Tipo de artículo: Artículo original

Componente para la firma digital en línea de documentos en la Plataforma GAPID

Component for online digital signature of documents on the GAPID Platform

Yan Carlos Escobar Pupo [1*], https://orcid.org/0009-0001-3541-6482
Arturo Orellana García [2], https://orcid.org/0000-0002-3652-969X
Leodan Vega Izaguirre [3], https://orcid.org/0000-0002-7052-9319
Cristian Rey Ruíz Castro [4], https://orcid.org/0009-0000-1304-6911

[1] Centro de Informática Médica. Universidad de las Ciencias Informáticas. Correo electrónico: yancep@estudiantes.uci.cu
[2] Centro de Informática Médica. Universidad de las Ciencias Informáticas. Correo electrónico: aorellana@uci.cu
[3] Centro de Informática Médica. Universidad de las Ciencias Informáticas. Correo electrónico: lizaguirre@uci.cu
[4] Facultad de Ciberseguridad. Universidad de las Ciencias Informáticas. Correo electrónico: cristianrrc@estudiantes.uci.cu

*** Autor para correspondencia: usuario@dominio.com**

Resumen

La investigación presenta el desarrollo de un componente para la firma digital de documentos en línea en la Plataforma GAPID, el cual desempeña un papel crucial en la gestión de Programas y Proyectos de Ciencia, Tecnología e Innovación. Se ha identificado la necesidad de fortalecer ciertos aspectos del sistema para garantizar la autenticidad, integridad y no repudio de los documentos digitales que se gestionan en el mismo. Actualmente, los usuarios dependen de métodos tradicionales que necesitan de un proceso de impresión y el escaneo para firmar documentos, así como de herramientas externas que dificultan la eficiencia del proceso documental. El objetivo principal de esta investigación es desarrollar un componente de firma digital en línea que garantice la autenticidad, integridad y no repudio de los documentos emitidos en el sistema GAPID, eliminando la dependencia de métodos tradicionales y herramientas externas. Para ello, se utilizó como tecnología principal Next.js para el desarrollo del sistema, destacándose por su eficiencia y escalabilidad. Los métodos utilizados para la investigación permitieron el análisis de soluciones similares, especificación de requisitos, prototipos de interfaz de usuario, de los diferentes conceptos. La solución propuesta involucra la integración de una firma digital robusta dentro de GAPID, mejorando la confiabilidad y seguridad de los procesos administrativos y financieros. La incorporación de este componente al sistema GAPID no solo elimina la necesidad de herramientas externas, sino que también aumenta la seguridad en la gestión de documentos digitales, beneficiando a todas las partes involucradas en los proyectos y programas suscritos.

Palabras clave: Gestión, firma digital, programa, proyecto, seguridad.

Abstract

The research presents the development of a component for the digital signature of online documents in the GAPID Platform, which plays a crucial role in the management of Science, Technology and Innovation Programs and Projects. The need to strengthen certain aspects of the system has been identified to guarantee the authenticity, integrity and non-repudiation of the digital documents managed in it. Currently, users depend on traditional methods that require a printing and scanning process to sign documents, as well as external tools that hinder the efficiency of the document process. The main objective of this research is to develop an online digital signature component that guarantees the authenticity, integrity and non-repudiation of documents issued in the GAPID system, eliminating the dependence on traditional methods and external tools. For this purpose, Next.js was

used as the main technology for the development of the system, standing out for its efficiency and scalability. The methods used for the research allowed the analysis of similar solutions, requirements specification, user interface prototypes, and different concepts. The proposed solution involves the integration of a robust digital signature within GAPID, improving the reliability and security of administrative and financial processes. The incorporation of this component into the GAPID system not only eliminates the need for external tools, but also increases security in the management of digital documents, benefiting all parties involved in the projects and programs subscribed.

Keywords: *digital signature, management, program, project, security.*

Recibido: 15/06/2024
Aceptado: 28/08/2024
En línea: 01/09/2024

Introducción

La información con el tiempo ha cambiado de soporte, en la actualidad es posible modificarla en formatos tan comprimidos como se desee, y a su vez enviarla muy fácilmente. El medio por donde viajan nuestros datos es vulnerable, actualmente nada pertenece al ámbito privado. (Quiroga, 2024)

Para garantizar la seguridad y confiabilidad de información, es esencial que datos como los documentos digitales cumplan con ciertos atributos fundamentales. La autenticidad asegura que el documento proviene efectivamente del remitente que afirma haberlo enviado, eliminando la posibilidad de suplantación. La integridad garantiza que el contenido del documento no ha sido alterado desde su creación, lo que protege contra modificaciones malintencionadas o errores accidentales. El no repudio implica que el autor del documento no puede negar su autoría ni haber enviado el documento, proporcionando una evidencia irrefutable de la transacción. (Rivera Anastacio, 2021)

La gestión de programas y proyectos de investigación, desarrollo e innovación (I+D+i) requiere de un alto nivel de confiabilidad, seguridad y transparencia en los procesos administrativos y financieros que se realizan. Estos procesos implican la generación, revisión, aprobación y almacenamiento de documentos digitales que contienen información sensible y de valor para las entidades ejecutoras, los financiadores y los beneficiarios de los resultados. Sin embargo, el sistema de gestión de programas y proyectos de I+D+i GAPID, desarrollado por el Parque Científico Tecnológico de La Habana, presenta limitaciones significativas en cuanto a la preservación de la integridad, autenticidad y no repudio de los documentos emitidos en línea. Estas deficiencias impactan directamente la seguridad de estos datos.

El sistema GAPID basa su evidencia documental en documentos que requieren la firma de diversos actores como jefes de proyecto, expertos, jefes de programa, secretarios de programa entre otros. Actualmente, los usuarios del sistema recurren a métodos tradicionales para la firma de documentos, los cuales necesitan en su proceso la impresión y el escaneo. Los usuarios también solventan esta problemática con herramientas auxiliares, algunas de pago, para

realizar firmas digitales. Herramientas como eFirma, aunque útiles, representan una barrera adicional para los usuarios, quienes deben invertir en software externo. En ocasiones, el mantenimiento y soporte de estas herramientas también requieren intervención en la empresa, lo que supone un gasto adicional en términos de tiempo y recursos.

La necesidad de firmar estos documentos radica en la validación y legitimación de las decisiones y acciones tomadas durante el desarrollo de programas y proyectos. Sin embargo, el proceso actual es laborioso, la mayoría de los documentos son firmados a mano, lo que obliga a imprimirlos, escanearlos, firmarlos y luego enviarlos por correo electrónico para que otras personas los firmen. Este procedimiento no solo es ineficiente, sino que también incrementa la posibilidad de errores y la pérdida de documentos durante el tránsito.

Materiales y métodos

En el presente artículo se aplicó el método Histórico – Lógico que permitió analizar la evolución y las tendencias actuales de la firma digital en el contexto de los programas y proyectos de I+D+i. Se recurrió al método Analítico – Síntesis para analizar la información sobre los distintos sistemas identificados para la firma digital y sintetizar las características que son de interés para la presente investigación. Se empleó el método Modelación para realizar una representación del diseño e implementación del componente de firma digital en línea mediante diagramas ingenieriles en las distintas etapas de la construcción del software. Análisis Documental se utilizó para revisar y evaluar la documentación existente relacionada con las normativas, estándares y tecnologías de firma digital aplicables a los programas y proyectos de I+D+i, proporcionando una base teórica sólida para el desarrollo del componente.

Soluciones similares

Las herramientas de firma digital, conocidas también como portafirmas digitales, están diseñadas para simplificar el uso de la firma digital en documentos por parte de las entidades y unidades administrativas. Estos documentos pueden provenir de diversos sistemas de información autónomos, lo que agiliza la actividad administrativa. Estas herramientas son para el usuario final y ofrecen servicios de autenticación y firma digital que, siempre que lo permita la legislación, tienen la misma validez que una firma escrita a mano.

Portafirmas a nivel internacional: En el ámbito internacional, se ha observado un creciente interés y adopción de los portafirmas digitales en diversas áreas que requieren la firma digital de documentos. A continuación, se presentan algunos portafirmas que han sido objeto de estudio debido a su relevancia y uso extendido:

Adobe Sign, parte de Adobe Document Cloud, es una solución avanzada de firma electrónica que permite a las organizaciones optimizar sus procesos de firma de documentos. Esta herramienta no solo facilita la firma electrónica de documentos, sino que también ayuda a automatizar flujos de trabajo, integrarse con otras aplicaciones y cumplir con los requisitos legales.

AutoFirma es un programa para Windows, Mac y Linux que el Ministerio de Hacienda y Administraciones Públicas de España ofrece sin coste. Esta es una herramienta de firma electrónica segura, fácil de usar y flexible que se adapta a diferentes necesidades empresariales. Aunque no ofrece todas las características avanzadas de Adobe Acrobat Sign, es una opción asequible y efectiva para pequeñas y medianas empresas que buscan una solución de firma electrónica básica.

DocuSign es una plataforma integral que lidera el mercado en la gestión de transacciones digitales y soluciones de firma electrónica. Esta plataforma proporciona un método seguro y confiable para firmar documentos electrónicamente, lo que permite a los usuarios realizar firmas legales desde cualquier dispositivo y en cualquier lugar, optimizando así la eficiencia y la conveniencia en una variedad de procesos empresariales. (DocuSign 2024)

Portafirmas a nivel nacional: El uso de los portafirmas digitales es un área poco explorada en el ámbito nacional, por lo que el único sistema homólogo estudiado es el siguiente:

e-Firma es una aplicación multiplataforma que permite el uso de Certificados Digitales emitidos por la Autoridad de Certificación Intermedia Softel (ACIS). La misma ha sido desarrollada en colaboración con INGENIUS, grupo que representa a Trabajadores por Cuenta Propia. La app automatiza la Firma Digital y la Verificación de estado de dicha Firma en ficheros electrónicos (pdf y excel), a través del uso seguro de servicios provistos en la Infraestructura de Llave Pública sostenida por la empresa Softel. De esta manera se garantiza la protección de la información.

Tabla 1: "Resumen del análisis de sistemas similares" [Fuente: Elaboración propia].

Sistema	Libre de costo	Tecnología Web	Soporte para firma con certificados digitales
AutoFirma	Si	No	Sí
DocuSign	No	Sí	Sí
Adobe Sign	No	Sí	Sí
eFirma (Cuba)	No	Si	Sí

El análisis incluyó varias soluciones como AutoFirma, DocuSign, Adobe Sign, y eFirma (Cuba), pero estas no cumplen con la necesidad específica debido a que, aunque estas plataformas son robustas y ampliamente utilizadas, no ofrecen una integración directa y personalizada con la plataforma GAPID y mantienen la dependencia de herramientas externas que pueden generar gastos innecesarios y flujos de trabajo ineficientes.

Resultados y discusión

El componente de firma digital se integra a la plataforma GAPID como un módulo adicional, accesible desde la interfaz web del sistema. Este componente permite a los usuarios visualizar los documentos generados por GAPID en formato PDF y realizar la firma electrónica de los mismos de forma segura. La interfaz del componente de firma digital consta con una opción para seleccionar el área específica del documento PDF donde se desea colocar la firma. Una vez seleccionada el área, aparece un menú de opciones de configuración de la firma.

En este menú, el usuario puede elegir entre diferentes opciones para personalizar su firma digital:

- Firma por imagen: El usuario puede seleccionar una imagen que se inserta como representación visual de la firma en el documento.
- Firma por texto: El usuario puede agregar datos como su nombre, fecha y hora de la firma, que se incluirán junto a la representación visual de la firma.
- Ambas: El usuario puede agregar ambas formas de visualización al mismo tiempo.
- Ninguna: El usuario puede firmar el documento sin agregar contenido visual

Una vez configurada la firma, el usuario deberá proporcionar su certificado digital en formato P12 para autenticar su identidad y realizar la firma electrónica.

A continuación, se explica el proceso de firma:

1.Lectura del Certificado: Se inicia el proceso usando la contraseña del certificado digital que proporcionó el usuario.

- Se utiliza la librería sign-pdf-lib para acceder al contenido del archivo P12.
- La contraseña proporcionada por el usuario permite desbloquear y extraer tanto la clave privada como el certificado público contenidos en el archivo P12.

2.Generación del Hash:

- Se calcula el hash del contenido del documento PDF. Este hash es una representación única del contenido del documento en ese momento.
- El hash se genera utilizando algoritmos criptográficos estándar, como SHA-256.

3.Firma del Hash:

- La clave privada extraída del certificado P12 se utiliza para cifrar el hash. Este paso es crucial, ya que la firma digital se basa en la capacidad de la clave privada para cifrar información que solo puede ser descifrada por la clave pública correspondiente.

4.Adjunción del Certificado:

- Junto con el hash cifrado, el certificado público también se adjunta al documento PDF.
- Este certificado contiene la clave pública que cualquier parte interesada puede utilizar para verificar la validez de la firma digital.
- El documento PDF ahora contiene la firma digital, que incluye el hash cifrado y el certificado público.

Es importante destacar que, durante todo el proceso, no se almacena ningún dato sensible del usuario ni del certificado. La privacidad y seguridad de la información se mantienen en todo momento, asegurando que solo el usuario tenga acceso a su clave privada y contraseña, Además, el uso de algoritmos criptográficos robustos y estándares de la industria asegura que la firma digital es segura y confiable.

La firma digital generada por el componente es técnicamente interoperable con otros sistemas que siguen los mismos estándares criptográficos. Esto significa que cualquier sistema que soporte las mismas normas de firma digital podrá verificar la validez de las firmas generadas, asegurando así una amplia compatibilidad y aceptación de los documentos firmados.

En el contexto de la era digital, los documentos electrónicos han reemplazado en gran medida a los documentos en papel, destacándose el formato PDF por su compatibilidad multiplataforma, seguridad robusta, interactividad multimedia y capacidad de compresión sin pérdida significativa de calidad. Paralelamente, la seguridad de la información se fortalece con criptosistemas, tanto simétricos como asimétricos. El AES, un criptosistema simétrico, y el RSA, un criptosistema asimétrico, se utilizan ampliamente debido a sus robustas características de seguridad (Pousa, A. 2011; Rankl, W., & Effing, W. 2004). En cuanto a la autenticación, los certificados digitales, como el estándar X.509v3, y la infraestructura de clave pública (PKI) garantizan la autenticidad y la integridad de la

información (Rivas Lara, A. E. 2020; Gitlan, D. 2023). Finalmente, las firmas digitales, mediante técnicas de autenticación criptográfica, aseguran la identidad del emisor y la integridad del mensaje, ofreciendo una solución integral para la seguridad de documentos para la Plataforma GAPID (Menezes, Oorschot y Vanstone 1996; Silva 2004).

Un modelo de dominio es un artefacto de la disciplina de análisis, construido con las reglas de UML durante la fase de ejecución. Este es una representación de las clases conceptuales del mundo real, no de componentes software. No se trata de un conjunto de diagramas que describen clases software, u objetos software con responsabilidades. (García-Holgado, Alicia, A. Vázquez-Ingelmo, y F. J. García-Peñalvo. 2022) En la Figura 1 se presenta el modelo de dominio que especifica los conceptos asociados al dominio del problema del componente de firma digital en la plataforma GAPID.

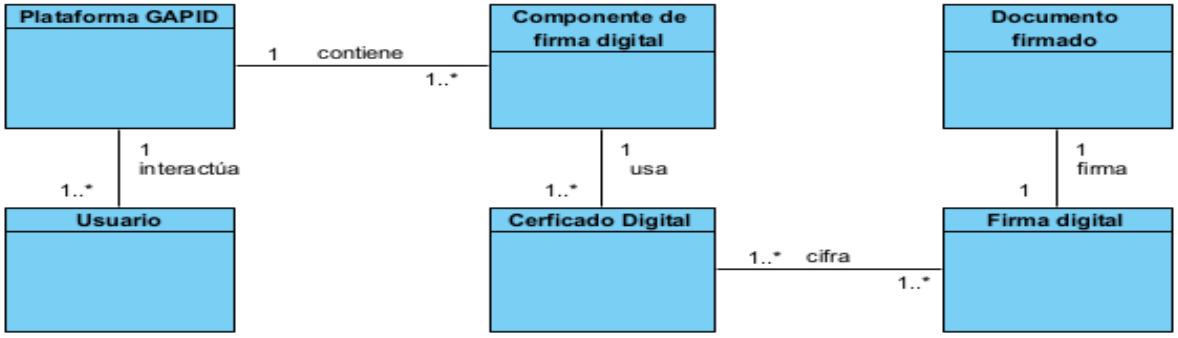

Figura 1. Modelo de dominio. Fuente: [Elaboración propia]

A continuación, se describe cada uno de los elementos identificados:

- Plataforma GAPID: Es un sistema de gestión de programas y proyectos de I+D+i.
- Componente de firma digital: Es una parte integral de la Plataforma GAPID que se utiliza para firmar documentos digitalmente.
- Usuario: Una persona o entidad que interactúa con la Plataforma GAPID y utiliza el Certificado Digital para firmar documentos.
- Certificado Digital: Un documento electrónico que vincula las credenciales de verificación del titular a su clave pública, permitiendo al usuario cifrar y firmar documentos digitalmente.
- Firma Digital: Un mecanismo criptográfico que se utiliza para verificar la autenticidad e integridad de un documento o mensaje. Se crea utilizando el Certificado Digital del usuario.

- Documento Firmado: Un documento o mensaje que ha sido verificado y autenticado mediante una Firma Digital.

  Prototipos de Interfaz de Usuario

  Para una mejor comprensión de la propuesta, la figura 2 muestra Prototipo de interfaz de usuario Visualizar selección de espacio de firma.

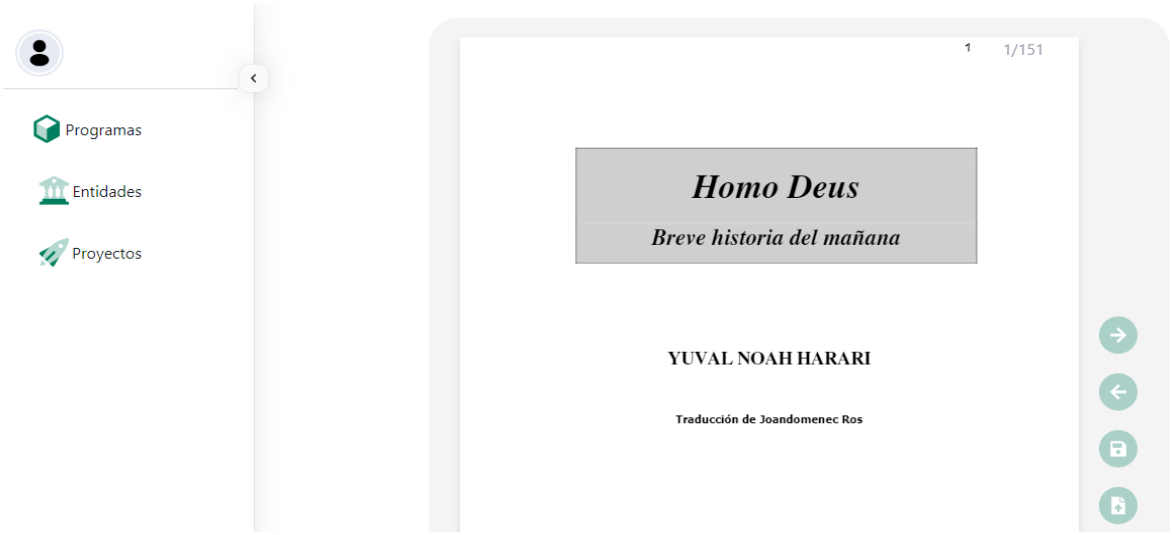

Figura 1. Prototipo de interfaz de "Visualizar selección de espacio de firma". [Fuente: Elaboración propia].

Los patrones GRASP son fundamentales para la distribución de responsabilidades en objetos dentro del diseño de software, presentados como patrones que constituyen un acrónimo para General Responsibility Assignment Software Patterns (Patrones Generales de Software para Asignar Responsabilidades) (Vargas Ortega, 2021). En la implementación del componente, se ejemplifican varios de estos patrones. El patrón Experto asigna la responsabilidad de ejecutar una tarea a la clase que posee los datos pertinentes, aplicado en la clase SignatureDataSources, la cual alberga toda la información necesaria para cumplir su función asignada. El patrón Controlador se encarga de gestionar el acceso a la lógica del negocio y controlar todo el proceso, como se evidencia en la clase PdfViewer, que maneja todo el proceso de firma de documentos y puede acceder a todas las clases del componente. Además, patrón de Bajo Acoplamiento pretende mantener el diseño de clases más independientes y reutilizables, con la clase SaveDocument interactuando únicamente con la clase controladora para minimizar el impacto de los cambios. Finalmente, el patrón de Alta Cohesión diseña la dependencia entre clases a partir de sus funcionalidades, presente en la clase CustomSignatureModal, que evita cargar de código innecesario a la controladora, mejorando la eficiencia del sistema.

Los estándares de código forman parte integral de las buenas prácticas en el desarrollo de software. Estas prácticas, aunque no formalizadas, son un conjunto de reglas que han evolucionado dentro de las comunidades de desarrolladores con el tiempo y que, cuando se aplican correctamente, pueden mejorar significativamente la calidad del código (Hamilton, 2023). En el desarrollo de la herramienta, se definió el estándar de codificación CamelCase después de un estudio preliminar. Este estándar fue elegido debido a su capacidad para reducir el esfuerzo necesario para leer y entender el código fuente, además de mejorar la apariencia del código al evitar el uso de abreviaturas (Prácticas de Codificación, 2024).

CamelCase es un estilo de escritura que se aplica a frases o palabras compuestas, nombrado así porque las mayúsculas intermedias en una palabra se asemejan a las jorobas de un camello (Hamilton, 2023). A continuación, se detallan algunas pautas específicas del estándar CamelCase aplicadas en el desarrollo:

- Los nombres de las clases serán en mayúscula, en caso de ser un nombre compuesto las siguientes palabras se escribirán de igual forma.
- Los nombres de los métodos serán con mayúscula, en caso de ser un nombre compuesto, la primera palabra será en minúscula y la siguiente en mayúscula.
- Los identificadores para las variables y los parámetros serán en minúsculas.
- Los nombres de variables o funciones deben ser lo suficientemente descriptivos no más de 15 caracteres.
- De haber comentarios serán en idioma español para una mejor comprensión.

La implementación de estas pautas de CamelCase busca estandarizar y optimizar el proceso de codificación, asegurando que el código sea legible, entendible y fácil de mantener, lo que en última instancia contribuye a la eficiencia y calidad del desarrollo del software.

Durante la fase de pruebas del sistema de firma digital, se realizaron pruebas en diferentes niveles: pruebas de sistema, pruebas de integración y pruebas de aceptación. Las pruebas de sistema, utilizando la técnica de caja negra, permitieron verificar que las funcionalidades del software cumplan con los requisitos esperados, identificando discrepancias y validando la calidad del producto. La partición equivalente, una técnica de caja negra, se aplicó para diseñar casos de prueba eficientes, cubriendo un amplio rango de entradas con menos pruebas. En la integración, se verificó la interoperabilidad entre los componentes del sistema GAPID, asegurando que el componente de firma digital funcionara correctamente dentro de la infraestructura existente.

Finalmente, las pruebas de aceptación validaron que el sistema satisface las necesidades del usuario final, evaluando escenarios críticos como la configuración del modo de firma y asegurando una experiencia de usuario satisfactoria. Estos resultados confirman la eficacia del proceso de pruebas para garantizar un software de alta calidad, fiable y seguro antes de su lanzamiento.

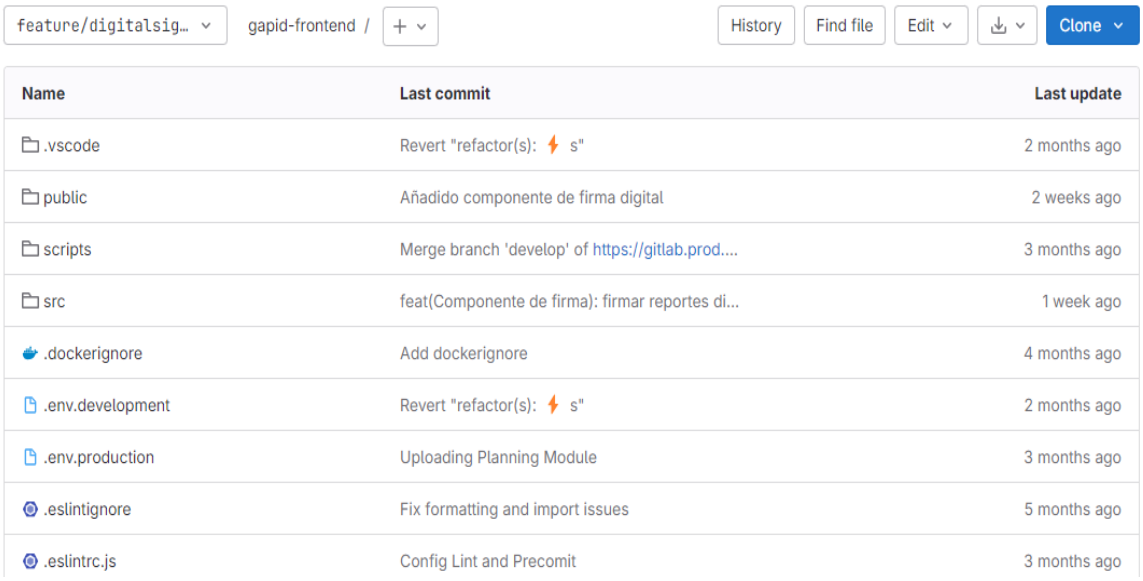

Figura 2. Pruebas de Integración – GitLab. [Fuente: Elaboración propia].

Realización de pruebas de integración y funcionamiento. Se realizaron comprobaciones para verificar el correcto funcionamiento dentro del sistema.

El desarrollo del Componente de firma digital en línea para el sistema de gestión de programas y proyectos de I+D+i GAPID se realizó definiendo ambiente de desarrollo, guiado por la metodología de desarrollo de software AUP-UCI. Visual Studio Code 1.89.1 es un editor de código fuente altamente popular y ampliamente utilizado por desarrolladores de software. Es una herramienta de código abierto desarrollada por Microsoft que ofrece una amplia gama de funciones y extensiones para mejorar la productividad y la eficiencia en el desarrollo de aplicaciones. Django REST Framework es un marco de trabajo (framework) web de Python de alto nivel que fomenta el desarrollo rápido y el diseño limpio y pragmático. Python 3.11 es un lenguaje de programación interpretado cuya filosofía hace hincapié en la legibilidad de su código. Se trata de un lenguaje de programación multiparadigma, ya que soporta parcialmente

la orientación a objetos, programación imperativa y, en menor medida, programación funcional. Es un lenguaje interpretado, dinámico y multiplataforma.

Como gestor de Bases de Datos se empleó PostgreSQL 14.0, el cual propicia crear bases de datos relacionales de código abierto que se destacan por su robustez, escalabilidad y cumplimiento de estándares. PostgreSQL ofrece una amplia gama de características avanzadas, como transacciones ACID, vistas, subconsultas, triggers y almacenamiento de procedimientos. Además, soporta una variedad de tipos de datos, incluyendo objetos JSON, arrays y hstore (para almacenar pares clave-valor).

Adicionalmente se empleó Docker 24.0.6, como plataforma diseñada para ayudar a los desarrolladores a construir, compartir y ejecutar aplicaciones con contenedores. Fue utilizado GitLab como plataforma de desarrollo colaborativo basada en la web que proporciona herramientas para la gestión del ciclo de vida del desarrollo de software, utilizando Git como sistema de control de versiones.

Conclusiones

En esta investigación se sustentaron las bases conceptuales y la necesidad de desarrollar un componente de firma digital en la plataforma GAPID. Esto permitió asegurar que la implementación de esta solución efectivamente permite cumplir los requisitos de autenticidad, integridad y no repudio de los documentos digitales en el sistema.

El análisis de soluciones similares permitió demostrar que la integración de un componente propio a la plataforma es la forma más efectiva de eliminar tanto la dependencia de herramientas externas que no ofrecen funcionalidades en línea como la necesidad de integraciones vía API que pueden generar costes innecesarios.

A partir de los requerimientos identificados en la investigación fue posible el desarrollo del componente de firma digital. En este sentido fue importante la definición de un ambiente de desarrollo y un modelo de dominio los cuales permitieron establecer la base estructural de la implementación del componente.

El componente desarrollado contribuye a la firma digital de los documentos generados y subidos a la plataforma GAPID propiciando un mecanismo ágil y seguro.

Conflictos de intereses

Los autores declaran no tener conflictos de interés sobre la investigación.

Contribución de los autores

1. Conceptualización: Arturo Orellana García.
2. Curación de datos: Yan Carlos Escobar Pupo, Leodan Vega Izaguirre
3. Análisis formal: Yan Carlos Escobar Pupo, Arturo Orellana García, Leodan Vega Izaguirre
4. Adquisición de fondos: Arturo Orellana García
5. Investigación: Yan Carlos Escobar Pupo
6. Metodología: Arturo Orellana García, Yan Carlos Escobar Pupo
7. Administración del proyecto: Arturo Orellana García
8. Recursos: Arturo Orellana García
9. Software: Yan Carlos Escobar Pupo
10. Supervisión: Arturo Orellana García, Leodan Vega Izaguirre
11. Validación: Yan Carlos Escobar Pupo
12. Visualización: Yan Carlos Escobar Pupo
13. Redacción – borrador original: Cristian Rey Ruiz Castro
14. Redacción – revisión y edición: Cristian Rey Ruiz Castro, Arturo Orellana García

Financiamiento

La investigación que da origen a los resultados presentados en la presente publicación recibió fondos del Programa Sectorial de Telecomunicaciones e Informatización de la Sociedad, bajo el código PS161LH001-022.

Referencias

Diaz, S. M. 2014. Pruebas de seguridad en aplicaciones web como imperativo en la calidad de desarrollo del software. 2014.

DocuSign. 2024 Electronic Signature: Fast & Easy e-Signature. Recuperado 14 de marzo de 2024, de https://www.docusign.com/products/electronic-signature

Fernández, J. F. (2022). Formatos digitales: Propiedades técnicas y contextos de uso. Editorial UOC.

Figueroa, R G Solís, C J Coelho, F (2012). Metodologías tradicionales VS. Metodologías.

García Holgado, Alicia, A. Vázquez-Ingelmo, y F. J. García-Peñalvo (2022). «Modelo de dominio».

GeeksforGeeks (s. f.). Fundamentals of Software Architecture. (2020, noviembre 1). https://www.geeksforgeeks.org/fundamentals-of-software-architecture/

Gitlan, D. (2023). Qué es un certificado x.509 Certificado. SSL Dragon. https://www.ssldragon.com/es/blog/que-es-certificado-x-509/

Gitnux (2023). https://blog.gitnux.com/es/metodologias-de-desarrollo-de-software

Guru99 (2024). ¿Qué son las pruebas de aceptación del usuario (UAT)? https://www.guru99.com/es/user-acceptance-testing.html

Hamilton, D. (2023). Estándares de codificación de software y pautas de programación. Parasoft. https://es.parasoft.com/blog/an-ounce-of-prevention-software-safety-security-through-coding-standards/

Identidad digital (2015). Identificación Y Estado Civil, R. La identificación desde los registros parroquiales al DNI electrónico.

López, M.J.L. (2010). Criptografía y Seguridad en los Computadores. 4ta Edición. España: s.n.

Menzes, A.J., Oorschop, P.C. van y Vanstone, S.A (1996). Handbook of applied cryptography [en línea]. S.l.: s.n. (Consulta: 12 mayo 2024). Disponible en: http://labit501.upct.es/~fburrull/docencia/SeguridadEnRedes/teoria/bibliography/HandbookOfAppliedCryptography_AMenezes.pdf.

Pérez Piedra, A., Hernández, J., Alfonso Cordoví, A., & Pérez Abileva, A. (2018). Portafirmas Digital de la Universidad de las Ciencias informáticas. Serie Científica de la Universidad de las Ciencias Informáticas, 11(8), 1-15.

Pousa, A. (2011). Algoritmo de cifrado simétrico AES [Tesis, Universidad Nacional de La Plata]. http://sedici.unlp.edu.ar/handle/10915/4210

Quiroga, H. E. (2024.). Criptografía de llave pública. Estudio y simulación de módulos que componen el sistema RSA. Recuperado 12 de marzo de 2024, de http://tesismatematica.ucoz.es/_ld/0/5_TFG_Quiroga_H..pdf

Ramírez-Bedoya, D. L., Branch-Bedoya, J. W., & Jiménez Builes, J. A. (2019). Metodología de desarrollo de software para plataformas educativas robóticas usando ROS-XP. Revista politécnica, 15(30), 55-69.

Rivas Lara, A. E. (2020). Influencia del uso del certificado digital en el proceso de formalización de negocios en la municipalidad distrital PÍTIPO–FERREÑAFE EN EL AÑO 2020. https://repositorio.udl.edu.pe/handle/UDL/408

Rivera Anastacio, D. K., & Valdivia Escobar, J. H. (2021). Implementación de la metodología Magerit V3 para mejorar la gestión de riesgos de Seguridad de la Información y propuesta de políticas de seguridad basadas en

norma técnica peruana ISO/IEC 27001:2014 en la Dirección Regional de Trabajo y Promoción del Empleo de Huánuco – 2021. http://repositorio.unheval.edu.pe/handle/20.500.13080/7066

Rodríguez, T (2015). Actualización de los roles de la metodología.

Silva, N.M.M (2004). Estudio monográfico sobre técnicas de criptografía. Soyapango, El Salvador: Universidad Don Bosco]. Disponible en: http://rd.udb.edu.sv:8080/jspui/bitstream/11715/580/1/034436_tesis.pdf

Sommerville, I (2005). Ingeniería del software. Pearson Educación.

Vargas Ortega, G. A. (2021). Lineamientos para el diseño de aplicaciones web soportados en patrones GRASP. Ciencia e Ingeniería: Revista de investigación interdisciplinar en biodiversidad y desarrollo sostenible, ciencia, tecnología e innovación y procesos productivos industriales, 8(2), 4.

Vega, A. (2019) Método basado en la programación por capas para generar código automático desde el diagrama de clases. Revista Peruana de Computación y Sistemas, 2(2):25-42. http://dx.doi.org/10.15381/rpcs.v2i2.17015