DESARROLLO DE UN ENTORNO DIGITAL SOBERANO EN ESPACIO CONTROLADO CON TECNOLOGÍAS DE CÓDIGO ABIERTO PARA GARANTIZAR LA CONTINUIDAD OPERATIVA.

Juan Sebastian Garavito Gallo

Semestre de industria para optar al título de Ingeniero de Telecomunicaciones

Modalidad de Práctica

Semestre de Industria o Práctica Empresarial

Asesor interno

Jaime Alberto Vergara Tejada

Docente Universidad de Antioquia

Asesor externo

Francisco Javier Muñoz Cortes

Director de ingeniería

Universidad de Antioquia

Facultad de Ingeniería

Pregrado en Ingeniería de Telecomunicaciones

Medellín

2025

Cita	Garavito Gallo
Referencia	Garavito Gallo, J. (2025). Desarrollo de un entorno digital soberano en espacio controlado con tecnologías de código abierto para garantizar la continuidad operativa, semestre de industria, Ingeniería de telecomunicaciones, Universidad de Antioquia, Medellín, 2025.

Tabla de contenido

Lista de tablas

Lista de figuras

Siglas, acrónimos y abreviaturas

UCS	Univention Corporate Server

Resumen

El proyecto desarrollado tuvo como propósito crear un entorno digital soberano basado en tecnologías de código abierto, con el fin de garantizar la continuidad operativa de la empresa ante interrupciones o bloqueos de servicios en la nube. Se diseñó e implementó una infraestructura alternativa en un entorno controlado que integra servicios clave de comunicación, colaboración y almacenamiento, todo bajo un enfoque de gestión automatizada y segura. La solución fue desplegada en un dispositivo de bajo consumo energético dentro de una red aislada, lo que permitió la validación funcional del sistema sin riesgos para el entorno productivo. Los resultados evidencian que es posible adoptar una infraestructura digital autónoma, robusta y adaptable a distintas realidades empresariales, disminuyendo la dependencia tecnológica y fortaleciendo la resiliencia digital.

Palabras clave: soberanía digital, tecnologías abiertas, continuidad operativa, autonomía tecnológica, resiliencia digital.

Abstract

The project aimed to establish a sovereign digital environment using open-source technologies, ensuring business continuity in the event of service interruptions or cloud-related failures. An alternative infrastructure was designed and implemented in a controlled setting, integrating essential communication, collaboration, and storage services that are all managed under a secure and automated framework. The deployment was carried out on a low-energy device within an isolated network, allowing real-world testing without affecting production systems. The findings confirm the feasibility of adopting a robust, autonomous digital infrastructure that reduces technological dependence and enhances digital resilience.

Keywords: digital sovereignty, open technologies, operational continuity, technological autonomy, digital resilience.

1. Introducción

Aligo Defensores Informáticos es una empresa especializada en ciberseguridad, dedicada a ofrecer servicios integrales de protección y vigilancia. Su enfoque incluye soluciones proactivas y reactivas diseñadas según las necesidades de cada cliente, con el objetivo de garantizar la integridad de la información y proteger su vida digital. En un entorno cada vez más digitalizado, la seguridad de la información no solo depende de las medidas internas, sino también de la infraestructura y fiabilidad de los servicios en la nube. En la actualidad, los espacios de trabajo y el almacenamiento en la nube se han convertido en herramientas fundamentales para las empresas y su uso sigue en constante crecimiento. Un espacio de trabajo digital es un entorno virtual que integra herramientas de colaboración, comunicación y gestión de archivos, permitiendo a los equipos operar desde cualquier ubicación con acceso seguro a la información y aplicaciones clave de la empresa. Sin embargo, esta dependencia tecnológica conlleva un riesgo importante: los datos empresariales y la continuidad operativa quedan bajo la supervisión de proveedores externos. Los principales proveedores de servicios en la nube tienen la capacidad de interrumpir de manera inmediata las actividades de una compañía, ya que una cancelación o suspensión del espacio de trabajo puede denegar el acceso a servicios esenciales, como el correo electrónico, afectando tanto las comunicaciones internas como externas. Asimismo, estas interrupciones impactan el acceso a recursos críticos de información relacionados con proyectos, clientes, nóminas y otros aspectos clave del negocio. Estas interrupciones suelen ser provocadas por fallos en el perfil de pago, errores en los procesos de facturación o problemas técnicos. Además, los tiempos de respuesta para resolver estos inconvenientes suelen ser prolongados, lo que puede afectar la operatividad de la empresa y ocasionar pérdidas significativas en sus procesos y recursos clave.

Por esta razón, en Aligo Defensores Informáticos, como promotores de la soberanía digital, busca a través de este proyecto la implementación e integración de un espacio de trabajo independiente basado en tecnologías de código abierto (OpenSource). Este espacio está diseñado para ofrecer una alternativa funcional y confiable como lugar de trabajo digital, con un enfoque especial en las aplicaciones críticas de la compañía, como el correo electrónico y el almacenamiento en la nube.

2. Objetivos

2.1 Objetivo general

Desplegar un entorno de trabajo basado en tecnologías de código abierto, que sirva como contingencia en situaciones críticas, con el fin de asegurar la continuidad de las operaciones empresariales convirtiéndose en alternativa digital soberana y confiable.

2.2 Objetivos específicos

1. Definir la arquitectura y el plan de implementación del espacio de trabajo digital soberano, garantizando su alineación con las necesidades operativas de la empresa y su disponibilidad en escenarios de contingencia.
2. Implementar la solución en un entorno controlado, integrando los servicios esenciales de correo empresarial y almacenamiento de archivos, con el objetivo de evaluar su desempeño y seguridad en un ambiente reducido.
3. Evaluar el desempeño, seguridad y usabilidad de los servicios implementados en un entorno controlado, para detectar posibles áreas de mejora, garantizando el adecuado funcionamiento en un escenario de producción.

3. Marco teórico

Un espacio de trabajo digital es esencialmente un entorno digital integral que reúne herramientas empresariales clave, plataformas y canales de comunicación en un solo sistema integrado [1].

Lo que diferencia a los espacios de trabajo digitales de los entornos de oficina tradicionales es la forma en que centralizan y agilizan los flujos de trabajo. En lugar de saltar entre aplicaciones o ubicaciones físicas, los empleados pueden acceder a todo lo que necesitan en un solo lugar virtual. Este cambio no solo es práctico, sino esencial para las empresas que navegan por modelos de trabajo híbridos y remotos. Por ejemplo, Google Workspace es una suite de productividad en

nube que incluye herramientas como Gmail, Google Drive y Google Meet, diseñadas para mejorar la colaboración y la eficiencia empresarial [2]. Además, ofrece aplicaciones como Google Docs y Google Sheets, que permiten a los usuarios trabajar en tiempo real, compartir archivos y acceder a sus datos desde cualquier dispositivo con conexión a internet. Sin embargo, la dependencia de estos servicios centralizados conlleva riesgos, como la interrupción del acceso debido a problemas técnicos, errores en la facturación o decisiones unilaterales del proveedor. El software de código abierto (open source) es aquel cuyo código fuente está disponible para que cualquier usuario lo visualice, modifique y distribuya libremente. Estas tecnologías se han convertido en una alternativa atractiva para espacios de trabajo digitales debido a su flexibilidad, transparencia y el respaldo de comunidades de desarrollo activas. A diferencia de las soluciones propietarias, las herramientas open source permiten a las organizaciones personalizar y adaptar las plataformas según sus necesidades específicas, sin depender de un único proveedor [3]. El concepto de "Lugar de Trabajo Soberano" busca garantizar la autonomía digital de las organizaciones mediante el uso de software de código abierto y el control sobre su propia infraestructura digital. Según OpenProject, este enfoque permite a las empresas y administraciones públicas reducir la dependencia de proveedores externos, aumentando la seguridad y privacidad de los datos. Al adoptar soluciones soberanas, las organizaciones pueden decidir dónde y cómo se almacenan sus datos, evitando bloqueos tecnológicos y asegurando el cumplimiento de normativas locales [4]. Una de las iniciativas más destacadas en este ámbito es openDesk, una plataforma de código abierto diseñada para mejorar la gestión de proyectos y la colaboración en entornos digitales. openDesk proporciona una infraestructura flexible y adaptable que permite a las organizaciones trabajar con independencia tecnológica, garantizando la privacidad y el control sobre sus datos. Esta solución facilita la
comunicación y el trabajo en equipo sin la necesidad de depender de servicios propietarios, ofreciendo una alternativa sostenible y segura para empresas y administraciones públicas. Para lograr estos objetivos, openDesk integra diversas herramientas de código abierto que cubren necesidades clave como almacenamiento, mensajería, colaboración y gestión de proyectos. A continuación, se describen algunas de las principales soluciones utilizadas en esta plataforma:

Figura 1: Participantes del proyecto OpenDesk [4]

Nextcloud: Plataforma de almacenamiento en la nube autogestionada que permite a los usuarios compartir archivos, colaborar en documentos en tiempo real y administrar sus datos con altos niveles de privacidad y seguridad. Ofrece sincronización automática de archivos, integración con otras herramientas de productividad y control total sobre la infraestructura utilizada.

Element: Aplicación de mensajería instantánea basada en el protocolo Matrix, que permite la comunicación segura y descentralizada. Soporta mensajería cifrada de extremo a extremo, videollamadas, conferencias y la integración con otras plataformas, garantizando privacidad y control sobre los datos.

OpenProject: Herramienta de gestión de proyectos de código abierto que facilita la planificación, el seguimiento y la colaboración en tareas. Incluye funciones como gestión de tareas, diagramas de Gantt, seguimiento de tiempos, control de versiones y reportes detallados, lo que la convierte en una opción ideal para equipos de trabajo distribuidos.

Open-Xchange: Proveedor de soluciones de correo electrónico y colaboración en línea que ofrece servicios como gestión de contactos, calendario, correo electrónico seguro y herramientas de productividad para empresas y organizaciones que buscan independencia de servicios centralizados.

Univention: Plataforma de infraestructura informática de código abierto que permite gestionar usuarios, dispositivos y servicios de TI dentro de una organización. Facilita la integración de distintas soluciones de software y ofrece administración centralizada para entornos empresariales y educativos.

Collabora Online: Suite ofimática basada en LibreOffice que permite el tratamiento de textos, la creación de presentaciones y hojas de cálculo en un entorno colaborativo en línea. Es compatible con múltiples formatos de archivo y permite la edición en tiempo real, ofreciendo una alternativa de código abierto a herramientas propietarias como Microsoft Office 365 o Google Docs.

Nordeck: Solución de pizarra blanca digital que se integra como un widget dentro de Element, permitiendo la colaboración visual en tiempo real. Facilita la creación de diagramas, notas y bocetos compartidos, lo que mejora la comunicación y el trabajo en equipo en entornos distribuidos.

Docker: Docker es una plataforma de software que permite crear, probar e implementar aplicaciones rápidamente. Docker empaqueta software en unidades estandarizadas llamadas contenedores que incluyen todo lo necesario para que el software se ejecute, incluidas bibliotecas, herramientas de sistema, código y versión ejecutable

Kubernetes: Es una plataforma de orquestación de contenedores de código abierto diseñada para automatizar el despliegue, la gestión, el escalado y la operación de aplicaciones en contenedores. Permite organizar múltiples contenedores distribuidos en un clúster de servidores, proporcionando mecanismos para la alta disponibilidad, balanceo de carga, gestión de configuraciones, actualizaciones sin tiempo de inactividad y recuperación ante fallos. Gracias a su enfoque declarativo y su amplio ecosistema, Kubernetes se ha convertido en un estándar para la administración de aplicaciones en entornos de producción, facilitando la implementación de arquitecturas modernas como microservicios y DevOps.

Argo CD: Argo CD es una herramienta declarativa de distribución continua para Kubernetes. Se puede utilizar como una herramienta independiente o como parte del flujo de trabajo de integración y distribución continuas (CI/CD) para distribuir los recursos que los clusters necesitan.

Rancher: Rancher es un software de administración de contenedores de código abierto para gestionar aplicaciones de contenedores en entornos virtuales. Está especialmente diseñado para

su uso con Kubernetes, el sistema de orquestación de contenedores más comúnmente utilizado y popular en la actualidad.

Keycloak: Es una solución de código abierto para la gestión de identidades y accesos en aplicaciones y servicios web. Ofrece funcionalidades como inicio de sesión único (SSO), autenticación multifactor, federación de usuarios y administración centralizada de usuarios.

OIDC (OpenID Connect): Es una capa de identidad basada en el protocolo OAuth 2.0 que permite verificar la identidad de los usuarios a través de un proveedor de autenticación. En *openDesk*, Keycloak actúa como proveedor OIDC, gestionando la autenticación de usuarios y emitiendo tokens para acceder de forma segura a las aplicaciones.

En la tabla [1] se ilustran algunos trabajos que utilizan las herramientas de los participantes de OpenDesk.

Autor	Año	Título	Resumen
Gonzalez Hernández, W. F., Martínez Báez, R. L., & Arteaga Sandoval, R. A.	2012	Instalación y configuración de un servidor de correo electrónico con Open-Xchange Server y sus protocolos con seguridad	El trabajo se centra en la instalación y configuración de un servidor de correo electrónico utilizando Open-Xchange Server, enfatizando la implementación de protocolos de seguridad para garantizar comunicaciones seguras.[5]
Márquez Holgado, Jose	2025	SecureCloud Entrerprise. Plataforma de Almacenamiento y Colaboración Empresarial Segura en la nube con Nextcloud y LDAP para entornos empresariales.	El presente Trabajo de Fin de Grado tiene como objetivo desarrollar una Plataforma de Almacenamiento y Colaboración Empresarial Segura en la Nube, basada en Nextcloud e integrada con LDAP para la gestión centralizada de usuarios.[6]
HIDALGO LARREA, Jorge, VÁSQUEZ BERMÚDEZ, Mitchell, BRAVO BALAREZO, Lorena 3, BURGOS	2019	Modelo de aceptación de tecnología TAM en NextCloud. Caso de estudio Escuela Computación e	Se propone una solución de almacenamiento en la nube, con infraestructura propia y describe el uso de la herramienta de

ROBALINO Freddy 4 y VARGAS MATUTE Yessenia 5		Informática	colaboración Nextcloud.[7]

Tabla 1. Trabajos realizados utilizando tecnologías Open Source.

La arquitectura de openDesk (Figura [2]) se fundamenta en un portal centralizado que permite a los usuarios autenticados acceder de manera unificada a diversas aplicaciones funcionales, tales como gestión de archivos, comunicación, correo electrónico, programación de citas, gestión de tareas, almacenamiento de conocimientos y videoconferencias. Este portal forma parte de la solución de gestión de identidades y accesos (IAM) conocida como Nubus, que incluye componentes clave como OpenLDAP y Keycloak. OpenLDAP se encarga de almacenar la información de usuarios, grupos y permisos, mientras que Keycloak gestiona la autenticación mediante inicio de sesión único (SSO), implementando el protocolo OpenID Connect (OIDC). De este modo, una vez que el usuario inicia sesión en el portal a través de Keycloak, puede acceder sin necesidad de volver a autenticarse a las distintas aplicaciones permitidas, tales como Next Cloud, Element, OX App Suite, Open Project, XWiki y Jitsi. Nubus actúa no solo como proveedor de identidad (IdP), sino también como una capa de control de acceso, hub de integración entre servicios y sistemas, y plataforma de provisión de usuarios, centralizando la administración a través de una versión adaptada de la Univention Management Console (UMC). Además, incorpora un componente denominado Intercom Service, que facilita la autenticación entre frontends y APIs de diferentes aplicaciones, siguiendo el patrón Backend-for-Frontend. Finalmente, el portal no solo sirve como punto de entrada unificado, sino que también ofrece funciones de autoservicio como el restablecimiento de contraseñas [9].

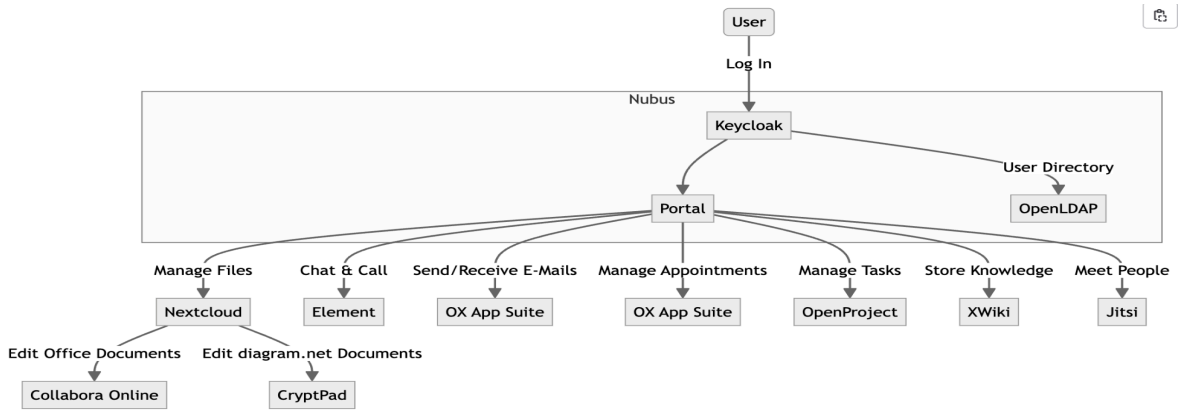


Figura 2. Arquitectura de Opendesk

En cuanto a los mecanismos de autenticación y autorización (Figura 3]), openDesk emplea el protocolo OpenID Connect (OIDC), lo que permite un control centralizado y seguro del acceso a los distintos servicios. La plataforma utiliza Keycloak como proveedor de identidad (IdP), configurando un cliente específico para cada componente que requiere autenticación, lo que garantiza la trazabilidad y control de acceso individualizado. Aquellos componentes que no manejan autenticación de forma autónoma confían en otros servicios para realizar esta tarea, siguiendo un modelo de confianza delegada dentro del ecosistema. Paralelamente, OpenLDAP actúa como fuente única de información de identidad, y es accedido por diversos servicios a través de cuentas de búsqueda LDAP específicas para cada uno, permitiendo así consultas directas a los datos de usuarios, grupos y permisos. Esta estructura asegura una distribución coherente y segura de los datos de identidad, mientras que el uso de flujos OAuth2 y OIDC en los distintos módulos garantiza compatibilidad y estandarización en la comunicación entre servicios, a menos que se indique explícitamente otro método de autenticación [9].

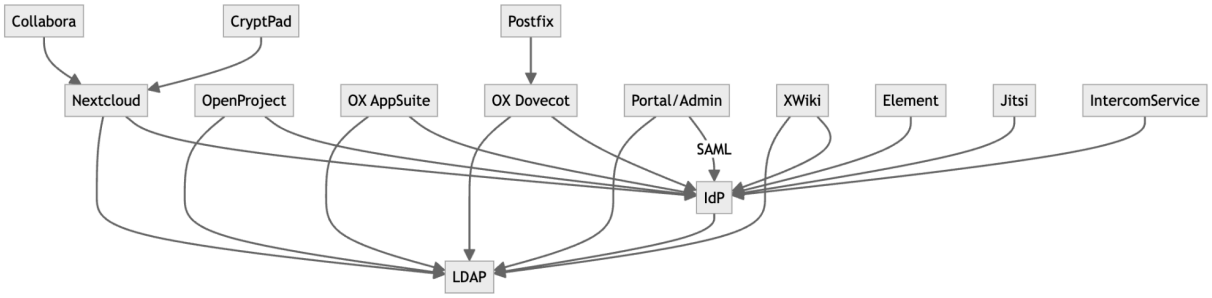


Figura 3. Autenticación

4. Metodología

Con el propósito de cumplir con los objetivos específicos establecidos, se llevaron a cabo las siguientes actividades, las cuales se detallan a continuación.

1. Definir la arquitectura y el plan de implementación del espacio de trabajo digital soberano, garantizando su alineación con las necesidades operativas de la empresa y su disponibilidad en escenarios de contingencia.

1.1 Selección de infraestructura

Para llevar a cabo el despliegue de la aplicación Opendesk, fue necesario contar con un dispositivo de procesamiento de tamaño reducido que permitiera ejecutar la solución en un entorno controlado. En este proyecto, se utilizó un mini servidor modelo IPC2 de la marca Compulab, el cual fue seleccionado por sus características técnicas adecuadas para el funcionamiento continuo de la aplicación.

Este equipo, mostrado en la Figura [4], actúa como el servidor principal donde reside y opera la aplicación. La elección de este dispositivo responde a la necesidad de contar con una plataforma de bajo consumo energético, con alta disponibilidad y confiabilidad para la realización de pruebas en tiempo real.

El despliegue se realizó dentro de una red interna aislada, diseñada específicamente para este entorno de pruebas. Esta configuración permite ejecutar todos los escenarios necesarios de validación sin interferencias externas, garantizando así un entorno seguro, controlado y reproducible durante todo el proceso de desarrollo y pruebas de la aplicación.

Figura 4. IPC2

1.2 Preparación del entorno de pruebas

Actualmente, la compañía cuenta con un directorio UCS de código abierto, el cual ha sido adoptado en concordancia con los requerimientos del proyecto, dado que es la alternativa que ofrece Opendesk para la gestión de directorio activo. Con el propósito de no intervenir directamente en el directorio activo principal de la organización —del cual dependen múltiples servicios internos críticos para la operación continua—, se procedió a exportar una imagen OVA del entorno UCS hacia un segundo dispositivo (IPC2). A este nuevo equipo se le asignó una dirección IP distinta dentro de la VLAN de pruebas habilitada para el proyecto. En este entorno aislado se migraron algunos usuarios seleccionados, tal como se observa en la Figura [5], permitiendo así realizar las pruebas necesarias sin comprometer la estabilidad ni la disponibilidad de los servicios productivos.

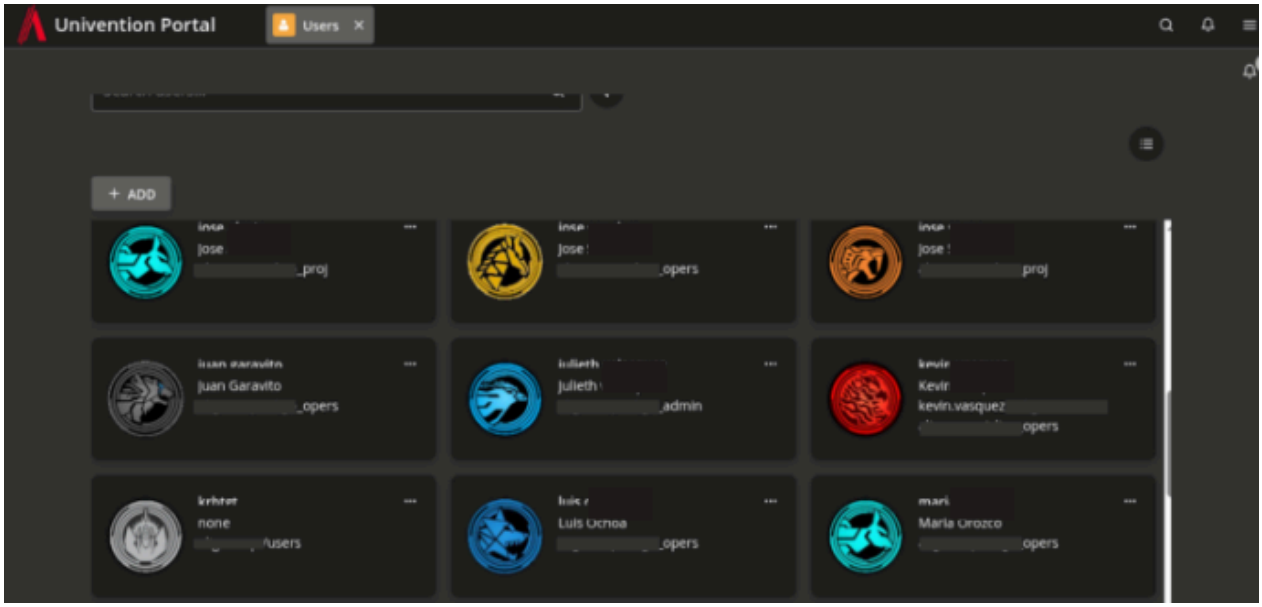


Figura 5. Usuarios de prueba

La **figura 6**, muestra de manera general la estructura lógica del entorno implementado, incluyendo los componentes principales y sus interconexiones

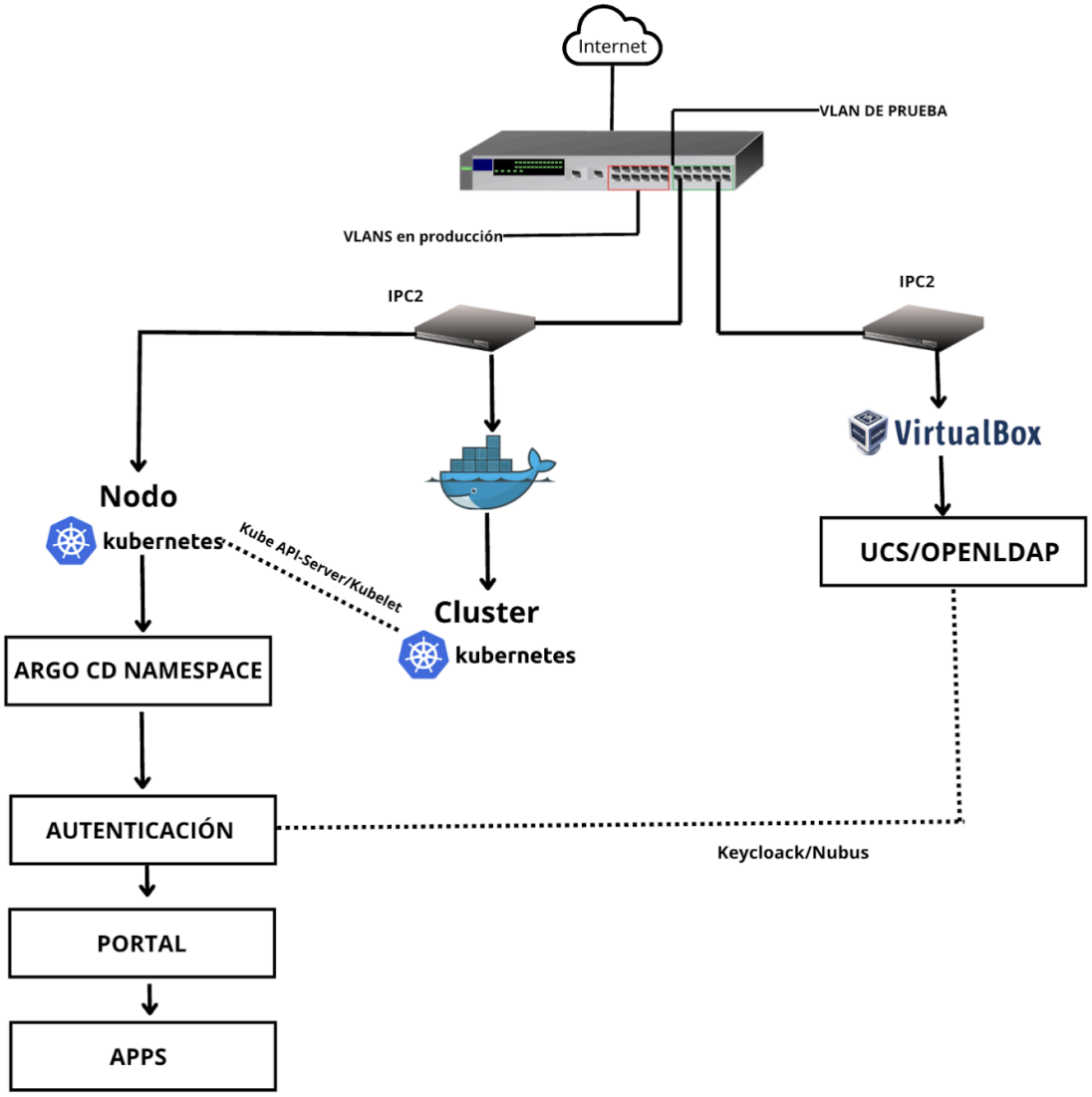


Figura 6. Arquitectura de la solución

2. Implementar la solución en un entorno controlado, integrando los servicios esenciales de correo empresarial y almacenamiento de archivos, con el objetivo de evaluar su desempeño y seguridad en un ambiente reducido.

Despliegue de openDesk

Para el despliegue de *openDesk*, se diseñó e implementó una metodología basada en los principios de GitOps, orientada a garantizar la automatización, trazabilidad y control total del

ciclo de vida de las aplicaciones dentro de un entorno Kubernetes. Todo el proceso fue realizado en un entorno controlado, específicamente diseñado para pruebas y validación.

2.1 Preparación del Clúster Kubernetes (K3s)

Se implementó un clúster Kubernetes utilizando K3s y Rancher, ejecutado en un contenedor dedicado. Este entorno controlado permite simular condiciones reales de operación, manteniendo al mismo tiempo la posibilidad de realizar ajustes y pruebas sin comprometer sistemas en producción. Esto se realizó debido a que OpenDesk es una solución que se ejecuta sobre Kubernetes. En la figura [7] se muestra la interfaz gráfica que confirma el correcto despliegue del orquestador.

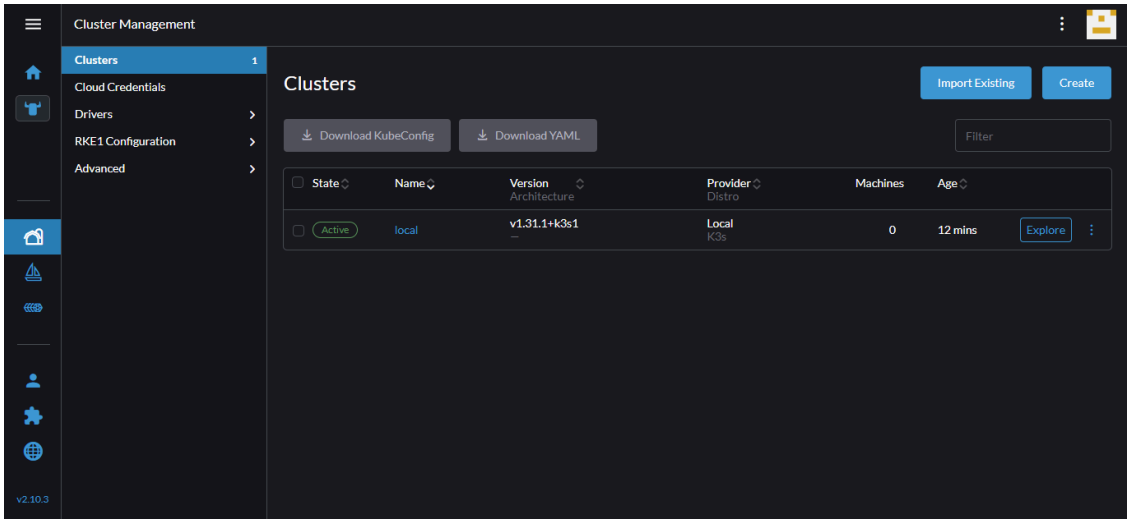


Figura 7. Despliegue de K3s

Para ello, se procedió al despliegue de un nodo local, el cual actúa como instancia de ejecución para las aplicaciones contenidas. Este nodo opera dentro de un entorno lógico denominado namespace, el cual permite aislar los recursos, facilitar la administración de los contenedores y mantener una estructura organizada dentro del entorno de pruebas.

En la figura [8] se muestra desde la interfaz gráfica de rancher el cluster desplegado en contenedor y el nodo local en el namespace llamado opendesk.

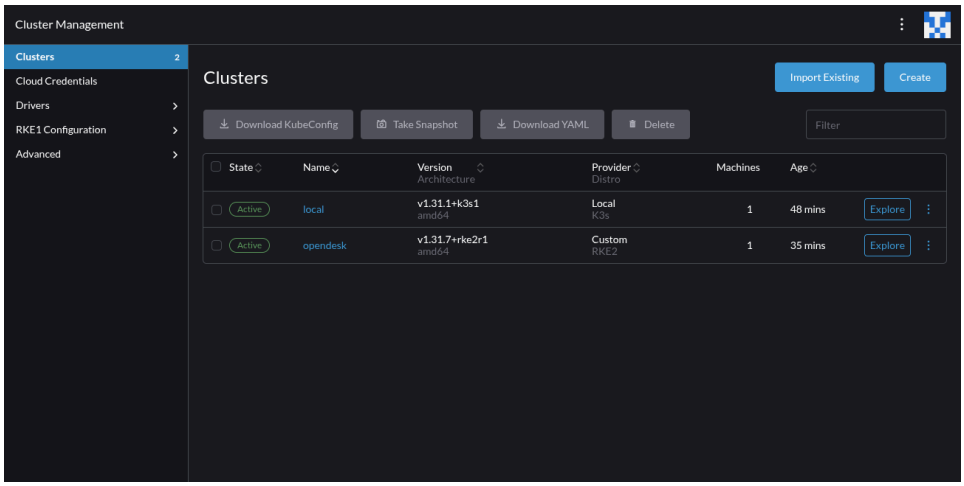


Figura 8. Despliegue nodo local

2.2. Implementación Argo CD

Se implementó Argo CD como plataforma de Continuous Delivery para Kubernetes. A través del patrón *App of Apps*, se gestionaron los distintos componentes de openDesk desde un repositorio Git central, permitiendo que el estado del sistema estuviese definido completamente como código. Para la correcta implementación de Argo CD se deben exponer los puertos correspondientes a través de nginx en el archivo nginx-ingress-nodeport.yaml como se muestra en la figura [9].

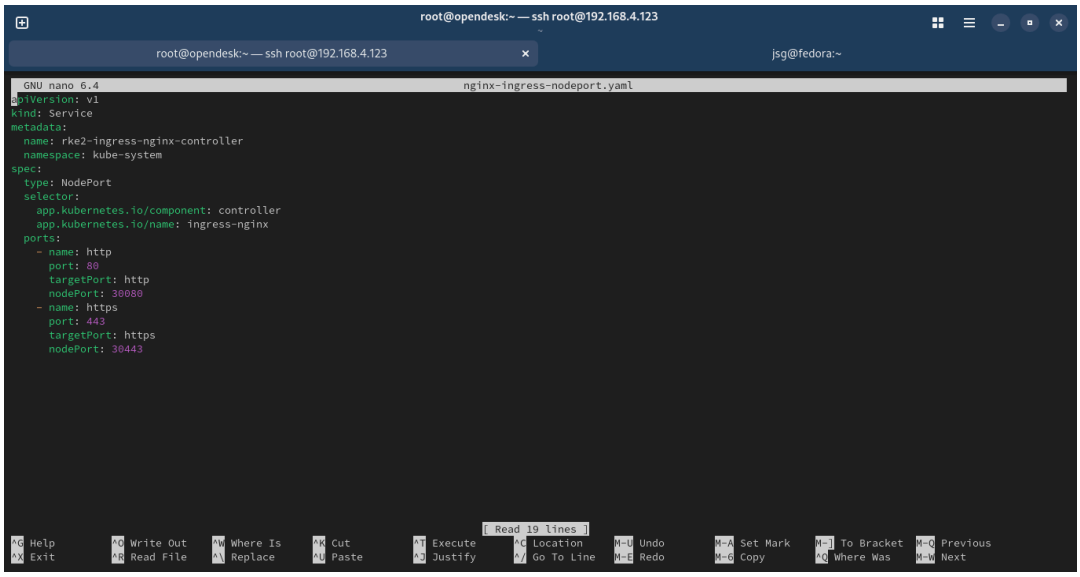


Figura 9. Exposición de puertos

Como parte del proceso de configuración de **Argo CD**, es indispensable establecer adecuadamente el componente **Ingress**, tal como se ilustra en la Figura [10]. Esta configuración permite habilitar el acceso externo a la interfaz web de Argo CD desde el entorno local o desde una red específica, facilitando así su administración y supervisión.

El ingreso a la interfaz gráfica es fundamental para una gestión centralizada y visual de las aplicaciones desplegadas, ya que permite monitorear el estado de los recursos, aplicar cambios en tiempo real y verificar la sincronización entre los manifiestos declarativos y el estado real del clúster.

Mediante la configuración del Ingress, se define una ruta de acceso y las reglas necesarias para que las solicitudes externas sean redirigidas correctamente hacia el servicio correspondiente dentro del clúster. Esta integración no solo mejora la experiencia del usuario al proporcionar una interfaz intuitiva, sino que también optimiza los procesos de despliegue continuo y control de versiones en un entorno de desarrollo basado en GitOps

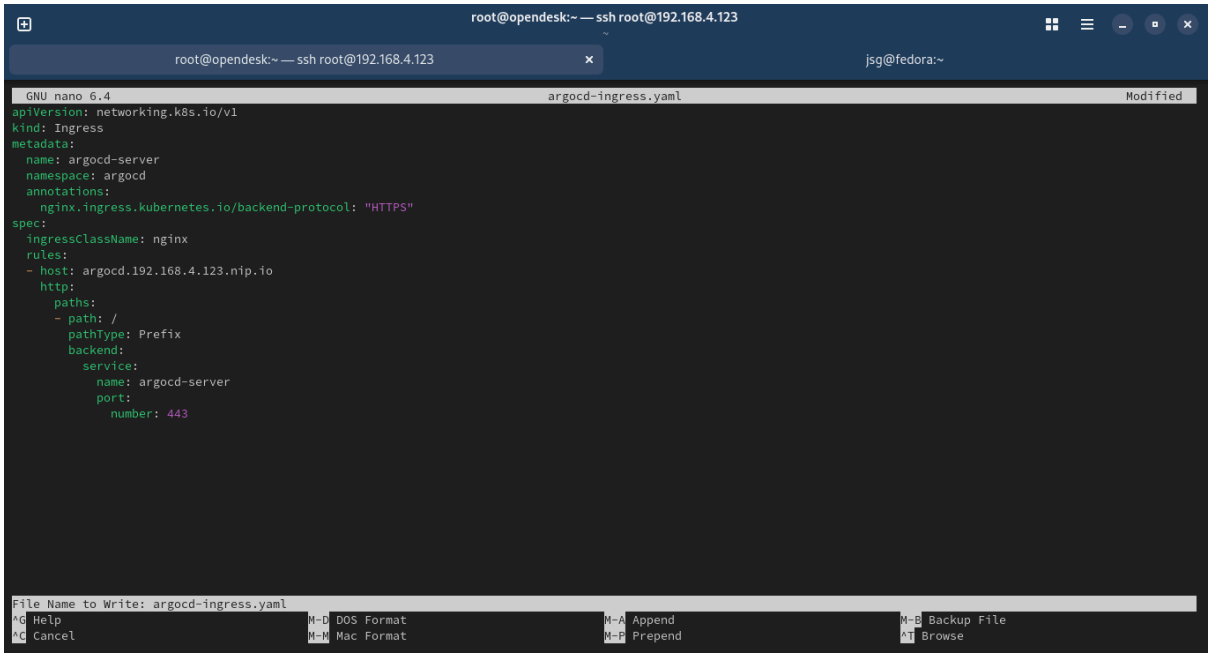


Figura 10. Configuración Ingress Argo CD

Si las configuraciones previamente realizadas para NGINX e Ingress han sido aplicadas correctamente, se habilita el acceso a la interfaz gráfica de Argo CD. Esta interfaz permite

visualizar y gestionar de forma intuitiva las aplicaciones desplegadas dentro del clúster Kubernetes. La Figura [11] muestra la vista de acceso de dicha interfaz, desde la cual es posible monitorear el estado de sincronización de los recursos, realizar despliegues manuales, y acceder a información detallada de cada componente administrado por Argo CD.

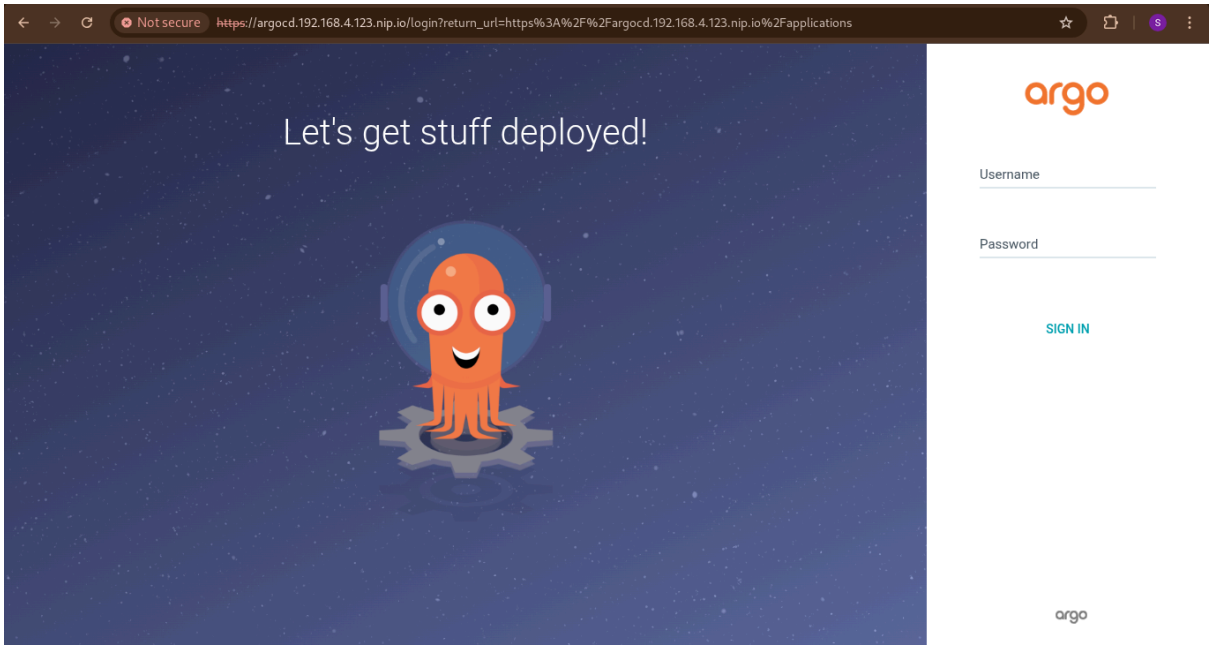


Figura 11. Interfaz web Argo CD

2.3 Configuración Argo CD

Una vez establecido el acceso a la interfaz web de **Argo CD**, se procede a la configuración del proyecto correspondiente a **OpenDesk**. Para ello, es necesario acceder al apartado **"Settings" > "Projects" > "OpenDesk"**, dentro de la interfaz gráfica.

En esta sección se definen los parámetros principales del proyecto, tales como los destinos permitidos para los despliegues, los repositorios autorizados y los *namespaces* habilitados. La Figura [12] muestra las configuraciones aplicadas en esta etapa, las cuales son fundamentales para delimitar el alcance del proyecto y asegurar una gestión controlada y segura de los recursos.

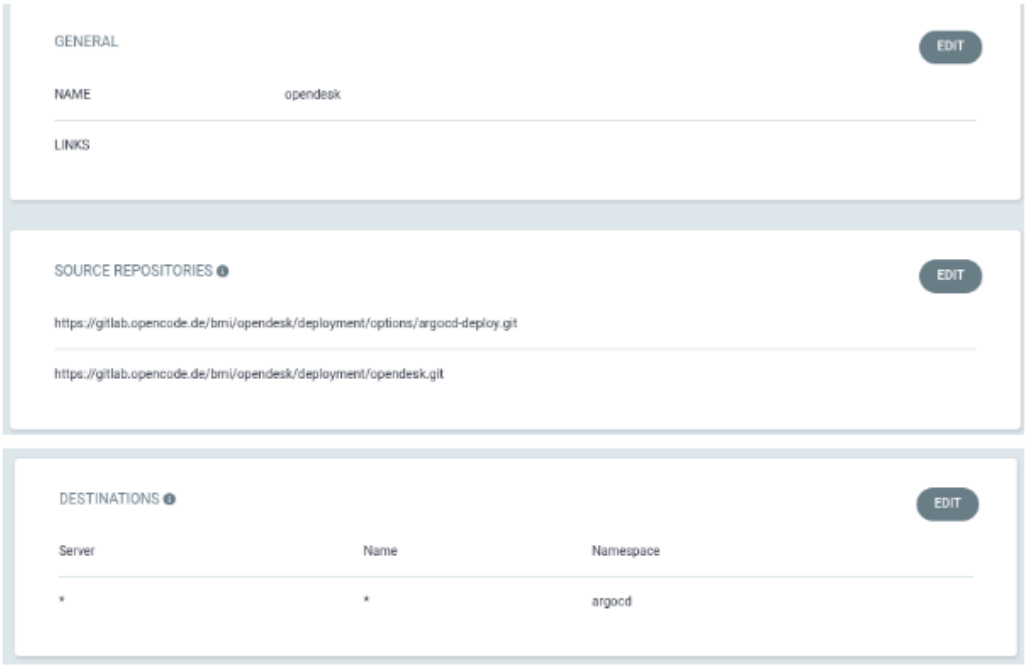


Figura 12. Configuración proyectos en Argo CD

3. Evaluar el desempeño, seguridad y usabilidad de los servicios implementados en un entorno controlado, para detectar posibles áreas de mejora, garantizando el adecuado funcionamiento en un escenario de producción.

3.1 Pruebas de usabilidad.

Para evaluar la experiencia del usuario con la nueva plataforma, se realizaron pruebas de usabilidad tipo observacional y tareas guiadas, con la participación de un grupo representativo de usuarios pertenecientes a las áreas de administración, ventas e ingeniería.

Durante las sesiones, se analizaron aspectos como la facilidad de navegación, la comprensión de funciones y la ejecución de tareas básicas dentro del sistema. Se observaron comportamientos, tiempos de respuesta, errores comunes y niveles de autonomía, lo que permitió identificar diferencias significativas en el grado de adaptación entre los distintos perfiles de usuarios.

5. Análisis de resultados

A. Integración de las apps desde ArgoCD

En la figura [13], se ilustra el dashboard principal de Argo Cd con las aplicaciones correspondientes a OpenDesk.

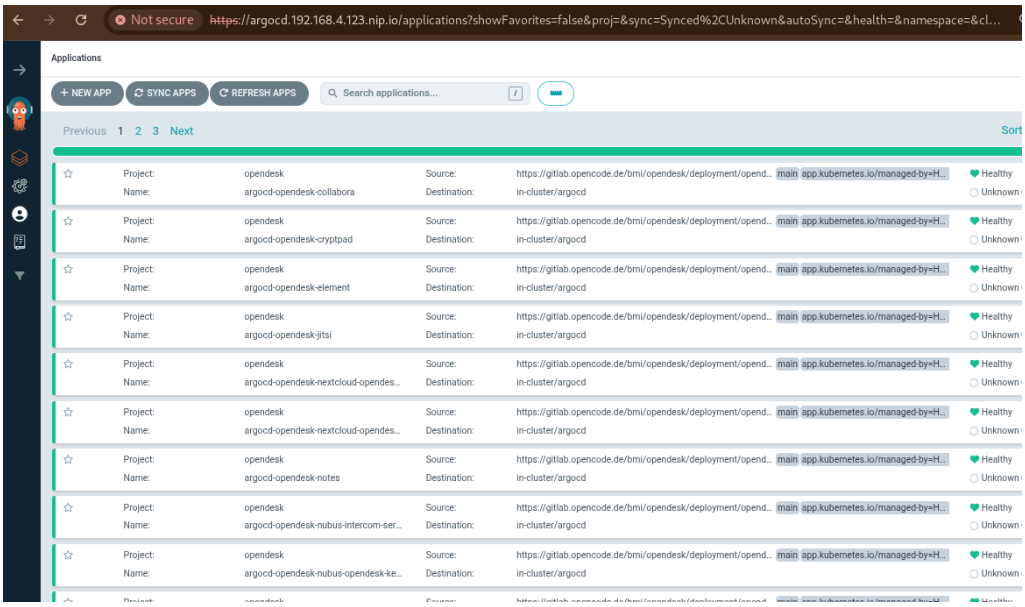


Figura 13. Dashboard ArgoCD

El despliegue de OpenDesk comienza con la activación del módulo Frontend, que proporciona la interfaz principal y actúa como punto de acceso centralizado para los usuarios, permitiéndoles visualizar y acceder a los diferentes servicios disponibles. Luego, se procede con la habilitación del servicio de correo electrónico, basado en Open-Xchange, que permite a los usuarios gestionar sus comunicaciones de manera integrada dentro de la plataforma. Finalmente, se implementa la aplicación de almacenamiento, ofreciendo un entorno digital seguro para la gestión, carga y organización de archivos, accesible desde la misma interfaz de OpenDesk. Con estos pasos, se asegura que los servicios fundamentales de la suite estén completamente operativos y accesibles desde una única plataforma, cumpliendo con los objetivos de integración y centralización del proyecto.

B. Opendesk

En la figura [14] se ve la ventana principal, la cual se encarga de redireccionar las demás aplicaciones.

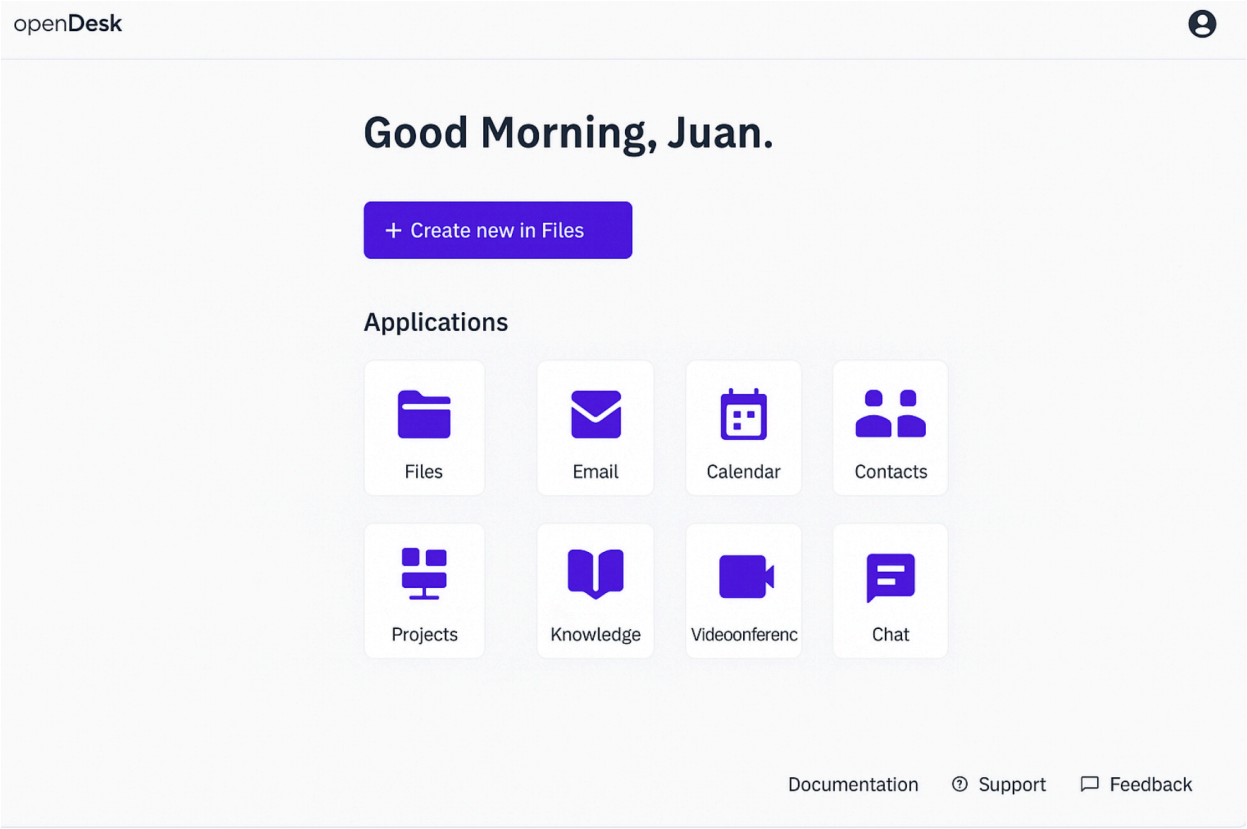


Figura 14. Ventana principal OpenDesk

C. Servicio de correo electrónico.

OpenDesk integra una solución de correo electrónico basada en la plataforma Open-Xchange. Gracias al despliegue de OpenDesk a través de ArgoCD, fue posible acceder correctamente a la interfaz principal del servicio de correo electrónico, como se muestra en la **Figura [15]**.

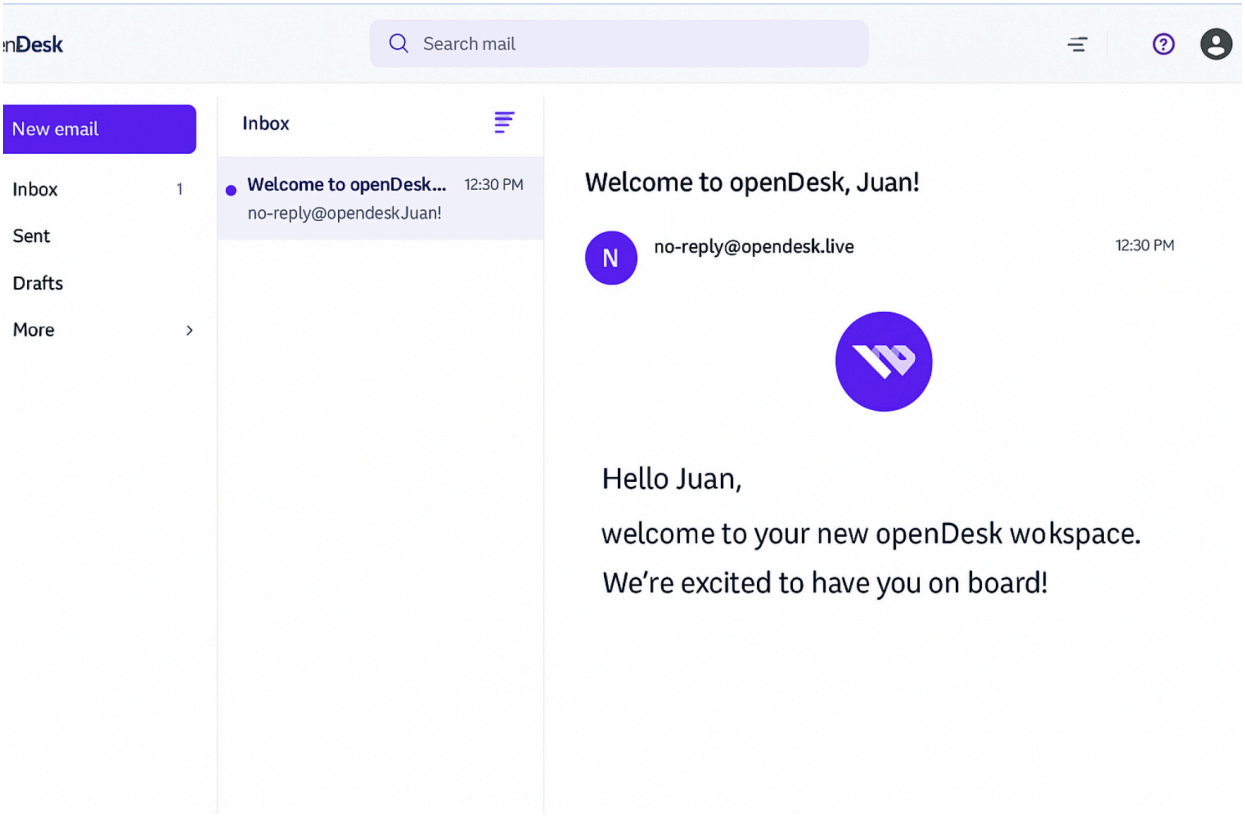


Figura 15. Correo electrónico Opendesk

D. Servicio de almacenamiento

Figura [16] muestra la interfaz del servicio de almacenamiento en la nube integrado en OpenDesk. En esta vista se aprecia un entorno limpio y ordenado, pensado para facilitar la gestión, organización y visualización de archivos dentro del ecosistema de OpenDesk. Este servicio permite a los usuarios trabajar de forma colaborativa y centralizada, optimizando el acceso y la administración de documentos en un espacio digital intuitivo.

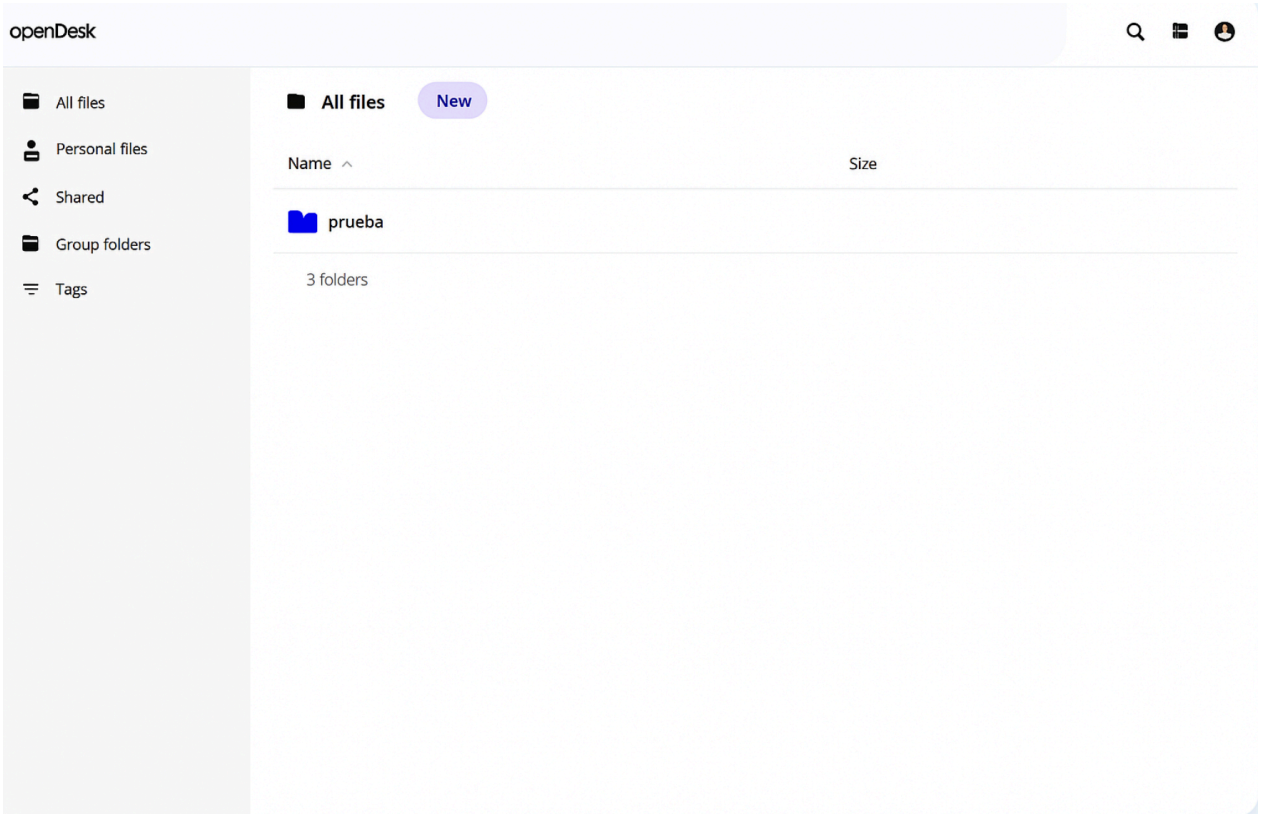


Figura 16. Interfaz de almacenamiento en la nube de OpenDesk

E. Otras Apps

Como parte del ecosistema de OpenDesk, se cuenta con una variedad de aplicaciones adicionales que complementan las funcionalidades principales de la plataforma. Entre estas se incluyen herramientas como **OpenProject** para la gestión de proyectos colaborativos y soluciones para videoconferencias, entre otras.

Estas aplicaciones están disponibles para su integración según las necesidades que se identifiquen a lo largo del tiempo. Se contempla su implementación de manera progresiva y planificada, priorizando aquellas que respondan a los requerimientos específicos de los usuarios y contribuyan a fortalecer el entorno de trabajo digital.

De esta forma, se busca que la plataforma evolucione de manera ordenada y adaptada al contexto de la organización, permitiendo ampliar sus capacidades sin comprometer la estabilidad ni la experiencia de uso.

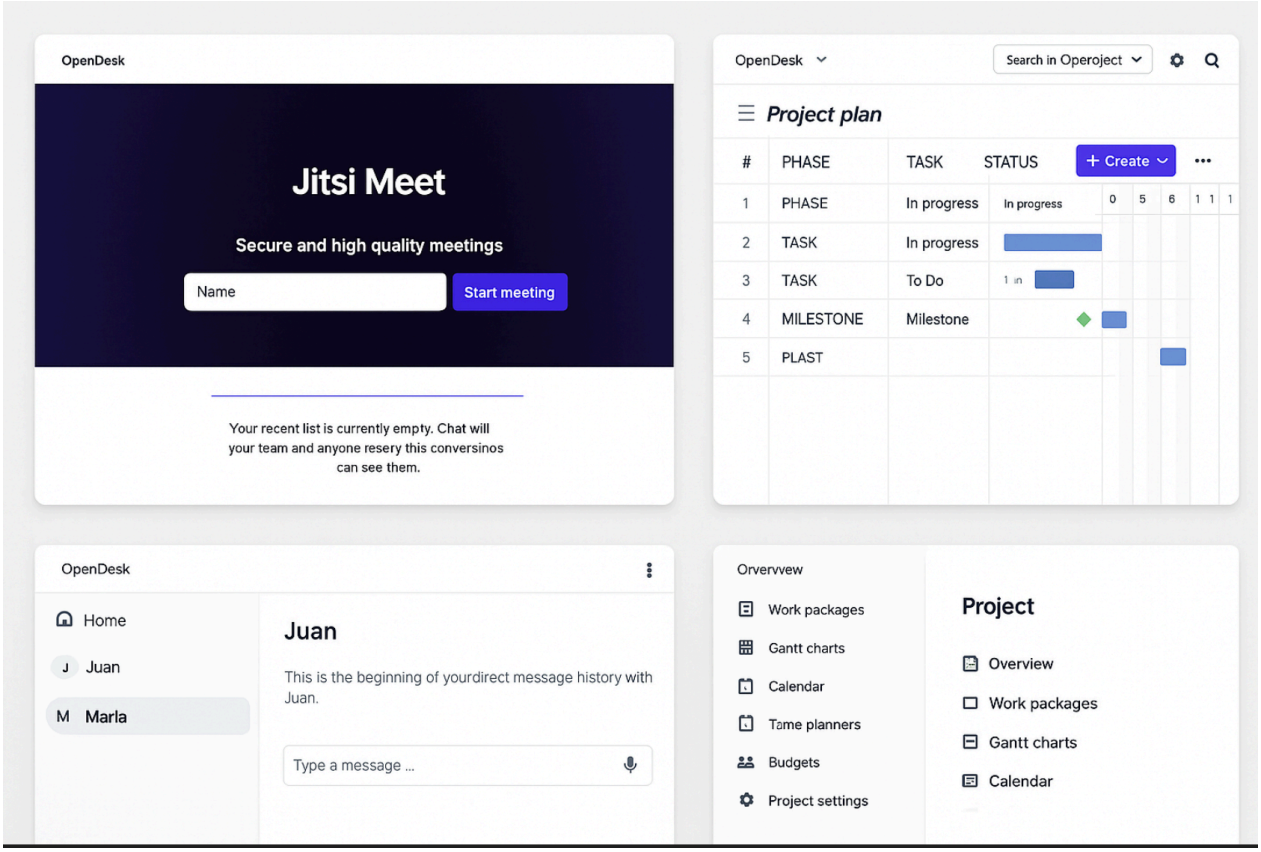


Figura 16. Otras Aplicaciones disponibles.

D. Resultados de las pruebas de usabilidad

En las pruebas de usabilidad realizadas con un grupo representativo de usuarios de las áreas de administración, ventas e ingeniería, se identificaron diferencias notables en la facilidad de uso y adaptación a la plataforma.

Los usuarios de administración y ventas experimentaron mayores dificultades al interactuar con las herramientas, particularmente en aspectos relacionados con la navegación, el reconocimiento de funciones y la comprensión general de la interfaz.

Estas dificultades se atribuyen principalmente a la costumbre de estos perfiles a trabajar en entornos más tradicionales y estructurados, con herramientas convencionales que difieren del enfoque digital integrado de la nueva plataforma. Como resultado, se observó un mayor tiempo de ejecución de tareas, una mayor tasa de errores y una dependencia significativa de asistencia externa. En contraste, los usuarios del área de ingeniería mostraron una rápida comprensión del sistema, logrando desenvolverse de manera autónoma y eficiente, debido a su familiaridad con entornos tecnológicos más dinámicos. A partir de estos hallazgos, se sugiere considerar ajustes enfocados en la simplificación

visual de ciertos módulos, así como una fase de familiarización previa al despliegue, en la que los usuarios puedan explorar la plataforma en contextos simulados que se asemejen a sus tareas cotidianas. Esto permitiría una integración más progresiva y natural del sistema en todas las áreas de la organización.

6. Conclusiones y recomendaciones

1. Viabilidad técnica para alcanzar la soberanía digital

El proyecto evidenció que es técnicamente viable diseñar e implementar un entorno digital soberano, utilizando exclusivamente tecnologías de código abierto. La integración de estas soluciones permitió construir una infraestructura funcional, segura y autónoma, capaz de cubrir las necesidades operativas y comunicacionales de una organización sin depender de servicios externos o propietarios. Esta demostración constituye un paso significativo hacia la consolidación de la soberanía digital, al proporcionar control completo sobre el ecosistema tecnológico y los datos que circulan en él.

2. Infraestructura eficiente, flexible y reproducible

La arquitectura desplegada, basada en contenedores, automatización declarativa y principios de GitOps, permitió construir un entorno altamente flexible y eficiente. La centralización de la gestión, la capacidad de escalar servicios según demanda, y la trazabilidad completa de cada cambio o despliegue, facilitaron tanto el mantenimiento como la posibilidad de reproducir o migrar el entorno a futuro. Esta infraestructura no solo reduce costos operativos, sino que mejora la capacidad de adaptación frente a nuevas necesidades o escenarios.

3. Seguridad, control de la información y mitigación de riesgos

La implementación en un entorno controlado permitió validar que el control sobre los datos permanece exclusivamente en manos de la organización. Esto reduce significativamente los riesgos relacionados con accesos no autorizados, pérdida de información crítica o vulneraciones a la privacidad. Este aspecto resulta especialmente relevante para instituciones que manejan datos

sensibles, estratégicos o confidenciales, posicionando la soberanía digital como una respuesta efectiva ante amenazas externas y dependencias tecnológicas.

4. Proyección hacia entornos productivos escalables

Si bien las pruebas realizadas demostraron un funcionamiento exitoso en un entorno de laboratorio, se recomienda avanzar hacia un despliegue progresivo en entornos productivos reales. Esta transición debe llevarse a cabo de manera gradual y planificada, incorporando mecanismos de alta disponibilidad, copias de seguridad automatizadas, balanceo de carga y pruebas de estrés, con el fin de asegurar la estabilidad, resiliencia y continuidad del sistema bajo condiciones exigentes de operación.

5. Monitoreo y respuesta proactiva ante incidentes

Para asegurar la continuidad operativa y la anticipación a posibles fallos, es fundamental implementar herramientas avanzadas de monitoreo y gestión de alertas. Estas herramientas deben permitir la supervisión en tiempo real del estado de los servicios, el rendimiento del sistema y la detección de vulnerabilidades o anomalías. Se recomienda desarrollar paneles de control intuitivos, con indicadores clave de rendimiento (KPIs) y alertas automáticas para facilitar una respuesta técnica oportuna.

6. Institucionalización de la soberanía digital

Finalmente, para garantizar la sostenibilidad del entorno construido y su adopción a largo plazo, se sugiere el diseño y adopción de una política institucional de soberanía digital. Esta política debe establecer lineamientos claros sobre el uso, mantenimiento, actualización, seguridad y escalabilidad de las tecnologías abiertas adoptadas, integrándolas formalmente dentro de la estrategia tecnológica de la organización. De este modo, se asegura la alineación entre la infraestructura desplegada y los objetivos organizacionales, fortaleciendo una cultura tecnológica soberana, responsable y resiliente.

Referencias

[1]. Guru. "Digital Workspace." Recuperado de https://www.getguru.com/es/reference/digital-workspace

[2]. Google. (n.d.). Google Workspace. Google. Recuperado de https://workspace.google.com/

[3]. Red Hat. "What is open source?" Recuperado de https://www.redhat.com/es/topics/open-source/what-is-open-source

4]. OpenProject. "Lugar de Trabajo Soberano." Recuperado de https://www.openproject.org/es/blog/lugar-de-trabajo-soberano

[5]. Gonzalez Hernández, W. F., Martínez Báez, R. L., & Arteaga Sandoval, R. A. (2012). Instalación y configuración de un servidor de correo electrónico con Open-Xchange Server y sus protocolos con seguridad (Doctoral dissertation).

[6]. Gutierrez Arizaca, F. H. (2023). Implementación de una nube privada con nextcloud para evitar la pérdida de información que genera la Municipalidad del Distrito de Orurillo.

[7]. HIDALGO, J., VASQUEZ, M., BRAVO, L., BURGOS, F., & VARGAS, Y. (2019). Modelo de aceptación de tecnología TAM en NextCloud. Caso de estudio Escuela Computación e Informática.

[8].OpenDesk. (s.f.). *Deployment options: ArgoCD*. OpenCoDE – GitLab. Recuperado el 17 de abril de 2025, de https://gitlab.opencode.de/bmi/opendesk/deployment/options/argocd-deploy

[9]. OpenDesk. (s.f.). *Architecture Manual*. OpenCoDE – GitLab. Recuperado el 17 de abril de 2025, de https://gitlab.opencode.de/bmi/opendesk/deployment/opendesk/-/blob/develop/docs/architecture.md

[10].OpenDesk. (s.f.). *OpenDesk deployment*. OpenCoDE – GitLab. Recuperado el 17 de abril de 2025, de https://gitlab.opencode.de/bmi/opendesk/deployment/opendesk

DESARROLLO DE UN ENTORNO DIGITAL SOBERANO EN ESPACIO CONTROLADO CON TECNOLOGÍAS DE CÓDIGO ABIERTO PARA GARANTIZAR LA CONTINUIDAD OPERATIVA.

Departamento de Ingeniería Electrónica y de Telecomunicaciones

UNIVERSIDAD DE ANTIOQUIA

Facultad de Ingeniería

DESARROLLO DE UN ENTORNO DIGITAL SOBERANO EN ESPACIO CONTROLADO CON TECNOLOGÍAS DE CÓDIGO ABIERTO PARA GARANTIZAR LA CONTINUIDAD OPERATIVA

PRACTICANTE: Juan Sebastian Garavito Gallo

ASESORES: Jaime Alberto Vergara Tejada y Francisco Javier Muñoz

PROGRAMA: Ingeniería de Telecomunicaciones

Semestre de la práctica: 2025-1

Introducción

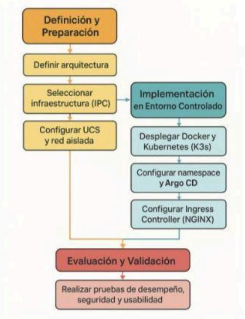
Aligo Defensores Informáticos es una empresa especializada en ciberseguridad, dedicada a ofrecer servicios integrales de protección y vigilancia. Su enfoque incluye soluciones proactivas y reactivas diseñadas según las necesidades de cada cliente, con el objetivo de garantizar la integridad de la información y proteger su vida digital. En un entorno cada vez más digitalizado, la seguridad de la información no solo depende de las medidas internas, sino también de la infraestructura y fiabilidad de los servicios en la nube. En la actualidad, los espacios de trabajo y el almacenamiento en la nube se han convertido en herramientas fundamentales para las empresas y su uso sigue en constante crecimiento.

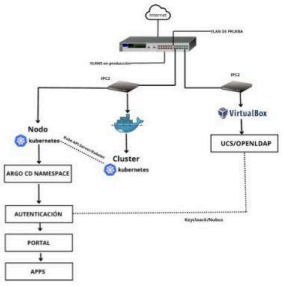
Por esto es necesario desplegar un entorno de trabajo basado en tecnologías de código abierto, que sirva como contingencia en situaciones críticas, con el fin de asegurar la continuidad de las operaciones empresariales convirtiéndose en alternativa digital soberana y confiable.

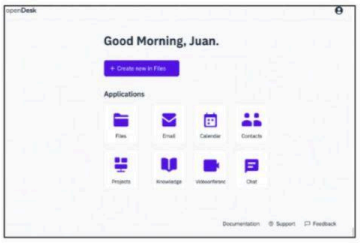
Objetivos

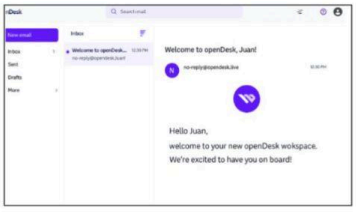
- Definir la arquitectura y el plan de implementación del espacio de trabajo digital soberano, garantizando su alineación con las necesidades operativas de la empresa y su disponibilidad en escenarios de contingencia.
- Implementar la solución en un entorno controlado, integrando los servicios esenciales de correo empresarial y almacenamiento de archivos, con el objetivo de evaluar su desempeño y seguridad en un ambiente reducido.
- Evaluar el desempeño, seguridad y usabilidad de los servicios implementados en un entorno controlado, para detectar posibles áreas de mejora, garantizando el adecuado funcionamiento en un escenario de producción.

Metodología









Resultados

La implementación de **OpenDesk** permitió desplegar una interfaz principal que funciona como el núcleo del entorno de trabajo digital, centralizando el acceso a herramientas esenciales como el correo electrónico, el almacenamiento y las aplicaciones de colaboración. Esta ventana unificada mejora significativamente la experiencia del usuario, al reducir la complejidad operativa y facilitar la gestión de tareas diarias desde un único punto de control. Su diseño intuitivo permite una interacción más ágil y eficiente, eliminando la necesidad de acceder a múltiples plataformas por separado.

Durante su validación en un entorno de pruebas, se logró comprobar el funcionamiento estable e integrado de los servicios principales, así como una gestión adecuada de usuarios, permisos y flujos de información. Estos resultados confirmaron la viabilidad del entorno como una alternativa funcional, segura y confiable, preparada para ser adoptada en entornos productivos sin depender de soluciones comerciales externas.

Conclusiones

- El proyecto evidenció que es técnicamente viable diseñar e implementar un entorno digital soberano, utilizando exclusivamente tecnologías de código abierto.
- La arquitectura desplegada, basada en contenedores, automatización declarativa y principios de GitOps, permitió construir un entorno altamente flexible y eficiente.
- La implementación en un entorno controlado permitió validar que el control sobre los datos permanece exclusivamente en manos de la organización.
- Si bien las pruebas realizadas demostraron un funcionamiento exitoso en un entorno de laboratorio, se recomienda avanzar hacia un despliegue progresivo en entornos productivos reales.

DATOS DE CONTACTO DEL AUTOR:

+57 3014289257 | sebastian.garavito@udea.edu.co | https://www.linkedin.com/in/juan-sebasti%C3%A1n-gallo-25a036249/