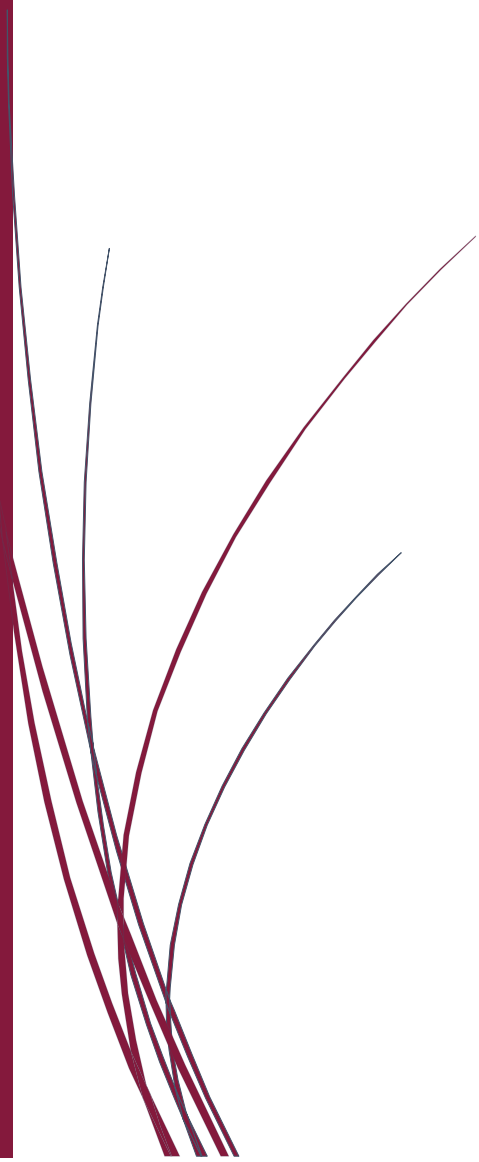
28-4-2023

GRUPO NASA TECNOLOGIA

Anexo de Arquitectura



Ing. Héctor Hernández
DIRECTOR DE OPERACIONES

Confianza, Servicio y Tecnología
Nasa Tecnología SC
T. 8347 77 22
www.nasa.com.mx

Introducción

¿Quién es NASA TECNOLOGÍA?

Grupo NASA es una empresa con más de 20 años de experiencia, ofrece un SERVICIO INTEGRAL de Asesoría en Ingeniería Industrial y de Sistemas, que permite a nuestros Socios-Clientes, cubrir sus necesidades de DESARROLLO DE APLICACIONES y tener acceso a SISTEMAS INTEGRALES listos para utilizarse, que se personalizan de acuerdo con sus necesidades. Somos un conjunto de profesionistas, de diferentes especialidades como Contadores Públicos, Licenciados en Informática, Ingenieros Industriales e Ingenieros en Electrónica que compartimos nuestra experiencia y conocimientos con nuestros Clientes a través de un nuevo concepto denominado "FAMILIA EMPRESARIAL".

CONFIANZA, SERVICIO Y TECNOLOGÍA

La definición de SISTEMAS es el conjunto de elementos que se interrelacionan como HARDWARE, SOFTWARE, COMUNICACIONES, CAPACITACION para lograr un fin común: AUTOMATIZAR LOS PROCESOS DE SU EMPRESA, para que pueda crecer y ganar más dinero.

Nuestra metodología se enfoca a resultados, buscando la eficiencia y productividad de SU EMPRESA, como socios con “ACTITUD DE DUEÑOS” buscamos juntos, mejorar la productividad de la Empresa, a costos accesibles.

En la FAMILIA EMPRESARIAL, usted encuentra CONFIANZA fundamentada en la experiencia de más de 20 años y logros obtenidos con nuestros Socios-Clientes, SERVICIO porque ponemos a su disposición todo el apoyo de nuestro Equipo de Ingenieros y toda la TECNOLOGÍA de vanguardia en sistemas modernos de administración y control computarizados, que amoldamos a sus necesidades.

Contenido

1. Tabla de control de versiones

Fecha	Versión	Descripción	Realizó
23/04/2020	1.0.0.0	Creación de Documento	Ing. Héctor Hernández
15/08/2021	1.0.0.1	Modificaciones y Cambios	Ing. Héctor Hernandez
18/07/2022	2.0.0.0	Actualizaciones y Cambios	Ing. Héctor Hernandez
28/04/2023	2.0.0.1	Actualizaciones y Cambios	Ing. Héctor Hernandez

2. Introducción

El presente documento tiene como propósito detallar los requerimientos técnicos de instalación y configuración enfocados a la plataforma ***CONSOFT,*** en este documento se establecerán los lineamientos mínimos de operación recomendados en base a la experiencia de implementación en distintos ambientes, así como las recomendaciones para entornos con distintas características, seguridad, arquitectura de instalación entre otros tópicos.

Para poder lograr el proceso de instalación y configuración del sistema en el entorno que mejor le convenga acorde con la infraestructura existente, es muy importante contar con el apoyo de su área de sistemas para proporcionar los siguientes requerimientos técnicos.

3. Arquitectura de instalación de la aplicación

En esta sección se definirán las distintas formas de instalación que son permitidas por la aplicación, esta flexibilidad de la plataforma le permite al cliente elegir la que se adecue en gran medida a las condiciones de la infraestructura disponible.

3.1. Opción de Despliegue Multi-Servidor

El siguiente modelo de despliegue es un entorno altamente recomendado para la alta demanda de la plataforma el cual se enfoca en dividir en diferentes capas el despliegue de la aplicación para poder garantizar y soportar el alto volumen, cada una de las diferentes capas serán definidas a continuación.

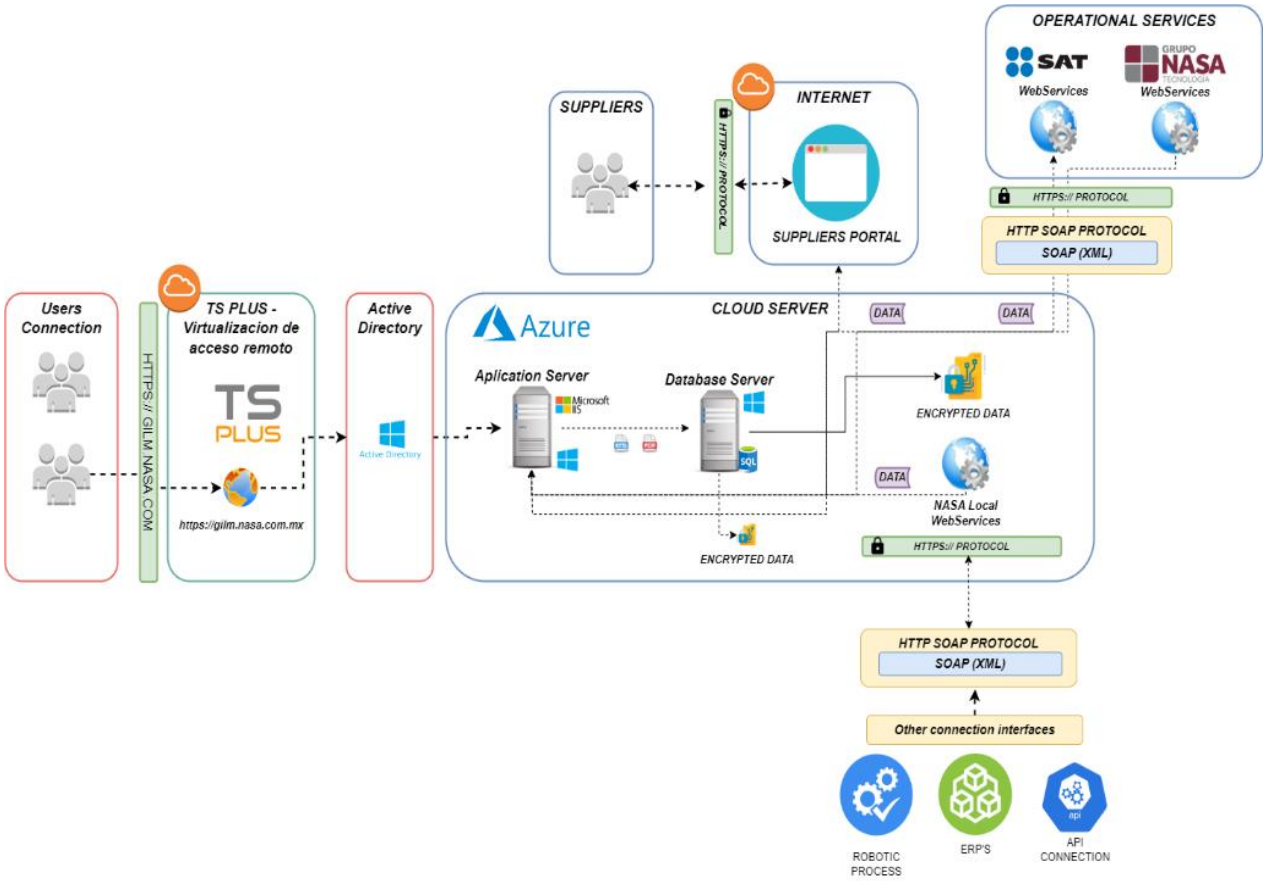


Imagen 1 – Diagrama de despliegue Multiservidor

3.2. Application Server

En este servidor es donde se llevará a cabo la instalación de la aplicación, así como también la configuración de los diferentes robots los cuales nos ayudan a la automatización de procesos. La finalidad de este servidor es albergar la aplicación, procesos automatizados.

3.3. Database Server

Este servidor tiene como objetivo contener exclusivamente la base de datos del sistema y almacenar los xml del cliente, a este servidor solamente es utilizado por la aplicación proveniente del servidor de aplicaciones.

3.4. ERP Server

Este es el servidor donde se encuentra instalado los sistemas administrativos del cliente y se busca que el servidor de aplicaciones tenga acceso a él para la extracción de los XML generados en la operación de la empresa, dichos xml posteriormente almacenados en el servidor de BD.

3.5. Connection Interface

Es el mecanismo mediante el cual los equipos del usuario final podrán conectarse al servidor de aplicación en algunos casos esta conexión se realiza mediante :

3.6. Escritorio Remoto

Esta decisión depende de las circunstancias en las que se encuentre la infraestructura del cliente y es decisión de este definir el mecanismo de conexión al servidor de aplicaciones.

En caso de no contar con licencias o conexiones al servidor para los usuarios finales se recomienda recurrir a una aplicación de un tercero llamada ***TSPLUS*** *la cual les permite emular múltiples licencias para los usuarios finales, así como el acceso mediante el navegador web.*

**** El costo de esta aplicación es totalmente aparte de los acuerdos comerciales con Grupo NASA Tecnología.***

3.7. NASA Local Web Services

Son interfaces de comunicación internas generalmente se utilizan para la comunicación del ERP con la Plataforma y el uso y despliegue de estas interfaces de comunicación depende de así requerirlo desde la etapa de preventa del Software.

3.8. NASA Web Services

La plataforma utiliza algunos de los WebServices que se encuentran en los servidores internos de Grupo NASA, en su mayoría es para temas de licenciamiento, validación y control.

3.9. SAT WebServices

Son los WebServices que ofrece el SAT como via de comunicación para la extracción de información del cliente.

3.10. User Connection

En esta última capa se hace referencia al medio por el cual el usuario final se conecta a nuestra aplicación que para el caso del actual diagrama el usuario desde su equipo local cuenta con un medio de comunicación al servidor de aplicaciones.

Esta arquitectura de distribución y despliegue es recomendada en base a las mejores prácticas técnicas, para de esta forma poder soportar la concurrencia de usuarios , carga operativa del servidor y un correcto balance entre las diferentes capas del diagrama de despliegue, así como para entornos de alto volumen.

4. Permisos y Seguridad

Dentro de la plataforma hay diferentes características de seguridad que deberán ser consideradas durante su instalación esto para permitir que la aplicación se pueda desempeñar de forma correcta dentro de la infraestructura. Debido a que la aplicación es instalada dentro de la infraestructura del cliente o de Azure, adopta y/o hereda los mecanismos externos de seguridad (firewall , Permisivos, dominio, etc..).

4.1. Autenticación de Usuarios

La plataforma cuenta con un mecanismo de autenticación independiente a la infraestructura utilizada por el cliente, dicho lo anterior, el sistema cuenta con el mecanismo de autenticación mediante usuario y password , siendo esta última encriptada por motivos de seguridad, Debido a que es una plataforma cliente servidor maneja su propia metodología de autenticación.

4.1.1. Mecanismo de encriptación

El método de encriptación utilizado por el sistema es AES-256 aplicado en los puntos de información críticos del sistema, los cuales por motivos de privacidad no se redactan en este documento.

Este módulo se refiere a que dentro del esquema de la base de datos ciertos datos sensibles que se manejan dentro de la aplicación están encriptados con el fin de reforzar la seguridad y confidencialidad de nuestro cliente.

Actualmente la información que se encuentra cifrada en posición de reposo en el sistema es la del usuario de la plataforma por motivos de seguridad.

Por otro lado, al utilizar el protocolo https como medio de comunicación entre las plataformas, aseguramos que la información viaja de forma segura a través de la red.

Respecto a los archivos almacenados en los blobs de Azure por la plataforma, pasan por un proceso de modificación de estructura esto por motivos de seguridad.

4.2. Autorización de Usuarios:

La autorización de los usuarios dentro de la plataforma Consoft se rige mediante la definición de ***Grupos, Usuarios y Acciones*** para gestionar la autorización del sistema.

4.3. Auditoria y Logging

- Accesos exitosos y fallidos de los usuarios.
- Creación, modificación y borrado de usuarios.
- Cambio de rol/permisos.
- Cambios en la configuración de la aplicación.

5. Integración con Active Directory.

En esta sección se describirá a fondo como es que se lleva a cabo la integración de la plataforma CONSOFT y Active Directory esto para adoptar las medidas pertinentes de seguridad establecidas por la compañía cliente.

5.1. Inicio de sesión

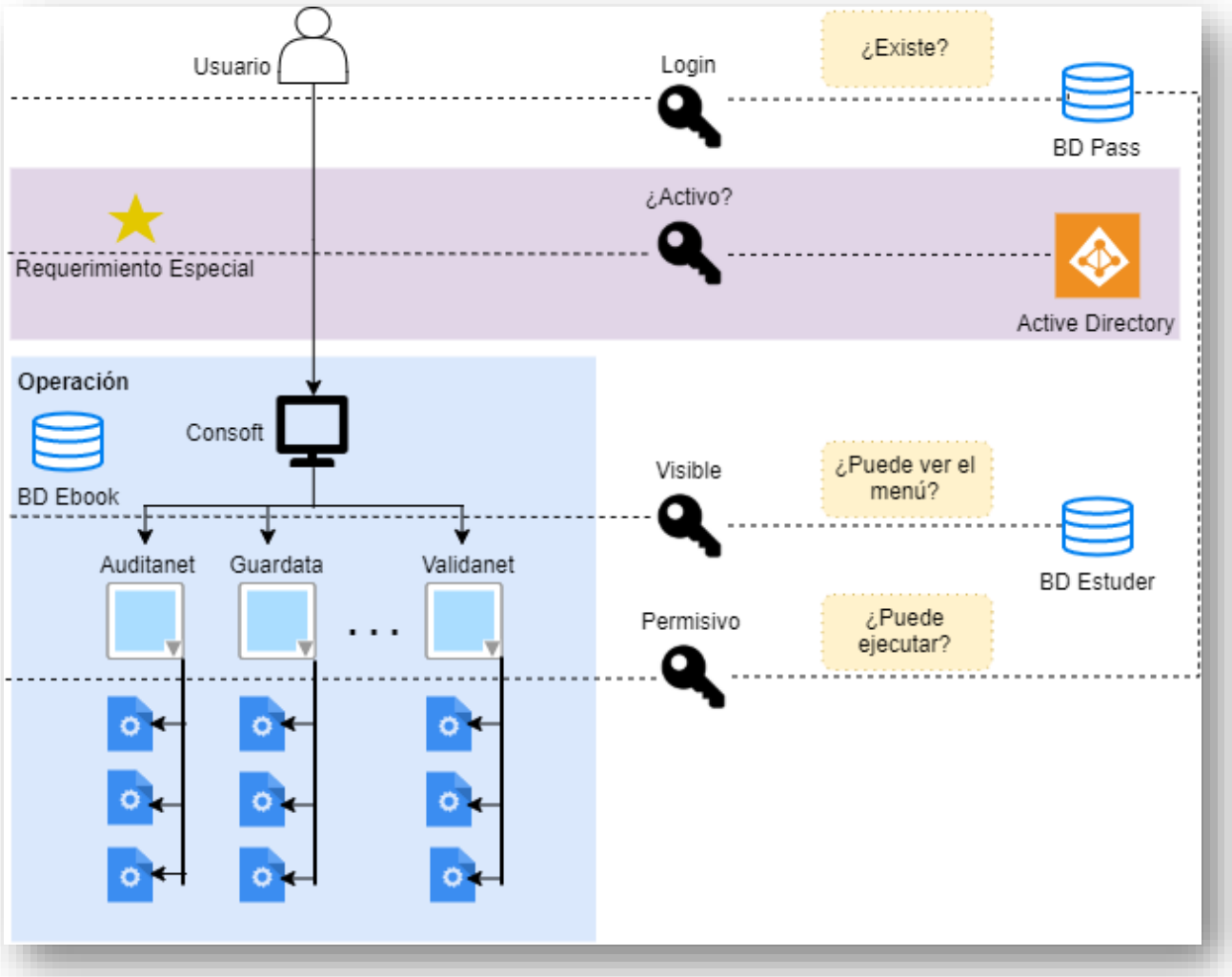
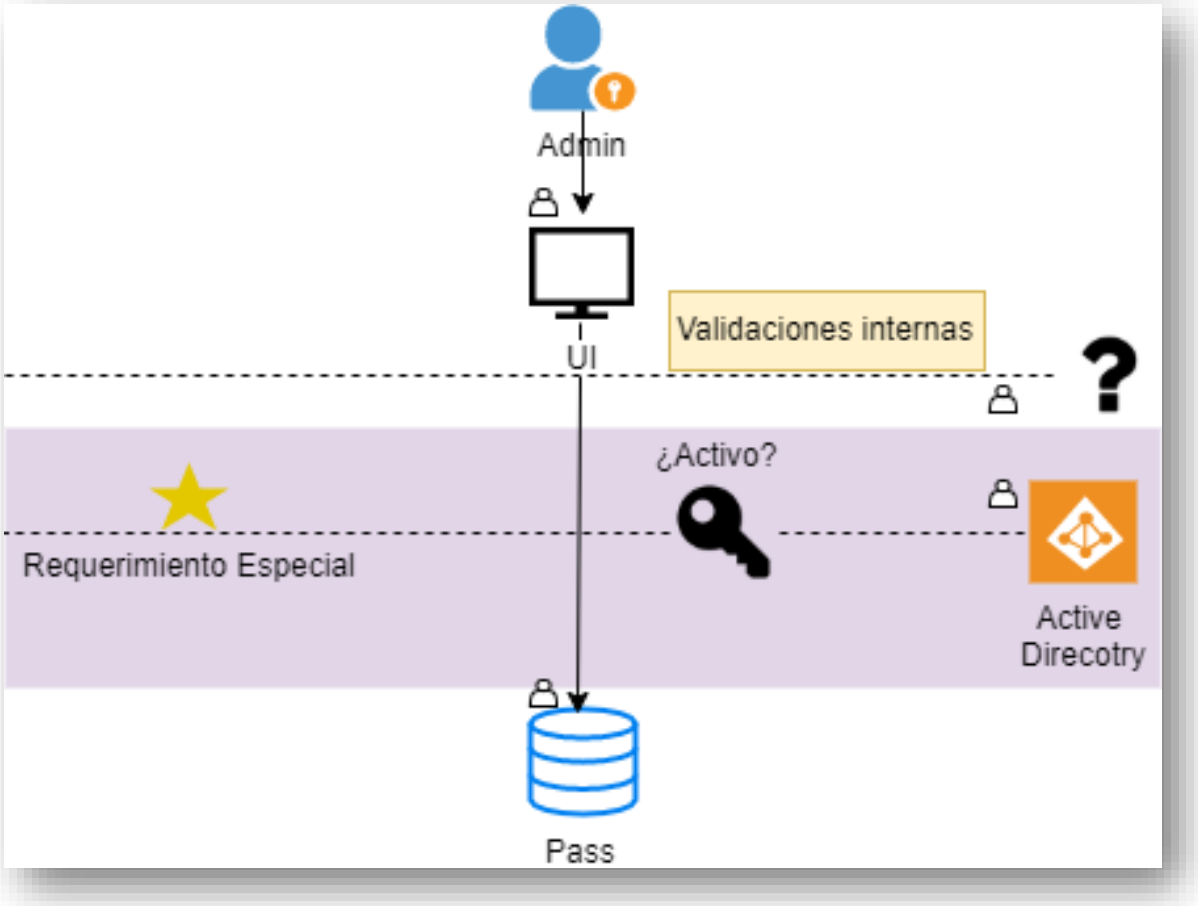


Diagrama 1. Login Active Directory

La conectividad con Active Directory se utiliza con el objetivo de cumplir con el nivel de seguridad requerido, es decir, no pueden loguearse en Consoft sin estar activo en su entorno.

5.2. Alta de Usuarios



El diagrama anterior representa el proceso de alta y asignación de permisivos a los usuarios, es decir para poder dar de alta los usuarios tienen que estar activos en su entorno.

5.2.1. Generales de Seguridad

La plataforma cuenta con distintas características de seguridad y configuración redactadas en este documento a las cuales se le suman las siguientes características generales:

- El código de la aplicación esta ofuscado, con certificados de NASA.
- Los mecanismos de comunicación de nuestros WS utilizan protocolos HTTPS.
- Al usuario fallar mas de 3 veces el usuario se bloquea, enviando un código de desbloqueo.
- Mecanismo de restablecimiento de password a usuarios bloqueados.
- La contraseña utiliza una máscara la cual contempla una serie de reglas a cumplir:
    - Mayúsculas.
    - Minúsculas.
    - Números.
    - Símbolos.
    - Longitud.
- Encripcion de archivos temporales.
- Ofuscación de archivos de configuración.
- Revisión de librerías externas para verificar que todas estén firmadas al momento de compilarse.

5.2.2. Estrategias de Respaldos

Copias de seguridad por día Incrementales durante 30 días. Servicio de APP. En Blob Storage. Las copias de seguridad se almacenan en VaultDb, GRS Global Redundancy.

En caso de ataque, la copia de seguridad que se despliega en el servidor sería la del último día.El tiempo de ejecución de la copia de seguridad sería de al menos un par de horas (2 aprox).

5.2.3. Esquema de Seguridad

- Las conexiones se realizan con una clave y un usuario de servicio de aplicación temporal.
- Las conexiones se realizan a través de VPN.
- Sólo las aplicaciones tenían acceso a los servidores.

- La comunicación es únicamente por Intranet. Entre las aplicaciones o app.
- Antivirus
    - Microsoft Defender for Cloud – Microsoft Defender.
        - Ramsomware
        - Viruses
        - Etc.
- Firewalls
- WAF
- Level security layers
    - User
    - Server
    - By VPN.
- Application security groups.
    - Ports
    - Applications.