https://doi.org/10.22201/dgtic.30618096e.2026.4.2.177 Vol. 4, Núm. 2. abril-junio 2026, págs. 99 - 107

Conector de gestión de pagos digitales en línea

Online digital payment management connector

Información del reporte:

Para citar este reporte técnico:

Cendejas Cervantes, N. (2026). Conector de gestión de pagos digitales en línea. *Cuadernos Técnicos Universitarios de la DGTIC, 4*(2), páginas (99 - 107). https://doi.org/10.22201/dgtic.30618096e.2026.4.2.177

Nidia Cendejas Cervantes
Dirección General de Cómputo y de Tecnologías de Información y Comunicación
Universidad Nacional Autónoma de México
nidia@unam.mx
ORCID: 0009-0001-2929-2575

Resumen

La digitalización de servicios institucionales ha incrementado la necesidad de integrar mecanismos seguros y eficientes para el procesamiento de algunos de los servicios que se pueden ofrecer, entre ellos, el pago en línea. En este contexto, se implementó un punto de acceso para la gestión de transacciones electrónicas, con el propósito de optimizar los procesos administrativos.

Para implementar el punto de acceso, la metodología se estructuró en cuatro etapas: diseño de la arquitectura basada en servicios web, configuración del entorno de comunicación, instalación de componentes en el servidor institucional, así como ejecución de pruebas funcionales y de seguridad. Asimismo, se estableció la conexión estructurada al *webservice* proporcionado por la Tesorería del Patronato Universitario mediante protocolos compatibles con sus especificaciones técnicas.

Los resultados mostraron una reducción en los tiempos de procesamiento de pagos, así como en el incremento de inscripciones con pago en línea y una disminución significativa en errores manuales de conciliación. Como principal aportación, se obtuvo un punto de acceso que permite la integración estandarizada con el *webservice*. Una limitación del trabajo es que la solución depende de la disponibilidad y especificaciones técnicas del servicio externo, por lo que los cambios en éste podrían requerir actualizaciones en el conector.

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.177 Vol. 4, Núm. 2. abril-junio 2026, págs. 100 - 107

Palabras clave: Cifrado de datos, servicios web estandarizados, automatización de pago en línea, validación transaccional.

Abstract

The digitalization of institutional services has increased the need to integrate secure and efficient mechanisms for processing some of the services that can be offered, including online payment. In this context, an endpoint was implemented for the management of electronic transactions, with the purpose of optimizing administrative processes.

For the implementation of the endpoint, the methodology was structured into four main stages: design of a web service-based architecture, configuration of the communication environment, installation of components on the institutional server, and execution of functional and security testing. Also, a structured connection was established to the webservice provided by the Tesorería del Patronato Universitario, using protocols compatible with its technical specifications.

The results showed a reduction in payment processing times, as well as an increase in registrations with online payment and a significant decrease in manual reconciliation errors. The main contribution of this work is an access point that enables standardized integration with the web service. A limitation of the work is that the solution depends on the availability and technical specifications of the external service, so changes to it could require updates to the connector.

Keywords: *Data encryption, standarized webservice, online payment automation, transactional validation.*

1. INTRODUCCIÓN

La transformación digital ha exigido la modernización de procedimientos para la gestión administrativa y financiera de las instituciones, particularmente en el procesamiento de pagos electrónicos. En los últimos años, la adopción de arquitecturas basadas en servicios y el uso de interfaces de programación de aplicaciones (API) han mejorado la interoperabilidad entre sistemas con características diferentes, fortaleciendo la seguridad en las transacciones digitales.

En el ámbito de la seguridad de APIs, el *OWASP API Security Top 10* (OWASP Foundation, 2023) ha identificado riesgos críticos tales como la exposición excesiva de datos, la asignación masiva y el consumo inseguro de APIs, los cuales son especialmente relevantes en sistemas de pago en línea. Adicionalmente, la integración con sistemas de pago externos requiere mecanismos robustos de autenticación y autorización; estándares como OAuth 2.0 permiten gestionar el acceso de manera controlada.

Investigaciones previas en materia de seguridad de interfaces de aplicaciones señalan que los puntos de acceso seguros contribuyen a la reducción de vulnerabilidades y a la optimización de tiempos de respuesta, al hacer más ágil el proceso de validación de transacciones (Behl & Behl, 2020; Stuttard & Pinto, 2021).

En la Dirección General de Cómputo y de Tecnologías de la Información y Comunicación (DGTIC), se identificó la necesidad de automatizar el pago en línea de eventos (cursos y diplomados), ya que el

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.177 **Vol. 4, Núm. 2.** abril-junio 2026, págs. 101 - 107

proceso previo dependía de validaciones manuales y conciliaciones administrativas que generaban retrasos e inconsistencias.

El objetivo principal del proyecto presentado en este reporte técnico fue integrar un mecanismo automatizado y confiable para el pago en línea que operara dentro de la infraestructura institucional, sin depender de procesos manuales externos.

La integración de sistemas internos con servicios externos requirió establecer una comunicación segura, controlada y estructurada. La implementación de un punto de acceso como capa intermedia ha permitido desacoplar la lógica institucional y abstraer el *webservice* externo, facilitando el flujo de información entre ambos sistemas. De acuerdo con el *Open Web Application Security Project* (OWASP Foundation, 2021), las interfaces de programación de sistemas representan uno de los principales riesgos en aplicaciones actuales, por lo que su adecuada implementación ayuda significativamente a la protección de la información.

2. DESARROLLO TÉCNICO

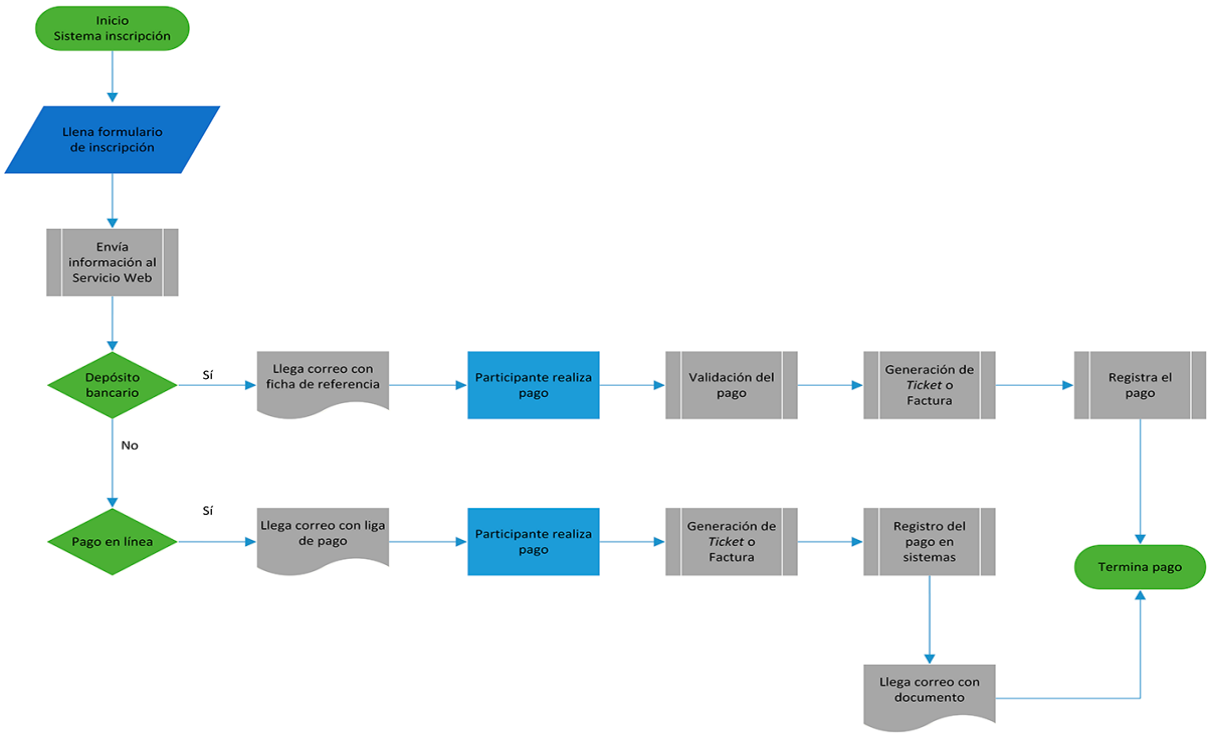
El punto de acceso se estableció como una capa intermedia entre el sistema institucional y el *webservice* de pago en línea de la Tesorería. Su función principal es desacoplar la lógica del sistema interno y abstraer la complejidad del servicio externo, centralizando procesos como la validación de datos, la autenticación y el control de la transacción. Esta arquitectura de tres capas (presentación, lógica de negocio e integración) permite separar responsabilidades, facilita el mantenimiento y aísla la lógica de negocio de posibles cambios en el servicio externo (Martin, 2020).

El proyecto se organizó en dos etapas principales: la definición de la arquitectura y el desarrollo funcional del flujo transaccional. El flujo general del proceso se muestra en la Figura 1.

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.177 Vol. 4, Núm. 2. abril-junio 2026, págs. 102 - 107

Figura 1

Proceso para realizar un pago en línea



Como se muestra en la Figura 1, el proceso de pago inicia cuando el usuario se registra en el sistema de inscripciones. Durante el registro, el sistema captura los datos necesarios (nombre, correo, monto) y genera una orden de pago. Posteriormente, estos datos son enviados al *webservice* de la Tesorería a través del punto de acceso, el cual actúa como intermediario. Este punto valida la integridad y el formato de la información, es decir, la estructura según los parámetros requeridos, y la transmite al servicio externo. Una vez recibida la confirmación, el sistema actualiza el estatus de la inscripción y notifica al usuario.

El proceso se divide en dos líneas según el método de pago: en el depósito bancario, el sistema genera una referencia de pago que es enviada por correo electrónico, el usuario realiza la transacción y, posteriormente, se ejecuta la validación mediante el punto de acceso. Mientras que en el pago en línea, el punto de acceso lleva a cabo la comunicación directa con el servicio de pago, valida la transacción en tiempo real y garantiza la integridad de la información.

En ambos procesos, el punto de acceso centraliza la lógica de validación y el control de la transacción, permitiendo el registro automático del pago y la generación de comprobantes (*ticket* o factura).

2.1 METODOLOGÍA

La metodología se estructuró en cinco etapas: análisis, diseño, configuración, instalación y pruebas.

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.177 Vol. 4, Núm. 2. abril-junio 2026, págs. 103 - 107

2.1.1 ANÁLISIS

Se analizaron las especificaciones técnicas del *webservice* de la Tesorería para comprender su funcionamiento, restricciones y mecanismos de interacción. Se identificaron los métodos disponibles para la gestión de transacciones, así como los parámetros obligatorios: referencia de pago, monto, concepto del pago y datos del usuario.

Se examinó la estructura de los mensajes de intercambio (formato JSON), y los códigos de respuesta emitidos por el servicio, lo que permitió clasificar las salidas del sistema en transacciones exitosas, rechazos operativos y errores técnicos. La correcta validación de los datos de entrada es esencial para la seguridad de las API, ya que un manejo incorrecto puede generar vulnerabilidades (Stuttard & Pinto, 2021; Acar *et al*., 2018). Adicionalmente, el *webservice* requiere el envío de datos mediante el protocolo XML-RPC (UTICT, 2024).

Derivado del análisis, se observó la necesidad de incorporar mecanismos de validación que garantizaran integridad y consistencia, dado que la información incorrecta en los parámetros establecidos ocasionaría la interrupción del proceso.

2.1.2 DISEÑO

Con base en el análisis, se definieron los siguientes criterios de validación que todo pago debe cumplir antes de ser enviado al servicio. La Tabla 1 muestra estos criterios, definidos según las especificaciones de la Tesorería, que establece formatos obligatorios para campos de Referencia CHAR (20), Importe (DECIMAL (22,6) y la exigencia de que todos los parámetros de entrada deben estar en mayúsculas (UTICT, 2024).

Tabla 1

Criterios de validación del punto de acceso

Campo	Criterio de validación	Acción en caso de incumplimiento
Referencia de pago	Formato alfanumérico de 20 caracteres, no vacío	Rechazar solicitud, código 400
Monto	Número decimal positivo, mínimo $10 MXN, Máximo $50,000 MXN	Rechazar solicitud, código 400
Concepto	Texto de hasta 100 caracteres, sin caracteres especiales peligrosos (< > & " ')	Sanitizar la cadena y validar, rechazar si persiste el error
Correo del usuario	Formato de correo electrónico válido (usuario@dominio)	Rechazar solicitud, código 400
Token de autenticación	Debe coincidir con el valor almacenado en configuración	Rechazar solicitud, código 400

Estos criterios se implementaron antes de enviar la solicitud al *webservice* externo, reduciendo así transacciones fallidas por errores de formato.

Se elaboró el flujo transaccional considerando tres escenarios: éxito, en el que la operación es válida y confirmada por el servicio; rechazo, cuando la transacción no cumple con los criterios mínimos establecidos

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.177 Vol. 4, Núm. 2. abril-junio 2026, págs. 104 - 107

por el *webservice*; y error técnico, cuando existe alguna falla en la comunicación y/o disponibilidad en el servicio. Ese modelado permitió definir la lógica de control del punto de acceso.

El punto de acceso contempla un esquema de manejo de errores que distingue tres categorías:

- Errores de validación (códigos 400): ocurren cuando los parámetros enviados no cumplen con los formatos esperados.
- Errores de autenticación (códigos 401): se visualizan cuando el *token* de acceso no es válido.
- Errores de comunicación (códigos 500 o de tiempo de espera): ocurren cuando el *webservice* no responde en un tiempo máximo de 30 segundos o hay fallas de red.

2.1.3 CONFIGURACIÓN

Se desarrolló un módulo en PHP bajo el principio de separación de responsabilidades, el cual establece que cada componente del sistema debe encargarse de una función específica, reduciendo la complejidad, facilitando el mantenimiento y mejorando la seguridad del software (Martin, 2020). La elección de PHP se basó en su amplia adopción en entornos institucionales, su madurez para integraciones de tipo transaccional y la disponibilidad de extensiones como cURL para consumo de servicios web. En este sentido, se diseñó el punto de acceso como un componente independiente.

El punto de acceso implementa un esquema de autenticación basado en *token* fijo, compartido entre el sistema institucional y el *webservice*. Cada solicitud debe incluir en el encabezado HTTP un *token* de acceso previamente acordado, el cual es validado por el servicio antes de procesar la transacción.

Según la documentación técnica de la Tesorería, cada dependencia debe tramitar un usuario y una contraseña que son únicos para acceder a los servicios web, los cuales se envían como parte de los parámetros de inicialización junto con la URL del servicio. También es necesario registrar las direcciones IP desde las cuales se consumirán los servicios (UTICT, 2024).

En este aspecto, se incorporó la validación de entrada de la información para asegurar que los datos recibidos cumplieran con los tipos de datos y restricciones definidos, evitando algún tipo de inconsistencia en la comunicación con el *webservice*. Esta validación previene el envío de datos malformados que podrían ser rechazados por el servicio externo o explotados como vectores de ataque (Stuttard & Pinto, 2021). Se emplearon consultas parametrizadas para prevenir ataques de inyección SQL (OWASP Foundation, 2021) y se implementó un registro estructurado de eventos en bitácoras para monitorear y detectar algún tipo de incidente de seguridad de manera temprana (Behl & Behl, 2020).

Para la integración con el *webservice*, se empleó la extensión cURL bajo protocolo seguro, garantizando así que todos los datos sensibles viajen cifrados durante la transmisión, además de utilizar JSON como formato de seriación de datos. Se configuraron tiempos de espera controlados y mecanismos de manejo de excepciones para garantizar la estabilidad transaccional.

2.1.4 INSTALACIÓN

El sistema fue desplegado en una máquina virtual proporcionada por el Centro de Datos de la DGTIC, habilitando únicamente el tráfico por HTTPS, con el cifrado TLS para proteger los datos durante la transmisión (Behl & Behl, 2020). Se configuró un certificado digital válido, logrando que todas las

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.177 Vol. 4, Núm. 2. abril-junio 2026, págs. 105 - 107

solicitudes al punto de acceso se realizaran a través de conexiones seguras. El uso de infraestructura virtualizada garantiza disponibilidad, respaldo y capacidades de recuperación ante contingencias, sin requerir inversión adicional en hardware dedicado.

Se estableció un entorno basado en software libre: Linux, Apache, PHP, PostgreSQL y Laravel. Estas tecnologías se seleccionaron porque combinan la madurez, estabilidad y amplio soporte, lo que reduce costos de licenciamiento y facilita el mantenimiento interno. Se pueden observar los componentes utilizados en la Tabla 2.

Tabla 2

Componentes tecnológicos utilizados para la implementación del punto de acceso

Componente	Descripción
Sistema operativo	Linux Debian
Servidor web	Apache HTTP Server 2.4
Lenguaje	PHP 8.1
Gestor de bases de datos	PostgreSQL 17.9
Framework de programación	Laravel
Extensión para consumo de servicios	cURL 7.68

Adicionalmente, se implementaron medidas de seguridad a nivel infraestructura, mediante la configuración de reglas de *firewall,* en este caso, con *IPTables*. Gracias a esto, se restringió el acceso a direcciones IP y puertos autorizados, permitiendo limitar la exposición de servicios y así reducir la posibilidad de ataques.

2.1.5 PRUEBAS

Se realizaron pruebas funcionales y de seguridad para validar el funcionamiento del punto de acceso (García-Peñalvo *et al*., 2021). Se verificó el correcto envío, procesamiento y recepción de datos, así como la consistencia de las respuestas. También se evaluaron riesgos tales como la inyección de código SQL, la manipulación de parámetros y el reenvío de solicitudes.

Durante la integración del *webservice,* se observó que la arquitectura requería del cumplimiento estricto de parámetros y tipos de datos. Al enviar información incorrecta, en automático, se cancelaba la transacción, fortaleciendo los mecanismos de validación y reducción de algún tipo de riesgo.

Finalmente, se efectuaron pruebas de conciliación contable para validar la correspondencia tanto en registros internos como en confirmación del servicio externo, proporcionado por la Tesorería.

3. RESULTADOS

La implementación logró establecer una comunicación estable y segura con el servicio, el cual permitió el registro automatizado de transacciones y la confirmación inmediata del estatus de pago.

Para evaluar la efectividad de la solución, se analizaron los datos operativos de los años 2024 y 2025:

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.177 Vol. 4, Núm. 2. abril-junio 2026, págs. 106 - 107

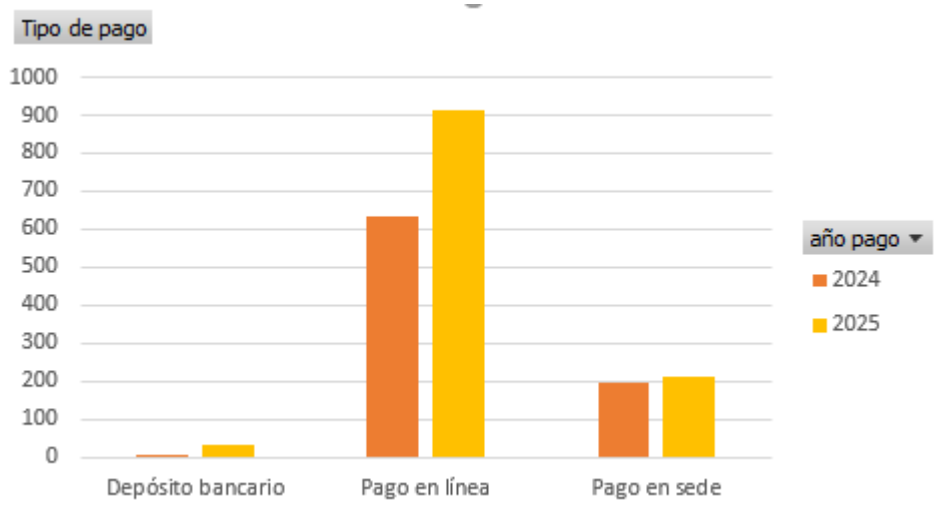
- Tiempo de procesamiento para pagos en línea: la mediana del tiempo de espera para la confirmación de pagos se redujo de 2.5 días (60 horas) en 2024 a 0.8 (19 horas) en 2025, lo que representa una disminución del 68%.
- Pagos sin conciliar: el porcentaje de transacciones que no lograron conciliarse automáticamente disminuyó del 26.5% en 2024 al 10.2% en 2025, una reducción del 61%.
- Generación automática de comprobantes (*ticket* o factura): se incrementó en un aproximado de 860 comprobantes en 2024 a 1,161 en 2025, lo que equivale a un aumento del 35%. Esto refleja una mayor adopción del sistema para la emisión de comprobantes fiscales.

También se observó una disminución significativa en errores de conciliación, debido a la generación automática de referencias únicas y a la sincronización directa con el sistema de pagos institucional.

Como resultado, se ha notado un incremento en la selección de tipo de pago por parte de los participantes que ingresan a los eventos, tal como se observa en la Figura 2:

Figura 2

Tipo de pago para inscripción a cursos y diplomados



Como se observa en la Figura 2, el pago en línea muestra una tendencia creciente en el periodo analizado, mientras que los métodos tradicionales (pago en sede y depósito bancario) presentan una disminución. En el último año registrado, el pago en línea representó el 54% del total de las transacciones, frente al 28% del pago en sede y el 18% del pago por depósito bancario. Esta distribución refleja que los usuarios prefieren la inmediatez y comodidad del pago electrónico sobre los métodos presenciales o diferidos. La disponibilidad de un punto de acceso seguro y confiable ha sido un factor clave para habilitar esta opción y diversificar los mecanismos de pago ofertados por la DGTIC.

El registro inmediato de los pagos en los ingresos facilitó la consulta en tiempo real de los ingresos percibidos por concepto de servicios y oferta académica.

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.177 **Vol. 4, Núm. 2.** abril-junio 2026, págs. 107 - 107

4. CONCLUSIONES

La principal aportación de este trabajo es la implementación de un punto de acceso seguro y funcional que actúa como capa intermedia entre el sistema institucional de la DGTIC y el w*ebservice* de pagos de la Tesorería. Este conector ha permitido automatizar el ciclo de pago en línea, desde la generación de la orden hasta la validación y registro de la transacción.

Como resultados concretos, se logró reducir los tiempos de procesamiento, minimizar errores operativos asociados a la conciliación manual y aumentar la adopción del pago en línea entre los usuarios de los cursos y diplomados ofertados. La arquitectura basada en servicios facilita el mantenimiento y la evolución independiente de cada capa.

El alcance del trabajo se limita a la integración con el *webservice* de la Tesorería en su versión actual. Cambios futuros en las especificaciones del servicio externo podrían requerir ajustes en el conector. No obstante, el diseño modular del punto de acceso permite adaptarse a dichos cambios con un menor impacto.

REFERENCIAS

Acar, Y., Backes, M., Fahl, S., Kim, D., Mazurek, M. L., & Stransky, C. (2018). You get where you're looking for: The impact of information sources on code security. *Proceedings of the IEEE Symposium on Security and Privacy*, 289–305.

Behl, A., Behl, K. (2020). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

García-Peñalvo, F. J., Cruz-Benito, J., & Therón, R. (2021). *Seguridad en sistemas de información: tendencias y desafíos actuales*. Ediciones Universidad de Salamanca.

Martin, R. C. (2020). *Arquitectura limpia: guía para especialistas en la estructura y el diseño del software*. Anaya Multimedia.

OWASP Foundation. (2023). *OWASP API Security Top 10 2023*. OWASP. https://owasp.org/API-Security

OWASP Foundation. (2021). *OWASP Top Ten 2021: The ten most critical web application security risk*. OWASP. https://owasp.org

Stuttard, D., & Pinto, M. (2021). *El libro del hacker de aplicaciones web: Cómo descubrir y explotar fallos de seguridad* (2a ed.). Anaya Multimedia.

UTICT. (2024). *Documentación de servicios web: Servicios Web y Servlet para la emisión de Facturas Digitales*. Unidad de Tecnologías de Información y Comunicación de la Tesorería, Universidad Nacional Autónoma de México.