

Arquitectura Software

Arquitectura del Sistema y Estándares de Seguridad

1. **Cloudflare:** Se utiliza exclusivamente para gestionar el DNS, asegurando la rápida resolución de nombres de dominio y la distribución global del tráfico hacia la infraestructura subyacente.
 - a. **Servicios Clave:** DNS
2. **NGINX:** Se encarga de manejar todas las reglas de firewall y proteger la aplicación contra amenazas a nivel de red y de aplicación, incluyendo el top 10 de OWASP.
 - a. **Firewall de Aplicación Web (WAF):** Configurado en NGINX para proteger contra inyecciones SQL, cross-site scripting (XSS), y otras amenazas comunes definidas en el top 10 de OWASP.
 - b. **SSL/TLS:** NGINX gestiona el cifrado del tráfico mediante la implementación de SSL/TLS, asegurando que todas las comunicaciones entre los usuarios y la aplicación estén protegidas.
 - c. **Optimización del Tráfico Web:** NGINX también se encarga de la optimización del tráfico, asegurando que las solicitudes se manejen de manera eficiente y que los recursos se distribuyan adecuadamente.
3. **Azure AD B2C:** Azure Active Directory B2C gestiona el registro y autenticación de usuarios, ofreciendo soporte para autenticación multifactor (MFA) para cuentas administrativas, garantizando un acceso seguro a los recursos críticos.
 - a. **Servicios Clave:** Autenticación, gestión de identidades, MFA.
 - b. **Seguridad:** Azure AD B2C protege las identidades de los usuarios y asegura que el acceso a la plataforma esté controlado por políticas de seguridad estrictas, incluyendo MFA para cuentas de administración. Esto reduce el riesgo de accesos no autorizados y protege los datos de los usuarios.

2. Front-End

- a. **Tecnologías:** El front-end está desarrollado usando React y Next.js, dos tecnologías modernas que permiten una interfaz de usuario dinámica y optimizada para la web.
- b. **Despliegue:** El front-end se despliega en contenedores Docker y se gestiona mediante Kubernetes, lo que asegura escalabilidad y alta disponibilidad. La infraestructura subyacente es proporcionada como servicio (IaaS), lo que permite flexibilidad en la gestión de los recursos.
- c. **Control de Código:** Todo el código del front-end es versionado y almacenado en GitHub, permitiendo un control de versiones robusto y una colaboración eficiente entre desarrolladores.
- d. **Seguridad:** Al estar desplegado en Docker y Kubernetes, el front-end se beneficia de la seguridad inherente de los contenedores, incluyendo aislamiento de procesos y gestión de dependencias controlada. Además, la infraestructura IaaS ofrece controles adicionales como firewalls y monitoreo de seguridad.

3. Back-End

- a. **Tecnologías:** El back-end está desarrollado usando Node.js con el framework NestJS, lo que proporciona una arquitectura modular y altamente mantenible.
- b. **Despliegue:** Similar al front-end, el back-end también se despliega en contenedores Docker y es gestionado mediante Kubernetes, lo que asegura la resiliencia y capacidad de escalar según la demanda.
- c. **Control de Código:** El código del back-end también se versiona en GitHub, lo que permite un seguimiento detallado de los cambios y una colaboración eficiente.
- d. **Seguridad:** NestJS ofrece soporte para prácticas de seguridad como validación de entrada, gestión de sesiones seguras, y controles de acceso basados en roles. Además, el uso de Docker y Kubernetes añade una capa adicional de seguridad y aislamiento.

4. Almacenamiento de Archivos

- a. **Tecnologías:** Los archivos generados y firmados electrónicamente se almacenan en Azure Blob Storage, utilizando Geographically Redundant Storage (GRS) para asegurar que los datos estén disponibles incluso en caso de fallos regionales.
- b. **Seguridad:** Los archivos se benefician de la seguridad proporcionada por Azure, incluyendo cifrado en reposo y en tránsito. Además, las copias de seguridad de estos archivos se manejan a través de Microsoft Azure Backups, garantizando que los datos estén protegidos contra pérdida o corrupción.

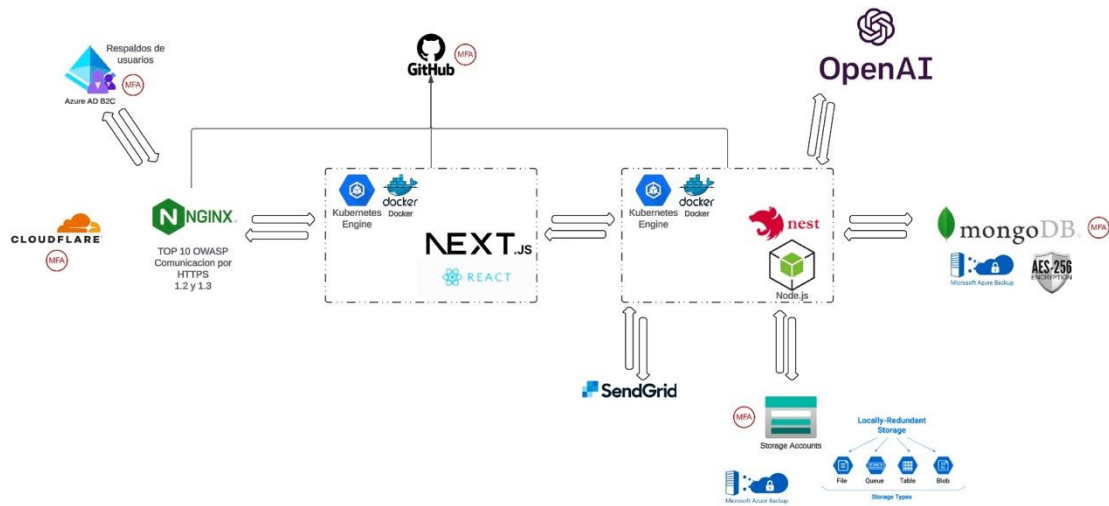
5. Base de Datos

- a. **Tecnologías:** Los datos de los usuarios y los metadatos de los documentos se almacenan en una base de datos MongoDB.
- b. **Cifrado:** Los datos sensibles se cifran utilizando AES256, un estándar de cifrado de alta seguridad. Esto asegura que incluso si los datos son comprometidos, no podrán ser leídos sin las claves de cifrado adecuadas.
- c. **Backups:** Se realizan copias de seguridad de la base de datos cada 6 horas, las cuales se almacenan en Microsoft Azure Backup, proporcionando un mecanismo de recuperación en caso de fallos o pérdida de datos.

6. Envío de Correos Electrónicos

- a. **Tecnologías:** Los correos electrónicos se envían utilizando SendGrid, un servicio de correo electrónico en la nube que facilita la entrega segura y eficiente de correos electrónicos transaccionales.
- b. **Seguridad:** SendGrid proporciona autenticación de correos electrónicos mediante SPF, DKIM y DMARC, asegurando que los correos electrónicos enviados desde la plataforma sean legítimos y no sean susceptibles de suplantación.

Diagrama de la Arquitectura descrita



Estándares de Seguridad

- **Cifrado:** Todos los datos sensibles, tanto en reposo como en tránsito, están cifrados utilizando estándares robustos como AES256 y TLS 1.2/1.3.
- **Autenticación Multifactor (MFA):** Azure AD B2C gestiona la autenticación, con MFA habilitado para cuentas administrativas, asegurando un acceso controlado y seguro.
- **Backups y Redundancia:** Se implementan copias de seguridad regulares y almacenamiento redundante en Azure, asegurando la disponibilidad y recuperación de datos en caso de fallos.
- **Control de Acceso:** Los accesos a los sistemas están controlados mediante políticas de acceso condicional y gestión de identidades, minimizando el riesgo de accesos no autorizados.
- **Protección Perimetral:** Cloudflare se utiliza para gestionar el tráfico entrante y proteger la plataforma contra amenazas a nivel de red y de aplicación.