Administración Segura de Documentos de Carpeta Ciudadana

Jonatan Legro, María Mancipe, David Mosquera, Carlos Pinilla
Estudiantes Maestría en Seguridad de la Información
Departamento de Ingeniería de Sistemas y Computación
Universidad de Los Andes. Bogotá, Colombia
Junio 2019

1. Introducción

El servicio de Carpeta Ciudadana es una iniciativa que "[…] permite el almacenamiento y conservación electrónica de mensajes de datos en la nube para las personas naturales o jurídicas, en donde éstas pueden recibir, custodiar y compartir de manera segura y confiable la información generada en su relación con el Estado a nivel de trámites y servicios." [1] De esta forma, los colombianos sabrán dónde encontrar los documentos más importantes que se han producido a lo largo de los años en su relación con el Estado, accediendo a ellos de forma fácil y con la posibilidad de compartirlos para agilizar trámites con las entidades públicas, a la vez que se fomentará la apropiación de las TIC. [2]

Este tipo de servicio no es una novedad:

- Estonia cuenta con el sistema Xroad Está basado en blockchain y es un desarrollo de código abierto (que no es propiedad de ninguna empresa) que aloja módulos de servicio tanto para las personas como para las empresas, que van desde la declaración de impuestos y la solicitud de una visa hasta la historia clínica en línea.[1]
- El Gobierno Vasco activará la carpeta ciudadana como un sitio web donde estarán disponibles todos los documentos, expedientes y notificaciones oficiales que el usuario pueda necesitar en su relación con la Administración.[2]
- El Ministerio de Planeación, Desarrollo y Gestión de Brasil cuentan con una plataforma de Ciudadanía Digital, por medio de la cual los ciudadanos pueden acceder a la información y prestación de servicios públicos digitales.[3]

El diseño e implementación de la Carpeta Ciudadana requiere considerar garantías de confidencialidad, integridad, disponibilidad y no-repudio, entre otras. Solo ofreciendo estas garantías tendríamos una administración apropiada de los documentos de una carpeta, dando acceso solo a usuarios autorizados, cuándo ellos lo requieran y creando confianza para los ciudadanos. Aunque el manejo apropiado de la identidad de los usuarios no es un servicio abordado en este documento, es relevante mencionar que el éxito de la carpeta ciudadana depende de dicho servicio.

Este documento analiza algunos aspectos de diseño que contribuyen a ofrecer confidencialidad, integridad, disponibilidad y no-repudio.

---

[1] https://www.eltiempo.com/tecnosfera/novedades-tecnologia/el-hombre-tras-la-primera-nacion-digital-del-mundo-en-estonia-286318
[2] https://www.elcorreo.com/sociedad/ciudadanos-podran-gestionar-20180208231651-nt.html
[3] https://impactotic.co/asi-va-la-ciudadania-digital-en-latinoamerica/

2. Análisis

Modelo de despliegue en la nube. Correr servicios en la nube ofrece altos niveles de disponibilidad y facilita el aprovisionamiento y des-aprovisionamiento automatizado de recursos de procesamiento y almacenamiento, de acuerdo a la demanda (elasticidad y autoescalado). Los costos tecnológicos son proporcionales a la cantidad de usuarios y de transacciones soportadas por una aplicación pues se paga únicamente por los recursos consumidos. Sin embargo, considerando los requerimientos de seguridad, privacidad en particular, de la información almacenada en una carpeta ciudadana, es necesario considerar las ventajas y limitaciones de los modelos de despliegue público, privado y comunitario. El modelo público ofrece el mayor beneficio económico, sin embargo conlleva el mayor riesgo de seguridad. El modelo privado conlleva el menor riesgo, pero tiene el mayor costo económico. El modelo comunitario amortizaría el costo garantizando un menor nivel de riesgo que una nube pública. [3]

Modelo de servicio en la nube. Es necesario considerar la mezcla de modelos de servicio PaaS y IaaS. El modelo PaaS permitiría usar almacenamiento no estructurado y un almacén criptográfico, mientras el modelo IaaS permitiría desplegar *virtual Appliances* para correr los componentes de seguridad e instancias virtuales de servidores para correr diferentes tipos de servicios, por ejemplo blockchain, base de datos y aplicaciones web.

Integración tecnológica.

Blockchain. El uso de tecnología blockchain permite garantizar la integridad de los documentos almacenados en la carpeta de cada ciudadano, es decir, permite garantizar que los documentos registrados no pueden ser adulterados; o más bien, cualquier modificación no autorizada puede ser detectada. Esta tecnología también garantiza inmutabilidad dado que cualquier adición o modificación crea un nuevo registro que indica el cambio, conservando todos los registros anteriores. Blockchain también permite establecer el orden cronológico de las transacciones, puesto que cada registro tiene una marca de tiempo. Sin embargo, hay cuestionamientos fuertes sobre el consumo de energía del protocolo de consenso (conocido como la prueba de trabajo) usado por un sistema blockchain completamente descentralizado, como el usado por bitcoin. Como consecuencia, es relevante considerar implementaciones privadas y con manejo de permisos.

Blobs. Ya que será necesario administrar información en diferentes formatos y tamaños se revisaron manejadores de datos que implementaran funciones básicas de seguridad, como cifrado y disponibilidad. Entre las opciones consideradas bases de datos no relacionales, administradores de archivos convencionales sobre dispositivos como NAS o sistemas como FTPS. No obstante, los servicios cloud pueden ofrecer blobs que permiten el almacenamiento de datos por demanda considerando criterios de seguridad como cifrado, con altos niveles de disponibilidad y respaldo redundante.

Arquitectura de Alto Nivel. La Ilustración 1 presenta el conjunto de componentes que deberían ser implementados para responder al conjunto mínimo de servicios que responderían a los requerimientos funcionales y las necesidades de seguridad identificados en el contexto de la Carpeta Ciudadana.

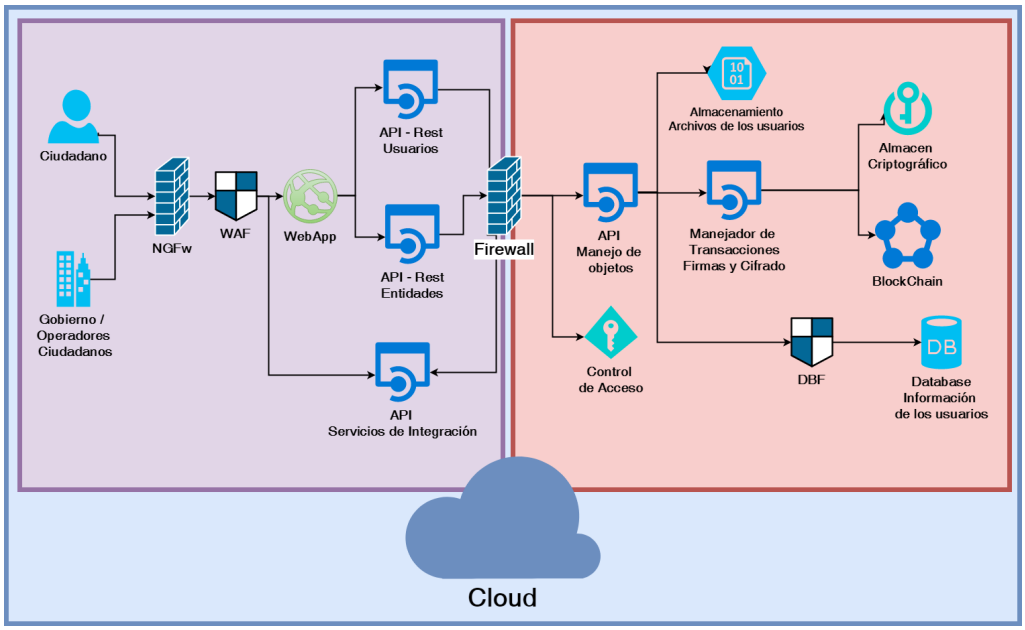

Ilustración 1. Arquitectura de componentes de la solución.

1. Web App. Implementa la capa de presentación e interfaz de usuario para los ciudadanos y entidades que sean clientes del servicio, será publicada toda la información comercial, de mercadeo y la información que deba ser conocida por el público en general, adicionalmente ofrecerá a los usuarios las funciones de autenticación necesarias para acceder al servicio.
2. WAF (*Web Application Firewall*). Brinda la protección necesaria para el correcto funcionamiento de la aplicación, protegiendo contra ataques de denegación de servicio de nivel 7, bloqueos por reputación de direcciones IP y dominios, protección contra vulnerabilidades conocidas de plataformas Web y vulnerabilidades de código de aplicación.
3. API–Rest Usuarios, API–Rest Entidades. Dado que las funcionalidades del servicio ofrecidas a los usuarios y a las entidades adscritas al servicio son muy diferentes, se propone crear dos API – Rest independientes, una para las interacciones propias de usuarios y otra para las operaciones realizadas por las entidades.
4. API – Servicios de Integración. Componente que permite la conexión de los operadores de carpeta ciudadana hacia el servicio de almacenamiento seguro y con las entidades del estado responsables de la supervisión del servicio. Será un servicio con la lógica que garantizará que la información se comparta entre los operadores ciudadanos.
5. API Manejo de Objetos. Establece las reglas operativas de manipulación de objetos dependiendo del rol del usuario. Realiza y registra las operaciones relacionadas con los documentos que se encuentran almacenados en el servicio de Carpeta Ciudadana, otorga a los usuarios las funcionalidades para realizar las operaciones de carga, descarga, almacenamiento, búsqueda, clasificación, recuperación, modificación, conservación, eliminación segura y en compañía del Manejador de Transacciones, la firma, estampa y cifrado de los documentos.
6. Control de Acceso. Mediante este componente se gestionan los diferentes roles que se manejan en el servicio (1. Ciudadano. 2. Empresas. 3. Administrativo). Será el servicio que otorgará acceso a las funcionalidades permitidas según el rol del usuario.

7. Manejador de Transacciones. Componente encargado de gestionar y registrar todas las transacciones realizadas por los usuarios sobre la información y documentos del servicio de carpeta ciudadana, incluyendo creación, modificación y borrado de usuarios, y anotaciones y actualizaciones sobre documentos. Además, en compañía del API de Manejo de Objetos, cumple la función de Signer-Certificador para la firma, estampa y cifrado de los documentos que son almacenados y compartidos por los ciudadanos con las entidades adscritas al servicio de Carpeta Ciudadana. Los archivos (BLOBs) se cifrarán de modo que pueda ser preservada la confidencialidad de la información contenida en ellos. Se propone usar un esquema de llaves públicas/privadas provistas por el servicio de autenticación ciudadana garantizando que solo el dueño de la información tenga acceso.
8. Almacén Criptográfico. Este componente ofrece almacenamiento de llaves y certificados propios, así como aquellos que han sido compartidos con otros operadores ciudadanos. El almacén criptográfico también puede realizar operaciones criptográficas para la firma, estampa y cifrado de los documentos cuando un ciudadano así lo requiera.
9. Database. Motor de base de datos relacional que almacena la información de los usuarios, incluyendo los enlaces a los archivos y documentos almacenados en el componente de almacenamiento de información no estructurada. Este componente también brinda funciones de seguridad de los datos e información de los usuarios como cifrado y enmascaramiento de información.
10. DBF (*Data Base Firewall*). Auditoría y protección de bases de datos, este componente brindara protección contra ataques de SQL, ataques al motor de bases de datos, prevención de fuga de información personal de los usuarios alojada en la base de datos, reglas de acceso a información almacenada, monitoreo y control de acciones de los usuarios y administradores.
11. Almacenamiento – Blobs. Este componente administra cantidades masivas de datos no estructurados, ajusta los recursos dependiendo de la demanda en un momento determinado, es el repositorio de archivos y documentos de los usuarios del servicio de Carpeta Ciudadana, todos los documentos almacenados en este repositorio van a estar firmados y cifrados para garantizar la confidencialidad e integridad de los archivos almacenados.
12. BlockChain. Permite validar la veracidad de los documentos almacenados en la carpeta de cada ciudadano. Este componente garantiza la inmutabilidad, autenticidad y no repudio de las transacciones, documentos y operaciones del servicio de Carpeta Ciudadana. Se propone el uso de Blockchain Ethereum por ser un proyecto público con amplia documentación y soporte.
13. Firewall. Este componente es el encargado de brindar las protecciones de seguridad perimetral requeridas por el servicio, incluyendo las funcionalidades de Firewall de nueva generación (NGFW), IPS, AntiDDoS, protección de aplicaciones, y bloqueo de direcciones IP por reputación y comportamiento.

3. Recomendaciones

Adelantamos un análisis de riesgos para el proyecto de implementación de carpeta ciudadana y encontramos que el principal riesgo y el que consideramos más difícil de mitigar está relacionado con las condiciones regulatorias, pues si se produce un cambio en las condiciones definidas y no existe un incentivo por parte del Estado para las entidades públicas y los ciudadanos para el uso de este tipo de servicios va a ser muy difícil que se logre su masificación.

Otro riesgo importante está relacionado con los cambios culturales que hoy en día está sufriendo la sociedad, pues para los nativos digitales y para los ciudadanos de las grandes ciudades la adopción de servicios electrónicos ya se ha vuelto una necesidad, pero todavía existe una gran parte de la población que está muy lejos de llegar a estos niveles de adopción tecnológica, lo cual está abriendo una brecha cultural (digital) la cual también puede impedir la masificación de este tipo de servicios.

Con base en nuestro análisis, presentamos las siguientes recomendaciones:

- Para que los servicios ciudadanos digitales sean una realidad debe existir un ambiente normativo adecuado que brinde las garantías necesarias para la adopción del servicio por parte de las entidades.
- Es necesario que el servicio de Autenticación Electrónica ya se encuentre disponible y evaluado para que el servicio de carpeta ciudadana pueda entrar en operación, pues uno de los requisitos más importantes es poder tener certeza de la identidad de la persona que está accediendo al servicio.
- El público objetivo del proyecto de carpeta ciudadano no se limita al sector público, los trámites privados tienen cabida y podrían representar una parte importante del negocio optimizando también los tramites que los ciudadanos deben realizar con empresas de capital privado.
- Es posible crear una solución con herramientas disruptivas que responda a las necesidades de servicios digitales ciudadanos, empleando herramientas como BlockChain para generar confianza en los mecanismos de protección de la información.
- El rápido desarrollo y evolución de los servicios tecnológicos ofrecidos a través de aplicaciones móviles e Internet y su rápida adopción por parte de la sociedad que ya se encuentra digitalizada, puede estar acrecentando la brecha digital existente en el país, pues una gran parte de la población todavía está muy lejos de llegar a estos niveles de adopción tecnológica, lo cual podría impedir la masificación de este tipo de servicios.
- El Estado debería considerar la adopción de un BlockChain comunitario para apoyar diferentes iniciativas tecnológicas que requieran validar la integridad, auditabilidad y no repudio de los registros generados.

Referencias

[1] Manual de Condiciones. Servicio de Carpeta Ciudadana. Ministerio de Tecnologías de la Información y las Comunicaciones y Corporación Agencia Nacional Gobierno Digital. Agosto, 2018.
[2] Carpeta Ciudadana. Ministerio de Tecnologías de la Información y las Comunicaciones. https://www.mintic.gov.co/portal/vivedigital/612/w3-article-19498.html. Consultado junio 2019.
[3] Cloud Computing Security Considerations. Australian Government, Australian Cyber Security Centre. https://www.cyber.gov.au/publications/cloud-computing-security-considerations. Consultado junio 2019.
[4] Libro Administración segura de documentos en carpeta ciudadana. Carlos Pinilla, David Mosquera, María Mancipe, Jonatan Legro. Proyecto Final. Universidad de los Andes. 2019.