Garantizando integridad y no repudio en acuerdos comerciales de Arkiify

Sebastián Quintero Zuluaga
Elkin Ferney Quintero Gomez
Universidad de los Andes
Proyecto Final

1. Resumen

Arkiify es un proyecto tecnológico enfocado en el sector de la construcción que quiere revolucionar la compra y venta de insumos de este. Actualmente está completando fase de MVP y se han venido detectando oportunidades de mejora en lo referente a la seguridad de los datos. Entre estos están asegurar la integridad y no repudio de los acuerdos comerciales y una falta de definición de roles y perfiles de usuario.

Para solucionar esto se desarrolló e implementó un módulo dirigido a los distribuidores que permite garantizar la integridad y el no repudio de los acuerdos comerciales cargados en Arkiify, junto con la definición e implementación del modelo de control de acceso y la identificación de riesgos para futura remediación.

Previo a esto se hizo un análisis sobre la mejor tecnología a implementar, eligiendo entre Block Chain y firma digital, y adicionalmente se hizo un análisis de riesgo y se definieron unos controles para mitigarlos.

2. Introducción - Contexto

Arkiify es una solución web que permitirá conectar a fabricantes, distribuidores, constructores y contratistas del sector de la construcción de viviendas. El objetivo es revolucionar la compra y venta de insumos del sector constructor, haciéndola más práctica, sencilla y efectiva. La solución está finalizando actualmente su fase cero o MVP.

Se identificaron todas las necesidades cubiertas y no cubiertas que hay entre los diferentes actores del mercado y adicionalmente se hizo un análisis del mismo encontrando que la mejor alternativa para iniciar con el proyecto y definir el MVP era cubrir el segmento B2B, específicamente la interacción entre distribuidores y constructores, con los siguientes argumentos:

- No se encontró en el mercado una aplicación o modelo de negocio basado en tecnología que ayudara a ambas partes a facilitar y agilizar el proceso de compra y distribución.
- Entre estos dos actores se cuenta con contactos cercanos que trabajan y conocen el negocio, facilitando información sobre cómo son los procesos que se ejecutan entre estos, sus falencias, ineficiencias y necesidades que no han podido cubrir.
- Las interacciones entre ferreteros y pequeños constructores (arreglos locativos, etc) ya están siendo abordadas por otras empresas de tecnología como Tul.
- Se decidió que los demás segmentos de negocio (incluidos los que ya cuenta con demanda y oferta cubierta) se cubrirían en etapas posteriores una vez que la primera fase fuera exitosa.

3. Elementos importantes en MVP

- Distribuidores: Estos son los que adquieren los insumos al por mayor de los fabricantes directamente y lo ofrecen al público en general
- Constructores: Son empresas que desarrollan proyectos de vivienda, comerciales o culturales.
- Solicitudes de cotización: Son todos los materiales que un constructor necesita para desarrollar el proyecto de construcción o parte del mismo.

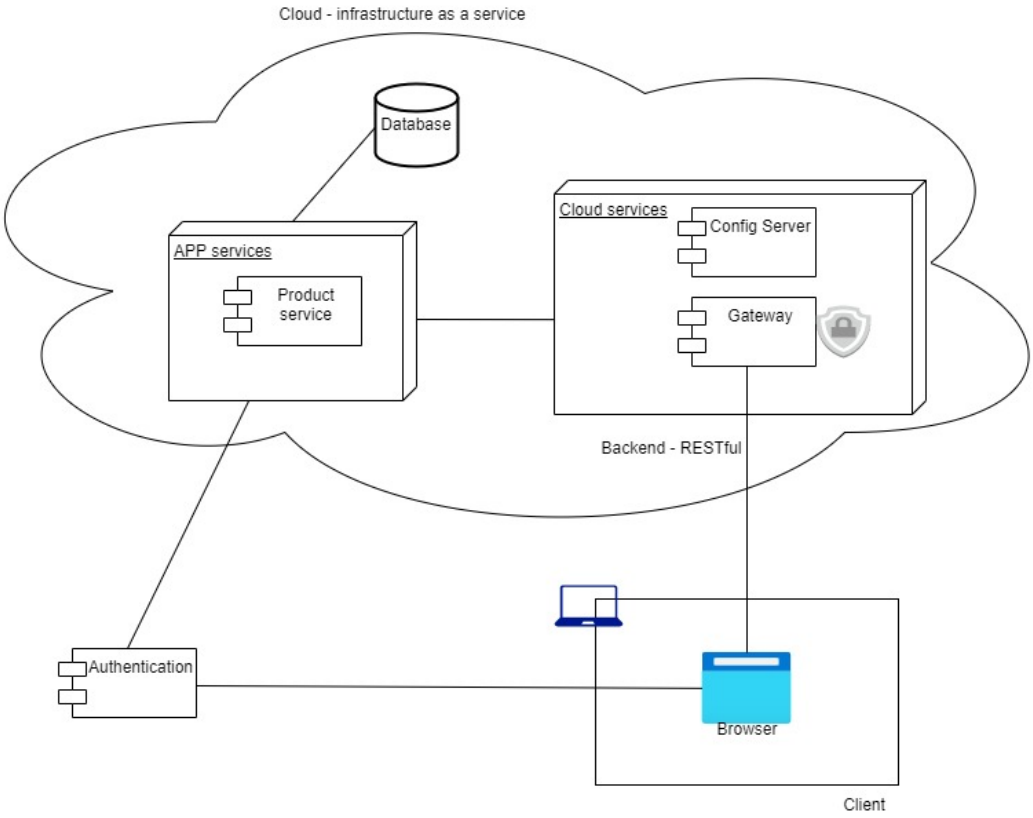
- Cotizaciones: Son las ofertas comerciales presentadas a los constructores y generadas por Arkiify a partir de las solicitudes de cotizaciones y los acuerdos comerciales con los distribuidores.
- Acuerdos comerciales: Uno de los componentes principales de la solución es la de los acuerdos comerciales, ya que a partir de estos es que se generan las cotizaciones y las órdenes.

Funciones principales de Arkify

- Seleccionar las combinaciones más económicas que cumplen con los criterios indicados por los fabricantes.
- Las combinaciones podrán ser de diferentes presentaciones del mismo producto y fabricante.
- Las combinaciones podrán ser de las mismas presentaciones de diferentes distribuidores

4. Problemas

Para dar contexto, a continuación, se presentan los componentes más importantes de la arquitectura actual. En esta se muestran a groso modo, cómo interactúan estos componentes para poder ejecutar las principales funciones del MVP.



Cloud: Se usan los servicios de nube pública ofrecidos en modalidad IaaS (Infraestructura como Servicio). En esta se tiene un servidor virtual que ejecuta contenedores como microservicios.

Los microservicios son los siguientes:

- **ConfigServer:** Esta instancia se usa para exponer propiedades de configuración que usan los contenedores que se encuentran en APP services.
- **Gateway:** Se encarga de direccionar las llamadas del API a los diferentes microservicios. Actualmente el único microservicio que expone funcionalidad es Product service.

- **Product service:** Este microservicio es el que actualmente expone toda la funcionalidad de Arkiify a través de los diferentes endpoints. Este es el único componente que se comunica actualmente con la base de datos

Database: Para la base de datos se usa una instancia DBaaS (Database as a Service) administrada por el proveedor de nube. Aquí se almacenan todos los datos de Arkiify incluidos los acuerdos comerciales.

Authentication: Este es usado para autenticar a los usuarios y generar los tokens de autenticación que usa el frontend para interactuar con el backend.

Client: Del lado del cliente se utilizan navegadores estándar como Chrome, Firefox, Edge, desde allí se renderizan los componentes visuales para interactuar con el Backend.

Arkiify al ser una solución web de fácil acceso, también se puede convertir en vector de ataque para organizaciones cibercriminales, ya sea simplemente por obtener algún beneficio económico o para demostrar que dicha plataforma es vulnerable. Independientemente de cuál sea la razón, si la solución web no es validada periódicamente para encontrar brechas de seguridad sobre los componentes usados en su arquitectura, en cualquier momento podría quedar expuesta la información de los terceros y los acuerdos que son fundamentales para el beneficio económico del negocio.

La probabilidad de ocurrencia de un evento de seguridad en donde queden comprometidos los datos de una Organización es mayor, y esto se puede evidenciar por las cifras de incrementos de ciberataques en el 2022. La Cámara Colombiana de Informática y Telecomunicaciones en su Estudio Semestral de tendencias del Cibercrimen menciona que entre enero de 2022 y junio de 2022 se han recibido 29.778 casos de ciberdelito lo cual corresponde a un incremento del 8% en comparación al 2021. De igual forma, el comportamiento del acceso abusivo a sistemas informáticos incrementó un 46% en el presente año, llegando a 6407 denuncias registradas (Cámara Colombia de Informática y Telecomunicaciones, 2022).

Dentro de las oportunidades presentadas con los distribuidores y constructores, se encuentra que:

- No es posible asegurar la integridad y el no repudio de los acuerdos comerciales que se cargan en el sistema, dejando riesgos asociados a cotizaciones incorrectas
- Al no contar con una definición de roles y perfiles de usuario, todos pueden acceder a los diferentes módulos y existe el riesgo de que haya manipulación y/o destrucción de información.

5. Análisis y evaluación de riesgos

Entendiendo el contexto de Arkiify, conociendo a detalle cómo es su arquitectura actual, sus funcionalidades, casos de uso, usuarios y administradores, para este proyecto nos pareció conveniente poder identificar a que riesgos está expuesta la aplicación y cuales controles son los requeridos para mitigar dichos riesgos.

Para realizar este ejercicio se tomó como referencia el estándar ISO 31000:2018 (ISO, 2018), el cual plantea que la Gestión de Riesgo es parte integral de los procesos y la toma de decisiones, por lo cual es necesario adaptarla de manera transversal en la Compañía y plataforma Arkiify. La matriz de riesgo a utilizar en este proyecto cuenta con las siguientes secciones:

IDENTIFICACIÓN DEL RIESGO			
# RIESGO	DESCRIPCIÓN DEL RIESGO	CAUSAS	CONSECUENCIAS

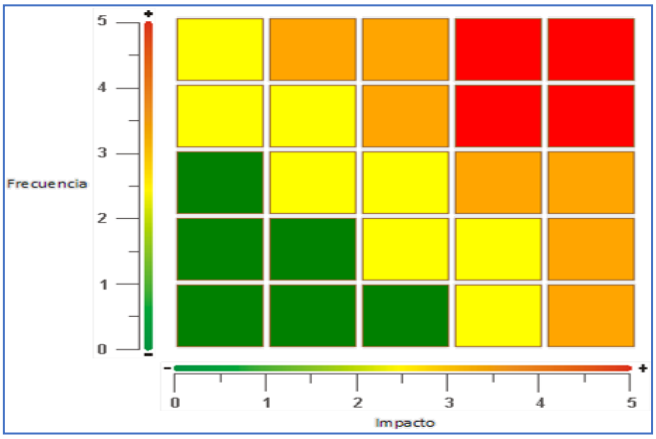
EVALUACIÓN DEL RIESGO – RIESGO INHERENTE			
PROBABILIDAD	IMPACTO	PERFIL DE RIESGO	ZONA DE RIESGO

CONTROLES Y RIESGO RESIDUAL					
DEFINICIÓN CONTROL	CLASE	TIPO	CALIFICACIÓN	EFECTIVIDAD	RIESGO RESIDUAL

Para la evaluación de riesgos se define una escala de calificación de 5x5, con los siguientes criterios:

#	PROBABILIDAD	IMPACTO
1	Muy Baja	Insignificante
2	Baja	Inferior
3	Media	Medio
4	Alta	Superior
5	Muy Alta	Extremo

ZONA DE RIESGO
Menor
Leve
Moderado
Mayor
Catastrófico



Para proceder a evaluar el riesgo, se definen unos criterios de medición a nivel de probabilidad e impacto:

Valor	Probabilidad	Descripción
5	Muy Alta	Se espera la ocurrencia del evento en más del 20% de los casos
		Casi con certeza se espera la ocurrencia del evento
		Podría ocurrir con cierta periodicidad (1 vez cada mes) o más de 12 veces al año
4	Alta	El evento ocurrirá entre el 15 y el 20% de los casos
		Significativa probabilidad de ocurrencia
		En el año se puede presentar entre 6 y 12 veces
3	Media	El evento puede ocurrir entre el 10 y 15% de los casos

		Mediana probabilidad de ocurrencia
		Se presenta con alguna frecuencia (1 vez al trimestre)
2	Baja	El evento puede ocurrir entre el 5 y el 10% de los casos
		Baja probabilidad de ocurrencia
		Se presenta con alguna frecuencia (1 vez al semestre)
1	Muy Baja	El evento puede ocurrir en menos del 1% de los casos
		Muy baja probabilidad de ocurrencia
		Puede ocurrir una vez al año

Valor	Nivel de Impacto	Económico	Reputacional	Legal
5	Extremo	Impacto que reduzca el patrimonio de la Compañía en más de un 10%	Divulgación de eventos y/o investigación por organismo regulador dando conocer al público en medios informativos masivos y/o principales noticias nacionales	Intervención a la Compañía por parte de entes reguladores o cualquier otra la entidad por incumplimientos legales y/o contractuales
4	Superior	Impacto que reduzca el patrimonio de la Compañía entre un 7 y 9%.	Critica de organismo regulador o clientes en medio masivo de comunicación	Multa a la Compañía por parte de entes de vigilancia y control por incumplimientos legales y/o contractuales. Multas o sanciones debido a la pérdida de un proceso judicial y al reconocimiento de los respectivos perjuicios
3	Medio	Impacto que reduzca el patrimonio técnico de la Compañía entre un 4 y 7%.	Aviso sorpresivo de prensa y otro medio masivo	Llamado de atención reincidente a la Compañía posterior o un requerimiento por parte de la Superintendencia de Industria y Comercio o cualquier otro ente de vigilancia y control por incumplimientos legales y/o contractuales
2	Inferior	Impacto que reduzca el patrimonio de la Compañía entre un 1 y 4%.	Situaciones que no trascienden a medios informativos	Observaciones por parte de la Superintendencia o cualquier ente de vigilancia y control por incumplimientos legales y/o contractuales
1	Insignificante	Impacto que reduzca el patrimonio de la Compañía en menos del 1%	No afecta la imagen de la Compañía en el mercado	Ningún pronunciamiento por parte de la Superintendencia o cualquier ente de vigilancia y control por incumplimientos legales y/o contractuales.

Con el fin de evaluar la efectividad de los controles, se propone una clasificación de estos por clase y tipo. De acuerdo con su clasificación así mismos tendrán una evaluación de efectividad, la cual nos indicará el riesgo residual.

Clase	Tipo	Calificación
Preventivo	Manual	4
	Automático	6
	Semiautomático	5
Detectivo	Manual	3
	Automático	5
	Semiautomático	4
Correctivo	Manual	2
	Automático	4
	Semiautomático	3

Para calcular el riesgo residual, se propone sumar la calificación de efectividad de los controles de cada riesgo, y el resultado compararlo con la siguiente tabla. Adicionalmente, realizar los desplazamientos de frecuencia e impacto según corresponda.

EFECTIVIDAD DE CONTROLES			DESPLAZAMIENTO FRECUENCIA - IMPACTO	
Calificación	**Descripción**	**Intervalo**	**Frecuencia**	**Impacto**
Excelente	Control que reduce la posibilidad de incumplir el objetivo del proceso, en el tiempo y con el costo más razonable posible.	12 a 15	3	2
Bueno	Control que reduce el riesgo, con actividades preventivas y un grado bajo de automatización, con un bajo costo unitario.	9 a 11,99	2	1
Regular	Control que reduce el riesgo, adoptando correctivos manuales, generando un alto costo de operación.	5 a 8.99	1	0
Deficiente	Control que no reduce el nivel de exposición del riesgo.	1 a 4.99	0	0

El análisis de riesgo fue ejecutado en conjunto con los socios de Arkiify, y como resultado de este ejercicio fueron identificados 10 riesgos, a los cuales se les asignaron unos controles para reducir el impacto y la probabilidad de materialización de los mismos. A continuación se da a conocer el detalle de la evaluación de uno de los riesgos críticos identificado:

Manipulación o alteración no autorizada de los acuerdos comerciales en Arkiify

CAUSAS	IMPACTOS	RIESGO INHERENTE					
		PROBABILIDAD		IMPACTO		PERFIL RIESGO	ZONA DE RIESGO
Ataques informáticos.	Pérdida de la confianza de las clientes de Arkiify	3	MEDIA	5	EXTREMO	15	CATASTROFICO
Mala intención de un colaborador de Arkiify	Sanciones legales por parte de los entes de control - Protección de datos.						
Asignación de perfiles y roles deficiente	Demandas por parte de alguna de las contrapartes relacionadas.						
Error humano por parte de los diferentes actores en Arkiify	Reprocesos para la reconstrucción de la información.						
	Pérdida de la integridad de la información.						

CONTROL	CLASE	TIPO	CALIFICACIÓN	EFECTIVIDAD	RIESGO RESIDUAL
Registro de eventos que almacenen información relevante de los acuerdos comerciales al momento de ser modificados.	Preventivo	Semi Automático	5	Excelente	Leve
Implementación de un módulo que permita asegurar la integridad y no repudio de los acuerdos comerciales.	Preventivo	Semi Automático	5		

Definir un modelo de control de acceso lógico (RBAC) que se ajuste a las necesidades de Arkiify sus terceros.	Preventivo	Manual	4		
Registro de criptogramas de cada uno de los acuerdos comerciales	Preventivo	Automático	6		
Definición de estrategias de copias de seguridad de la plataforma Arkiify	Correctivo	Manual	2		

El resultado general de la evaluación de riesgos es la siguiente:

		Riesgo Inherente	Riesgo Residual
R1	Indisponibilidad de Arkiify para la gestión de ordenes	**CATASTROFICO**	**LEVE**
R2	Pérdida o daño de la informacion de la base de datos de Arkiify	**MAYOR**	**LEVE**
R3	Indisponibilidad del componente de autenticación de Arkiify	**CATASTROFICO**	**LEVE**
R4	Suplantación de identidad de usuarios de Arkiify y de terceros	**MAYOR**	**LEVE**
R5	Exposición de código fuente del aplicativo Arkiify	**MAYOR**	**MODERADO**
R6	Revocación de controles criptográficos en Arkiify	**MAYOR**	**LEVE**
R7	Inconsistencia en la generación de comisiones	**CATASTROFICO**	**LEVE**
R8	Inconsistencia en la generación de cotizaciones	**CATASTROFICO**	**LEVE**

R9	Fuga o divulgación no autorizada de información privada o confidencial de Arkiify	**CATASTROFICO**	**LEVE**
R10	Manipulación o alteración no autorizada de los acuerdos comerciales en Arkiify	**CATASTROFICO**	**LEVE**

Como conclusión del análisis y evaluación de riesgos, se logró evidenciar que existen múltiples oportunidades de mejora sobre la plataforma y el proceso de Arkiify, todo con el fin de buscar asegurar la información que allí se custodia y se procesa. Para el alcance del proyecto y según divulgación con los socios de negocio, se procedió a implementar los siguientes controles de seguridad evidenciados previamente:

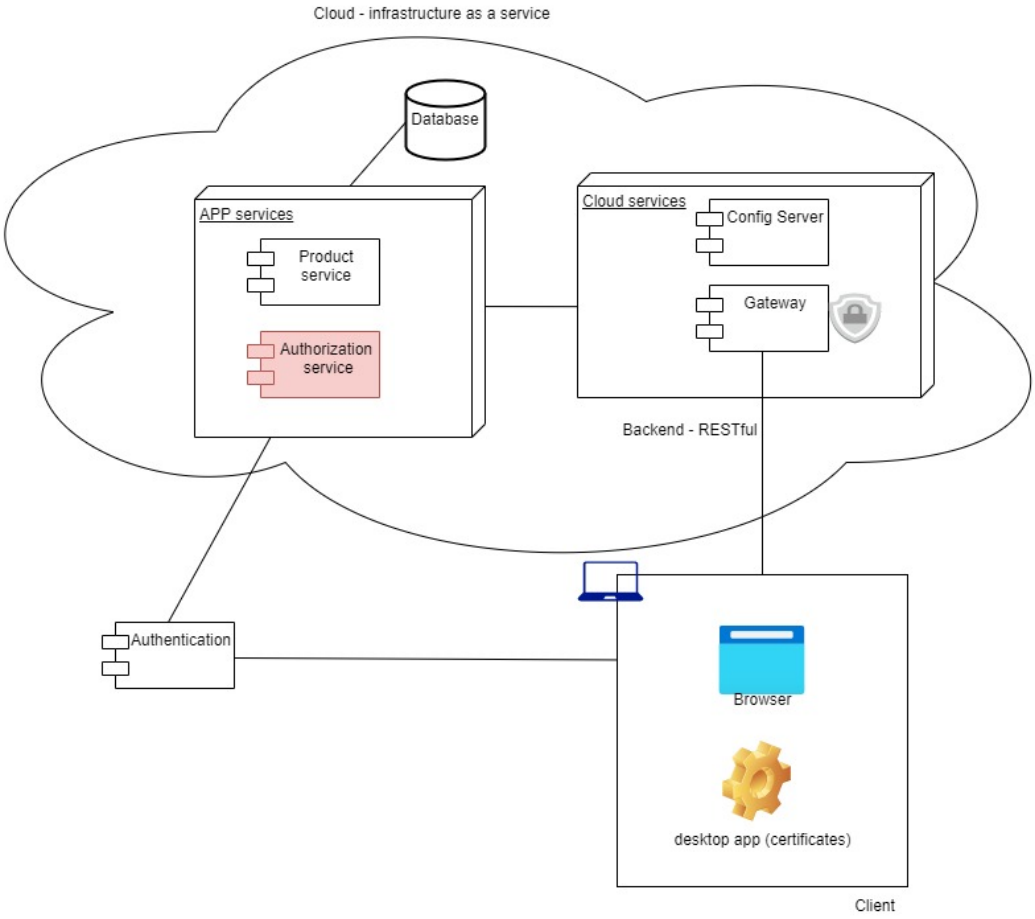
- Implementación de un módulo que permita asegurar la integridad y no repudio de los acuerdos comerciales.
- Definir un modelo de control de acceso lógico (RBAC) que se ajuste a las necesidades de Arkiify sus terceros.
- Registro de criptogramas de cada uno de los acuerdos comerciales.

6. Solución propuesta

De acuerdo con la arquitectura inicial y el conocimiento de los casos de usos de la herramienta Arkiify, se identificaron los siguientes problemas de seguridad:

- La imposibilidad de asegurar que los acuerdos no sean alterados
- No se cuenta con una definición de roles y perfiles de usuario, haciendo que todos pueden acceder a los diferentes módulos y existe el riesgo de que haya manipulación y/o destrucción de información

Para afrontar estos problemas se propone desarrollar un módulo que permita asegurar la integridad y no repudio de los acuerdos comerciales, se definirá e implementará un modelo de control de acceso.



Objetivo General:

- Desarrollar e implementar un módulo dirigido a los distribuidores que permita garantizar la integridad y el no repudio de los acuerdos comerciales cargados en Arkiify, junto con la definición e implementación del modelo de control de acceso y la identificación de riesgos para futura remediación.

Objetivos Específicos:

- A través de un modelo ponderado de evaluación de tecnologías, identificar cual es la mejor alternativa entre las siguientes opciones: Firma de acuerdos a través de certificados (Local), o Firma de acuerdos usando tecnología Blockchain
- Implementar mecanismo para firmar los acuerdos comerciales.
- Implementar mecanismo de verificación de firma de los acuerdos comerciales para determinar validez de estos.
- Garantizar la propiedad de no repudio en los acuerdos comerciales entre Arkiify y los distribuidores permitiendo verificar a los diferentes actores la firma generada.
- Desarrollar un modelo de roles de Arkiify junto con su respectiva matriz de clasificación.
- Identificar los riesgos de seguridad existentes en la aplicación Arkiify y proponer controles para futuras remediaciones.

Evaluación de la tecnología a utilizar

Con el fin de dar solución a los riesgos de seguridad previamente expuestos, se realizó una verificación de cuáles tecnologías podrían ser las que nos permitan aplicar controles para asegurar la integridad y no repudio de los acuerdos comerciales. Dentro del ejercicio, se tomaron

dos soluciones: la primera corresponde al uso de certificados digitales para firma de acuerdos comerciales y la segunda el uso e incorporación de blockchain en la arquitectura de Arkiify.

Para realizar la evaluación de la tecnología, el equipo de trabajo del presente proyecto elaboró una matriz con unos criterios de evaluación los cuales a su vez se les asignó un porcentaje de impacto y un peso en la calificación.

Criterios de Evaluación	%	Calif Max
Tecnológico	**25%**	**45**
Operativo	**19%**	**30**
Funcional	**34%**	**10**
Costos	**23%**	**5**

Ejecutando dicha evaluación en todos los criterios, podemos concluir que de acuerdo con el alcance del proyecto Arkiify, la mejor alternativa a utilizar es la firma de acuerdos comerciales a través de certificados digitales.

Criterios	Part %	Calif Max	Firma con certificados	Blockchain
Tecnológico	**25%**	**45**	22,22%	11,67%
Operativo	**19%**	**30**	17,73%	5,70%
Funcional	**34%**	**10**	30,60%	17,00%
Costos	**23%**	**5**	18,40%	4,60%
PUNTUACIÓN			**88,96%**	**38,97%**

Aplicación de escritorio

Debido a las limitantes que presentan los navegadores para usar certificados digitales para firmar mensajes, es necesario instalar una aplicación de escritorio (desktop App) con el fin de poder hacer uso de los certificados locales libremente (tanto en almacenes de certificados locales como en dispositivos de seguridad).

Para esto, se desarrolló una aplicación en Java que permite inspeccionar y usar los certificados digitales locales del usuario. Esta aplicación interactúa con el backend de Arkiify a través de protocolo HTTP usando la API RESTful ya expuesta actualmente.

En el backend se exponen los endpoint que permitirán la interacción entre este y la aplicación de escritorio.

Backend

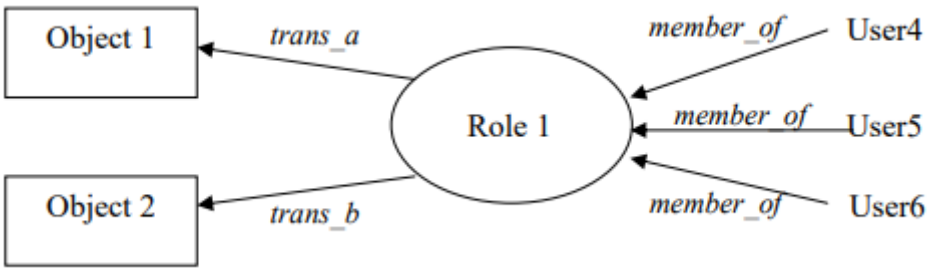
- **Nuevos endpoints**

Que exponen los métodos que utiliza la aplicación de escritorio para intercambiar los mensajes de firma digital para firmar los acuerdos.

- **Authorization Service**

Dentro de la arquitectura también se incluye un componente con nombre “Authorization service”, sobre el cual son controladas las funcionalidades y perfiles de los usuarios que ingresan a la aplicación Arkiify.

Este componente se implementó basado en el modelo RBAC (Rol- Based Control Access), el cual a la fecha se encuentra desarrollado en diferentes aplicaciones a nivel mundial (National Institute of Standards and Technology NIST, 2020).

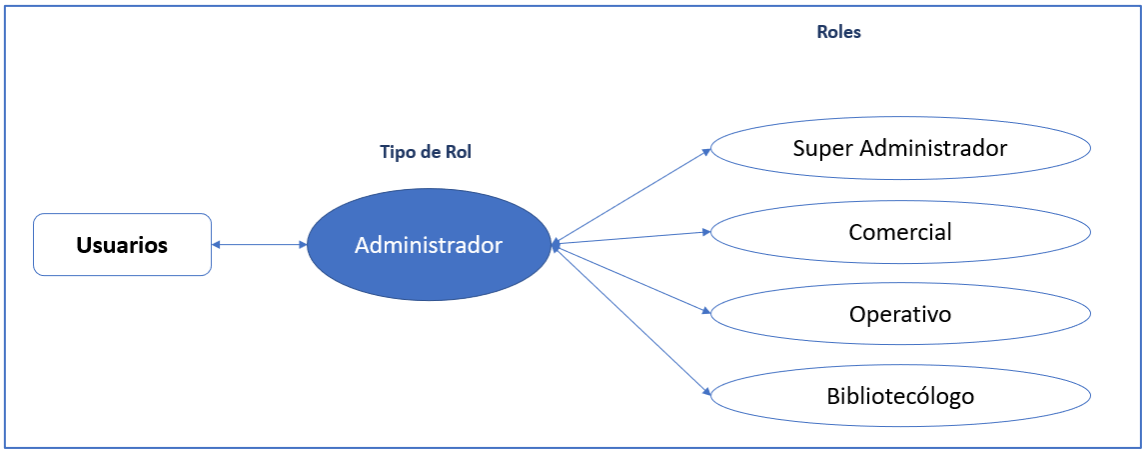


El modelo consiste en que dentro de los diferentes niveles de una aplicación deben existir unos roles los cuales se relacionan a opciones u objetos que pueden ser visualizados y/o manipulados por aquellos usuarios autorizados.

Previo a la implementación de este proyecto, el único control de acceso que existía era la autenticación, sin embargo, no había una definición de roles que pensara en la segregación de funciones de acuerdo con los diferentes actores y clientes que interactúan con Arkiify.

El equipo de trabajo desde el entendimiento funcional de Arkiify propuso la creación de 3 tipos de roles:

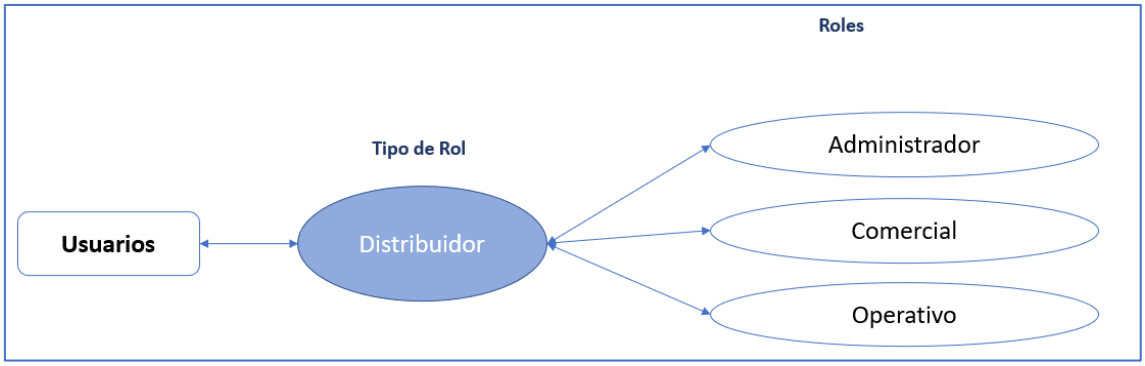
a. **Administradores:** Roles asignados exclusivamente al personal de Arkiify, utilizado exclusivamente para labores administrativas de la herramienta.



De acuerdo con los roles visualizados en la imagen anterior, se detallan los módulos y las acciones que le son permitidas:

Módulo	Superadministrador		Comercial		Operativo		Bibliotecólogo	
	Lectura	Escritura	Lectura	Escritura	Lectura	Escritura	Lectura	Escritura
Tablas Maestras	X	X	X		X	X		
Distribuidor	X	X	X		X		X	
Cliente	X	X	X	X	X			
Catálogos	X	X	X		X		X	X
Requisiciones	X	X	X	X	X			
Cotizaciones	X	X	X	X	X			
Pre - Orden	X	X	X	X	X			
Orden	X	X	X	X	X			
Acuerdos	X	X	X		X			
Sucursales	X	X						

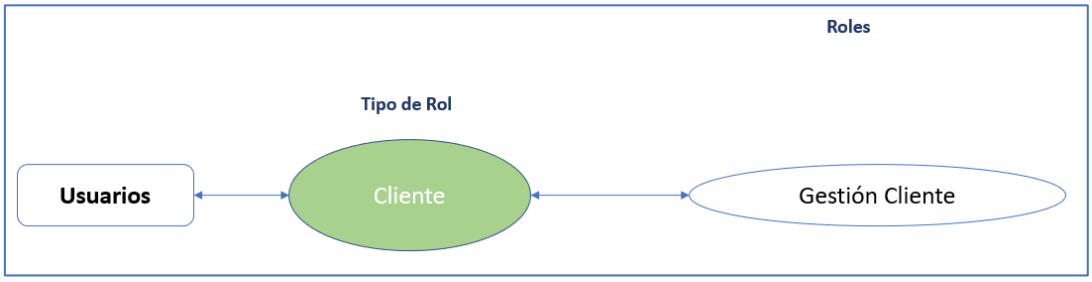
b. **Distribuidores:** Roles asignados exclusivamente de distribuidores para la ejecución de sus actividades.



De acuerdo con los roles visualizados en la imagen anterior, se detallan los módulos y las acciones que le son permitidas:

Módulo	Administrador		Comercial		Operativo	
	Lectura	Escritura	Lectura	Escritura	Lectura	Escritura
Tablas Maestras						
Distribuidor	X	X				
Cliente						
Catálogos	X		X			
Requisiciones						
Cotizaciones	X		X		X	
Pre – Orden						
Orden	X				X	
Acuerdos	X	X	X	X		
Sucursales	X	X	X	X	X	X

c. **Clientes:** Rol asignado exclusivamente a los clientes finales de la aplicación Arkiify.



De acuerdo con los roles visualizados en la imagen anterior, se detallan los módulos y las acciones que le son permitidas:

Módulo	Gestión Cliente	
	Lectura	Escritura
Tablas Maestras	X	
Distribuidor		
Cliente	X	X
Catálogos	X	
Requisiciones	X	X
Cotizaciones	X	
Pre – Orden	X	X
Orden	X	X
Acuerdos		
Sucursales		

Operaciones criptográficas

Para dar cumplimiento con los requerimientos de no repudio e integridad, se hace uso de la firma digital (Microsoft, s.f.), integrando el sistema RSA con SHA (puede aumentarse la capacidad a otros grupos de sistemas como curva elíptica). A continuación, se resumen los pasos y las operaciones criptográficas que se realizan.

- Cada usuario distribuidor debe tener un certificado digital, junto con la llave privada, que es usado desde la aplicación de escritorio.
- El certificado, sin la llave privada, se carga al backend y es asocia al usuario.
- En la aplicación se realiza la firma de la cadena calculada por el backend usando algoritmo RSA (National Institute of Standards of Technology, s.f.) con SHA256 y se retorna al backend la cadena firmada para asociarla al acuerdo comercial.
- Antes de asociar la firma al acuerdo comercial, se realiza validación de la misma con el certificado cargado previamente por el usuario y con el mismo algoritmo con el que se generó, para verificar coincidencia o que no exista manipulación en la transmisión.
- Cada vez que se visualiza un acuerdo comercial es posible realizar esta misma operación de validación, que recalcula la cadena del acuerdo y verifica validez de la firma con esta.

Adicionalmente se consideraron los siguientes aspectos de seguridad entre la aplicación de escritorio y el backend:

- La aplicación sirve como una extensión al frontend (la aplicacíón WEB) y por lo tanto utiliza los mismos mecanismos de seguridad de este.
- La aplicación autentica al usuario a través del mismo módulo de autenticación (cógnito) y utiliza los mismos Bearer tokens para hacer cualquier petición al backend.
- El backend mantiene los mismos mecanismos de seguridad ya que los nuevos endpoints usan las mismas características de los anteriores.
- Toda interacción con el backend se hace a través de protocolo HTTPS con un certificado RSA con llave de 2048 y cifradores seguros.
- La aplicación no almacena ningún secreto o contraseña en archivos de propiedades o dentro de código fuente.
- Para evitar que se carguen firmas incorrectas o de un certificado diferente, los endpoints expuestos en el backend realizan validación de la firma del acuerdo antes de agregarla a este en la base de datos.

7. Conclusiones

Arkiify es una solución web robusta que busca revolucionar la compra y venta de insumos del sector constructor, pero al estar expuesta existen ciertos riesgos que deben ser mitigados para garantizar la protección de la información.

Entendiendo el funcionamiento de la solución y aplicando metodología de riesgos basados en el estándar ISO 31000:2018, se lograron identificar aquellos riesgos que podrían ocasionar la materialización de incidentes de seguridad sobre la solución de arkiify, esto fue de gran valor para el equipo de trabajo y los socios de la Compañía debido a que nos permitió proponer controles los cuales tienen viabilidad de implementación.

Durante el proyecto nos concentramos en mitigar el riesgo de manipulación o alteración no autorizada de los acuerdos comerciales, para ellos fueron diseñados e implementados los siguientes controles: un módulo que permitió asegurar la integridad y no repudio de los acuerdos comerciales y la definición de un modelo de control de acceso lógico RBAC que se ajusta a las necesidades de Arkiify.

Para elaborar el módulo de seguridad que permitiera garantizar la integridad y no repudio se contemplaron diferentes tipos de tecnología como lo fue la firma a través de certificados y la implementación de blockchain, sin embargo, el resultado de la evaluación de tecnologías aplicado durante el proyecto nos llevó a la conclusión de es más viable trabajar a través de firmas por costos y fácil implementación hacia los diferentes clientes. Pensando en la usabilidad de este módulo, se propuso una aplicación la cual permitía conectarse a Arkiify y firmar los acuerdos comerciales existentes con un certificado digital previamente cargado y validado entre el usuario y la plataforma.

Existen otros riesgos que en su materialización dejarían expuesta información confidencial de la Compañía, distribuidores o clientes, por lo cual, la definición del modelo roles a través de la metodología RBAC fue de gran valor y tuvo gran acogida para los socios de la plataforma. Dicha definición se estructuró contemplando las funcionales de Arkiify.

Los controles propuestos e implementados en este proyecto fueron presentados a los socios de Arkiify, los cuales recibieron la solución a satisfacción y estuvieron de acuerdo en su despliegue de forma controlada a sus clientes potenciales.

8. Referencias

Cámara Colombia de Informática y Telecomunicaciones. (12 de Julio de 2022). *Cámara Colombia de Informática y Telecomunicaciones.* Obtenido de Estudio semestral Tendencias del cibercrimen: Ciberseguridad en la era de la movilidad digital: https://www.ccit.org.co/wp-content/uploads/ciberseguridad-en-la-era-de-la-movilidad-digital-version-digital.pdf

ISO. (2018). *ISO 31000*. Obtenido de Gestión del Riesgo - Directrices: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

Microsoft. (s.f.). *Firmas Digitales y Certificados*. Obtenido de https://support.microsoft.com/es-es/office/firmas-digitales-y-certificados-8186cd15-e7ac-4a16-8597-22bd163e8e96

National Institute of Standards and Technology NIST. (Mayo de 2020). *NIST Special Publication 800-57 Part 1.* Obtenido de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

National Institute of Standards of Technology. (s.f.). *National Institute of Standards of Technology*. Obtenido de https://csrc.nist.gov/glossary/term/RSA