útil para nuestro equipo de TI en el futuro. Estamos muy satisfechos con el producto final."

Declaración de Aceptación

Por medio del presente documento, se certifica que el sistema de autenticación sin contraseña desarrollado e implementado por "Technotec" ha sido revisado y cumple con todos los criterios de aceptación previamente acordados. El cliente [Nombre del Cliente] acepta formalmente el sistema como satisfactorio y considera que ha cumplido con todos los objetivos y requerimientos establecidos en el alcance del proyecto.

Firmas de Aceptación

Nombre	Cargo	Firma	Fecha
[Nombre del Cliente]	Cliente	_____	[15/12/2024]
Citlalli Martínez Díaz	Gerente del Proyecto		15/12/2024]
Marlem Rodríguez Torres	Departamento de TI		15/12/2024]

Reporte final del desempeño del proyecto

Proyecto: Implementación de Autenticación sin Contraseña

Duración: 8 meses

Fecha de inicio: 09 de mayo de 2024

Fecha de Finalización: 13 de diciembre de 2024

Cliente: [Nombre del Cliente]

Gerente del Proyecto: Citlalli Martínez Díaz

Equipo de Proyecto: Marlem Rodríguez Torres – Técnico en soporte

Wendy Viveros Bermúdez – Desarrollo de Software

José María Zambrano Zambrano – Especialista en seguridad

Análisis del Desempeño Pasado

Durante el curso del proyecto, el equipo de desarrollo trabajó en varias fases clave: planificación, diseño, desarrollo, pruebas e implementación. A lo largo de estas

fases, el desempeño del proyecto fue monitoreado mediante indicadores clave de desempeño (KPIs) como:

- **Cumplimiento de Hitos:** Todos los hitos críticos se cumplieron dentro de los plazos establecidos, con una desviación mínima en las entregas de ciertos componentes debido a ajustes de último momento en los requisitos del cliente.
- **Productividad del Equipo:** El equipo mantuvo una alta productividad, completando la mayor parte de las tareas dentro de los plazos previstos y con alta calidad, lo que se reflejó en la ausencia de reprocesos significativos.
- **Satisfacción del Cliente:** El cliente expresó su satisfacción durante las revisiones periódicas, destacando la claridad en la comunicación y la calidad de los entregables.

Conclusión: El desempeño general fue sólido, con todos los objetivos principales alcanzados dentro de los parámetros planificados.

Riesgos Identificados

A lo largo del proyecto, se identificaron varios riesgos que fueron gestionados mediante un plan de respuesta efectivo:

- **Riesgo de Integración:** Existía la posibilidad de que la nueva solución de autenticación sin contraseña no se integrara adecuadamente con las aplicaciones existentes. Mitigación: Pruebas de integración exhaustivas y la colaboración cercana con el departamento de TI mitigaron este riesgo.
- **Riesgo de Resistencia al Cambio:** Algunos usuarios podrían haber mostrado resistencia al cambio de sistema, afectando la adopción del nuevo método de autenticación. Mitigación: Se llevaron a cabo sesiones de formación y se proporcionaron recursos de apoyo para facilitar la transición.
- **Riesgo de Seguridad:** Dado que la autenticación sin contraseña es una tecnología relativamente nueva, existía el riesgo de vulnerabilidades de seguridad desconocidas. Mitigación: Se realizaron pruebas de seguridad rigurosas y se implementaron múltiples capas de protección.

Resultado: Todos los riesgos identificados fueron manejados con éxito, y no se materializaron en problemas significativos durante la implementación.

Incidentes Recientes

Al cierre del proyecto, se presentaron dos incidentes notables:

- **Incidente de Compatibilidad:** Durante la fase final de pruebas, se identificó un problema de compatibilidad con un dispositivo móvil específico utilizado por un pequeño grupo de usuarios. Este incidente se resolvió mediante una actualización rápida del sistema, que solucionó el problema sin afectar el cronograma general.
- **Retraso en la Documentación:** Se produjo un pequeño retraso en la entrega de la documentación técnica final debido a la necesidad de incluir ajustes de última hora en la configuración del sistema. El equipo de documentación trabajó horas adicionales para cumplir con los plazos ajustados.

Resultado: Ambos incidentes fueron gestionados rápidamente y no afectaron de manera significativa el éxito del proyecto.

Análisis del Presupuesto Ejercido

Presupuesto	Total	Asignado:	\$50,000	MXN
--------------------	--------------	------------------	----------	-----

Presupuesto Ejercido: \$48,500 MXN

Detalles:

- **Recursos Humanos:** \$25,000 MXN
Costos relacionados con el equipo de proyecto, incluyendo salarios y honorarios de los especialistas involucrados en el desarrollo e implementación del sistema de autenticación sin contraseña. Este rubro representó el 50% del presupuesto total asignado.
- **Tecnología y Herramientas:** \$12,000 MXN
Comprende los costos de licencias de software necesarias para el desarrollo y pruebas del sistema, así como la adquisición de hardware adicional para garantizar la compatibilidad y pruebas en diferentes dispositivos.
- **Capacitación y Formación:** \$7,000 MXN
Incluye los costos de las sesiones de formación para el equipo técnico y los usuarios finales, cubriendo tanto el desarrollo de material de capacitación como la realización de talleres y seminarios.

- **Imprevistos:** \$4,500 MXN
Gastos en incidentes no previstos, como la solución de problemas de compatibilidad y pequeñas modificaciones de último minuto que fueron necesarias para asegurar el correcto funcionamiento del sistema en todos los entornos.

Análisis:

El proyecto finalizó ligeramente por debajo del presupuesto total asignado, con un ahorro del 3% debido a una gestión eficiente de recursos y la optimización de ciertos procesos. Las variaciones en el presupuesto se debieron principalmente a gastos menores en la adquisición de licencias y recursos de formación, lo que permitió redirigir fondos hacia la resolución de imprevistos sin exceder el presupuesto total.

Cumplimiento del cronograma

Duración **Planificada:** 8 meses

Duración Real: 8 meses

Detalles:

- **Cumplimiento de Hitos:**
Los principales hitos del proyecto, que incluyen las fases de planificación, desarrollo, pruebas e implementación, se cumplieron dentro del marco de tiempo previsto. Cada fase fue completada de acuerdo con el cronograma, lo que permitió mantener el flujo de trabajo sin interrupciones significativas.
- **Retrasos:**
Aunque hubo pequeños retrasos en la fase final de documentación, estos no afectaron la fecha de finalización general del proyecto. El equipo de documentación ajustó su plan de trabajo para cumplir con los plazos, asegurando que todo el material necesario estuviera disponible para la entrega final.

Análisis:

El proyecto fue completado a tiempo, con una adherencia cercana al cronograma original. Las desviaciones menores fueron gestionadas de manera efectiva, y no tuvieron impacto en la fecha de entrega final. Este éxito en la gestión del tiempo

refleja una planificación cuidadosa y una ejecución disciplinada, lo que permitió alcanzar los objetivos del proyecto dentro del período previsto.

Cumplimiento del Alcance Establecido

Alcance Inicial: Implementación de un sistema de autenticación sin contraseña para mejorar la seguridad y la experiencia del usuario.

Alcance Final: El sistema de autenticación sin contraseña se implementó con éxito, cumpliendo con todos los requisitos definidos en la fase de planificación. Se incluyeron todas las características especificadas, como autenticación multifactor, integración con sistemas existentes, y cumplimiento con los estándares de seguridad.

Detalles:

- **Funcionalidades Entregadas:** Todas las funcionalidades planificadas fueron implementadas y validadas.
- **Satisfacción del Cliente:** El cliente confirmó que el sistema cumple con sus expectativas y con el alcance acordado inicialmente.

Análisis: El proyecto cumplió completamente con el alcance establecido, entregando todas las funcionalidades y resultados esperados sin desviaciones significativas.

Lecciones aprendidas

Gerente del proyecto

- Desde el principio, vimos que las contraseñas eran un punto débil en nuestra infraestructura. Implementar una autenticación sin contraseña nos parecía esencial para reducir riesgos, especialmente contra ataques de phishing y robo de credenciales. Nos aseguramos desde el principio, vimos que las contraseñas eran un punto débil en nuestra infraestructura. Implementar una autenticación sin contraseña nos parecía esencial para reducir riesgos, especialmente contra ataques de phishing y robo de credenciales.

Técnico en soporte

- Exploramos varios métodos, desde autenticación biométrica hasta claves de seguridad físicas. Al final, optamos por una combinación que nos dio el mejor equilibrio entre seguridad y usabilidad. Nos aseguramos de que el proceso fuera lo mejor para los usuarios

Desarrollo de Software

- Integrar el nuevo sistema no fue sencillo, pero logramos adaptarlo bien a nuestra arquitectura existente. Nos enfocamos en realizar pruebas exhaustivas para asegurarnos de que funcionara sin problemas en diferentes escenarios. Probar desde distintos dispositivos y en condiciones de red variables fue crucial

Especialista en seguridad

- Una de las lecciones más importantes que aprendí durante este proyecto fue la necesidad de ver más allá de la tecnología. Al principio, me enfoqué en las características técnicas de la autenticación sin contraseña y cómo podía fortalecer nuestras defensas contra ataques. Sin embargo, a medida que avanzaba el proyecto, me di cuenta de que la seguridad no solo depende de la robustez del sistema, sino también de cómo se integra con las operaciones diarias y la aceptación por parte de los usuarios.

Acceso al repositorio del proyecto

<https://github.com/dcitolalli98/AuCcontrase-a.git>



Bitácoras individuales de trabajo

AGENDA INDIVIDUAL DE TRABAJO

NOMBRE DEL PROYECTO:	Plan De Ciberseguridad	NOMBRE (SIGLAS) DEL PROYECTO	CLAVE DEL	PC
PROJECT MANAGER DEL PROYECTO	Citlalli Martínez Díaz			

NOMBRE DEL PARTICIPANTE	Marlem Rodríguez Torres	ROL:	Desarrollador de Software
-------------------------	-------------------------	------	---------------------------

FECHA	ACTIVIDAD	PRODUCTO ENTREGABLE
04/08/2024	Identificación de Riesgos	Reporte
09/08/2024	Análisis de desempeños pasados	Informe de Desempeño
19/08/2024	Revisión de Tecnologías y Herramientas	Reporte de Inventario
16/08/2024	Identificación de Incidentes	Informe


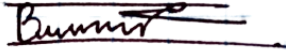
	
FIRMA PROJECT MANAGER	FIRMA PARTICIPANTE

AGENDA INDIVIDUAL DE TRABAJO

NOMBRE DEL PROYECTO:	Plan De Ciberseguridad	NOMBRE (SIGLAS) DEL PROYECTO	CLAVE DEL	PC
PROJECT MANAGER DEL PROYECTO	Citlalli Martínez Díaz			

NOMBRE DEL PARTICIPANTE	Wendy Viveros Bermúdez	ROL:	Desarrollador de Software
-------------------------	------------------------	------	---------------------------

FECHA	ACTIVIDAD	PRODUCTO ENTREGABLE
08/08/2024	Reporte de Gestión de Usuarios	Reporte
13/08/2024	Compatibilidad con Aplicaciones	Reporte de Integración
05/08/2024	Pruebas de usuario	Documento de Evaluaciones
20/08/2024	Encuesta de satisfacción	Reporte de Resultados



	
FIRMA PROJECT MANAGER	FIRMA PARTICIPANTE

AGENDA INDIVIDUAL DE TRABAJO

NOMBRE DEL PROYECTO:	Autenticación sin contraseña	NOMBRE (SIGLAS) DEL PROYECTO	CLAVE DEL	ASC
PROJECT MANAGER DEL PROYECTO	Citlalli Martínez Díaz			

NOMBRE DEL PARTICIPANTE	José María Zambrano Zambrano	ROL:	Especialista en Seguridad
-------------------------	------------------------------	------	---------------------------

FECHA	ACTIVIDAD	PRODUCTO ENTREGABLE
13/08/2024	Pruebas de Integración	Reporte Compatibilidad
07/08/2024	Pruebas de carga	Reporte de Evaluación del Desempeño del Sistema Bajo Uso Intensivo
18/8/2024	Interoperabilidad con Dispositivos	Informe de Verificación
03/08/2024	Pruebas de seguridad	Reporte de Simulaciones Cibernéticas
02/08/2024	Evaluaciones de Criptografía	Entrega de Algoritmos Criptográficos Utilizados en el Sistema
06/08/2024	Pruebas de Sesión	Informe de la Verificación Sobre los Usuarios



	
FIRMA PROJECT MANAGER	FIRMA PARTICIPANTE

AGENDA INDIVIDUAL DE TRABAJO

NOMBRE DEL PROYECTO:	Plan De Ciberseguridad	NOMBRE (SIGLAS) DEL PROYECTO	CLAVE DEL	PC
PROJECT MANAGER DEL PROYECTO	Citlalli Martínez Díaz			

NOMBRE DEL PARTICIPANTE	Citlalli Martínez Díaz	ROL:	Gerente del proyecto
--------------------------------	------------------------	-------------	----------------------

FECHA	ACTIVIDAD	PRODUCTO ENTREGABLE
19/08/2024	Análisis del presupuesto ejercido	Informe de presupuesto
20/08/2024	Cumplimiento del cronograma	Reporte
20/08/2024	Cumplimiento del Alcance establecido	Reporte
21/08/2024	Informe Final del Desempeño	Informe

	
FIRMA PROJECT MANAGER	FIRMA PARTICIPANTE