REVISTA CIENTÍFICA
CONECTIVIDAD
Instituto Tecnológico Superior Universitario Rumiñahui

Fecha de recepción: 03 / 09 / 2025
Fecha de aceptación: 18 / 11 / 2025
Fecha de publicación: 20 / 02 / 2026

Artículo Científico

Sistema de validación mediante SMS integrado a un sistema web de control de ventas a crédito

System of validation via SMS integrated into a web-based credit sales management system

Anthony JeanPaul Reyes Risco[1], Ronald David Villacorta Carranza[2], Joseph Luis Rodriguez Bermudez[3], Alberto Carlos Mendoza de los Santos[4]

[1] Universidad Nacional de Trujillo, areyesri@unitru.edu.pe, La Libertad - Perú
[2] Universidad Nacional de Trujillo, rvillacortac@unitru.edu.pe, La Libertad - Perú
[3] Universidad Nacional de Trujillo, jrodriguezbe@unitru.edu.pe, La Libertad - Perú
[4] Universidad Nacional de Trujillo, amendozad@unitru.edu.pe, La Libertad - Perú

Autor para correspondencia: areyesri@unitru.edu.pe

RESUMEN

Este estudio presenta la implementación y evaluación de un mecanismo de validación de accesos mediante SMS en un sistema web de gestión de ventas a crédito orientado a microempresas comerciales. El objetivo principal fue reforzar la seguridad en los procesos de autenticación, garantizando que únicamente los usuarios legítimos puedan acceder a sus cuentas. La metodología empleada fue de tipo aplicada preexperimental, utilizando un diseño pre-prueba y post-prueba con un solo grupo. El sistema fue desarrollado bajo arquitectura cliente-servidor con tecnologías Spring Boot, Angular y MySQL, integrando un servicio de envío de códigos de verificación (OTP) vía SMS. Los resultados evidenciaron una tasa de validación exitosa del 100% en accesos legítimos y un bloqueo efectivo del 100% en intentos de suplantación; con un tiempo promedio de validación de 4.8 segundos. Estos hallazgos confirman que la autenticación basada en SMS constituye una solución práctica, segura y de bajo costo para microempresas, fortaleciendo la ciberseguridad y la confianza de los usuarios en la gestión digital de créditos.

Palabras clave: Validación de accesos; SMS; Autenticación OTP; Seguridad de la información; Microempresas.

ABSTRACT

This study presents the implementation and evaluation of an SMS-based access validation mechanism in a web-based credit sales management system for commercial microenterprises. The main objective was to strengthen security in the authentication processes, ensuring that only legitimate users can access their accounts. The methodology employed was a pre-experimental approach, using a pre-test and post-test design with a single group. The system was developed using a client-server architecture with Spring Boot, Angular, and MySQL technologies, integrating an SMS verification code delivery service (OTP). The results showed a 100% successful validation rate for legitimate access and a 100% effective blocking of impersonation attempts; with an average validation time of 4.8 seconds. These findings confirm that SMS-based authentication constitutes a practical, secure, and low-cost solution for microenterprises, strengthening cybersecurity and user confidence in digital credit management.

Keywords: Access validation; SMS; OTP Authentication; Information security; Micro-enterprises.

Citas
Reyes Risco, A. J., Villacorta Carranza, R. D., Rodriguez Bermudez, J. L., & Mendoza de los Santos, A. C. (2026). Sistema de validación mediante SMS integrado a un sistema web de control de ventas a crédito . *CONECTIVIDAD*, *7*(1), 514–529. https://doi.org/10.37431/conectividad.v7i1.403

Fecha de recepción: 03 / 09 / 2025
Fecha de aceptación: 18 / 11 / 2025
Fecha de publicación: 20 / 02 / 2026

1. INTRODUCCIÓN

En Perú, las pequeñas y medianas empresas minoristas (Pymes) siguen siendo un soporte económico y social; aunque muchas funcionan con escasa digitalización y registran ventas a crédito manualmente (fiado). Este método provoca errores contables, pérdidas de datos, dificultad para supervisar saldos y alertas, y altos índices de morosidad que afectan la liquidez y viabilidad del negocio (Rivas Oloya, 2023). La digitalización en cobranzas mejora la eficiencia y permite implementar controles de seguridad para proteger la información financiera; así, la adopción de métodos robustos de autenticación es esencial para confiar datos de clientes a plataformas digitales (National Institute of Standards and Technology, 2020).

En el ámbito de la autenticación digital, se reconoce que los sistemas multifactor (MFA/2FA) aumentan notablemente la protección frente a contraseñas simples (Suleski et al., 2023). Entre estos, el envío de códigos de un solo uso (OTP) por SMS es muy usado por su facilidad y bajo costo, especialmente en ambientes con gran acceso a telefonía móvil y escasos recursos tecnológicos (OWASP Foundation, 2022). No obstante, la literatura señala limitaciones y riesgos del SMS-OTP, como por ejemplo problemas en roaming; ataques locales por apps maliciosas; generación predecible de OTP y vulnerabilidades como SS7 o SIM swapping (Lei et al., 2021; Ma et al., 2021). Estas limitaciones no descartan el uso de SMS como segundo factor, pero exigen diseños que atenúen sus debilidades (National Institute of Standards and Technology, 2020; OWASP Foundation, 2022).

Partiendo de este contexto, este estudio no busca innovar teóricamente el OTP por SMS, sino evaluar y adaptar un sistema seguro y práctico para microempresas con ventas a crédito; nuestros objetivos serán (1) crear un mecanismo 2FA que combine OTP vía SMS con un segundo canal el cual será WhatsApp para aumentar disponibilidad y resiliencia en movilidad y roaming; (2) validar experimentalmente que esta solución reduce errores de envío, impide suplantaciones y es viable tecnológica y operativamente para negocios pequeños. Se eligió WhatsApp como canal redundante debido a la variabilidad en entrega de SMS y evidencias del sector que muestran mejor entrega usando mensajería OTT (como APIs de Twilio) en condiciones adversas.

2. MATERIALES Y MÉTODOS

Fecha de recepción: 03 / 09 / 2025
Fecha de aceptación: 18 / 11 / 2025
Fecha de publicación: 20 / 02 / 2026

2.1. Diseño de la investigación

La presente investigación es de enfoque práctico y preexperimental (con diseño pre-test; post-test a un solo grupo), concebido como una prueba de concepto. Este diseño es apropiado para estudios que buscan comprobar la efectividad de un sistema de autenticación en condiciones controladas y ha sido empleado anteriormente en investigaciones sobre autenticación multifactor en entornos distribuidos (Ometov et al., 2018; Meyer et al., 2023). Aunque la metodología limita la generalización de los resultados, permite evidenciar claramente la eficiencia del mecanismo de doble factor para bloquear accesos ilegítimos y validar accesos autorizados.

2.2. Entorno técnico y desarrollo

Para la implementación del sistema, se empleó una arquitectura cliente-servidor. El Back-end fue desarrollado en Spring Boot 3.5.6 (Java); gestionando la lógica de autenticación, generación y validación de códigos OTP así también como la conexión a la base de datos. El Front-end fue desarrollado usando Angular 16 (TypeScript); para formularios de ingreso de credenciales y validación de códigos. La Base de datos fue hecha usando MySQL 8.0 para el almacenamiento de las credenciales, números telefónicos y registros de acceso.

Para la incorporación del sistema de códigos OTP, se empleó únicamente la plataforma Twilio como proveedor externo, que brinda tanto al servicio de mensajes SMS convencional como el envío de mensajes por WhatsApp desde un único entorno de desarrollo. Cabe resaltar que, aunque ambos canales se administran mediante Twilio, presentan diferencias en su naturaleza técnica; el SMS no es un servicio OTT, dado que se transmite a través de la red celular administrada por los operadores móviles; mientras que WhatsApp sí es un servicio OTT, ya que envía los mensajes mediante internet y la infraestructura propia de la aplicación. En la Tabla 1 se muestra una tabla donde se resume la configuración técnica usada en el sistema.

Tabla 1. Configuración técnica del sistema

Componente	Tecnología/Versión	Descripción
Back-end	Spring Boot 3.5.6	Lógica de autenticación y OTP
Front-end	Angular 16	Interfaz de validación
Base de datos	MySQL 8.0	Almacenamiento de usuarios y accesos
OTP Provider	Twilio (SMS + WhatsApp)	Envío de códigos OTP

Fuente: Elaboración propia.

Fecha de recepción: 03 / 09 / 2025
Fecha de aceptación: 18 / 11 / 2025
Fecha de publicación: 20 / 02 / 2026

2.3. Procedimiento de validación por SMS

El proceso de verificación se organizó en dos etapas. Primero, el usuario introducía sus credenciales (usuario y clave). Si eran correctas, el sistema creaba un código OTP de 6 dígitos numéricos, válido durante 2 minutos y con política de un solo uso.

El OTP se enviaba inicialmente por SMS como canal principal. Si el usuario no lograba validarlo, el sistema no enviaba automáticamente un segundo mensaje; en cambio, después de un lapso de 5 segundos, se activaba en la interfaz un botón que permitía reenviar el mismo código al número registrado mediante WhatsApp. Así, se aseguró que el SMS funcionara como primera opción y WhatsApp como canal alternativo bajo demanda, especialmente útil en casos de roaming o fallos en la red móvil.

A diferencia de otros sistemas, este mecanismo no definió un límite máximo de intentos por usuario, ya que cada OTP expiraba automáticamente al cumplirse los 2 minutos. Si el código vencía, el proceso debía iniciarse nuevamente con la creación de un nuevo OTP.

Este método de autenticación de doble factor es ampliamente valorado como una defensa eficaz contra accesos no autorizados y suplantaciones de identidad, incluso en situaciones donde las credenciales han sido vulneradas (Bartłomiejczyk y El Fray, 2024).

2.4. Escenarios evaluados

La evaluación del sistema se dividió en dos bloques principales: pruebas funcionales y pruebas de seguridad. En el bloque funcional se consideraron tres casos representativos, véase Tabla 2. Primero, se analizó el acceso legítimo vía SMS, donde un usuario autorizado ingresaba sus datos correctamente, recibía el OTP por SMS y lo confirmaba en la plataforma. Segundo, se evaluó el acceso fraudulento, en el que un tercero usaba credenciales válidas de otro usuario, pero al no disponer del dispositivo registrado, no lograba completar la autenticación con OTP. Finalmente, se probó la falla en SMS y acceso exitoso por WhatsApp, escenario en el que el usuario legítimo no recibía el código por SMS, pero podía activar la opción de envío vía WhatsApp tras cinco segundos, validando el mismo código.

En el bloque de seguridad, el sistema fue sometido a pruebas de penetración automatizadas con el software OWASP ZAP, enfocadas en los endpoints críticos de autenticación, /login y /api/auth/verify-sms. Se realizó un escaneo activo generando múltiples solicitudes con

Fecha de recepción: 03 / 09 / 2025
Fecha de aceptación: 18 / 11 / 2025
Fecha de publicación: 20 / 02 / 2026

cargas maliciosas para simular ataques de fuerza bruta sobre la validación OTP, intentos de inyección SQL, incluyendo técnicas blind, y pruebas de Cross-Site Scripting (XSS) reflejado y almacenado; véase Tabla 3. Estas pruebas se ejecutaron en un entorno local controlado, con SMS desactivados para evitar costos, ya que el objetivo era evaluar la resistencia de los endpoints frente a ataques automatizados.

Tabla 2. Escenarios funcionales evaluados

Escenario	Descripción	Resultado esperado
Acceso válido por SMS	El usuario legítimo ingresa usuario y contraseña correctos, recibe el OTP por SMS y valida el código en el sistema.	Acceso permitido
Acceso inválido (suplantación)	Un tercero utiliza credenciales correctas de otra persona. El OTP (SMS o WhatsApp) se entrega al dispositivo del usuario legítimo, por lo que el suplantador no puede confirmar el inicio de sesión.	Acceso denegado
Falla de SMS y acceso válido por WhatsApp	El usuario legítimo no recibe el OTP por SMS; solicita el código mediante WhatsApp y valida el código recibido por esa vía.	Acceso permitido

Fuente: Elaboración propia.

Tabla 3. Escenarios de seguridad evaluados

Escenario	Descripción	Resultado esperado	Método / Criterio
Fuerza bruta	Intentar adivinar OTP/probar muchos códigos consecutivos generados con la expresión regular ([0-9])\d{5,5}.	Bloqueo de las solicitudes con códigos inválidos	1000 intentos automatizados → esperar respuestas 400
Inyección SQL	Enviar payloads de MySQL para inferir datos.	No se puede extraer	Suite de pruebas integrado en ZAP → no hay filtración de información.
XSS (Cross-Site Scriping)	Inyectar script en campos mostrados en páginas de gestión.	Inputs escapados; no ejecución JS.	Ataques XSS → reflejado y almacenado con OWASP ZAP

Fuente: Elaboración propia.

Este método garantiza que únicamente el usuario autorizado tenga el control de acceso; en concordancia con las prácticas óptimas de seguridad señaladas por otros investigadores (Timko et al., 2023).

3. RESULTADOS

3.1. Desempeño ante pruebas realizadas para los escenarios planteados

Se empleó el software OWASP ZAP para pruebas de seguridad web, realizadas con autorización.

Fecha de recepción: 03 / 09 / 2025
Fecha de aceptación: 18 / 11 / 2025
Fecha de publicación: 20 / 02 / 2026

El proyecto fue descargado desde el repositorio GitHub en donde se encuentra alojado y fue ejecutado localmente; separada de la configuración estándar del proyecto. Además, los códigos OTP se generaban en consola, sin enviarse por SMS o WhatsApp, esto con el fin práctico de facilitar las pruebas. Se llevaron a cabo tres tipos de análisis: Ataque de fuerza bruta, pruebas de inyección SQL y pruebas XSS (Cross-Site Scriping); en la Tabla 4 se muestra un resumen de los resultados obtenidos de las pruebas realizadas.

Tabla 4. Resumen de pruebas realizadas

Prueba	Códigos	RTT (tiempo de ida y vuelta promedio)	Intentos
Fuerza bruta	400	139	1000
SQLi	400 y 401	102,4	520
XSS	500 y 202	184	223

Fuente: Elaboración propia.

3.1.1. Fuerza bruta

Se atacó el endpoint de verificación del código OTP generado con la expresión regular ([0-9])\d{5,5}, realizando un total de 1000 intentos. Solo se registraron respuestas HTTP 400 (Bad Request); esto se da por diferentes factores como sintaxis de petición mal formada, solicitud inválida de enmarcado de mensajes o enrutamiento engañoso de peticiones (400 Bad Request, 2025). No se obtuvo acceso al sistema mediante estos intentos.

Como interpretación podemos rescatar que esto sugiere que la API tiene validaciones server-side que previenen la aceptación de la gran mayoría de entradas automáticas. Esto evidencia la validación inicial básica. Por la naturaleza de los códigos OTP existe seguridad por la caducidad y único uso de los códigos. Sin embargo, se recomienda bloqueos por variedad de intentos, lo cual puede ser explotado.

3.1.2. QL Injection (MySQL)

Se lanzó un escaneo activo con política de SQLi dentro de la propia aplicación de ZAP a los endpoints del inicio de sesión y de la verificación del código OTP. Se pudo observar que el endpoint “http://localhost:4200/verify_sms” devolvió respuestas HTTP 400 y el endpoint “http://localhost:4200/login”, respuestas HTTP 401 (Unauthorized). De esto se puede rescatar que las inyecciones SQL no fueron tratadas como consultas válidas; mostrando que la capa de

Fecha de recepción: 03 / 09 / 2025
Fecha de aceptación: 18 / 11 / 2025
Fecha de publicación: 20 / 02 / 2026

autenticación funciona correctamente. No hay evidencia de explotación exitosa y el software no detectó mensajes filtrados con las pruebas automatizadas. El uso de consultas parametrizadas contribuyó a esta protección.

Los resultados obtenidos, con respuestas predominantes HTTP 400 en /verify_sms y 401 en /login frente a cargas maliciosas de inyección, evidencian empíricamente que la capa de autenticación y las validaciones del lado servidor funcionan como primera línea de defensa. En cuanto a los escenarios funcionales, este comportamiento sostiene directamente el caso de acceso no autorizado (suplantación): incluso si un atacante tuviera credenciales o intentara manipular solicitudes para ejecutar consultas, las peticiones mal formateadas o no autorizadas son rechazadas antes de cualquier validación del OTP. Por lo tanto, la falta de explotación exitosa por SQLi fortalece la conclusión de que el proceso de verificación del OTP (ya sea por SMS o WhatsApp) constituye una barrera eficaz para bloquear accesos ilegítimos al sistema.

3.1.3. XSS (fuzzing en edición de perfil - admin)

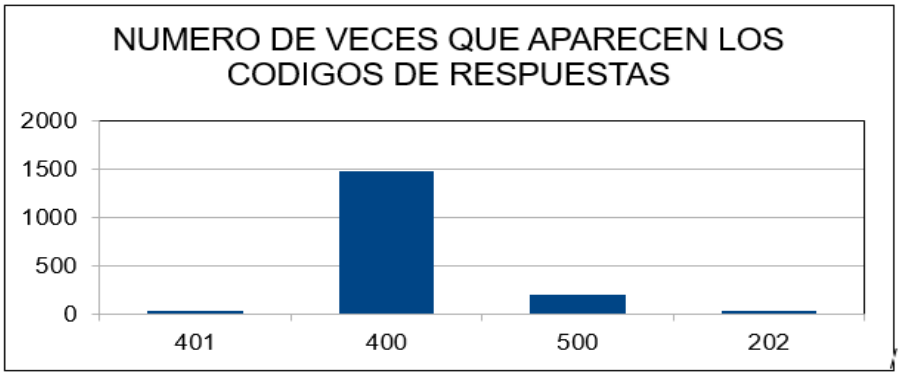
Por último, se ingresó con la cuenta de administrador validándose correctamente, y se navegó a la opción de edición del nombre de perfil, en esa entrada se realizó el ataque con datos de un fuzzer de ZAP. Fueron un total de 224 solicitudes. Se detectaron 33 respuestas reflejadas alrededor del 14.7%. Y además se devolvió el hash de la contraseña del usuario en el cuerpo JSON; el campo de código SMS apareció como null.

La presencia de respuestas reflejadas indica que ciertos campos se retornan sin un adecuado encoding o escape en el servidor o en la plantilla de renderizado, evidenciando una vulnerabilidad distinta al código OTP. Esto permite que datos del usuario, incluido el hash de la contraseña, sean expuestos al editar la información, lo cual constituye una falla grave de filtrado de datos (data leakage). Sin embargo, resalta la importancia de los códigos OTP y la autenticación robusta. El valor “null” en el campo SMS impidió la explotación de esa funcionalidad, aunque alerta sobre posibles ataques internos o descifrado de datos interceptados una vez que los usuarios están autenticados.

En la Figura 1 se muestra un gráfico resumen de los códigos de respuesta.

Fecha de recepción: 03 / 09 / 2025
Fecha de aceptación: 18 / 11 / 2025
Fecha de publicación: 20 / 02 / 2026

Figura 1. Resumen de los códigos de respuesta.

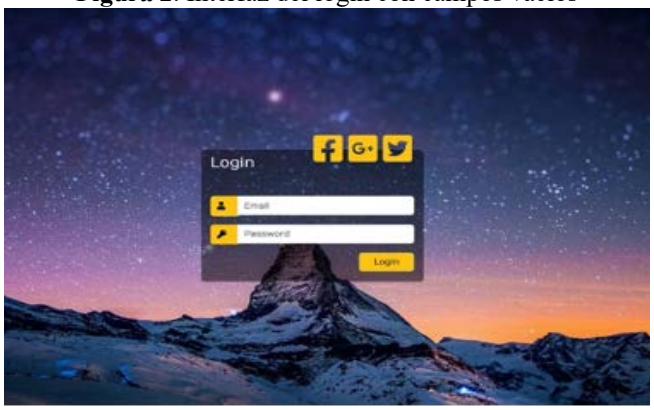


Fuente: Elaboración propia.

3.2. Flujo visual del procedimiento de verificación del código OTP

Se documentó el flujo visual del proceso de verificación híbrido (SMS + WhatsApp) en la plataforma web, mostrando capturas de pantalla que ilustran las etapas fundamentales de la autenticación de doble factor, evidenciando tanto su correcto funcionamiento como la secuencia lógica de interacción entre el usuario y el sistema. En la Figura 2 se muestra la pantalla inicial de ingreso al sistema, donde los campos de usuarios y contraseña están vacíos.

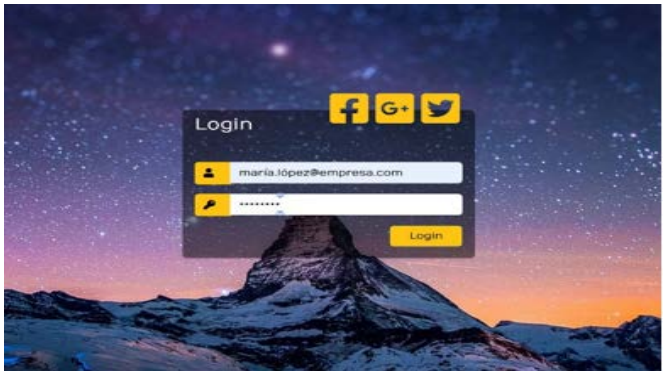
Figura 2. Interfaz del login con campos vacíos



Fuente: Elaboración propia.

En la Figura 3 se muestran estos campos llenados con las credenciales del usuario autorizado.

Figura 3. Interfaz de login con credenciales ingresadas



Fuente: Elaboración propia.

Fecha de recepción: 03 / 09 / 2025
Fecha de aceptación: 18 / 11 / 2025
Fecha de publicación: 20 / 02 / 2026

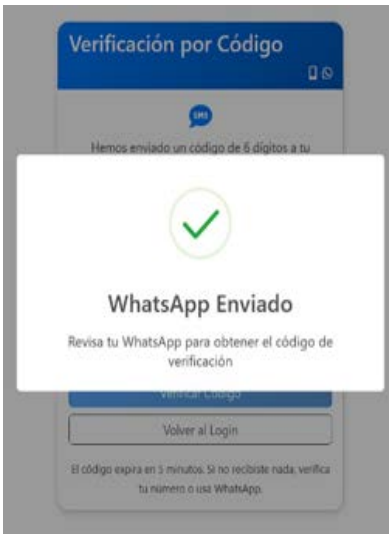
Después de validar las credenciales, el sistema notifica al usuario mediante una ventana emergente que se envió un código de verificación por SMS al número registrado, como muestra la Figura 4. Esta ventana incluye la opción "¿Problemas con SMS? Prueba por WhatsApp" y un botón que se activa tras 5 segundos, permitiendo solicitar el código por ese canal alternativo.

Figura 4. Ventaja emergente indicando envío de código SMS y opción de validación por WhatsApp

Fuente: Elaboración propia.

Si el usuario elige el envío por WhatsApp, la plataforma muestra una pantalla confirmando el procedimiento, como se observa en la Figura 5.

Figura 5. Mensaje de confirmación de envío del código OTP a WhatsApp

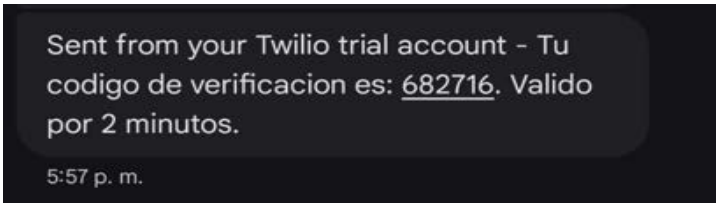


Fuente: Elaboración propia.

La Figura 6 muestra el mensaje SMS recibido en el dispositivo móvil con el código OTP válido por 2 minutos, y la Figura 7 muestra el mensaje de WhatsApp con el mismo código y validez.

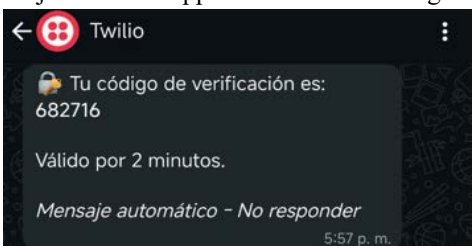
Fecha de recepción: 03 / 09 / 2025
Fecha de aceptación: 18 / 11 / 2025
Fecha de publicación: 20 / 02 / 2026

Figura 6. Mensaje SMS recibido con el código de verificación



Fuente: Elaboración propia.

Figura 7. Mensaje de WhatsApp recibido con el código de verificación



Fuente: Elaboración propia.

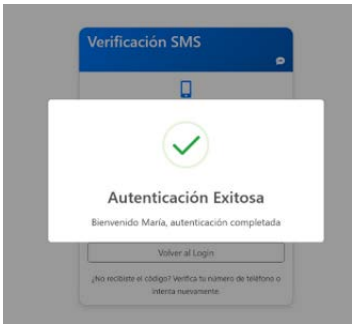
Luego, la Figura 8 ilustra la entrada del código en el formulario del sistema, lo que permite completar la verificación.

Figura 8. Ingreso del código de verificación en la plataforma

Fuente: Elaboración propia.

Finalmente, la Figura 9 confirma la autenticación exitosa mediante un mensaje de validación y en la Figura 10 se muestra el acceso autorizado al sistema.

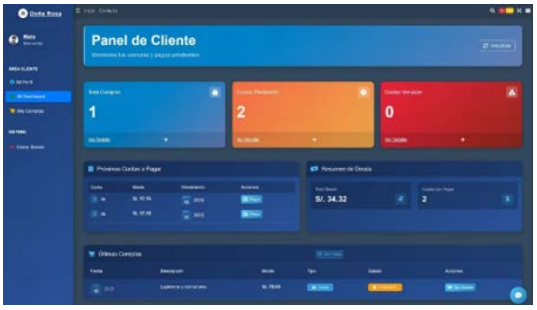
Figura 9. Confirmación que la autenticación fue exitosa



Fuente: Elaboración propia.

Fecha de recepción: 03 / 09 / 2025
Fecha de aceptación: 18 / 11 / 2025
Fecha de publicación: 20 / 02 / 2026

Figura 10. Acceso al sistema tras la validación correcta



Fuente: Elaboración propia.

4. DISCUSIÓN

4.1. Relación de los resultados con los objetivos del estudio

El objetivo principal fue evaluar y adaptar un mecanismo híbrido 2FA (OTP por SMS + WhatsApp) que aumentara la disponibilidad y resistencia de la autenticación en sistemas de gestión de ventas a crédito para microempresas. Los resultados indican que el mecanismo funcionó conforme a lo previsto: el flujo operativo se ejecutó correctamente, el canal alternativo WhatsApp se activó de forma controlada tras cinco segundos, y las pruebas de seguridad con OWASP ZAP confirmaron que la validación OTP soportó intentos de fuerza bruta e inyección SQL.

Con base en los resultados obtenidos, se concluye que el sistema híbrido no pretende innovar teóricamente el OTP, sino adaptarlo y validarlo en un entorno económico y técnico a pequeña escala, garantizando su viabilidad y bajo costo para las microempresas.

El enfoque práctico coincide con las pautas de los estándares de seguridad digital como NIST SP 800-63B (National Institute of Standards and Technology, 2020) y las directrices de la OWASP (OWASP Foundation, 2022), que priorizan la implementación de la Multifactor Authentication (MFA) en proporción al riesgo y contexto del usuario.

4.2. Comparativa de 2FA: OTP vía SMS y WhatsApp (híbrido) frente a otras alternativas

Para apreciar la importancia del enfoque híbrido, es útil compararlo con métodos de autenticación tanto clásicos como más avanzados; véase la Tabla 5.

Fecha de recepción: 03 / 09 / 2025
Fecha de aceptación: 18 / 11 / 2025
Fecha de publicación: 20 / 02 / 2026

Tabla 5. Comparación entre métodos de autenticación

Método	Descripción	Ventajas	Desventajas	Adecuación a microempresas
1FA: Usuario + Contraseña	Autenticación básica con credenciales.	Simplicidad, bajo coste, adopción universal.	Vulnerable a robo de credenciales y phishing.	Baja (Klivan et al., 2023).
1FA: Código de acceso	Un PIN/código elegido al registrarse (sin contraseña).	Mayor simplicidad para usuarios con baja alfabetización digital.	Vulnerable a fuerza bruta y reutilización de códigos.	Baja (Klivan et al., 2023).
2FA: OTP vía SMS	Contraseña de un solo uso enviada por red móvil.	Amplia cobertura, integración sencilla.	Riesgo de SIM swap e interceptación SS7.	Media-Alta (Lei et al., 2021).
2FA: OTP vía SMS + WhatsApp (híbrido)	OTP generado en servidor, enviado primero por SMS; opción de reenviar por WhatsApp tras 5 s.	Mayordisponibilidad; resiliencia ante fallos de SMS; bajo coste adicional; WhatsApp es de uso masivo.	Dependencia de proveedor externo (Twilio); vulnerabilidad si el dispositivo está comprometido.	Alta (Twilio, 2023).
2FA: TOTP (apps autenticadoras)	OTP generado localmente en apps como Google Authenticator.	No depende de red móvil; más resistente a SIM swap.	Requiere instalación/ configuración; menor adopción en usuarios no técnicos.	Media (Binti Sofian et al., 2024).
2FA: Push notifications	Confirmación en app autenticadora mediante notificación.	Fluido y resistente a phishing.	Depende de conectividad estable; requiere apps específicas.	Media (Alqaralleh et al., 2022).
2FA: Tokens físicos (U2F/ FIDO)	Dispositivo físico usado como segundo factor.	Muy seguro; resistente a phishing.	Coste elevado; logística compleja.	Baja (Klivan et al., 2023).

Fuente: Elaboración propia.

Como se mencionó, el método híbrido (SMS y WhatsApp) ocupa una posición intermedia, siendo más accesible y más sencillo de usar en relación con TOTP o tokens físicos. Además, resulta más resistente que el SMS exclusivo, gracias al canal OTT (WhatsApp) que mejora la tasa de entrega y la disponibilidad en situaciones de roaming. También es más seguro que la autenticación de un solo factor, ya sea con contraseña o código, al incorporar un segundo factor que reduce considerablemente la probabilidad de accesos no autorizados.

4.3. Conformidad con normas y buenas prácticas de seguridad

El diseño de este sistema siguió normas de seguridad reconocidas. La generación segura de OTP en el servidor, su expiración en 2 minutos, el uso exclusivo de los códigos y la verificación íntegra del lado servidor son medidas compatibles con NIST SP 800-63B (NIST, 2017). A su vez, las configuraciones aplicadas, incluyendo la protección contra ataques de fuerza bruta

Fecha de recepción: 03 / 09 / 2025
Fecha de aceptación: 18 / 11 / 2025
Fecha de publicación: 20 / 02 / 2026

evidenciada en las pruebas con OWASP ZAP, cumplen con las recomendaciones de la OWASP Cheat Sheet Series (OWASP Foundation, 2022); que destacan controles como caducidad breve, políticas de reintentos y aislamiento del canal de autenticación. Esto fortalece la conclusión de que, aunque el OTP vía SMS presenta riesgos conocidos; la implementación híbrida reforzada y supervisada brinda un nivel de seguridad adecuado para sistemas de microempresas con recursos limitados.

4.4. Implicaciones para la aplicación en microempresas

Los resultados indican que tener un OTP debería aumentar la seguridad en las plataformas de gestión financiera de los propietarios de microempresas sin un elevado gasto tecnológico para el usuario. Para las empresas que actualmente implementan registros manuales o prácticas de autenticación débiles que subestiman los riesgos involucrados, los sistemas OTP aseguran un acceso sólido sin gastar mucho. Esto refuerza la confianza en la protección de los datos de los clientes, los riesgos de fraude, interno o externo, reduciendo significativamente el riesgo de fraude empresarial.

5. CONCLUSIONES

El presente estudio tuvo como objetivo principal evaluar y adaptar un sistema híbrido de autenticación de doble factor, basado en OTP por SMS con un canal redundante vía WhatsApp, en una plataforma web para la gestión de ventas a crédito en microempresas. Los resultados permiten afirmar que las metas establecidas fueron alcanzadas, ya que se logró desarrollar un mecanismo 2FA híbrido que combina SMS y WhatsApp, demostrando ser técnicamente factible y operativamente viable en entornos con recursos limitados. Además, se validó experimentalmente la eficacia de la solución, mostrando que el sistema permitió accesos autorizados, bloqueó intentos de suplantación y garantizó resiliencia frente a fallos en la entrega de SMS mediante el uso de WhatsApp como canal alternativo.

Desde un enfoque teórico, la contribución de esta investigación no consiste en innovar el concepto de OTP, ya consolidado en la literatura, sino en evidenciar su adaptación contextualizada al ecosistema de microempresas; donde la simplicidad, los bajos costos y la cobertura tecnológica limitan las posibilidades de adopción. En este sentido, se puede generalizar que la incorporación de un segundo factor de autenticación accesible y redundante aumenta la seguridad y la

Fecha de recepción: 03 / 09 / 2025
Fecha de aceptación: 18 / 11 / 2025
Fecha de publicación: 20 / 02 / 2026

continuidad operativa de sistemas financieros en organizaciones de pequeña escala, aportando evidencia empírica en un sector poco explorado académicamente.

El estudio también se alinea con estándares reconocidos de seguridad digital como NIST SP 800-63B y las directrices de OWASP, lo que fortalece su validez metodológica y su aplicabilidad en escenarios reales. Sin embargo, se identificaron limitaciones propias del diseño preexperimental y del entorno controlado, lo cual restringe la extrapolación de los resultados y abre la necesidad de investigaciones futuras en condiciones de operación real y con comparaciones frente a otros mecanismos de autenticación más avanzados.

Contribución de los Autores (CRediT): AJRY: Conceptualización, Análisis formal, Investigación, Metodología, Administración del proyecto, Recursos, Visualización, Redacción-borrador original, Redacción-revisión y edición. RDVC: Conceptualización, Curación de datos, Análisis formal, Investigación, Metodología, Administración del proyecto, Recursos, Software, Visualización. JLRB: Conceptualización, Curación de datos, Análisis formal, Investigación, Recursos, Visualización, Redacción-borrador orginal. ACMDLS: Conceptualización, Supervisión, Validación, Visualización.

Conflicto de Intereses: Los autores declaran que no existen conflictos de intereses en esta publicación.

REFERENCIAS

400 Bad Request. (4 de Julio de 2025). *MDN Web Docs*. 400 Bad Request: https://developer.mozilla.org/es/docs/Web/HTTP/Reference/Status/400

Bartłomiejczyk, M., y El Fray, I. (Julio de 2024). Analysis of attacks on SMS OTP-based authentication process. *PACIS 2024 Proceedings*. https://aisel.aisnet.org/pacis2024/track07_secprivacy/track07_secprivacy/1/

Binti Sofian, A., Binti Peradus, A., Yong, F., Shearer, I., Binti Ismail, N., Mahendran, Y., y Faisal, M. (2024). Enhancing Authentication Security: Analyzing Time-Based One-Time Password Systems. *International Journal of Computer Technology and Science, 1*(3), 56-70. https://doi.org/https://doi.org/10.62951/ijcts.v1i3.25

Klivan, S., Höltervennhof, S., Huaman, N., Krause, A., Simko, L., Acar, Y., y Fahl, S. (2023). "We've Disabled MFA for You": An Evaluation of the Security and Usability of Multi-Factor Authentication Recovery Deployments. *CCS '23: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security.* https://doi.org/https://doi.org/10.1145/3576915.3623180

Lei, Z., Nan, Y., Fratantonio, Y., y Bianchi, A. (2021). On the Insecurity of SMS One-Time

Fecha de recepción: 03 / 09 / 2025
Fecha de aceptación: 18 / 11 / 2025
Fecha de publicación: 20 / 02 / 2026

Password Messages against Local Attackers in Modern Mobile Devices. *Network and Distributed Systems Security (NDSS) Symposium 2021, 21-25 February 2021, Virtual*. https://doi.org/https://dx.doi.org/10.14722/ndss.2021.24212

Ma, S., Li, J., Kim, H., Bertino, B., Nepal, S., Ostry, D., y Sun, C. (2021). Fine with "1234"? An Analysis of SMS One-Time Password Randomness in Android Apps. *Proceedings of ICSE 2021, 1*. https://doi.org/https://doi.org/10.48550/arXiv.2103.05758

Meyer, L. A., Romero, S., Bertoli, G., Burt, T., Weinert, A., y Lavista Ferres, J. (1 de Mayo de 2023). How effective is multifactor authentication at deterring cyberattacks? *arXiv*. https://doi.org/https://doi.org/10.48550/arXiv.2305.00945

National Institute of Standards and Technology. (2020). *Digital Identity Guidelines: Authentication and lifecycle management (NIST SP 800-63B)*. NIST. https://pages.nist.gov/800-63-3/sp800-63b.html

National Institute of Standards and Technology. (Junio de 2017). *Digital identity guidelines: Authentication and lifecycle management (SP 800-63B)*. https://doi.org/https://doi.org/10.6028/NIST.SP.800-63B-4

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., y Koucheryavy , Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography, 2*(1), 1. https://doi.org/https://doi.org/10.3390/cryptography2010001

OWASP Foundation. (2022). *Authentication Cheat Sheet*. OWASP Foundation Web site: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

Rivas Oloya, M. C. (26 de Abril de 2023). *Marco teórico y conceptual del financiamiento de las micro y pequeñas empresas del sector comercio del Perú, 2017* [Tesis de grado, Universidad Católica los Ángeles Chimbote] Repositorio institucional. https://repositorio.uladech.edu.pe/handle/20.500.13032/33247

Suleski, T., Ahmed, M., Yang, W., y Wang, E. (22 de Mayo de 2023). A review of multi-factor authentication in the Internet of Healthcare Things. *Digital health, 9*(20552076231177144). https://doi.org/https://doi.org/10.1177/20552076231177144

Timko, D., Hernandez Castillo, D., y Rahman, M. (12 de Noviembre de 2023). A Quantitative Study of SMS Phishing Detection. *Proceedings of the 16th ACM Conference on Security*

Fecha de recepción: 03 / 09 / 2025
Fecha de aceptación: 18 / 11 / 2025
Fecha de publicación: 20 / 02 / 2026

and Privacy in Wireless and Mobile Networks (WiSec '23). https://doi.org/https://doi.org/10.48550/arXiv.2311.06911

Twilio. (2023). *Five Reasons To Use The WhatsApp Business API - Messaging*. Twilio: https://www.twilio.com/en-us/resource-center/five-reasons-to-use-whatsapp-business-api