Tipo de artículo: Artículo original

Propuesta de solución para la gestión de la seguridad informática de los datos personales del ciudadano

Proposal of solution for the computer security management of the personal data of the citizen

Aivys Benitez Lavastida[1*] **https://orcid.org/0000-0002-7186-7002**
Haidee Tamayo Ramos[2] **https://orcid.org/0000-0002-3531-0960**
Ivette Barrientos Núñez[3] **https://orcid.org/0000-0002-7334-4475**

[1] Dirección de Informatización, Universidad de Ciego de Ávila Máximo Gómez Báez. aivys@unica.cu
[2] Empresa de Tecnologías de la Información para la Defensa, Xetid. htamayo@xetid.cu
[3] Dirección de Informatización, Universidad de Ciego de Ávila Máximo Gómez Báez. ivette@unica.cu

*** Autor para correspondencia: aivys@unica.cu**

Resumen

Como parte del proceso de informatización de la sociedad cubana, a las tareas relacionadas con el Gobierno Electrónico se le ha prestado especial atención, con la finalidad de mejorar la información y los servicios ofrecidos a los ciudadanos, incrementar la transparencia del sector público y la participación de la población. En este contexto, la Ficha Única del Ciudadano, constituye la plataforma informática que permite la interoperabilidad entre los registros públicos, y de estos con las instituciones, organismos y entidades que prestan servicios y trámites a las personas naturales y jurídicas, para el acceso a los datos de identidad de los ciudadanos. En este marco se hace imprescindible garantizar la autenticación, seguridad, legitimidad y autenticidad de dicha plataforma en tanto la misma procesa información clasificada. El objetivo esencial de la presente investigación es proponer una solución para la gestión de la seguridad informática de los datos personales en la plataforma Ficha Única del Ciudadano.

Palabras clave: gestión de la seguridad; seguridad informática; seguridad de la información; datos personales; *WSO2 Identity Server*

Abstract

As part of the computerization process of Cuban society, special attention has been paid to tasks related to Electronic Government, in order to improve the information and services offered to citizens, increase the transparency of the public sector and the participation of the population. In this context, the Citizen's Single Record constitutes the computer platform that allows interoperability between public registries, and of these with the institutions, organizations and entities that provide services and procedures to natural and legal persons, for access to the identity data of citizens. In this context, it is essential to guarantee the authentication, security, legitimacy and authenticity of this platform as it processes classified information. The essential objective of this research is to propose a solution for the management of the computer security of personal data on the platform Citizen's Single Record.

Keywords: *security management; computer security; information security; personal data; WSO2 Identity Server*

Recibido: 20/04/2021
Aceptado: 26/09/2021

Introducción

La aplicación de las Tecnologías de la Información y las Comunicaciones (TIC) en la gestión de la información y el conocimiento ha tenido un significativo impacto tanto en la gestión empresarial como en las diversas esferas de la vida social, lo cual ha demandado un cambio de perspectiva en la organización de los procesos y en la gestión de la seguridad informática.

En el caso particular de Cuba, el marco legal para el proceso de informatización de la sociedad establece que: "Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular determinan los servicios que brindan a la población, facilitan y optimizan los trámites y el acceso a la información, así como la atención ciudadana en línea, y son responsables del uso de las plataformas tecnológicas que protejan los datos del usuario y garanticen la veracidad y autenticidad de la información" (Consejo de Estado de la República de Cuba, 2019).

Para apoyar lo anterior planteado se crea la Ficha Única del Ciudadano, que "constituye la plataforma informática que permite la interoperabilidad entre los registros públicos, y de estos con las instituciones, organismos y entidades que prestan servicios y trámites a las personas naturales y jurídicas, para el acceso a los datos de identidad de las personas naturales" (Ministerio de Justicia, 2020). Por lo que se hace necesario diseñar una propuesta de solución para la gestión de la seguridad informática de los datos personales del ciudadano en dicha plataforma.

Materiales y métodos

Para el cumplimiento de los objetivos específicos trazados en esta investigación se tiene en cuenta el método histórico lógico para determinar los antecedentes fundamentales del proceso de gestión de la seguridad informática de los datos personales; el analítico-sintético para la caracterización de la gestión de seguridad informática de los datos personales; el método de inducción deducción: para la conceptualización y caracterización del sistema de gestión de la seguridad informática de los datos personales; el hipotético deductivo para avanzar de lo general a lo particular a la hora de elaborar conclusiones parciales y generales; el sistémico estructural funcional para la elaboración de la propuesta del sistema informático, comprobando la compatibilidad con otros subsistemas, obteniendo la información necesaria de las bases de datos y posteriormente haciendo peticiones a las Interfaces de Programación de Aplicaciones (API). Se emplean las técnicas de observación y las entrevistas para determinar y comprender el proceso de gestión de la seguridad informática de los datos personales. Se determina una población de tres entidades de Ciego de Ávila,

Aduana, XetiD y Cepil, 8 directivos del Registro Civil entre ellos el director, la registradora principal, los abogados en funciones, oficinistas de registro y 4 oficiales del MININT que ocupan el cargo de administradores de red.

Antecedentes históricos y conceptuales del proceso de gestión de la seguridad informática de los datos personales del ciudadano

Los hombres entendidos desde su concepción existencial, se caracterizan por la posesión de rasgos distintivos que permite individualizarlos, lo cual se ha traducido en una identidad, compuesta por diferentes atributos que posibilitan caracterizarlos tanto sus rasgos intangibles como sus particularidades físicas. Dichos atributos (que pueden ir desde su nombre hasta sus creencias), permiten su reconocimiento como sujeto con particularidades y como individuo distinguible de otros (Tejada Berrio, 2021).

El estudio de la literatura especializada evidencia que antes de 1990, pocos elementos de la identidad personal estaban digitalizados y apenas existía interconexión entre los centros que almacenaban y gestionaban esta información, que como tendencia se encontraban en grandes ordenadores centrales de las Administraciones Públicas, entidades financieras y empresas de servicios. De ahí que se coincida con (Subías, 2012) que la irrupción de Internet, a finales de esa década, propició el desarrollo de un proceso acelerado de digitalización de la información de las personas naturales y jurídicas, dotándola de un carácter estratégico para las instituciones, organismos y entidades que prestan servicios y trámites en correspondencia con el avance socioeconómico.

El reconocimiento de la información como un activo de vital importancia ha exigido la adopción de un "conjunto de medidas administrativas, organizativas, físicas, legales y educativas dirigidas a prevenir, detectar y responder a las acciones que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce o conserva por medio de las TIC" (Consejo de Estado de la República de Cuba, 2019). De ahí que la seguridad informática adquiere un papel significativo, donde los protocolos, las tecnologías (hardware o software), los dispositivos, las herramientas y las técnicas permiten proteger los datos que son esenciales para la disminución de las amenazas presentes (Ríos Gutiérrez, Bohada Jaime, y Delgado González, 2018).

En la actualidad existen varios autores que abordan el tema de la seguridad informática, así como su definición y principales componentes que la conforman, entre ellos destacan (Gil Vera y Gil Vera, 2017; Gómez Vieites, 2014; Hurtado Valero, 2021; Voutssas M., 2010; Solarte Solarte, Enriquez Rosero, y Benavides Ruano, 2015).

La literatura revisada de los autores antes citados aparecen como elementos que contribuyen a la definición de seguridad informática los siguientes:

- Proceso o conjunto de medidas.
- Conformado por métodos, técnicas, procedimientos, normas y estrategias.
- Con el propósito asegurar la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información, incluyendo hardware y software. De igual manera permite reducir la posibilidad de que se produzcan incidentes de seguridad, facilitar su rápida detección, minimizar su impacto y conseguir la rápida recuperación de los daños causados.

Valoración de la situación actual del proceso de gestión de la seguridad informática de los datos personales del ciudadano

En Cuba los Registros Públicos son los responsables de inscribir o anotar en los libros registrales o cualquier otro soporte, los elementos esenciales respecto a los hechos, actos, bienes, personas, documentos, derechos, obligaciones y otras circunstancias de interés general, para otorgar certeza y validez como fundamento de la seguridad jurídica; además, su funcionamiento se rige por los principios de integración, veracidad, interoperabilidad, auditabilidad, vitalidad, seguridad y publicidad que norma el derecho a consultar por las personas naturales y jurídicas que tengan interés de su conocimiento (Consejo de Estado de la República de Cuba, 2015).

Como parte del cambio de perspectiva en la organización de los procesos en el Sistema de Registros Públicos de la República de Cuba, impulsado por la implementación de las TIC, se refleja en el Proyecto de Ley de Persona Natural la necesidad de establecer “el derecho de toda persona de acceder a sus datos personales en los Registros Públicos, interesar la protección de estos y obtener la debida corrección, rectificación, modificación, actualización o cancelación”. Además, se incorporan varios principios que son fundamentales para la identificación única como la unicidad, validez jurídica de los documentos electrónicos, así como seguridad de la información bajo la protección de los órganos, organismo de la Administración Central del Estado y entidades nacionales que tienen a su cargo los mismos; dicha información será modificada únicamente por el registrador o por decisión judicial, y donde quede asentada será inamovible solamente para permitir la rectificación de la correcta identidad de la persona (Consejo de Estado, 2019).

Añade la interoperabilidad semántica en el uso de nomencladores y clasificadores establecidos por la Oficina Nacional de Estadística e Información (ONEI) de manera obligatoria y uniforme, y las instituciones que están

obligadas a utilizar datos e información de las personas naturales lo hagan con la información que consta en los registros. De esta forma se garantiza que los datos registrales estén centralizados y controlados para su posterior uso por parte de las organizaciones y entidades, propiciando una respuesta efectiva en su gestión (Consejo de Estado, 2019).

Pese a lo legalmente establecido en el proyecto de Ley de Persona Natural, en la actualidad el país cuenta con dos sistemas informáticos que se dedican a registrar los datos de los ciudadanos, el Sistema Informático del Registro del Estado Civil (SIREC) que se encarga de registrar los datos de nacimiento, estado civil y defunción de las personas, perteneciente al Ministerio de Justicia; y el Sistema Único de Identificación Nacional (SUIN) que registra el número de carnet de identidad, la dirección particular, todos los cambios de dirección que realiza la persona en el transcurso de su vida, además de los datos fenotípicos. SUIN pertenece al Ministerio del Interior (MININT), donde se protege la información en una red de alta seguridad, y solo tienen acceso a ella personal militar autorizado. No siendo así en el caso de SIREC, que es una institución civil en la cual labora personal civil capacitado y han ocurrido sucesos de fraude de identidad. Se debe añadir que SIREC centraliza la información digital en el Registro Central y se nutre de la gestión de la información realizadas en las provincias, pero no tiene interoperabilidad con SUIN por lo que se duplica la información de las personas naturales.

A partir de la técnica de observación realizada y las entrevistas aplicadas a trabajadores de estas dos entidades, enfocándolas al acceso de la información, los permisos que se les concede, y del tránsito de los datos antes de llegar a la base de datos del software, se constata que un 90% de los trabajadores del Registro Civil no introducen inmediatamente los datos registrados en el libro oficial, un 30% afirma no haber tenido acceso al sistema por cuestiones de ausencia laboral de los responsables. En las observaciones hechas a las entidades que han informatizado sus procesos como Aduana, Cepil y XetiD; se reflejan dificultades asociadas a errores en nombres, cambios de apellidos, certificados falso y direcciones erróneas, al no tener una fuente confiable para nutrir sus software. De ahí que se evidencia la necesidad de diseñar un sistema de gestión de la seguridad informática para la centralización y control de la información de las personas naturales cubanas.

Resultados y discusión

Propuesta de solución para la seguridad informática de los datos personales del ciudadano

Con el propósito de superar las insuficiencias expuestas, se ha desarrollado un trabajo conjunto por los ministerios de Justicia, del Interior, de las Comunicaciones y la Empresa de Tecnologías de la Información para la Defensa, con el objetivo de crear la plataforma informática Ficha Única del Ciudadano, la cual está estructurada para almacenar los datos ya unificados de los ciudadanos en varios microservicios, e integrarlos, para desde allí hacer las peticiones. El software favorece que las empresas y servicios públicos del país puedan informatizar sus procesos, nutriéndolos con información legal, integrándolos a otros registros como el de la División Política Administrativa y el de Bienes e Inmuebles, el de Vivienda, entre otros.

Lo anterior expuesto revela la importancia de la centralización y control de la información, tratarla con altos niveles de seguridad que contribuya, desde una dinámica de relaciones de coordinación e integración, contar con una infraestructura para disponer de su propia información, compartir sus recursos y poseer canales de comunicación rápidos y eficientes.

Caracterización de las herramientas

Como propuesta para garantizar la seguridad dentro de la plataforma de Ficha Única del Ciudadano se encuentra *WSO2 Identity Server*, que forma parte de la gran gama de productos de *WSO2 ESB* (Bus se Servicios Empresariales), donde se utiliza además *API Manager* para gestionar las interfaces de acceso a los recursos y servicios que darán respuesta a las peticiones por parte del cliente.

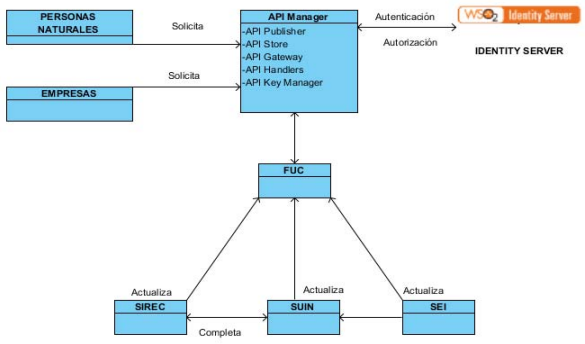

Figura 1. Modelo de dominio implementando *Identity Server* de *WSO2*.

WSO2 es una compañía que ofrece una plataforma *Open Source* con distintas aplicaciones bajo un modelo de Arquitectura Orientada a Servicios *(SOA)* y con licencia Apache cuyo objetivo es crear, publicar y gestionar todos los aspectos relativos a *API*s y su ciclo de vida. El ecosistema de productos *WSO2* está soportado sobre una suite que permite el manejo de diversos escenarios para la gestión de identidades y procesos de autorización y autenticación (CHAKRAY, 2021).

WSO2 Identity Server (IS) es la herramienta de la suite de productos de *WSO2* que posibilita la gestión y administración de identidades, privacidad y seguridad en un sistema. Está basado en distintos estándares abiertos como *SAML*, *OAuth* o *OIDC* y con la posibilidad de realizar implementación local, en la nube o híbrida (WSO2, 2021).

Se considera a continuación realizar un contraste desde la planteado por (Gómez Vieites, 2014) refiriéndose a las funciones y servicios de seguridad de la información que contribuyen a cumplir los objetivos dentro de la gestión de la seguridad informática, hasta los requisitos que implemente *IS* determinando de esa forma la aplicación de lo teórico a lo práctico.

Figura 2. Requisitos de seguridad implementados por *Identity Server* de WSO2.

Tomado de: (CHAKRAY, 2016)

Los componentes relacionados con la arquitectura planteada por (WSO2, Identity Server Documentation, 2021) son:

- Proveedores de servicios (*Service Providers*): es una entidad que brinda servicios web a los usuarios. Un proveedor de servicios confía en un proveedor de identidad (*IdP*) confiable para la autenticación y

autorización. IS actúa como *IdP* y realiza la tarea de autenticar y autorizar al usuario del proveedor de servicios.

- Autenticación entrante (*Inbound authentication*): puede manejar cualquiera de las siguientes solicitudes:
    - *SAML SSO*: es un estándar abierto de *OASIS* para representar e intercambiar la identidad del usuario y los datos de autenticación entre las partes. *SAML* proporciona la capacidad de inicio de sesión único basado en la web. *IS* es compatible con *SAML 2.0*.
    - *OAuth/OpenID Connect*: *OAuth2* parte de 3 fases: solicitar una concesión de autorización (*Authorization Grant*), intercambiar la concesión de autorización por un token de acceso (*Access Token*) y acceder a los recursos utilizando este token de acceso. *OpenID Connect* es otra capa de identidad sobre *OAuth 2.0*. Permite a los clientes verificar la identidad del usuario final en función de la autenticación realizada por un servidor de autorización, así como obtener información de perfil básica sobre el usuario final de una manera interoperable y de tipo *REST*.
    - Servicio de token de seguridad pasivo (*Passive STS*): es un proveedor de identidad basado en software, responsable de emitir tokens de seguridad, especialmente tokens de software, como parte de un sistema de identidad basado en *claims*.
- Framework de Autenticación (*Authentication framework*): ayuda a asignar *claims* locales a *claims* de proveedores de servicios y viceversa. También le permite asignar *claims* locales a *claims* de proveedores de identidad y viceversa. El aprovisionamiento *Just-in-Time* (*JIT*) le permite crear usuarios sobre la marcha sin tener que crear cuentas de usuario por adelantado. *JIT* funciona con su proveedor de identidad para pasar la información correcta del usuario al *IS*.
- Autenticadores locales (*Local authenticators*): son procesos de autenticación disponibles dentro del propio IS. La autenticación de *username/password* se realiza autenticando las credenciales ingresadas contra los valores en el almacén de usuarios conectado al *IS*.
- Autenticadores federados (*Federated authenticators*): son procesos de autenticación que no están disponibles en *IS*. Estos deben estar configurados para llegar a aplicaciones externas para realizar el proceso de autenticación y enviar la respuesta de vuelta al *IS*.
- Proveedores de identidad (*Identity providers*): realizan la autenticación. también se conocen como aplicaciones externas (*External Applications*). Los autenticadores específicos del protocolo (*SAML2, OpenID Connect, WS-Federation* (pasivo)) representan aplicaciones que usan estos protocolos para solicitudes de autenticación.

- Framework de Aprovisionamiento (*Provisioning framework*): es responsable de todo el trabajo de aprovisionamiento realizado por *IS*. Este se integra con el componente *User Store Manager* y también recibe solicitudes de aprovisionamiento del marco de autenticación.
- Gestor de autorizaciones (*Authorization manager*): *IS* contiene una gestión y auditoría de derechos avanzadas. Proporciona gestión de derechos para cualquier llamada *REST* o *SOAP*. Proporciona control de acceso basado en atributos y *claims* a través de *XACML*, *WS-Trust*, *OpenID Connect* y gestión de *claims*.
- Configuraciones de *IdP* y *SP*: Las configuraciones de proveedor de identidad y proveedor de servicios proporcionan la base para todas las acciones que ocurren dentro de los *frameworks* de autenticación y de aprovisionamiento.
- Aprovisionamiento entrante (*Inbound provisioning*): puede venir en forma de *SCIM* (*System for Cross-domain Identity Management*) o *SOAP* (*Simple Object Access Protocol*). La especificación *SCIM* está diseñado para facilitar la gestión de identidades de usuario en el *IS*, crea, mantiene y elimina cuentas de usuario e identidades relacionadas en uno o más sistemas o aplicaciones en respuesta a procesos de negocios que son iniciados por humanos directamente o por tareas automatizadas. *SOAP* es un protocolo para intercambiar mensajes basados en *XML* a través de una red, normalmente usando *HTTP*. Los servicios *SOAP* se definen mediante el lenguaje de definición de servicios web (*WSDL*) y se puede acceder a ellos mediante una *URL* que se conoce como punto final *SOAP*. Aquí, se utiliza una *API SOAP* para aprovisionar usuarios al *IS*.
- Gestor de almacenamiento de usuarios (*User store manager*): IS implementa un almacén de usuarios flexible a través de *LDAP* incorporado (con tecnología de *ApacheDS*), *LDAP* externo, *Microsoft Active Directory* o cualquier base de datos *JDBC* (*Java Database Connectivity*).
- Gestor de *claims* (Claim manager): Un *claims* es una información sobre un tema en particular. Puede ser cualquier cosa de la cual el sujeto es propietario o está asociado, como nombre, grupo, preferencias, etc.
- Auditoria (*Auditing*): *IS* admite la auditoría de operaciones privilegiadas mediante el sistema de auditoría distribuido (*XDAS*). También le permite monitorear y recopilar estadísticas de acceso y rendimiento estándar. El componente de análisis de *IS* admite sesiones de monitoreo y estadísticas de autenticación.
- Gestor de identidad (*Identity Manager*): Tiene una interfaz de usuario muy personalizable y se puede implementar fácilmente para garantizar la máxima seguridad de su sistema.

- Aprovisionamiento saliente (*Outbound provisioning*): puede enviar solicitudes de aprovisionamiento a aplicaciones que admitan los siguientes conectores. *SCIM*, *SPML*, *Google* o *Salesforce*. Estos conectores se usan para llegar a los proveedores de identidad que realizan el aprovisionamiento

API Publisher: Aplicación web utilizada para publicar *API*s, gestionarlas y documentarlas.
API Store: Aplicación web utilizada como catálogo de *API*s que permite la suscripción a las mismas.
API Gateway: Esta pieza está basada en el *ESB* de *WSO2*. Actúa como un proxy que intercepta las peticiones entrantes y aplica políticas de seguridad y disponibilidad.
API Handlers: Componentes utilizados por *API Gateway* para añadir determinados comportamientos ante los mensajes entrantes como pueden ser: monitorización, autenticación, publicación en *Google Analytics*.
API Key Manager: Componente que gestiona la seguridad y tokens de acceso. Está basado en el protocolo *OAuth 2.0*.

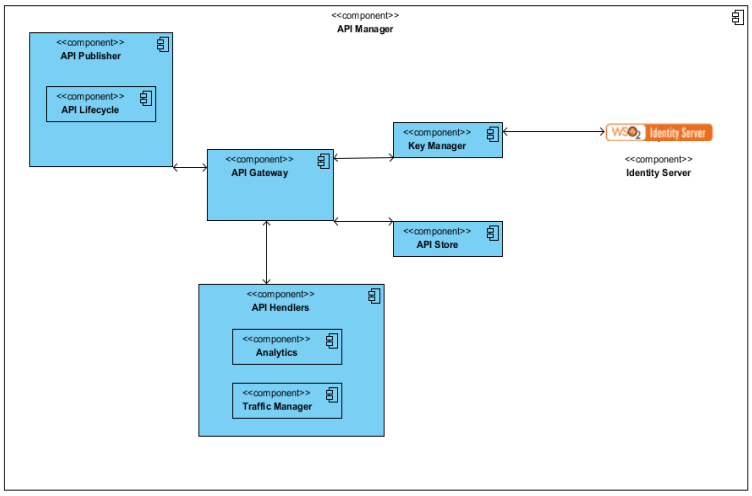

Figura 3. Diagrama de componentes del API *Manager*.

A continuación, se muestra el diagrama de despliegue de la solución propuesta teniendo en cuenta los elementos anteriormente analizados.

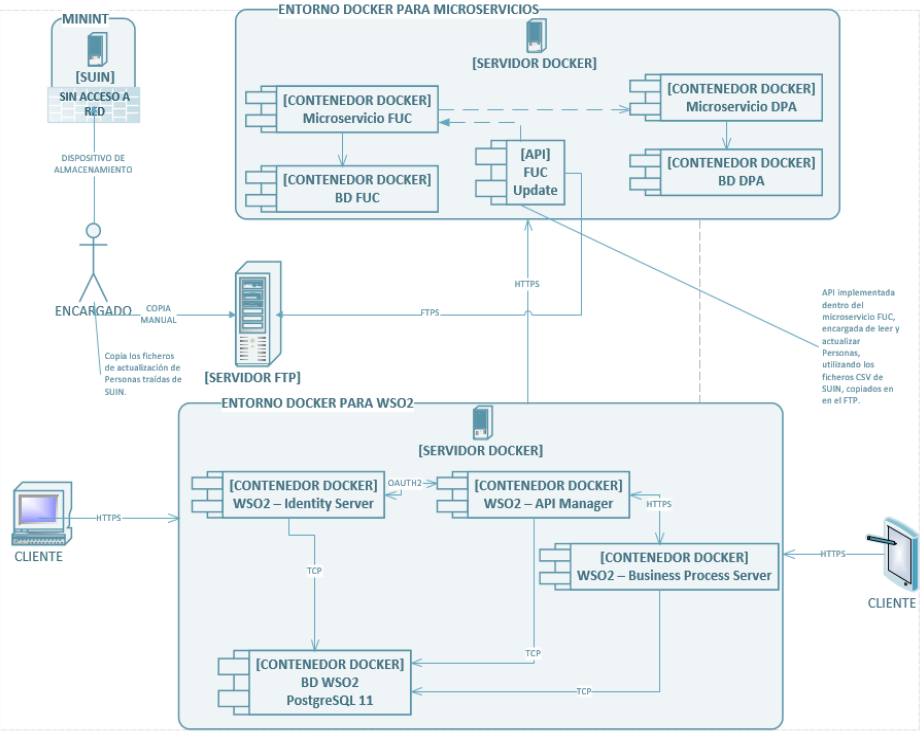

Figura 3. Requisitos implementados por *Identity Server de WSO2*.

Conclusiones

El análisis del proceso de gestión de la seguridad informática de los datos personales de los ciudadanos, de conjunto con la revisión bibliográfica permitieron corroborar la necesidad de crear una propuesta informática simple y fácil de usar, que facilite el manejo de la información en proceso. La necesidad de interactuar con subsistemas y terceros demandó el uso de las APIs, al ser ellas el basamento de la transformación digital. El modelo de despliegue ha demostrado ser factible, rápido, escalable y se propone utilizarlo de referencia en futuras situaciones similares, por ejemplo, en el despliegue del resto de los registros.

Conflictos de intereses

Los autores no poseen conflictos de intereses.

Contribución de los autores

1. Conceptualización: Aivys Benitez Lavastida
2. Curación de datos: Aivys Benitez Lavastida, Haidee Tamayo Ramos
3. Análisis formal: Aivys Benitez Lavastida, Haidee Tamayo Ramos
4. Investigación: Aivys Benitez Lavastida
5. Metodología: Aivys Benitez Lavastida
6. Software: Aivys Benitez Lavastida, Haidee Tamayo Ramos, Ivette Barrientos Núñez.
7. Supervisión: Haidee Tamayo Ramos
8. Validación: Haidee Tamayo Ramos, Ivette Barrientos Núñez
9. Visualización: Haidee Tamayo Ramos, Ivette Barrientos Núñez
10. Redacción – borrador original: Aivys Benitez Lavastida, Haidee Tamayo Ramos, Ivette Barrientos Núñez
11. Redacción – revisión y edición: Aivys Benitez Lavastida, Haidee Tamayo Ramos, Ivette Barrientos Núñez.

Financiamiento

El trabajo no requirió financiación. Este forma parte del desarrollo de la Empresa de Tecnologías de la Información para la Defensa en colaboración con la Universidad de Ciego de Ávila Máximo Gómez Báez.

Referencias

CHAKRAY. Implementación de autenticación federada con WSO2 Identity Server 5.1. [Sitio Web], 2016. [Recuperado el 15 de Febrero de 2021] Disponible en: [https://www.chakray.com/es/wso2-que-es-y-que-soluciones-ofrece/]

CONSEJO DE ESTADO DE LA REPÚBLICA DE CUBA. De los registros públicos de personas naturales. Proyecto-Ley, Consejo de Estado, La Habana, 2019.

CONSEJO DE ESTADO DE LA REPÚBLICA DE CUBA. Del sistema de registros públicos de la república de cuba. Decreto Ley No. 335, Consejo de Estado, La Habana, 2015. Disponible en: https://www.gacetaoficial.gob.cu/es/gaceta-oficial-no-40-extraordinaria-de-2015

CONSEJO DE ESTADO DE LA REPÚBLICA DE CUBA. Sobre la Informatización de la Sociedad en Cuba. Decreto-Ley No. 370, Consejo de Estado, La Habana, 2019. Disponible en: https://www.gacetaoficial.gob.cu/es/gaceta-oficial-no-45-ordinaria-de-2019

GIL VERA, V. D., & GIL VERA, J. C. Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. Scientia Et Technica, 2017, 22 (2): 193-197. Disponible en: https://www.redalyc.org/pdf/849/84953103011.pdf

GÓMEZ VIEITES, Á. Enciclopedia de la Seguridad Informática, 2da Edición. España, RA-MA, S.A, 2014. 830 p. Disponible en: https://books.google.com.ec/books?id=Bq8-DwAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=true

HURTADO VALERO, D. F. Manual de buenas prácticas de seguridad informática en redes domésticas. Tesis de Maestría, Universidad Nacional Abierta y a Distancia – UNAD, Bogotá - Colombia, 2021. Disponible en: https://repository.unad.edu.co/handle/10596/39430

MINISTERIO DE JUSTICIA. Reglamento sobre la organización y el funcionamiento de la Ficha Única del Ciudadano. Resolución 484/2020, Ministerio de Justicia, La Habana, 2020, Disponible en: https://www.gacetaoficial.gob.cu/es/gaceta-oficial-no-67-extraordinaria-de-2020

RÍOS GUTIÉRREZ, G. V., BOHADA JAIME, J. A., & DELGADO GONZÁLEZ, I. A. Gestión de seguridad de la información en las organizaciones. Investigación e Innovación en Ingeniería de Software. Investigación e Innovación en Ingeniería de Software, 2018, (2): 111-178. Disponible en: https://www.researchgate.net/profile/Ivan_Delgado_Gonzalez/publication/343167096_Seguridad_de_la_Informacion_en_las_organizaciones/links/5f19eb2345851515ef44b578/Seguridad-de-la-Informacion-en-las-organizaciones.pdf

SOLARTE SOLARTE, F. N., ENRIQUEZ ROSERO, E. R., & BENAVIDES RUANO, M. D. Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica ESPOL – RTE, 2015, 492-507. Disponible en: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

SUBÍAS, M. P. Identidad digital. Revista de Pensamiento, Sociedad y Tecnología, 2012, (91): 1-5. Disponible en: https://books.google.com/books?hl=en&lr=&id=0KnHCgAAQBAJ&oi=fnd&pg=PA55&dq=Identidad+digital+Sub%C3%ADas&ots=KZ8OCLRPIO&sig=okJc0MDondZaOJjmf0SYEGssHSY

TEJADA BERRIO, J. Datos personales y pilares de la seguridad de la información. Tesis de grado, Universidad Pontificia Bolivariana, Facultad de Derecho, Medellín - Colombia, 2021 Disponible en: https://repository.upb.edu.co/handle/20.500.11912/8341

VOUTSSAS M., J. Preservación documental digital y seguridad informática. Investigación Bibliotecológica, 2010, 24(50), 127-155. Disponible en: http://www.scielo.org.mx/pdf/ib/v24n50/v24n50a8.pdf

WSO2. Arquitectura [Sitio Web], 2021. [15 de Febrero de 2021] Disponible en: [https://is.docs.wso2.com/en/latest/get-started/architecture/]

WSO2. Identity Server Documentation [Sitio Web], 2021. [15 de Febrero de 2021] Disponible en: de [https://is.docs.wso2.com/en/latest/]