efflux solutions

efflux-solutions.com

Efflux Solutions Limited
Suite 4, 2nd Floor The West Wing Montarik House, 3 Bedlam Ct, GX11 1AA, Gibraltar

Efflux Cloud Capture:
Libro Blanco sobre Seguridad.

Libro blanco
Ver. 1.0
Enero, 2026

Contents

1. System Overview 3

2. Introducción: El panorama cambiante del procesamiento de documentos 3
2.1 Portal del proveedor raíz 4
2.2 Portal de proveedores 4
2.3 Portal para inquilinos y propietarios 5
2.4 Portal de usuario 5
2.5 Cliente de escritorio 6
2.6 Cliente MFP 6
2.7 Almacenamiento en la nube 6
2.8 Almacenamiento ECC 6

3. Arquitectura multiinquilino 7

4. Control de acceso basado en roles (RBAC) 8
4.1 Matriz de acceso de gestión 8
4.2 Matriz de acceso funcional 9

5. Identificación y autenticación de usuarios 10

6. Política de contraseñas 10

7. Cierre de sesión automático y gestión de sesiones 11
Cliente MFP ..... **Error! Bookmark not defined.**
Portal web y cliente de escritorio ..... **Error! Bookmark not defined.**

8. Autenticación mediante PIN 12

9. Integración con Microsoft Entra ID 13

10. Flujo de autenticación y gestión de tokens 14

11. Seguridad de red y aislamiento de servicios 15

12. Protección de datos y aislamiento de inquilinos 15

13. Registros de actividad y de auditoría 16

1. System Overview

Efflux Cloud Capture es una solución de captura de documentos basada en la nube que permite a las organizaciones recopilar, procesar y enrutar documentos de forma segura desde múltiples fuentes de entrada. La plataforma es compatible con una amplia gama de marcas de impresoras multifunción (MFP), ofrece un cliente dedicado para Windows y permite la carga de archivos a través del navegador web, lo que posibilita la captura de documentos independientemente del dispositivo o la ubicación. Los administradores pueden gestionar usuarios de forma centralizada, registrar dispositivos compatibles y configurar flujos de trabajo de captura mediante una interfaz unificada en la nube.

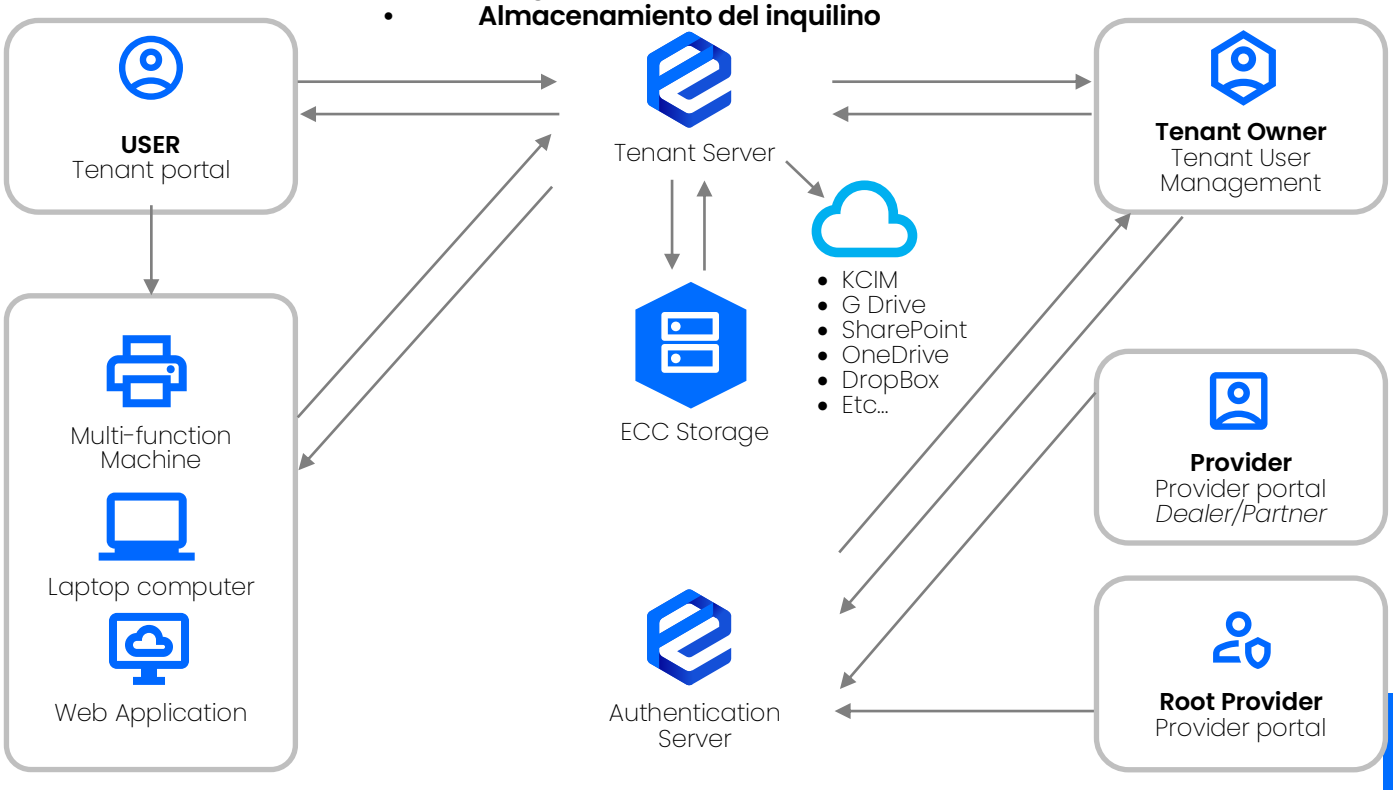
Este documento técnico ofrece a distribuidores y usuarios una visión general de las medidas de seguridad implementadas en Efflux Cloud Capture. La protección de la información de los clientes y de los datos de los documentos es un objetivo fundamental del diseño de la plataforma. Todos los activos de información gestionados por Efflux Cloud Capture están protegidos mediante una arquitectura de sistema segura, una configuración controlada y mecanismos de seguridad por capas integrados en el servicio.

---

2. Introducción: El panorama cambiante del procesamiento de documentos

Efflux Cloud Capture consta del siguiente componente:

- **Panel de administración del proveedor raíz**
- **Portal del proveedor (socios y distribuidores)**
- **Portal del propietario del inquilino**
- **Portal del usuario**
- **Cliente de escritorio**
- **Cliente MFP**
- **Integraciones de almacenamiento en la nube**
- **Almacenamiento del inquilino**



2.1 Portal del proveedor raíz

El Panel de Administración del Proveedor Raíz es una interfaz administrativa segura basada en la web, accesible únicamente para el personal de soporte autorizado de Efflux Solutions. Se utiliza para operar, dar soporte y gestionar la plataforma Efflux Cloud Capture, y no es accesible para distribuidores, socios ni clientes finales.

A través del panel de administración, el personal de soporte de Efflux puede gestionar las operaciones del ciclo de vida de los inquilinos, incluidas las activaciones pendientes, la verificación de nuevas organizaciones y el monitoreo de los inquilinos activos. El sistema ofrece visibilidad sobre los pedidos de instancias y licencias, lo que permite a los equipos de soporte revisar, aprobar y gestionar el aprovisionamiento y las renovaciones de manera controlada.

El panel de administración también permite la gestión centralizada de licencias, la administración de socios y distribuidores, y la gestión de cuentas administrativas. Las funciones de gestión de versiones permiten al equipo de soporte de Efflux controlar las versiones de software disponibles y asignar o modificar versiones específicas para cada organización, según sea necesario.

Todas las funciones administrativas están organizadas en una interfaz estructurada para garantizar la separación de responsabilidades, la trazabilidad de las acciones y un funcionamiento seguro de la plataforma.

2.2 Portal de proveedores

El Portal de Proveedores es una interfaz web diseñada para que los socios y distribuidores gestionen a sus clientes y las interacciones comerciales relacionadas con Efflux Cloud Capture. El acceso a este portal está restringido a cuentas autorizadas de socios y distribuidores, y no otorga control administrativo a nivel de plataforma.

A través del portal de proveedores, los socios y distribuidores pueden enviar a Efflux Solutions solicitudes para crear nuevos inquilinos y pedidos de renovación de licencias. El portal ofrece visibilidad sobre el historial y el estado actual de los pedidos, así como sobre el estado operativo de los inquilinos asociados, incluyendo su estado de activación y la validez de las licencias.

Los controles de acceso basados en roles definen el alcance de la visibilidad y las capacidades de gestión:

- Los socios pueden gestionar su red de distribuidores añadiendo distribuidores a su cuenta. Tienen visibilidad de todos los inquilinos y pedidos asociados tanto a su propia organización como a sus distribuidores registrados.
- Los distribuidores tienen acceso restringido y solo pueden ver y gestionar los inquilinos y pedidos asociados a sus propias cuentas.

Esta separación de funciones garantiza límites claros de responsabilidad, al tiempo que permite a los socios y distribuidores gestionar de manera eficiente las actividades de incorporación de clientes y de licenciamiento.

2.3 Portal para inquilinos y propietarios

El Portal del Inquilino (Tenant Owner Portal) es una interfaz de gestión basada en web que utilizan los administradores del inquilino para configurar y operar su propio entorno de Efflux Cloud Capture. El acceso está limitado a usuarios autorizados dentro del inquilino y no permite visualizar otros inquilinos ni acceder a controles a nivel de plataforma.

A través de este portal, los propietarios y administradores del inquilino pueden gestionar los usuarios y el control de acceso dentro de su organización. Esto incluye la creación y gestión de cuentas de administrador y de usuario estándar, la definición de grupos de usuarios y la asignación de permisos a dichos grupos. El portal admite la integración con Microsoft Azure Entra ID, lo que permite a los inquilinos conectar su servicio de directorio e importar usuarios a la plataforma..

El Portal del Inquilino (Tenant Owner Portal) también proporciona visibilidad operativa del entorno del inquilino. Los administradores pueden supervisar el estado de sus servicios, revisar los registros del sistema provenientes de la infraestructura del inquilino alojada en Azure y realizar comprobaciones operativas básicas.

Es posible crear cuentas de usuario temporales cuando sea necesario para facilitar escenarios de acceso a corto plazo.

Estas capacidades permiten a los inquilinos mantener el control sobre el acceso de los usuarios, la integración de identidades y la supervisión operativa, al tiempo que permanecen aislados de otros inquilinos y de la administración de la plataforma Efflux subyacente.

2.4 Portal de usuario

El Portal de Usuario es una interfaz web que los usuarios finales utilizan para llevar a cabo actividades cotidianas de captura y procesamiento de documentos dentro de Efflux Cloud Capture. El acceso a las funcionalidades está determinado por los roles de usuario y los permisos asignados.

A través del Portal de Usuario, los usuarios pueden cargar documentos para su procesamiento y realizar un seguimiento del estado de los documentos enviados a lo largo del flujo de trabajo de captura. Según sus permisos, los usuarios pueden crear, actualizar y eliminar plantillas, conexiones y listas de selección utilizadas para el procesamiento y el enrutamiento de documentos.

Los documentos procesados quedan disponibles en la sección de descargas del portal, donde los usuarios pueden acceder de forma segura a los resultados finales y recuperarlos. La visibilidad se limita a los documentos asociados al *tenant* (inquilino) y a los permisos del usuario, lo que garantiza el aislamiento entre usuarios y organizaciones.

2.5 Cliente de escritorio

Efflux Desktop Client es una aplicación basada en Windows que permite a los usuarios capturar y cargar documentos directamente desde su estación de trabajo. Después de iniciar sesión, el cliente carga y muestra las plantillas a las que puede acceder el usuario según sus permisos asignados.

Los usuarios pueden seleccionar una plantilla y cargar documentos para su procesamiento a través del flujo de trabajo de captura configurado. El cliente de escritorio también admite la funcionalidad de carpetas activas (*hot folders*), lo que permite a los usuarios definir carpetas locales que se supervisan de forma continua. Los documentos depositados en una carpeta activa configurada se cargan y procesan automáticamente utilizando plantillas predefinidas y reglas de automatización.

Esta capacidad permite escenarios de captura de documentos desatendidos o semiautomatizados, manteniendo al mismo tiempo una lógica de procesamiento coherente y la aplicación de los permisos correspondientes.

2.6 Cliente MFP

El cliente Efflux MFP es una aplicación integrada que se instala en impresoras multifunción (MFP) compatibles y permite a los usuarios capturar documentos directamente desde el panel del dispositivo. Tras la autenticación, el cliente muestra las plantillas accesibles para el usuario que ha iniciado sesión, según los permisos asignados.

Los usuarios pueden escanear documentos utilizando una plantilla seleccionada y enviarlos a Efflux Cloud Capture para su procesamiento. Los documentos capturados siguen el flujo de trabajo configurado asociado a la plantilla, lo que garantiza un procesamiento y enrutamiento uniformes.

2.7 Almacenamiento en la nube

Como solución de almacenamiento en la nube de terceros, ECC admite integraciones con Google Drive, Dropbox, KCIM OneDrive y SharePoint Online. Al establecer una conexión con su almacenamiento en la nube, ECC puede cargar automáticamente el documento procesado en dicho almacenamiento.

2.8 Almacenamiento ECC

Cada inquilino dispone de un espacio de almacenamiento aislado de 10 GB que puede utilizarse para guardar y descargar el documento procesado.

3. Arquitectura multiinquilino

Efflux Cloud Capture se ha diseñado utilizando una arquitectura de inquilino dedicado para garantizar un alto nivel de aislamiento entre clientes. A cada nuevo cliente se le asigna su propio entorno de inquilino alojado en Microsoft Azure.

Para cada inquilino, se despliega una instancia de servidor independiente con su propia dirección IP asignada y una URL de servicio única. Todo el procesamiento de documentos, el acceso de los usuarios y la ejecución de flujos de trabajo tienen lugar exclusivamente dentro del entorno de dicho inquilino.

Los recursos de procesamiento no se comparten entre inquilinos. Cada inquilino opera con servicios de computación, almacenamiento y aplicaciones aislados, lo que garantiza que el rendimiento, la disponibilidad y la actividad de la carga de trabajo de un inquilino no afecten a otro. Ningún dato de documentos, metadatos, configuración ni recurso del sistema es accesible entre los límites de los inquilinos.
Esta arquitectura proporciona una sólida separación de seguridad, un rendimiento predecible y un cumplimiento normativo simplificado, al eliminar la exposición de datos entre inquilinos y aplicar un aislamiento estricto a nivel de inquilino en las capas de infraestructura y aplicación.

4. Control de acceso basado en roles (RBAC)

Efflux Cloud Capture implementa el control de acceso basado en roles (RBAC) en todos los portales y componentes del sistema. El acceso a las funciones y a los datos se determina según el rol asignado al usuario, garantizando que este solo pueda visualizar información o realizar acciones expresamente permitidas dentro de su ámbito de responsabilidad.

El modelo RBAC se aplica de manera uniforme en la gestión de inquilinos, el procesamiento de documentos y el acceso de los clientes, con el fin de mantener la separación de seguridad y la rendición de cuentas.

4.1 Matriz de acceso de gestión

	Estado de la licencia	Estado del Tenant	Usuarios	Grupos de usuarios	Azure Entra
Proveedor raíz(Soporte de Efflux)	✓	✓	✓	✗	✗
Proveedor (Socio / Distribuidor)	✓	✓	✗	✗	✗
Propietario residente	✓	✓	✓	✓	✓

Notas:

- El acceso de nivel raíz del proveedor se limita exclusivamente a funciones operativas y de soporte.
- Los proveedores pueden consultar el estado del inquilino y de las licencias, pero no pueden gestionar los usuarios del inquilino ni la configuración de identidad.
- Los propietarios del inquilino tienen control total sobre su propio inquilino, incluida la integración de identidades y la gestión de la estructura de usuarios.

4.2 Matriz de acceso funcional

Esta tabla define el acceso a las funciones de captura, procesamiento y configuración de documentos en función de los roles del inquilino.

Rol	Carga	Estado	Estadísticas	Uso de recursos de creación	Uso de recursos	Cliente	Documentos almacenados
Propietario	Todas las plantillas	Todos los usuarios	Todos los usuarios	✓	Todo	Todo	Todo
Administrador	Todas las plantillas	Todos los usuarios	Todos los usuarios	✓	Todo	Todo	Todo
Usuario	Plantillas asignadas	Solo subidas propias	Solo estadísticas propias	Si se concede el permiso	Asignado o creado	Asignado o creado	Solo documento propio

Notas:

- Los propietarios y administradores del inquilino (*tenant*) tienen una visibilidad operativa equivalente, pero difieren en cuanto a la autoridad administrativa, según lo definido por la política del inquilino.
- Los usuarios estándar del inquilino tienen acceso restringido a sus propios documentos y a los recursos que se les hayan asignado explícitamente.
- El acceso a plantillas, conexiones, el cliente de escritorio y el cliente MFP se basa en permisos y puede controlarse mediante la asignación a grupos de usuarios.

5. Identificación y autenticación de usuarios

Para acceder a Efflux Cloud Capture, los usuarios deben iniciar sesión con una cuenta verificada y activa. Durante el registro, se envía un correo electrónico de verificación a la dirección registrada del usuario. La cuenta solo queda habilitada para su uso una vez que se ha confirmado correctamente el enlace de verificación incluido en dicho correo.

Solo se permite el acceso al sistema a cuentas verificadas y activas. A las cuentas no verificadas o desactivadas se les deniega la autenticación y no pueden acceder a ningún portal ni servicio.

Los propietarios del inquilino (*Tenant Owners*) pueden desactivar cuentas de usuario en cualquier momento. Una vez desactivada una cuenta, se revoca inmediatamente el acceso a Efflux Cloud Capture, independientemente del estado de autenticación previo.

6. Política de contraseñas

Efflux Cloud Capture aplica una política de contraseñas para garantizar un nivel mínimo de seguridad de la cuenta. Las contraseñas de los usuarios deben cumplir los siguientes requisitos:

- Longitud mínima de **8 caracteres**
- Al menos **una letra mayúscula (A–Z)**
- Al menos **una letra minúscula (a–z)**
- Al menos **un dígito numérico (0–9)**

Las contraseñas que no cumplen con estos requisitos son rechazadas durante su creación o modificación. Esta política ayuda a reducir el riesgo de acceso no autorizado derivado de credenciales débiles o fáciles de adivinar.

7. Cierre de sesión automático y gestión de sesiones

Efflux Cloud Capture implementa controles de cierre de sesión automático y gestión de sesiones para reducir el riesgo de acceso no autorizado derivado de sesiones desatendidas o persistentes.

Cada usuario puede visualizar sus sesiones activas a través del portal web. Desde este panel, los usuarios pueden finalizar sesiones de forma remota, lo que permite cerrar la sesión inmediatamente en otros navegadores, dispositivos o clientes si fuera necesario.

El comportamiento del tiempo de espera de la sesión varía según el tipo de cliente:

Cliente MFP
La sesión de los usuarios se cierra automáticamente tras un periodo de inactividad definido en el dispositivo. Esto evita el acceso no autorizado en entornos de impresoras compartidas o públicas.

Portal web y cliente de escritorio
Cuando la opción **«Mantener la sesión iniciada»** está activada, la sesión permanece activa hasta **30 días**, a menos que se cierre manualmente o se revoque.

Cuando la opción no está habilitada, la sesión de los usuarios se cierra automáticamente tras **3 horas de inactividad**.

Asimismo, las sesiones finalizan de inmediato si un administrador del inquilino desactiva la cuenta de usuario o si el usuario realiza una acción de cierre de sesión remoto.

Estos controles garantizan una seguridad de sesión uniforme en todos los puntos de acceso, al tiempo que equilibran la facilidad de uso y la protección para diversos escenarios de utilización.

8. Autenticación mediante PIN

Efflux Cloud Capture admite la autenticación mediante PIN para iniciar sesión en la MFP, como alternativa al método estándar de introducir credenciales en el panel del dispositivo. La autenticación por PIN se utiliza exclusivamente para acceder a la MFP y no sirve para iniciar sesión en el portal web ni en el cliente de escritorio.

El propietario del inquilino (Tenant Owner) debe habilitar primero la autenticación por PIN. Una vez habilitada, los usuarios pueden generar y gestionar sus propios PIN.

Para la autenticación por PIN se aplican las siguientes reglas:

- Los PIN pueden constar de entre **6 y 10 dígitos numéricos**
- Los PIN tienen una validez de **tres (3) meses** y deben regenerarse una vez caducados
- Los usuarios pueden eliminar su PIN en cualquier momento, lo que deshabilita inmediatamente el inicio de sesión mediante PIN.
- Los propietarios del inquilino (tenant owners) pueden deshabilitar la autenticación por PIN a nivel global o revocar el uso de PIN en cualquier momento.
- Las sesiones de inicio de sesión mediante PIN se configuran con una duración más breve para reducir el riesgo de exposición en dispositivos multifunción (MFP) compartidos.

La autenticación mediante PIN está diseñada para proporcionar un acceso rápido y cómodo a los equipos multifunción, manteniendo al mismo tiempo los controles de seguridad adecuados para entornos de dispositivos compartidos.

9. Integración con Microsoft Entra ID

Efflux Cloud Capture admite la integración con **Microsoft Entra ID** para permitir la gestión centralizada de identidades y el inicio de sesión único (SSO) para los usuarios del inquilino (*tenant*).

Para habilitar esta integración, **el propietario del inquilino debe otorgar primero su consentimiento** para que Efflux Cloud Capture acceda al entorno de Microsoft Entra ID de su organización. Este consentimiento permite a Efflux Cloud Capture interactuar con Entra ID exclusivamente con fines de federación de identidades.

Una vez otorgado el consentimiento, el propietario del inquilino puede **importar usuarios seleccionados** desde Microsoft Entra ID a Efflux Cloud Capture. Cuando un usuario importado pertenece a uno o varios grupos de usuarios en Entra ID, dichos grupos se crean automáticamente en Efflux Cloud Capture y el usuario se asigna a ellos en consecuencia.

Una vez agregados, los usuarios reciben una notificación por correo electrónico y pueden iniciar sesión en Efflux Cloud Capture utilizando la opción de inicio de sesión único **«Sign in with Azure»**.

Efflux Cloud Capture **no accede a las credenciales de Microsoft Entra ID, ni las almacena ni las gestiona**. La autenticación se realiza mediante tokens de identidad seguros emitidos por Microsoft Entra ID. En ningún momento se almacenan contraseñas de usuario ni credenciales de directorio en la plataforma Efflux Cloud Capture.

El propietario del inquilino (Tenant Owner) puede **revocar el consentimiento de Entra ID en cualquier momento**. Una vez revocado el consentimiento, los usuarios ya no podrán autenticarse mediante el inicio de sesión único de Azure.

10. Flujo de autenticación y gestión de tokens

Efflux Cloud Capture utiliza una **arquitectura de autenticación basada en tokens** para gestionar de forma segura las sesiones de usuario.

Cuando los usuarios se autentican mediante credenciales locales, Efflux Cloud Capture emite un **JSON Web Token (JWT)** tras una autenticación correcta. Este token contiene la identidad del usuario y las declaraciones de autorización, y es necesario para las solicitudes posteriores.

Cuando se utiliza la autenticación de Microsoft Entra ID:

- El usuario es redirigido a una página de inicio de sesión controlada por Microsoft.
- La autenticación es realizada íntegramente por Microsoft Entra ID.
- Microsoft Entra ID devuelve un token de identidad a Efflux Cloud Capture.
- Efflux Cloud Capture valida el token recibido..

Se genera y se emite al usuario un token de acceso ECC (JWT) de corta duración.

Efflux Cloud Capture no almacena credenciales de Microsoft Entra ID. Toda la autenticación se realiza mediante tokens de identidad seguros.

Los tokens de acceso se emiten con un **periodo de validez limitado**. Cuando un token de acceso caduca, se utiliza un **mecanismo de renovación** para obtener uno nuevo sin necesidad de que el usuario vuelva a introducir sus credenciales, a menos que la sesión haya sido revocada o haya expirado.

Todos los tokens se validan en cada solicitud. Los tokens caducados o no válidos son rechazados, lo que impide el acceso no autorizado.

Este modelo basado en tokens reduce el riesgo de exposición, limita el uso indebido de la sesión y garantiza una autenticación segura en todos los componentes del sistema..

11. Seguridad de red y aislamiento de servicios

Efflux Cloud Capture se implementa en Microsoft Azure mediante una arquitectura basada en contenedores.

Cada inquilino cuenta con un entorno Kubernetes dedicado, aislado de otros inquilinos a nivel de red y de aplicación.

Dentro del entorno de un inquilino:

- El servicio de **interfaz web (Web UI)** se expone a través de un punto de enlace público seguro para el acceso de los usuarios.
- El **servicio del motor** de procesamiento no es accesible públicamente y solo puede ser contactado internamente por la interfaz web.
- Las bases de datos y el almacenamiento de documentos se despliegan dentro de la red privada del inquilino (tenant) y no están expuestos a redes externas.
- Toda la comunicación entre servicios se realiza a través de **redes internas privadas** y no es accesible desde la internet pública.

Este diseño garantiza que los componentes sensibles, como los servicios de procesamiento de documentos y los sistemas de almacenamiento, permanezcan protegidos frente a accesos externos.

12. Protección de datos y aislamiento de inquilinos

Todos los datos de los clientes procesados por Efflux Cloud Capture se almacenan en el entorno de Azure dedicado del inquilino.

Los documentos, los metadatos y los registros del sistema se conservan en un **almacenamiento aislado para cada inquilino** y no se comparten entre ellos.

El acceso a las bases de datos y al almacenamiento de documentos está restringido a los servicios internos del entorno del inquilino. Ningún sistema o usuario externo puede acceder directamente a los datos almacenados.

Todas las comunicaciones entre servicios se protegen mediante canales cifrados. El acceso a los datos se controla mediante autorización a nivel de aplicación y control de acceso basado en roles.

Esta arquitectura garantiza la confidencialidad, la integridad y el aislamiento de la información del cliente..

13. Registros de actividad y de auditoría

Efflux Cloud Capture ofrece capacidades de registro para facilitar la auditoría, la resolución de problemas y la supervisión operativa.

Están disponibles los siguientes registros::

- **Los registros de trabajos** que documentan las actividades de procesamiento de documentos se conservan durante **30 días**.
- El administrador del inquilino puede habilitar **los registros del motor de procesamiento**. El nivel de registro puede configurarse según los requisitos operativos.
- Los registros de procesamiento se conservan hasta por **un (1) año** y se almacenan de forma segura en el almacenamiento aislado del inquilino..

Solo los administradores de inquilinos autorizados pueden acceder a los registros y descargarlos. Los registros no se comparten entre inquilinos y otras organizaciones no pueden acceder a ellos.

Estos registros proporcionan trazabilidad de la actividad del sistema, al tiempo que mantienen un estricto aislamiento entre inquilinos.

efflux solutions

bps@efflux-solutions.com
efflux-solutions.com

Europe
South Africa
Asia