INFRAESTRUCTURA TECNOLOGICA Y ESPECIFICACIONES TECNICAS DEL SOFTWARE

Historial de modificaciones

Fecha	Versión	Descripción de la modificación
16/05/2023	1.0	Documento Original
29/09/2023	2.0	- El nombre “Especificaciones 2écnicas de los sistemas de Elthon en la Nube ISO27001, 27017,27018” cambia a Infraestructura tecnológica y Especificaciones Software Elthon. - Se incluye la sección Infraestructura Elthon-Telconet. - El etiquetado de la información cambia a Uso público.
15/02/2024	3.0	- Se incluye Anexos Diagrama de Red. - Se actualiza formato control de documentación. - Se incluye cuadro para evidenciar la creación, revisión y aprobación de documentos.
11/9/2025	4.0	Actualización según norma ISO 27001:2022. Actualización de Logo empresarial y encabezado.
25/9/2025	5.0	-Se incluyen nuevas medidas de seguridad como el 2fa(autenticación dos factores) y cierre de sesión por tiempo inactivo.

Creado por:	Revisado por:	Aprobado por:
Firmado electrónicamente por: GUILLERMO BERNARDO HERRERA MONTERO Validar únicamente con FirmaEC	Firmado electrónicamente por: JACQUELINE PATRICIA GUANOLIQUE TENE Validar únicamente con FirmaEC	Firmado electrónicamente por: ALFREDO PAUL NOBOA GARCIA Validar únicamente con FirmaEC
_____ Ing. Guillermo Herrera Jefe de TI	_____ Eco. Jacqueline Guanolique Jefe de Gestión Calidad (e)	_____ Eco. Paúl Noboa Administrador

TABLA DE CONTENIDO

1. OBJETIVO

Describir la arquitectura, infraestructura y demás especificaciones técnicas del sistema de gestión de riesgos de ELTHON CEO en la nube con AZURE, incluyendo los componentes principales, la infraestructura de red, los servicios en la nube utilizados, su integración y la gestión de datos, así como las medidas de seguridad implementadas en el diseño de la arquitectura, gestión de identidades, accesos, cifrado de datos, la monitorización y gestión de amenazas, la recuperación de desastres.

2. ALCANCE

Se proporcionarán descripciones detalladas de los componentes principales de la arquitectura, infraestructura, especificaciones técnicas y cómo interactúan entre sí para lograr la escalabilidad, mantenibilidad y seguridad del sistema. Además, se incluirá una descripción para los diferentes componentes, con el fin de brindar una comprensión clara de cómo se optimiza y personaliza para satisfacer las necesidades del sistema de gestión de riesgos de ELTHON CEO en la nube con AZURE.

El alcance del documento no incluirá detalles técnicos de implementación ni detalles de configuración de los componentes.

3. NORMATIVA

- Norma ISO 9001:2015
- Norma ISO 27001:2022
- Norma ISO 22301:2019
- Norma ISO 31000:2018
- Normas ISO 27017:2021
- Norma ISO 27018:2019
- Norma ISO 27701:2019

4. DEFINICIONES Y SIGLAS

- **Microsoft AZURE**: Es una plataforma en la nube de servicios de cómputo que ofrece una amplia gama de servicios de infraestructura, plataforma y software como servicio para la creación, implementación y administración de aplicaciones y servicios en la nube.
- **Stack Tecnológico:** La combinación de tecnologías y herramientas utilizadas en un proyecto de software.
- **Web Apps:** son aplicaciones web que se ejecutan en servidores remotos y se acceden a través de un navegador web. En este caso, se utilizan Web Apps de AZURE para implementar y alojar los sitios web de ELTHON.

- **Microservicios:** son una arquitectura de software que descompone una aplicación en pequeñas partes autónomas e independientes que se comunican entre sí mediante una API.
- **API:** siglas en inglés de "Application Programming Interface" o interfaz de programación de aplicaciones. Es un conjunto de reglas, protocolos y herramientas para construir software y aplicaciones que permiten la comunicación y la integración entre diferentes sistemas.
- **Arquitectura de sistemas:** es el proceso de diseñar y planificar la estructura de los sistemas de información, incluyendo hardware, software, redes, procesos y procedimientos.
- **Infraestructura de sistemas:** se refiere a los componentes físicos y virtuales de una red de computadoras, incluyendo servidores, almacenamiento, redes, software de sistemas operativos, middleware y aplicaciones.
- **CDN:** siglas de "Red de Distribución de Contenido" (Content Delivery Network en inglés), es una red de servidores distribuidos geográficamente que se utilizan para acelerar la entrega de contenido web.
- **CDM:** significa Common Data Model (Modelo de Datos Común). Es un conjunto de estándares de datos y vocabulario compartido que se utiliza para permitir la interoperabilidad de datos en aplicaciones y servicios de AZURE.
- **Script SQL:** es un conjunto de instrucciones que se utilizan para interactuar con bases de datos relacionales. Estas instrucciones se utilizan para crear, modificar o eliminar tablas, índices, procedimientos almacenados, entre otros elementos de la base de datos.
- **Query:** es una solicitud de información que se realiza a una base de datos. Una consulta SQL es un ejemplo de una query que se utiliza para recuperar información específica de una base de datos.

5. STACK TECNOLÓGICO

ELTHON CEO utiliza varias tecnologías para desarrollar su arquitectura las cuales se describen a continuación.

- **Spring Boot con Gradle:** framework para la creación de aplicaciones en Java.
- **Java 11:** versión del lenguaje de programación Java.
- **Artefactos con Maven:** herramienta de construcción de proyectos para Java.
- **Angular:** framework para la creación de aplicaciones web.
- **Node.js 16 para Angular:** entorno de tiempo de ejecución para JavaScript que se utiliza para construir aplicaciones web en Angular.
- **Flutter:** framework para la creación de aplicaciones móviles para iOS y Android.
- **AZURE Blobs Storage:** servicio de almacenamiento en la nube que permite almacenar grandes cantidades de datos no estructurados, como imágenes, videos y archivos.

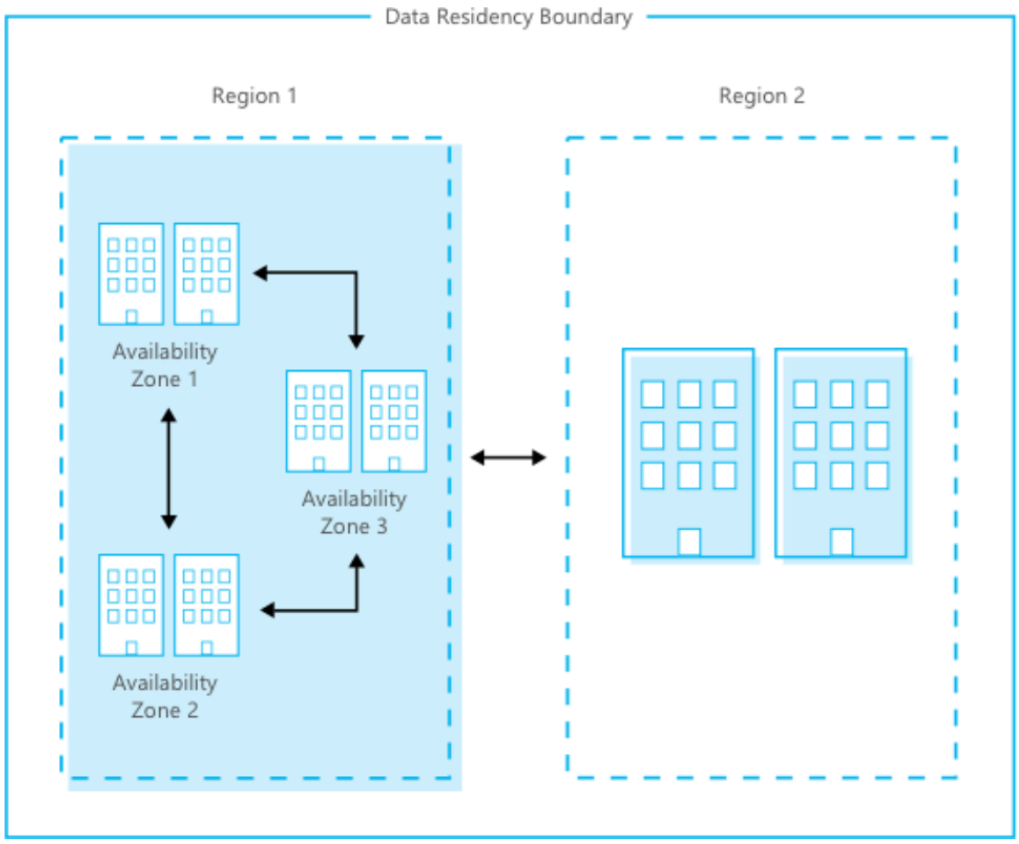
- **Arquitectura basada en microservicios:** en esta arquitectura, una aplicación se divide en pequeños servicios independientes que trabajan juntos para proporcionar la funcionalidad completa de la aplicación.
- **REDIS Cache:** para la gestión de sesiones y cacheo de datos.
- **AZURE Monitor:** para la supervisión y análisis de aplicaciones en tiempo real.
- **AZURE SQL Database y MongoDB Atlas:** como bases de datos como servicio en la nube.

6. INFRAESTRUCTURA ELTHON

6.1. INFRAESTRUCTURA AZURE

Microsoft AZURE opera en instalaciones de centros de datos gestionados y dirigidos por Microsoft. Estos centros de datos, distribuidos geográficamente, cumplen con los estándares de seguridad y confiabilidad de la industria, incluyendo ISO/IEC 27001:2013 y NIST SP 800-53. La gestión y supervisión de estos centros de datos recae en el equipo de operaciones altamente experimentado de Microsoft, que cuenta con un historial de éxito en la prestación de servicios en línea de gran envergadura, garantizando operatividad continua las 24 horas del día, los 7 días de la semana.

La infraestructura de centros de datos de AZURE se extiende a nivel global, abarcando más de un centenar de instalaciones altamente seguras que respaldan una amplia gama de servicios en línea. Su diseño se centra en acercar aplicaciones a usuarios de todo el mundo, garantizar la integridad de los datos y ofrecer soluciones integrales de cumplimiento y resiliencia. Con más de 60 regiones estratégicamente ubicadas en todo el mundo y disponibilidad en más de 140 países o regiones, AZURE se posiciona como un líder en flexibilidad para la implementación de aplicaciones según las necesidades del cliente.



- **Distribución global:** AZURE cuenta con una infraestructura de centros de datos distribuida globalmente con más de 100 instalaciones en todo el mundo. Esto permite

acercar las aplicaciones a los usuarios y brindar opciones integrales de cumplimiento y resiliencia.

- **Regiones y geografías:** AZURE se organiza en regiones, que son conjuntos de centros de datos interconectados. Las geografías garantizan el cumplimiento de requisitos de residencia, soberanía y seguridad de datos dentro de límites geográficos.
- **Zonas de disponibilidad:** Dentro de una región, AZURE ofrece zonas de disponibilidad, que son ubicaciones físicamente independientes con alimentación, refrigeración y redes independientes. Esto permite ejecutar aplicaciones de alta disponibilidad y baja latencia.
- **Seguridad física:** Microsoft implementa una serie de capas de seguridad física en sus centros de datos para controlar el acceso no autorizado. Esto incluye aprobación de acceso, acceso de visitantes, seguridad en el perímetro, entrada del edificio y seguridad en la planta del centro de datos.
- **Eliminación de equipos:** Se siguen procedimientos rigurosos para la eliminación segura de equipos al final de su vida útil, incluyendo el borrado seguro de discos duros y la destrucción de unidades que no se pueden borrar.
- **Conformidad:** AZURE cumple con una amplia variedad de estándares de cumplimiento internacionales y específicos del sector, lo que incluye ISO 27001, HIPAA, FedRAMP, SOC 1 y SOC 2, entre otros. Se realizan auditorías de terceros para verificar el cumplimiento de estos estándares.

Ver el Anexo 1 Diagrama arquitectura general ELTHON CEO - AZURE

6.1.1. COMPONENTES Y LÍMITES DEL SISTEMA DE INFORMACIÓN DE AZURE

6.1.1.1. REDES EN AZURE

Red de Producción de Microsoft AZURE (Red de AZURE)

AZURE cuenta con dos redes esenciales en su entorno: la Red de Producción de Microsoft AZURE, también conocida como Red de AZURE, y la Red Corporativa de Microsoft (CORPNET). Cada una de estas redes es gestionada por equipos de TI diferentes, encargados de operaciones y mantenimiento respectivos.

Arquitectura de AZURE

AZURE se basa en una plataforma de informática en la nube, respaldada por una red de centros de datos administrados por Microsoft. Estos centros de datos están diseñados para alojar aplicaciones y servicios, siendo responsabilidad exclusiva de Microsoft su operación y mantenimiento.

Funcionamiento de las Máquinas Virtuales (VM) en AZURE

En AZURE, las máquinas virtuales (VM) se crean según los recursos necesarios y se ejecutan en su propio entorno de nube. Cada nodo físico en AZURE está equipado con un hipervisor que administra varias máquinas virtuales invitadas. Además, se implementa un firewall de Windows en cada máquina virtual para controlar el tráfico.

6.1.1.2. ADMINISTRACIÓN EN AZURE

Controladores de Tejido

Las máquinas virtuales en AZURE se agrupan en clústeres de alrededor de 1000 unidades, y su gestión es independiente gracias a los controladores de tejido. Estos controladores administran aplicaciones, supervisan hardware y realizan tareas autónomas, como la reencarnación de instancias de VM en servidores en buen estado tras un fallo.

Inventario de Hardware

Para asegurar un control efectivo, se realiza un inventario de hardware y dispositivos de red de AZURE durante el proceso de configuración de arranque. Cualquier nuevo hardware debe seguir este proceso antes de ser admitido en el entorno de producción de AZURE.

Imágenes del Sistema Operativo Administradas por Controladores de Tejido

Las imágenes del sistema operativo en AZURE se dividen en tres tipos: imágenes de host, imágenes nativas e imágenes de invitados, diseñadas específicamente para la nube y no accesibles públicamente. Estas imágenes son gestionadas por los controladores de tejido.

6.1.1.3. ASPECTOS DE SEGURIDAD

Autenticación y Comunicación

La autenticación y comunicación dentro de AZURE se aseguran mediante cifrado TLS y certificados X.509. Estos certificados son autofirmados en la mayoría de los casos, salvo excepciones para conexiones externas a la red de AZURE. Además, se utilizan certificados emitidos por una autoridad de certificación (CA) respaldada por una CA raíz de confianza en los controladores de tejido (FC).

Autenticación de Dispositivos de Hardware

Los controladores de tejido gestionan credenciales utilizadas para autenticar dispositivos de hardware bajo su control. Se utiliza un sistema de cifrado basado en la clave pública de identidad maestra del FC para mantener estas credenciales seguras y protegidas.

6.1.1.4. INFRAESTRUCTURA Y GESTIÓN DE SERVICIOS

Infraestructura Física y Gestión de Centros de Datos

El equipo de Microsoft Cloud Infrastructure and Operations (MCIO) es responsable de gestionar la infraestructura física y las instalaciones de los centros de datos de AZURE. Esto incluye controles físicos y ambientales, así como la administración de dispositivos de red perimetral exterior. Los clientes no tienen acceso directo a esta infraestructura.

Gestión de Servicios y Equipos de Servicio

La gestión de servicios en AZURE se lleva a cabo a través de equipos de servicio especializados, cada uno responsable de un área de soporte técnico específica. Estos equipos deben proporcionar soporte continuo para investigar y resolver problemas de servicio. Sin embargo, los equipos de servicio no tienen acceso físico al hardware de AZURE.

6.1.1.5. TOPOLOGÍA DE RED

Red perimetral:

- Punto de demarcación entre la red de Microsoft y otras redes (Internet, red empresarial)
- Proporciona conexión de conexión de Internet y ExpressRoute en AZURE

Red de área amplia

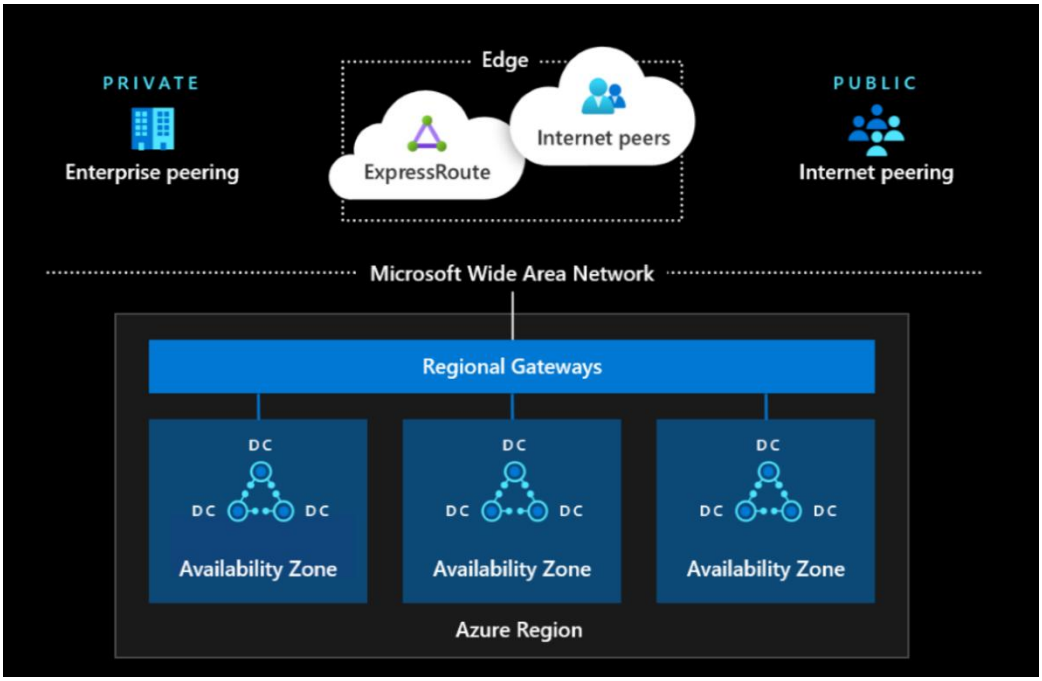
- Red troncal inteligente de Microsoft que cubre el mundo
- Proporciona conectividad entre regiones de AZURE

Pasarela regional

- Punto de agregación para todos los centros de datos de una región de AZURE
- Proporciona conectividad masiva entre centros de datos dentro de una región de AZURE (varios cientos de terabits por centro de datos)

Red de centros de datos

- Proporciona conectividad entre servidores dentro del centro de datos con poco ancho de banda sobresuscrito



6.1.1.6. ENRUTAMIENTO DE INTERNET Y TOLERANCIA A FALLOS

En AZURE, se implementa una infraestructura de Servicio de Nombres de Dominio (DNS) tanto interna como externa, respaldada por una redundancia global. Esta infraestructura incorpora múltiples clústeres de servidores DNS primarios y secundarios para asegurar la tolerancia a fallos. Además, se emplean medidas adicionales de seguridad de red de AZURE, como NetScaler, para mitigar los ataques de denegación de servicio distribuido (DDoS) y proteger la integridad de los servicios DNS en AZURE.

Los servidores DNS de AZURE se distribuyen en diversas instalaciones de centros de datos. La configuración de DNS de AZURE incluye una jerarquía de servidores DNS secundarios y primarios para resolver nombres de dominio públicos de los clientes de AZURE. Estos nombres de dominio generalmente se resuelven en direcciones CloudApp.net, que encierran la Dirección IP Virtual (VIP) correspondiente al servicio del cliente. La VIP específica para la Dirección IP Dedicada Interna (DIP) de la traducción del inquilino es gestionada por los equilibradores de carga de Microsoft, que son responsables de dicha VIP.

AZURE opera en centros de datos distribuidos geográficamente en los Estados Unidos y se basa en tecnología de enrutamiento de vanguardia que cumple con sólidos estándares arquitectónicos escalables. Algunas de sus características destacadas incluyen:

- Ingeniería de tráfico basada en Multiprotocol Label Switching (MPLS) para un uso eficiente del ancho de banda y una degradación elegante del servicio en caso de interrupciones.

- Implementación de redes con arquitecturas de redundancia "need plus one" (N+1) o superiores.
- Conectividad externa a través de circuitos de red dedicados de alto ancho de banda que conectan las propiedades de AZURE con más de 1,200 proveedores de servicios de Internet en todo el mundo en múltiples puntos de interconexión, proporcionando una capacidad perimetral de más de 2,000 gigabytes por segundo (GBps).
- Al poseer sus propios circuitos de red entre centros de datos, Microsoft garantiza una disponibilidad de red superior al 99.9% sin depender de proveedores de servicios de Internet externos.

Para mayor referencias, ver Anexo 2 Diagrama Arquitectura Crítica de Red Azure, Anexo 3 Diagrama Topología de red en estrella tipo HUB – AND – SPOKE en Azure, Anexo 4 Diagrama Azure Front Door y Anexo 5 Diagrama Topología Tradicional de Redes de Azure.

6.1.2. CONEXIÓN A LA RED DE PRODUCCIÓN Y FIREWALLS ASOCIADOS

La directiva de flujo de tráfico de Internet de la red de AZURE canaliza el tráfico hacia el centro de datos de producción más cercano en los Estados Unidos. Los centros de datos de producción de AZURE mantienen una arquitectura y hardware coherentes en todos los centros de datos, lo que permite aplicar la descripción del flujo de tráfico de manera uniforme.

Luego de dirigir el tráfico de Internet hacia AZURE, se establece una conexión con los enrutadores de acceso, que sirven para aislar el tráfico entre los nodos de AZURE y las máquinas virtuales creadas por los clientes. Los dispositivos de infraestructura de red en ubicaciones de acceso y borde son los puntos donde se aplican filtros de entrada y salida mediante listas de control de acceso (ACL) por niveles. Estas ACL filtran el tráfico no deseado y aplican límites de velocidad de tráfico según sea necesario.

Los dispositivos de equilibrio de carga externos, ubicados detrás de los enrutadores de acceso, realizan la traducción de direcciones de red (NAT) de direcciones IP enrutables de Internet a direcciones IP internas de AZURE. Además, enrutan paquetes a las direcciones IP internas de producción válidas y actúan como una capa de protección para limitar la exposición del espacio de direcciones de la red de producción interna.

A diferencia de la arquitectura tradicional de seguridad, en AZURE no se emplean firewalls de hardware dedicados ni dispositivos especializados de detección o prevención de intrusiones en la red de AZURE. En su lugar, las funciones de seguridad están integradas en el software que ejecuta AZURE, proporcionando una sólida seguridad en varias capas, incluyendo funcionalidades de firewall.

Características Clave de Seguridad y Firewall

AZURE implementa características sólidas de seguridad y firewall en diferentes niveles para garantizar la seguridad en el perímetro principal de autorización de seguridad. Algunos aspectos importantes incluyen:

- Firewalls basados en host, incluyendo un firewall de hipervisor, firewall de host nativo y firewall de host en las máquinas virtuales del cliente.
- Componentes de infraestructura con direcciones IP de DIP asignadas que no pueden ser alcanzados por atacantes en Internet.
- Firewalls que solo aceptan paquetes de un conjunto limitado de direcciones IP de origen, proporcionando una defensa en profundidad contra ataques DDoS.
- Uso predeterminado de HTTPS para el tráfico a los navegadores web de los clientes, asegurando un túnel seguro mediante TLS v1.2.
- Reglas de firewall en enrutadores de acceso y núcleo para garantizar la consistencia con el tráfico esperado.

6.2. INFRAESTRUCTURA E OPEN SOLUTIONS

E-Open Solutions Cia. Ltda. tiene 15 años en el mercado ecuatoriano provee:

- SERVICIO GESTIONADO DE TI: Plan anual de soporte técnico corporativo pyme, proyectos de TI , gestión y monitoreo infraestructura, mesa de ayuda help desk con atención remota y en sitio, mantenimiento preventivo y correctivo infraestructura it, gestión equipamiento, capacitación personal.
- SOLUCIONES DE USUARIO FINAL: Gestión dispositivos, virtualización, equipamiento informático.
- SOLUCIONES DE CONECTIVIDAD Y COLABORACIÓN: Diseño soluciones redes cableadas e inalámbricas, telefonía ip, comunicaciones unificadas, seguridad IP.
- INFRAESTRUCTURA DE CENTROS DE DATOS
- SEGURIDAD DE LA INFORMACIÓN: Seguridad perimetral, seguridad de la información, gestión riesgos seguridad, seguridad endpoint, seguridad nube , consultoría seguridad informática, continuidad de negocio, capacitación.
- SOLUCIONES DE INFRAESTRUCTURA: Hardware tradicional, almacenamiento, renta equipamiento e impresoras, virtualización aplicaciones, respaldo/contingencia/continuidad negocio, soluciones cloud hibridas, privadas y públicas.
- SOLUCIONES DE SOFTWARE, LICENCIAMIENTO: Microsoft, Adobe, Symantec , Comunicación , consultoría de servicios de infraestructura, gestión identidad, gestión de bases de datos, cloud.
- SOLUCIONES OFFICE 365: Licenciamiento, Diseño, implementación, migración de datos, capacitación, soporte

- MICROSOFT AZURE: Diseño soluciones híbridas, migración de centros de datos a la nube, implementación de proyectos en nube privada, pública e híbrida.

6.2.1. SOLUTIONS PARTNER DESIGNATION

Este proveedor es un socio de soluciones de Microsoft en las siguientes áreas: Trabajo moderno. El partner de negocios elige estos elementos, que Microsoft no debe considerar confirmación de aprobación.

Servicios
- Consultoría
- Hardware
- Implementación o migración
- Licencias
- Servicios administrados (MSP)

Focus areas
- Backup & Disaster Recovery
- Big Data
- Chatbot
- Cloud Database Migration
- Cloud Migration
- Data Warehouse
- Database on Linux
- Dynamics 365 for Customer Service
- Dynamics 365 for Sales
- Dynamics on Azure
- Information Management
- Mobile Applications
- MySQL/Postgres Migration to Azure
- Seguridad
- Threat Protection

Sectores
- Administración Pública
- Distribución
- Medios de comunicación y comunicaciones
- Productos de venta directa y consumidor
- Professional Services
- Public Safety & National Security
- Recursos y fabricación
- Salud
- Servicios financieros
- Transportation

Productos
- Azure
- Dynamics 365
- Dynamics 365 Enterprise
- Enterprise Mobility & Security
- Equipos
- Microsoft 365
- Office 365
- Power BI
- SQL
- SharePoint
- Skype for Business
- Windows
- Yammer

6.3. INFRAESTRUCTURA ELTHON - TELCONET

En esta sección, se describe el núcleo de la infraestructura física de TELCONET, un lugar donde se fusiona la excelencia tecnológica y la protección inquebrantable. Aquí, se muestra información sobre la infraestructura proporcionados por TELCONET, los cuales resguardan y optimizan los servidores que ELTHON adquiridos como el corazón de su operación tecnológica. Desde la certificación TIER 3 hasta las políticas de seguridad rigurosas, definirá como TELCONET se convierte en el guardián confiable que respalda los requerimientos tecnológicos de ELTHON.

6.3.1. INFORMACIÓN TÉCNICA DEL DATACENTER (QUITO)

GENERAL	GUAYAQUIL – TIER IV TCC I	QUITO – TIER III TCC II
Tipo de edificio	Independiente (400 RACKS)	Independiente (360 RACKS)
Personal	24x7x365	24x7x365
Caminos de distribución	2 activos	1 activo / 1 pasivo
Redundancia	2N (Tolerante a Fallas)	N+1 (mantenimiento concurrente)
Climatización	Ininterrumpida	1 activo / 1 pasivo
Puntos únicos de fallo	Ninguno	Ninguno
Disponibilidad	99,995%	99,982%
Conexión entre DC´s	2 Lambdas (20Gbps) REDUNDANTE	2 Lambdas (20Gbps) REDUNDANTE

ARQUITECTÓNICA	GUAYAQUIL – TIER IV TCC I	QUITO – TIER III TCC II
Suelo técnico (reforzado, antiestático, antideslizante, antielástico)	2500 m² - Construcción	2400 m² - Construcción
Separación de clientes	1000 m² - Área Útil	900 m² - Área Útil
Servidores	400 racks de capacidad	360 racks de capacidad
Otros espacios	Jaula dedicada, rack dedicado, rack compartido, Servidores Físicos y Virtuales, Espacio para oficinas, aparcamiento, zona de descarga, almacén	

AMBIENTE	GUAYAQUIL – TIER IV TCC I	QUITO – TIER III TCC II
Parámetros de control ambiental	2500 m² - Construcción	2400 m² - Construcción
Refrigeración de salas	1000 m² - Área Útil	900 m² - Área Útil
Temperatura controlada de 20°C+/-1°C y humedad relativa del 50% (+/- 5%)	400 racks de capacidad	360 racks de capacidad

SEGURIDAD	GUAYAQUIL – TIER IV TCC I	QUITO – TIER III TCC II
Control de incendios	Sistema de detección constituido por detectores iónicos de humos y gases de combustión	
	Zonas de detección controladas por central analógica micro procesada modular con la plena autonomía de señalización, centralización de fuego y avería. Agente extintor ECARO - 25	
Seguridad con personal	Equipo de seguridad 24x7x365	
Circuito cerrado de televisión	Total cobertura de zonas externas e internas	
Control de accesos	Control de acceso biométricos con lectores de tarjetas de proximidad	
Grabación digital de imágenes	Registro de accesos a los Datacenters	

6.3.2. DESCRIPCIÓN SERVICIO CLOUD HOUSING

Alojamiento Seguro: Condiciones necesarias para alojar los servidores que son propiedad del cliente y están bajo su administración.

Disponibilidad Certificada: Disponibilidad respaldada por certificaciones del UPTIME INSTITUTE, con un 99.995% de disponibilidad en TIER IV y un 99.985% en TIER III en infraestructura, comunicaciones, energía y climatización.

Monitoreo de Infraestructura: Monitoreo constante de la infraestructura para asegurar su rendimiento óptimo.

Espacio Adicional en Pool de Recursos: Flexibilidad para ampliar sus recursos según sus necesidades cambiantes.

Manos Remotas Lógicas y Físicas: Acceso a soporte remoto para resolver problemas lógicos y físicos.

Soporte Técnico Especializado: Equipo de soporte técnico altamente especializado está disponible las 24 horas, los 7 días de la semana, los 365 días del año

.

6.3.3. ALCANCE

TELCONET se compromete a proporcionar a ELTHON una amplia gama de servicios de alojamiento y gestión segura en sus DATACENTER de propiedad. Estos servicios se llevarán a cabo de acuerdo con los términos y condiciones establecidos en el contrato, que incluye el pago de valores recurrentes mensuales por parte de ELTHON. El alcance de servicio abarca los siguientes aspectos:

- **Alojamiento Seguro de Equipos:** TELCONET albergará y administrará los equipos especificados en el anexo técnico presentado por ELTHON.
- **Condiciones Físicas Optimal:** TELCONET proporcionará un entorno físico que cumple con todas las condiciones necesarias, incluyendo climatización, energía eléctrica regulada y medidas de seguridad adecuadas.

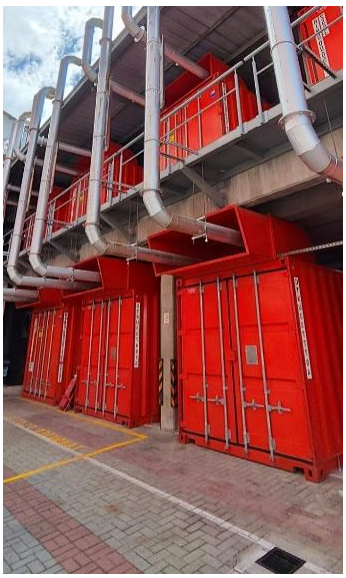


Figura: TELCONET UPS (Sistema de Alimentación Ininterrumpida)

- **Informes de Disponibilidad:** A solicitud de ELTHON, TELCONET proporcionará informes detallados sobre la disponibilidad del servicio, incluyendo incidentes reportados.
- **Estándares de Disponibilidad:** TELCONET garantiza niveles de disponibilidad que cumplen con los estándares del Uptime Institute Inc., con un 99.98% anual para el Datacenter en Quito.
- **Servicios Incluidos:** El alcance abarca servicios disponibles en el Datacenter, como sistemas de conectividad de datos, cuartos de cross conexión, energía eléctrica, climatización, detección y extinción de incendios, suelo técnico y seguridad física.
- **Exclusiones:** Se excluyen los tiempos causados por fallas técnico-operativas responsabilidad del cliente, cableado LAN y SAN, interrupciones autorizadas por mantenimientos programados o fuerza mayor.
- **Mantenimientos Informados:** TELCONET informará oportunamente a ELTHON sobre los mantenimientos programados en el Datacenter.
- **Manos Remotas:** Se ofrecen servicios de manos remotas para la atención de equipos en el Datacenter, sujeto a la entrega de un manual o procedimiento por parte de ELTHON.
- **Soporte y Mejora Continua:** TELCONET establecerá procesos internos de soporte, ofreciendo recomendaciones y notificaciones de oportunidades de mejora para los equipos de ELTHON.
- **Registro de Seguridad:** TELCONET mantendrá registros del sistema de video seguridad durante un período de hasta 90 días para fines de auditoría.

6.3.4. DIAGRAMA DE LA INFRAESTRUCTURA ELTHON / TELCONET

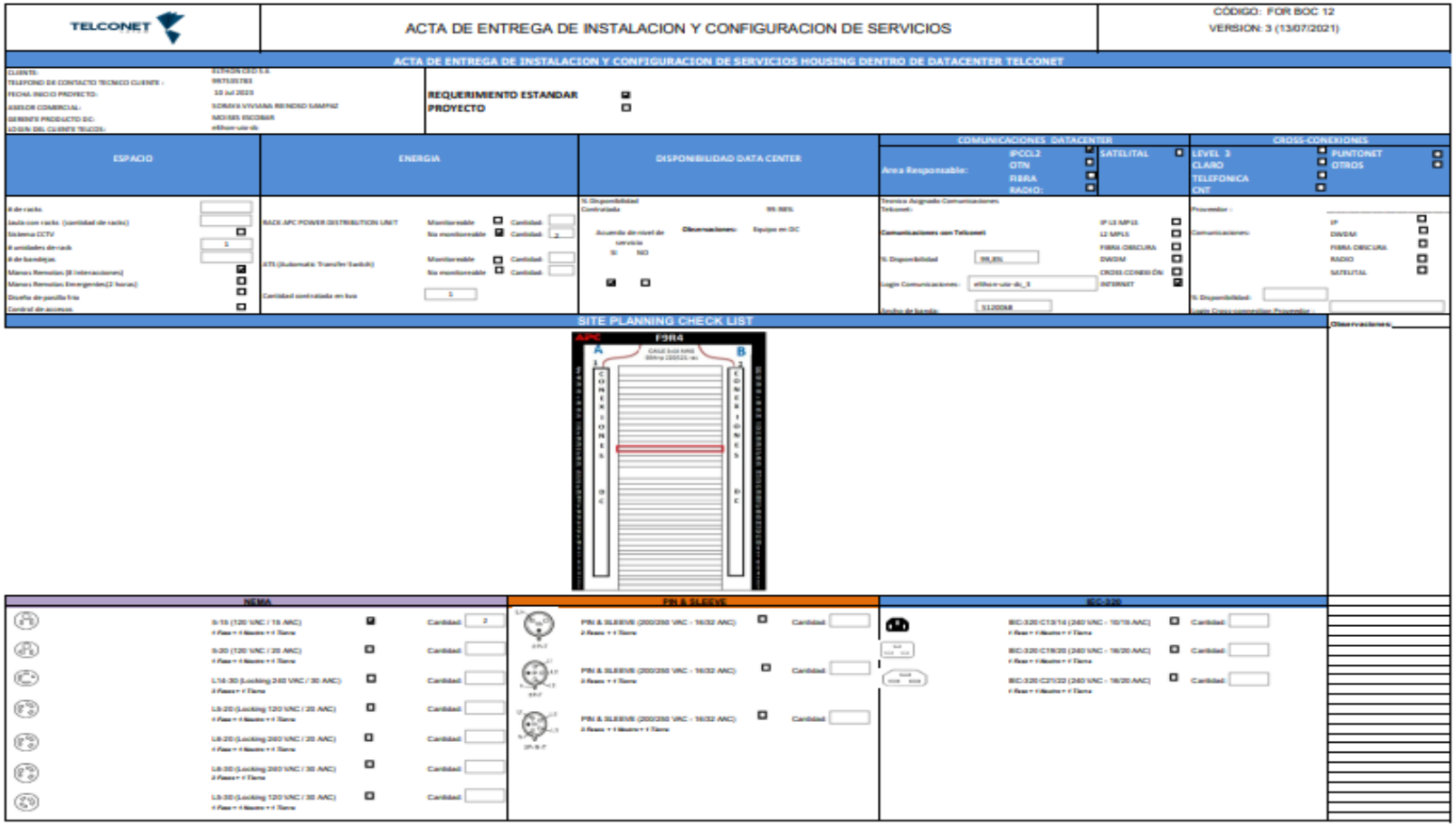
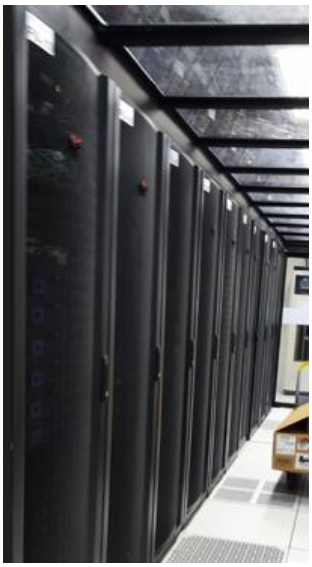


Diagrama ELTHON - TELCONET



TELCONET Espacio para servidor ELTHON

6.3.5. POLÍTICAS DE INGRESO A LAS INSTALACIONES FÍSICAS TELCONET

- **Ingreso Autorizado**

Toda persona que desee ingresar al Datacenter debe solicitar un permiso de acceso previo, que incluye información detallada como nombre, empresa, cédula de identidad, fecha y hora de ingreso, fecha y hora de salida, persona responsable, lugar de trabajo, detalle de trabajo y si ingresa o retira equipamiento.

- **Aprobación Requerida**

El ingreso solo se permite después de que el Centro de Operación de Negocios (BOC) apruebe el permiso de acceso. Ningún visitante puede acceder sin autorización previa.

- **Control Riguroso**

El personal de seguridad externo no permite el acceso a ninguna área sin confirmar la autorización con el BOC o el personal de recepción, excepto en casos de emergencia.

- **Acceso Restringido**

El uso de equipos inalámbricos, antenas, cámaras y teléfonos está prohibido en el cuarto de TI, a menos que se obtenga autorización por escrito del cliente.

- **Registro Obligatorio**

Todos deben registrarse al ingresar con identificación o pasaporte. El personal que ingrese con mochilas o equipos electrónicos debe someterse a una revisión y registrar cualquier equipo.

- **Acompañamiento Obligatorio**

El personal externo debe estar acompañado por personal de Datacenter en las instalaciones del área blanca para garantizar que el trabajo se realice sólo en áreas autorizadas.

- **Limitación de Personas**

Se permite el acceso de un cliente y un máximo de 3 personas por rack, hasta 6 personas en una jaula y hasta 10 personas en migraciones de centros de cómputo.

- **Control de Acceso**

El acceso se limita a las áreas específicas asignadas al cliente y se controla mediante tarjetas de acceso y supervisión del personal.

- **Prohibición de Acceso a Áreas Restringidas**

El personal externo no tiene acceso a áreas de administración exclusiva del Datacenter.

- **Protocolo de Emergencia**

En caso de emergencia, se emite una lista de personal autorizado y se valida la identidad antes de permitir el acceso.

- **Normas de Seguridad**

No se deben bloquear áreas comunes ni usarlas para almacenamiento. Los baños deben utilizarse solo para su propósito. No se permiten perforaciones en las paredes ni el uso de aspiradoras o taladros sin autorización.

- **Uso de Energía Controlado**

Se espera que los clientes cumplan con la regla del 80/20 para el consumo de energía.

- **Respeto a la Privacidad de Otros Clientes**

Se prohíbe el acceso, manejo o inspección de equipos, gabinetes y jaulas de otros clientes.

6.3.6. ESPECIFICACIONES FÍSICAS DEL SERVIDOR ELTHON

ELTHON dispone de un servidor priorizando la potencia, la confiabilidad y el rendimiento. Este servidor no es simplemente una máquina; es el corazón de nuestra operación, la columna vertebral de nuestra capacidad para innovar y ofrecer soluciones de continuidad tecnológicas de vanguardia. A continuación, exploraremos en detalle las especificaciones físicas de esta impresionante máquina, que nos impulsa hacia un futuro más brillante en el mundo digital.

Item	Descripción
SERDEL R650XQ3V1	PowerEdge R650XS R650XSERQ3v1 2.5" Chassis with up to 8 Hard Drives (SAS/SATA), 1 CPU Intel® Xeon® Silver 4310 2.1G, 12C/24T, 10.4GT/s, 18M Cache, Turbo, HT (120W) DDR4-2666 32GB RDIMM, 3200MT/s, Dual Rank, 16Gb BASE x8 480GB SSD SATA Read Intensive 6Gbps 512 2.5in Hot-plug AG Drive, 1 DWPD 8 x 2.5" NO S.O. Dual, Hot-plug, Fully Redundant Power Supply (1+1), 800W, Mixed Mode 2x NEMA 5-15P to C13 Wall Plug, 125 Volt, 15 AMP, 10 Feet (3m), Power Cord, North America No Internal Optical Drive On-Board Broadcom 5720 Dual Port 1Gb LOM Broadcom 57414 Dual Port 10/25GbE SFP28, OCP NIC 3.0 Riser Config 4, 1xOCP 3.0(x16)+ 1x16LP PERC H755 with front load bracket RAID 0, 1, 10, 5, 6, 50, 60 iDRAC9 Enterprise Puertos frontales: 1 x iDRAC Direct (Micro-AB USB), 1 x USB 2.0, 1 x VGA | Puertos posteriores: 1 x USB 2.0, 1 x USB 3.0, 2 x Ethernet, 1 x VGA ReadyRails™ Sliding Rails With Cable Management Arm Black 3 Years ProSupport with Next Business Day Onsite Service-LA

- **Potencia de Procesamiento:** El servidor ELTHON está equipado con un procesador Intel® Xeon® Silver 4310 de alto rendimiento con 12 núcleos y 24 hilos. Esta potencia de procesamiento asegura un rendimiento excepcional para aplicaciones intensivas.

- **Memoria Amplia y Rápida:** Con 32GB de memoria RDIMM a 3200MT/s, el servidor ELTHON ofrece una capacidad de memoria amplia y una velocidad de acceso rápida, lo que es esencial para ejecutar múltiples aplicaciones y cargas de trabajo de manera eficiente.
- **Almacenamiento de Estado Sólido:** El servidor está equipado con una unidad de estado sólido (SSD) SATA de 480GB. Esto proporciona un almacenamiento de alto rendimiento y confiabilidad, lo que se traduce en tiempos de carga rápidos y una mayor eficiencia en el acceso a datos críticos.
- **Conectividad Avanzada:** Ofrece conectividad avanzada con puertos duales de 10/25GbE SFP28 y puertos Gigabit Ethernet. Esto permite una conectividad rápida y fiable para las necesidades de red de su empresa.
- **Control de Almacenamiento:** El servidor está equipado con un controlador PERC H755, que admite múltiples niveles de RAID (0, 1, 10, 5, 6, 50, 60). Esto garantiza la integridad y disponibilidad de los datos almacenados.
- **Gestión Remota:** Con la incorporación de iDRAC9 Enterprise, el servidor ELTHON permite una gestión remota avanzada y un monitoreo de hardware, lo que facilita la administración y el mantenimiento de manera eficiente.
- **Diseño de Alta Disponibilidad:** El servidor cuenta con fuentes de alimentación redundantes y hot-plug, lo que garantiza la máxima disponibilidad y reducción de tiempo de inactividad en caso de falla de energía.
- **Facilidad de Mantenimiento:** El servidor viene con ReadyRails™ Sliding Rails y un Cable Management Arm, lo que simplifica la instalación y el mantenimiento, ahorrando tiempo y recursos.
- **Soporte Profesional:** La compra incluye 3 años de servicio ProSupport con Next Business Day Onsite Service, lo que proporciona tranquilidad con un soporte técnico profesional y una rápida respuesta en caso de problemas.

7. INSTALACIÓN DE SOFTWARE DE EXPLOTACIÓN

La instalación de software de explotación es un proceso crítico que debe ser gestionado de manera cuidadosa y controlada. En ELTHON, se han establecido rigurosas políticas y procedimientos para garantizar la seguridad durante la instalación de software de explotación en nuestros sistemas.

El objetivo principal de esta sección es enfatizar que únicamente se instalarán aquellas herramientas y software de explotación que cumplan con los más altos estándares de seguridad. Para ello, se seguirán los siguientes lineamientos y consideraciones:

- **Evaluación exhaustiva de las herramientas:** Antes de proceder con la instalación de cualquier software de explotación, se realizará una evaluación minuciosa para asegurarse de que cumple con los requisitos de seguridad establecidos por ELTHON. Esto incluye revisar las características de seguridad, la reputación del proveedor, las actualizaciones y parches disponibles, y cualquier otra consideración relevante.
- **Fuentes confiables de software:** Se utilizarán únicamente fuentes confiables y autorizadas para la obtención del software de explotación. Esto puede incluir proveedores de renombre, repositorios seguros y licencias legítimas.
- **Procedimientos de instalación estandarizados:** Se seguirán procedimientos de instalación estandarizados y documentados para garantizar la consistencia y la correcta configuración de los componentes de software. Esto incluye el uso de listas de verificación y scripts de instalación predefinidos, que han sido previamente revisados y aprobados por el equipo de seguridad de ELTHON.
- **Actualizaciones y parches:** Se establecerá un proceso para gestionar las actualizaciones y parches de seguridad del software de explotación instalado. Esto implica mantenerse al tanto de las últimas versiones y actualizaciones, evaluar su relevancia y aplicarlos de manera oportuna y segura, minimizando así la exposición a posibles vulnerabilidades.
- **Registro y seguimiento:** Se llevará un registro detallado de todas las instalaciones de software de explotación realizadas en los sistemas de ELTHON. Esto permitirá realizar un seguimiento de las herramientas instaladas, sus versiones, fechas de instalación y cualquier otra información relevante para fines de auditoría y gestión de cambios.

7.1. ENTORNO DE DESARROLLO: INTELLIJ IDEA

IntelliJ IDEA proporciona una variedad de características y funcionalidades que facilitan y agilizan el proceso de desarrollo de software. Algunas de sus características destacadas incluyen:

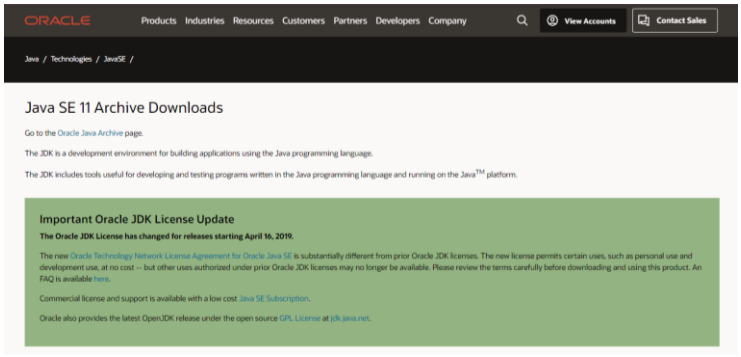
- **Editor inteligente:** Ofrece un editor de código avanzado con funciones de autocompletado, refactorización de código, navegación rápida entre archivos y clases, resaltado de sintaxis, y soporte para múltiples lenguajes.
- **Depuración y pruebas:** Permite depurar y realizar pruebas de código de manera eficiente, con herramientas integradas para rastrear y solucionar errores, evaluar expresiones en tiempo de ejecución y ejecutar pruebas unitarias.
- **Gestión de proyectos:** Proporciona herramientas para administrar proyectos de software, como la organización de módulos, la gestión de dependencias, la integración con sistemas de control de versiones (como Git), y la generación de estructuras de proyecto.

- **Soporte para tecnologías y frameworks:** Incluye integraciones y soporte específico para una amplia gama de tecnologías y frameworks populares, como Spring, Hibernate, Android, Maven, Gradle, y muchos más, lo que facilita el desarrollo en entornos específicos.
- **Productividad mejorada**: Ofrece características que aumentan la productividad del desarrollador, como plantillas de código, inspecciones y correcciones automáticas, refactorización rápida, generación de código automatizada y sugerencias inteligentes.

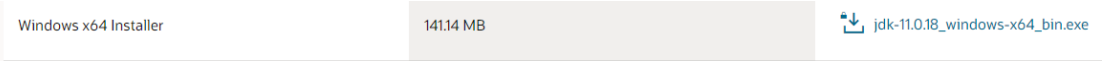
7.1.1. INSTALACIÓN

Instalación JDK

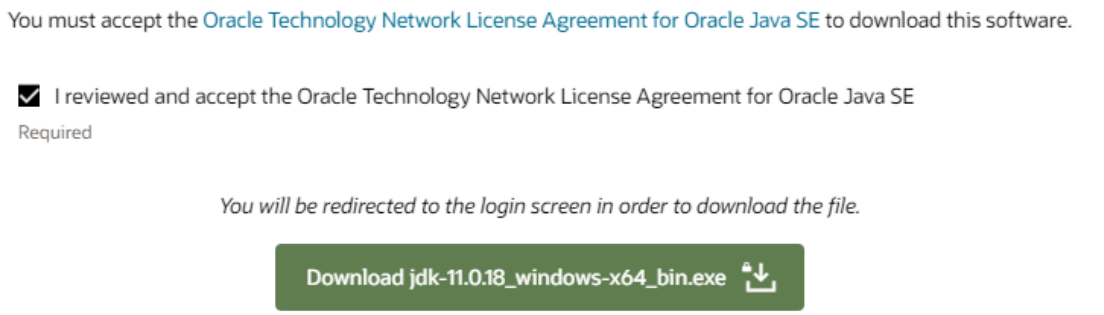
1. Para comenzar a utilizar y crear proyectos dentro del entorno de IntelliJ IDEA, es necesario descargar el JDK (Kit de Desarrollo de Java), el cual le proporciona al IDE las distintas herramientas para compilar, ejecutar y depurar aplicaciones Java.
2. Para descargar y utilizar el JDK, visita el sitio web oficial de Oracle, el desarrollador de Java: https://www.oracle.com/java/technologies/javase/jdk11-archive-downloads.html



3. En la página de descargas, asegúrate de elegir la versión del JDK que deseas descargar. Se selecciona la versión adecuada para tu sistema operativo.

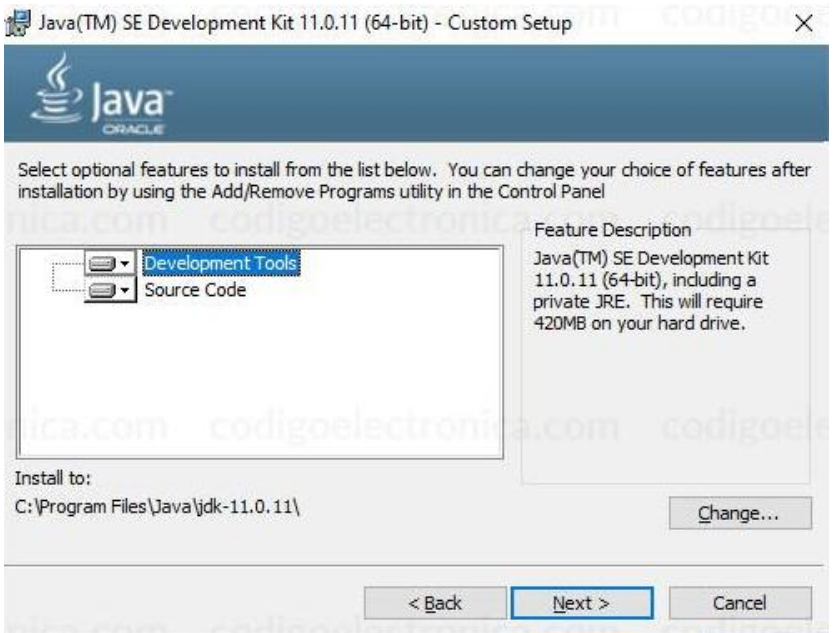


4. Acepta los términos de la licencia y haz clic en el enlace de descarga para iniciar la descarga del archivo de instalación.



5. Una vez que se complete la descarga, ejecuta el archivo de instalación del JDK. El asistente nos dará la bienvenida. Hacemos clic en Next

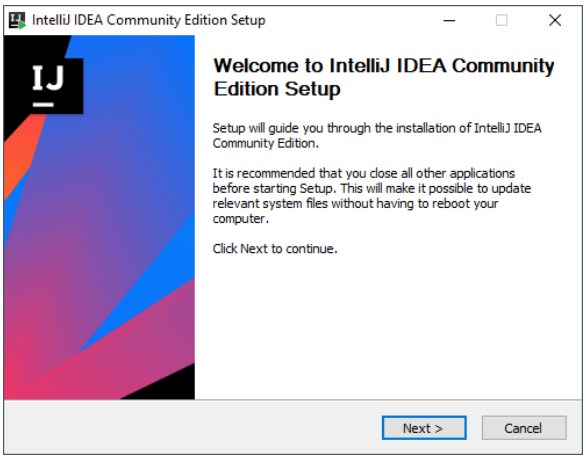
6. En esta etapa, se muestra la opción de seleccionar las características que deseas instalar. Se puede cambiar la ruta de instalación si así lo deseas, pero recuerda recordar la nueva ubicación seleccionada. Luego, haz clic en "Siguiente" o "Next" para continuar.



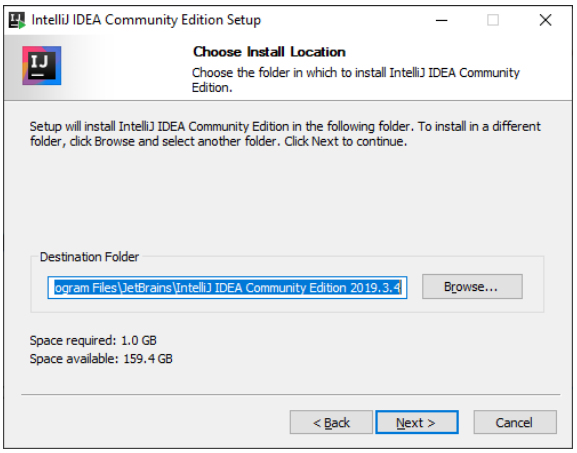
7. Una vez finalizado la instalación, el JDK está listo para utilizarse en el entorno IDE.

Instalación 1.1. INTELLIJ IDEA

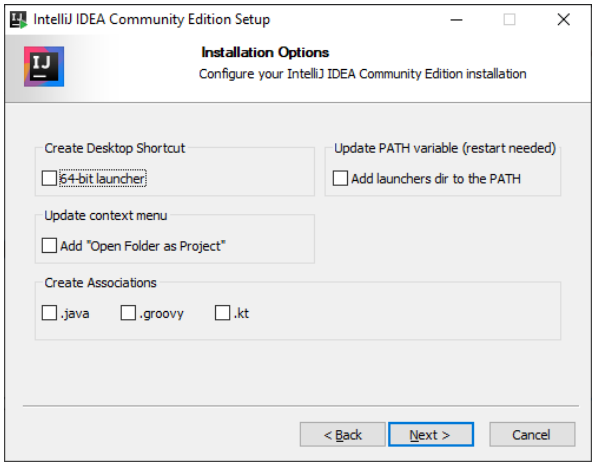
1. Visita el sitio web oficial de JetBrains y selecciona la edición que deseas descargar. Elige tu sistema operativo y haz clic en el enlace "Download" en la página principal de IntelliJ IDEA: https://www.jetbrains.com/idea/ para iniciar con la descarga del instalador.
2. Ejecutar el archivo de instalación .exe de tu carpeta de descargas y haz clic en Next para iniciar la instalación.



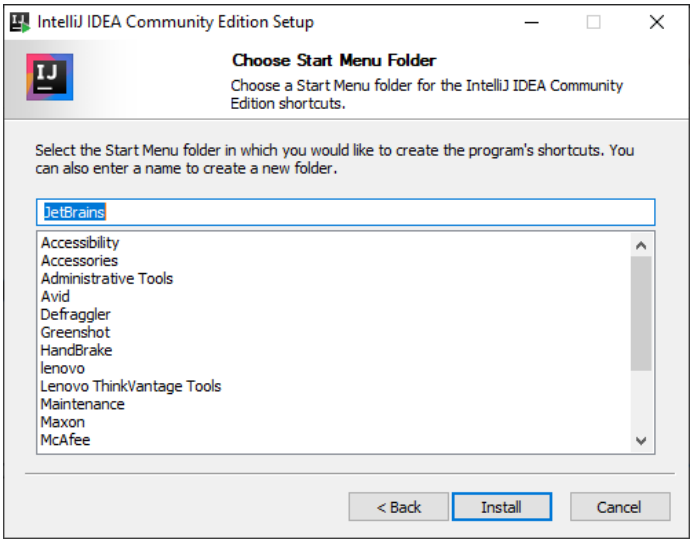
3. Se selecciona la opción "Next" para proceder con la instalación del software en la ubicación predeterminada. También puedes optar por cambiar la carpeta de destino si así lo deseas.



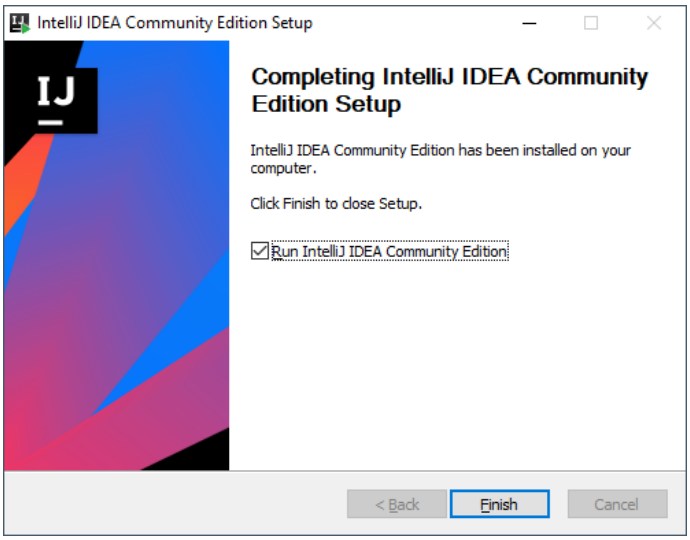
4. Se selecciona las opciones adicionales según tus preferencias, como la creación de un acceso directo en el escritorio, adiciones a los menús contextuales o asociaciones de archivos.



5. Haz clic en "Instalar" para dar inicio al proceso de instalación.



6. Se selecciona la casilla para ejecutar el programa y luego haz clic en "Finalizar".



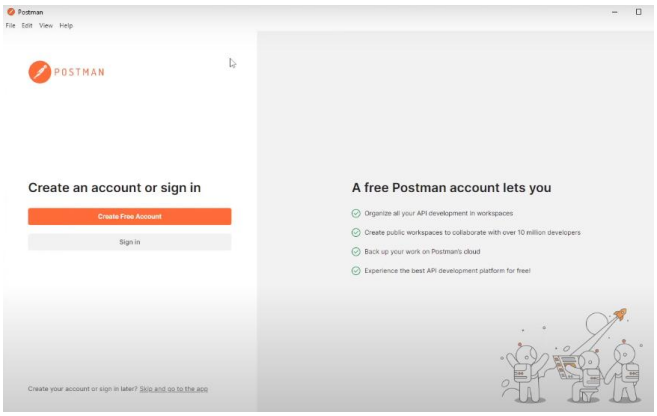
7.2. ENTORNO DE PRUEBAS APIS: POSTMAN

Las principales características y funcionalidades de Postman son las siguientes:

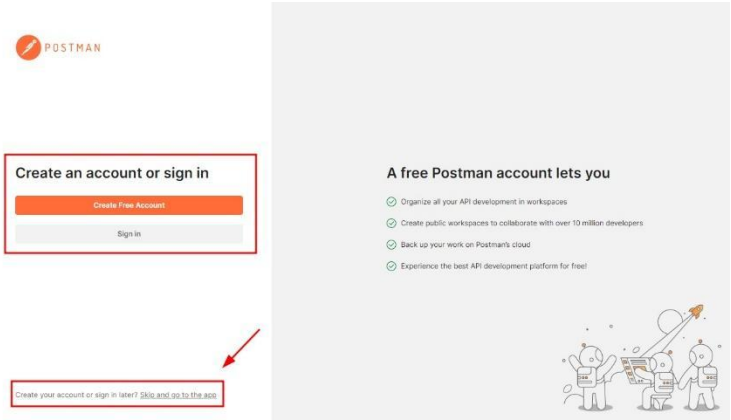
- **Envío de solicitudes HTTP/HTTPS:** Postman permite enviar diferentes tipos de solicitudes HTTP/HTTPS, como GET, POST, PUT, DELETE, PATCH, entre otros. Los usuarios pueden especificar los parámetros, encabezados y cuerpo de la solicitud según las necesidades de la API.
- **Pruebas automatizadas:** Postman permite crear y ejecutar pruebas automatizadas para las API. Los usuarios pueden escribir scripts de prueba utilizando JavaScript y realizar diversas validaciones, como verificar códigos de estado, contenido de respuestas, tiempos de respuesta, entre otros.
- **Colecciones y entornos:** Los usuarios pueden organizar las solicitudes en colecciones, lo que facilita la gestión y ejecución de múltiples solicitudes relacionadas. Además, se pueden utilizar entornos para definir variables y configuraciones específicas de cada entorno (entorno de desarrollo, entorno de pruebas, entorno de producción).
- **Documentación de API:** Postman permite generar documentación de API a partir de las solicitudes y las descripciones proporcionadas. Esto facilita la documentación de las API y su compartición con otros miembros del equipo o usuarios externos.
- **Colaboración y compartir:** Los usuarios pueden compartir fácilmente colecciones, solicitudes y entornos con otros miembros del equipo o usuarios externos. Esto permite la colaboración en el desarrollo y la prueba de API.

7.2.1. INSTALACIÓN

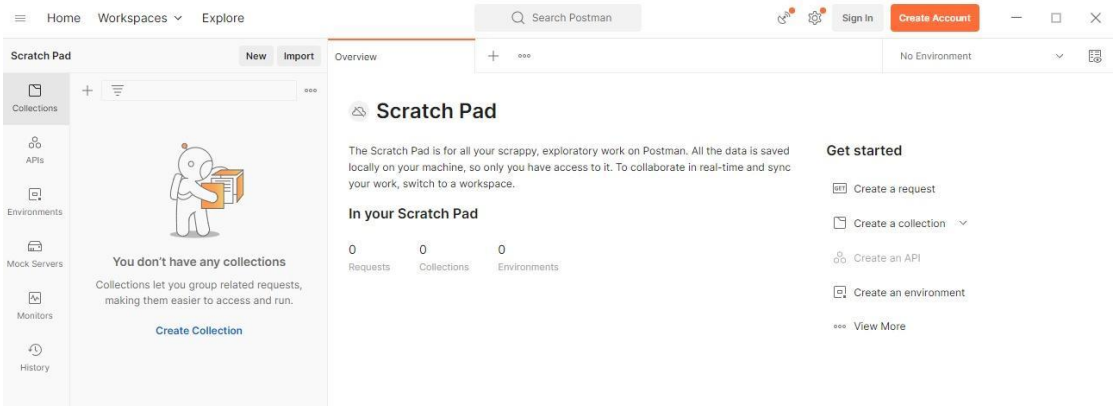
1. Visita el sitio web oficial de Postman en https://www.postman.com/downloads/ y descarga la versión adecuada para tu sistema operativo.
2. Ejecuta el archivo de instalación descargado.



3. A continuación, se te pedirá que inicies sesión o crees una cuenta de Postman. Se puede optar por iniciar sesión con una cuenta existente o seleccionar "Skip signing in" para continuar sin iniciar sesión.



4. Después de iniciar sesión u omitir el inicio de sesión, llegarás a la interfaz principal de Postman. En la parte superior izquierda de la interfaz, puedes hacer clic en "New" para crear un nuevo espacio de trabajo. Los espacios de trabajo son entornos separados para organizar tus proyectos. Se puede crear uno nuevo o unirte a uno existente.



5. Una vez dentro de un espacio de trabajo, puedes crear una colección de solicitudes haciendo clic en "New" y seleccionando "Collection". Las colecciones son conjuntos de solicitudes API relacionadas.
6. Añade solicitudes a tu colección haciendo clic en "New" y seleccionando el tipo de solicitud que deseas realizar (GET, POST, etc.). Luego, completa los detalles de la solicitud, como la URL, los encabezados y los parámetros.

7.3. DBEAVER

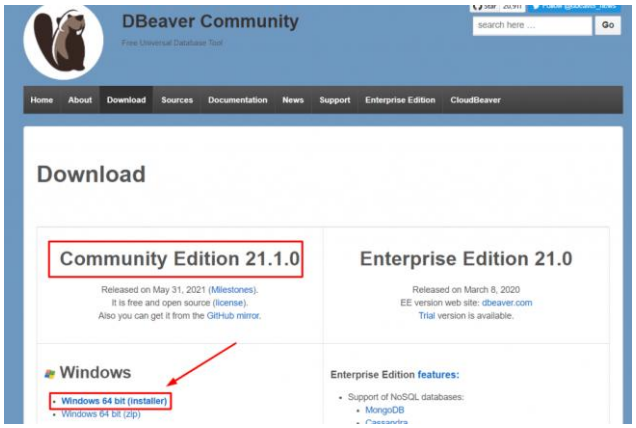
DBeaver es una herramienta de administración y desarrollo de bases de datos multiplataforma. Proporciona una interfaz gráfica intuitiva y potente que permite a los desarrolladores y administradores de bases de datos interactuar con diversas bases de datos de manera eficiente.

Algunas características importantes de DBeaver son:

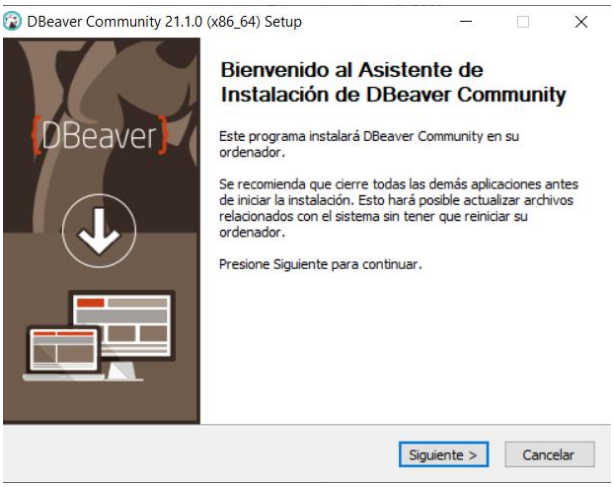
- **Editor de consultas SQL:** DBeaver proporciona un editor de consultas SQL con resaltado de sintaxis y autocompletado, lo que facilita la escritura y ejecución de consultas SQL complejas. También ofrece herramientas visuales para diseñar y visualizar consultas.
- **Explorador de bases de datos:** DBeaver ofrece un explorador de bases de datos que muestra la estructura de la base de datos, incluyendo tablas, vistas, procedimientos almacenados y otros objetos. Esto permite a los usuarios navegar por la base de datos y realizar acciones como crear tablas, modificar datos y administrar esquemas.
- **Importación y exportación de datos:** DBeaver permite importar y exportar datos desde y hacia diferentes formatos, como CSV, Excel, SQL scripts, entre otros. Esto facilita la migración de datos entre diferentes bases de datos y la manipulación de grandes conjuntos de datos.
- **Administración de usuarios y permisos:** DBeaver ofrece herramientas para administrar usuarios, roles y permisos en la base de datos. Los usuarios pueden crear y modificar usuarios, asignar privilegios y gestionar la seguridad de la base de datos.

7.3.1. INSTALACIÓN

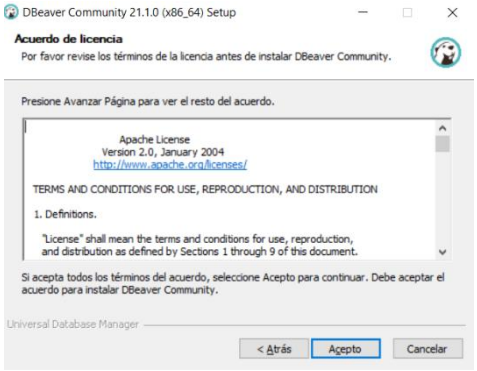
1. Visita el sitio web oficial de DBeaver en https://dbeaver.io/
2. En la página de descargas, asegúrate de seleccionar la versión del JDK que deseas descargar. Elige la versión adecuada para tu sistema operativo.



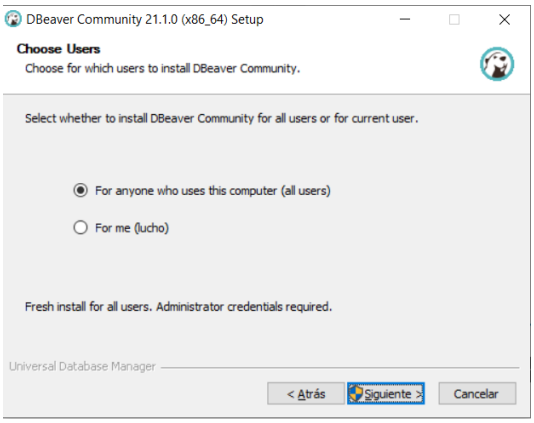
3. Una vez que se haya descargado el archivo de instalación, ejecuta el archivo descargado y selecciona el idioma de tu preferencia. A continuación, se abrirá la siguiente ventana en donde se visualizará la bienvenida al software. Se selecciona el botón “Siguiente”.



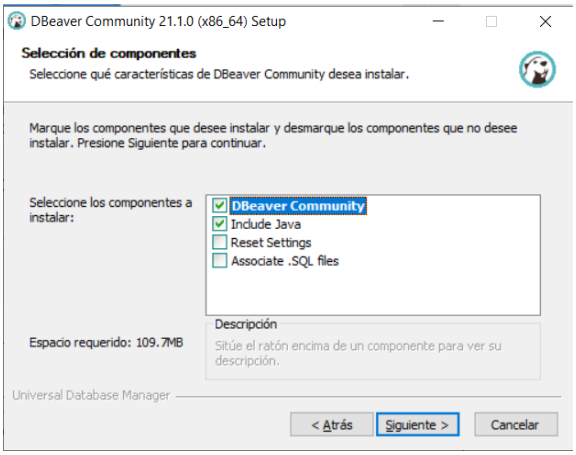
4. Aceptamos los términos y condiciones del acuerdo de licencia.



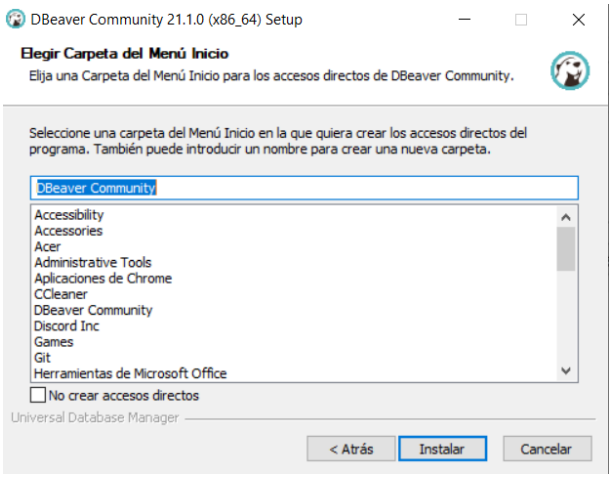
5. Se puede aceptar las opciones predeterminadas o personalizar la instalación según tus preferencias. En la siguiente ventana selecciona si el DBeaver es para uso de todos los usuarios o solamente del usuario actual.



6. Se selecciona la versión comunista y, si se desea, puedes optar por asociar los archivos SQL al editor e incluir Java.



7. Se selecciona la ubicación de la carpeta en donde se instalará el programa y agrega al menú de inicio.



8. Una vez finalizada la instalación, ejecuta DBeaver.

7.4. GIT: GITBASH

Git Bash es una aplicación de línea de comandos que proporciona una interfaz de usuario para interactuar con Git, un sistema de control de versiones distribuido. Git Bash está

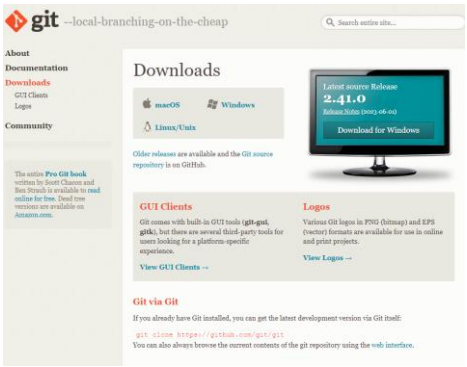
disponible para sistemas operativos Windows y proporciona una emulación de la terminal de Unix, lo que permite a los usuarios ejecutar comandos Git y realizar tareas relacionadas con el control de versiones.

Algunas características de Git Bash incluyen:

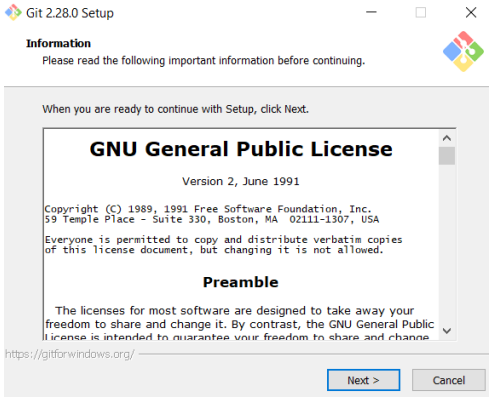
- **Interfaz de línea de comandos:** Git Bash permite a los usuarios ejecutar comandos Git y utilizar la mayoría de las funcionalidades de Git desde la línea de comandos. Esto incluye comandos para crear repositorios, realizar confirmaciones, fusionar ramas, gestionar ramas y etiquetas, entre otros.
- **Compatibilidad con scripts y automatización:** Git Bash admite scripts y automatización mediante la ejecución de comandos Git en secuencia. Esto permite a los desarrolladores automatizar tareas relacionadas con el control de versiones y la gestión de repositorios.
- **Integración con Git:** Git Bash se integra estrechamente con Git, lo que significa que los comandos y las opciones disponibles en Git Bash son compatibles con Git. Esto permite a los usuarios familiarizados con Git utilizar Git Bash de manera eficiente.
- **Acceso a herramientas de línea de comandos de Unix:** Git Bash proporciona una emulación de la terminal de Unix, lo que significa que los usuarios tienen acceso a herramientas de línea de comandos comunes de Unix, como ls, cd, mv, rm, entre otros. Esto facilita la navegación y manipulación de archivos y directorios desde la línea de comandos.

7.4.1. INSTALACIÓN

1. Accede al sitio web oficial de Git en https://git-scm.com/ y dirígete a la sección de descargas.
2. Descarga la versión correspondiente de Git para tu sistema operativo (Windows, macOS o Linux).

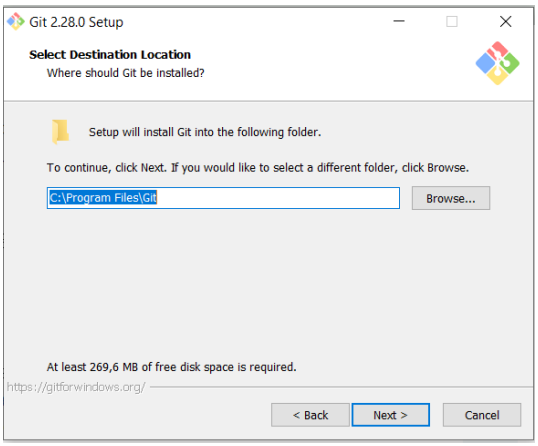


3. Una vez que se haya descargado el archivo de instalación, ejecútalo.

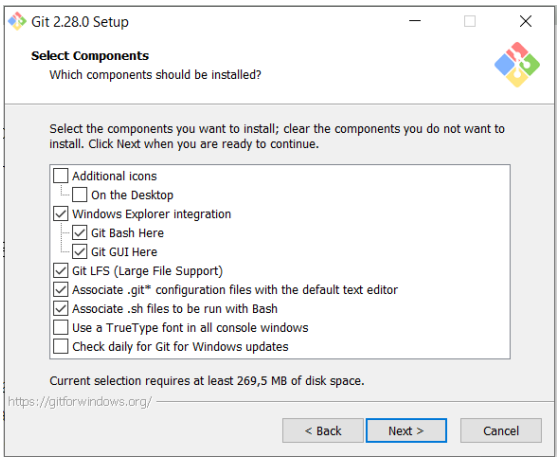


En la ventana actual se visualizará información sobre la licencia GNU que posee Git. Se selecciona el botón “Next” para continuar.

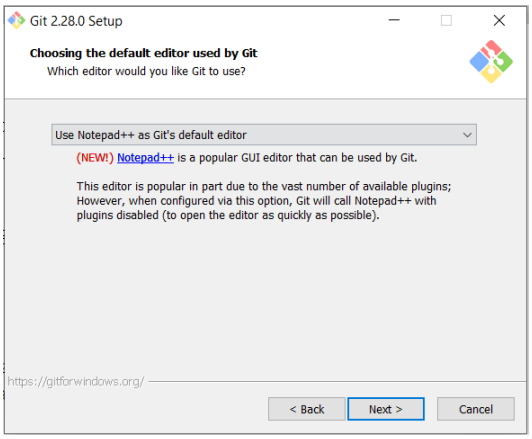
4. Se selecciona la ubicación donde se requiere ser instalada el programa, al continuar estableceremos los diferentes componentes que se desea instalar.



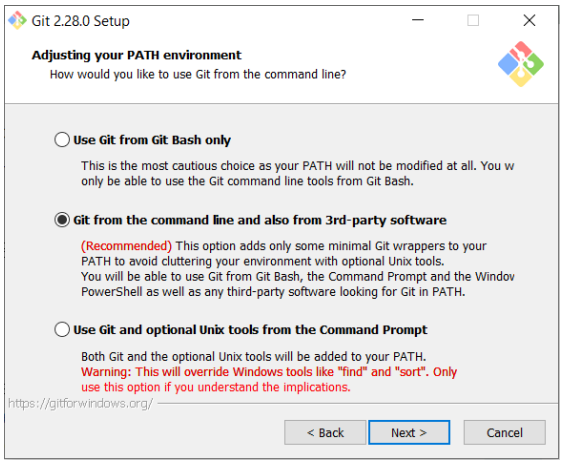
5. A continuación, se establece el nombre del archivo que se va a instalar y seleccionamos “Next” para continuar



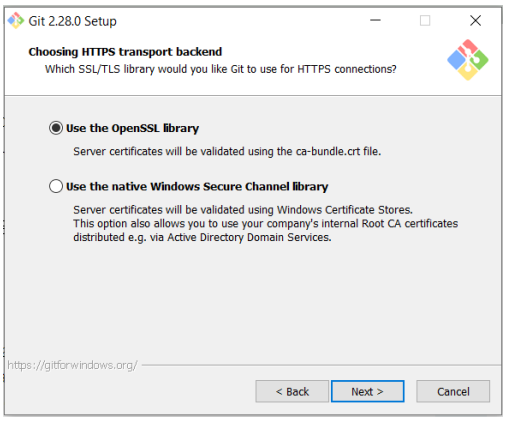
6. En la siguiente configuración, establecemos el editor por defecto que utilizar cuando ingresemos los comandos de Git.



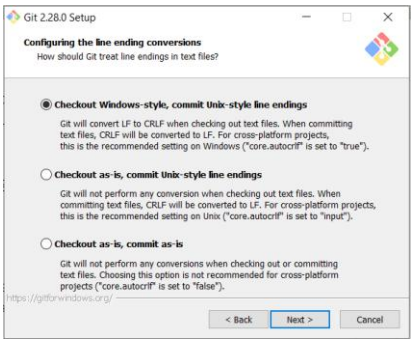
7. En el siguiente apartado, seleccionamos que programas pueden utilizar Git. En la configuración se recomienda que se establezca la opción de línea de comando y otros programas.



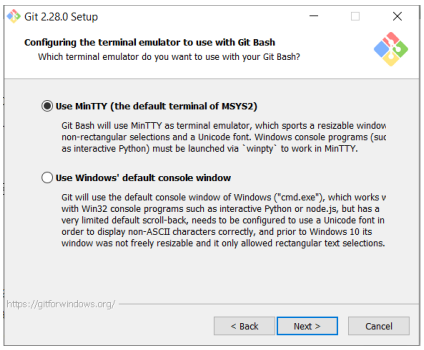
8. La siguiente configuración permite establecer el tipo de comunicación se requiere utilizar para conectar nuestra maquina remota con el repositorio.



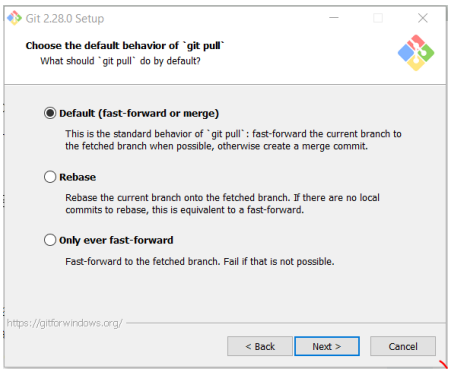
9. Se configura como deseamos utilizar los saltos de línea.



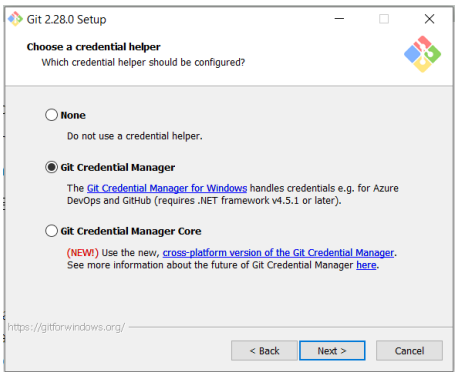
10. Configura el emulador de terminal para su uso con GIT Bash y haz clic en Next



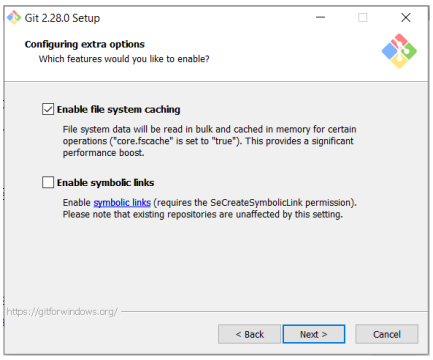
11. Se selecciona el comportamiento por defecto para "git pull" y haz clic en Siguiente.



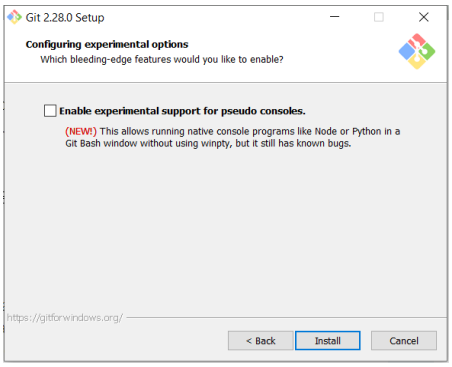
12. Se selecciona qué asistente de credenciales debe configurarse y haz clic en Next.



13. Se selecciona las funcionalidades que desees habilitar y haz clic en Siguiente.



14. Finalmente, si así lo prefieres, activa las opciones experimentales y haz clic en Instalar. A continuación, comenzará el proceso de instalación.



15. Una vez finalizada la instalación, abre una nueva ventana de terminal (símbolo del sistema o consola) y ejecuta el siguiente comando para verificar que Git se haya instalado correctamente:

    a. Configura tu nombre de usuario ejecutando el siguiente comando en la terminal (reemplaza "Tu nombre" con tu nombre real):

```arduino
git config --global user.name "Tu nombre"
```

    b. Configura tu dirección de correo electrónico ejecutando el siguiente comando en la terminal (reemplaza "tu-correo@example.com" con tu dirección de correo electrónico):

```css
git config --global user.email tu-correo@example.com
```

7.5. ENTORNO DESARROLLO FRONT: VISUAL STUDIO CODE

Visual Studio Code es un entorno de desarrollo integrado (IDE) de código abierto y multiplataforma desarrollado por Microsoft. Es ampliamente utilizado por los desarrolladores de Angular, ya que proporciona una amplia gama de características y extensiones que facilitan el desarrollo de aplicaciones con este framework.

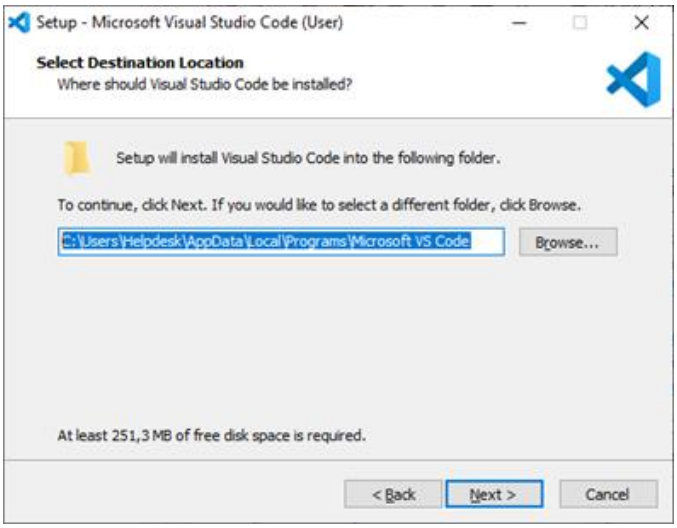
Algunas características importantes de Visual Studio Code para trabajar con Angular son:

- **Edición de código:** Visual Studio Code ofrece una potente capacidad de edición de código, con resaltado de sintaxis, sugerencias inteligentes, autocompletado, refactorización y soporte para múltiples lenguajes de programación, incluido TypeScript utilizado en Angular.
- **Depuración integrada:** Visual Studio Code cuenta con un potente sistema de depuración integrado que permite a los desarrolladores depurar fácilmente sus aplicaciones Angular. Los puntos de interrupción se pueden establecer en el código TypeScript y se pueden inspeccionar variables y ejecutar el código paso a paso para identificar y solucionar problemas.
- **Integración con Angular CLI:** Angular CLI es una herramienta de línea de comandos utilizada para crear y gestionar proyectos de Angular. Visual Studio Code proporciona una integración directa con Angular CLI, lo que permite ejecutar comandos de Angular CLI desde la interfaz de usuario del IDE, como la generación de componentes, servicios, módulos, pruebas unitarias, entre otros.
- **Extensiones de Angular:** Visual Studio Code cuenta con una amplia variedad de extensiones desarrolladas específicamente para trabajar con Angular. Estas extensiones ofrecen funcionalidades adicionales, como la generación automática de código, plantillas de código predefinidas, herramientas de linting y formateo, entre otros.
- **Control de versiones:** Visual Studio Code ofrece una integración nativa con sistemas de control de versiones, como Git. Esto permite a los desarrolladores realizar acciones comunes de control de versiones, como confirmar cambios, cambiar ramas, fusionar código y resolver conflictos directamente desde el IDE.
- **Terminal integrada:** Visual Studio Code incluye una terminal integrada que permite a los desarrolladores ejecutar comandos directamente desde el IDE. Esto facilita la ejecución de comandos de compilación, pruebas y otras tareas relacionadas con el proyecto sin la necesidad de alternar entre ventanas o aplicaciones.

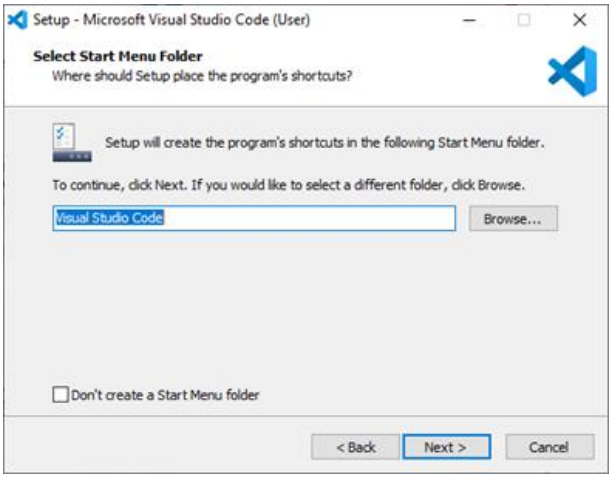
7.5.1. INSTALACIÓN

1. Ve a la página de Microsoft Visual Studio Code (https://code.visualstudio.com/) y haz clic en el botón 'Descargar Visual Studio Code' para descargar el archivo de instalación.
2. Abre el archivo de instalación .exe en tu carpeta de descargas para iniciar la instalación.
3. Lee y acepta el acuerdo de licencia. Haz clic en Next para continuar.

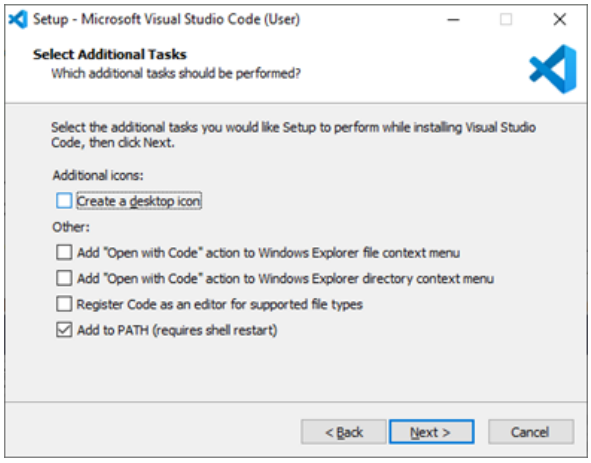
4. Se puede cambiar la ubicación de la carpeta de instalación o mantener la configuración predeterminada. Haz clic en Next para continuar.



5. Elige si se desea cambiar el nombre de la carpeta de accesos directos en el menú Inicio o si no deseas instalar accesos directos en absoluto. Haz clic en Next.

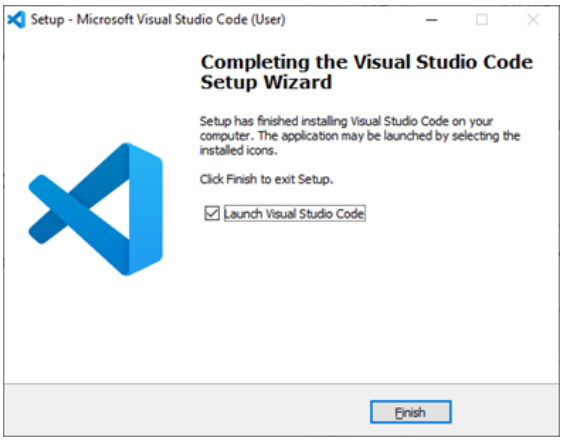


6. Se selecciona las tareas adicionales, por ej. crear un icono en el escritorio o añadir opciones al menú contextual de Windows Explorer. Haz clic en Next.



7. Haz clic en Instalar para iniciar la instalación.

8. La instalación del programa ha culminado. Haz clic en "Finalizar" para completar el proceso de instalación y abrir el programa.



8. RESTRICCIÓN EN LA INSTALACIÓN DE SOFTWARE

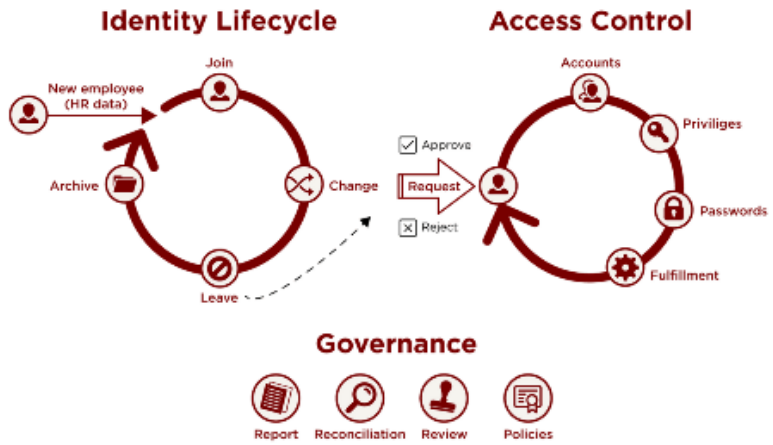
El objetivo principal de esta sección es destacar las políticas y acciones tomadas por ELTHON para limitar la instalación de software no deseado o inadecuado en los equipos y dispositivos proporcionados por la organización a sus empleados. A continuación, se describen las medidas adoptadas:

- **Privilegios de instalación:** Se han establecido roles y privilegios de usuario que restringen la capacidad de instalar software en los equipos y dispositivos proporcionados por ELTHON. Los usuarios se les asignan permisos específicos y solo aquellos con privilegios de administrador tienen la capacidad de instalar software.
- **Políticas de uso aceptable:** Se han definido políticas claras de uso aceptable que prohíben la instalación de software no autorizado en los equipos y dispositivos proporcionados por ELTHON. Estas políticas se comunican a todos los empleados y se espera que cumplan con ellas en todo momento.
- **Software autorizado:** Se ha establecido una lista de software autorizado y aprobado por ELTHON, que puede ser instalado en los equipos y dispositivos proporcionados. Esto garantiza que el software utilizado cumpla con los estándares de seguridad y sea compatible con el entorno de la organización.
- **Herramientas de monitoreo:** Se utilizan herramientas de monitoreo y gestión de activos de software para supervisar y auditar la instalación de software en los equipos y dispositivos de ELTHON. Esto permite identificar cualquier instalación no autorizada y tomar las medidas necesarias para remediarlo.

8.1. IMPLEMENTACIÓN

La implementación de medidas de control de accesos adecuadas en entornos empresariales de Windows ayuda a garantizar la seguridad de la información. Estos controles permiten proteger los recursos y datos sensibles de la empresa, mitigar el riesgo de amenazas internas y externas, además permite prevenir accesos no autorizados y sobre todo a cumplir con los requisitos de privacidad y cumplimiento normativo.

Con el fin de prevenir el acceso no autorizado a los sistemas de información, es importante establecer procedimientos formales que permitan controlar la asignación de derechos de acceso a sistemas de información, bases de datos y servicios de información. Estos procedimientos deben ser documentados de manera clara, comunicados a los usuarios pertinentes y controlados para garantizar su cumplimiento.



Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La norma ISO 27001 recomienda la implementación de controles para una gestión adecuada de las cuentas de usuario. Estos controles incluyen la definición de políticas para la creación de contraseñas seguras, la realización de revisiones periódicas de los derechos de acceso de los usuarios, y el aseguramiento de que las cuentas de usuario sean desactivadas o eliminadas de forma oportuna cuando los empleados dejan la organización o cambian de roles.

En Windows, es posible crear una cuenta de usuario con privilegios administrativos y locales. Un usuario con una cuenta de administrador tiene acceso completo al sistema, lo que significa que un usuario con privilegios de administrador tiene acceso completo al sistema y puede realizar cambios significativos. Por lo tanto, es recomendable otorgar

el nivel de acceso de administrador solo a aquellos usuarios que tienen roles o responsabilidades específicas que lo requieren.

Por otro lado, un usuario estándar tiene permisos limitados y no puede realizar cambios que afecten directamente al sistema en general, como la instalación de software o la modificación de configuraciones críticas.

8.1.1. USUARIO ADMINISTRADOR

- Para crear un usuario administrador se debe presionar el botón de “Inicio” y seleccionar la configuración del sistema que se simboliza con el siguiente icono
- En la ventana de configuración, ingresa al apartado de "Cuentas" y luego en "Familia y otras personas".
- En el panel derecho, selecciona en "Agregar otra persona a este equipo".
- Cuando se abra la ventana, se te solicitará ingresar la dirección de correo electrónico o el número de teléfono del usuario que deseas agregar. En este caso, debes hacer clic en la opción "No tengo la información de inicio de sesión de esta persona".
- En la siguiente pantalla, selecciona "Agregar un usuario sin una cuenta de Microsoft".
- A continuación, procede a completar los campos requeridos para crear un nombre de usuario y una contraseña para la cuenta. También tienes la opción de agregar una pista de contraseña que pueda ayudar al usuario a recordarla en caso de olvido.
- Se selecciona "Siguiente" y el nuevo usuario se agregará al sistema con acceso total.

8.1.2. USUARIO EMPLEADO (POR ROL DENTRO DE LA EMPRESA)

- En esta categoría de cuenta, es necesario seguir los mismos cinco primeros pasos para acceder a la ventana de creación de usuario.
- En lugar de hacer clic en "Agregar un usuario sin una cuenta de Microsoft", selecciona la opción "Agregar una cuenta de Microsoft para esta persona".
- Introduce la dirección de correo electrónico vinculada a una cuenta de Microsoft ya existente o crea una cuenta de Microsoft nueva para el usuario.
- Completa los campos requeridos y selecciona "Siguiente".
- En la pantalla siguiente, se te solicitará configurar la privacidad y las opciones de configuración del usuario. Este paso es el más importantes, debido a que en el siguiente apartado tienes la opción de restringir los permisos para instalar software.
- Se selecciona la opción de "Administrar la pertenencia al grupo" y se abrirá una ventana de configuración.

- En la siguiente ventana de configuración, elige el usuario que creaste previamente y selecciona la opción "Estándar" en lugar de "Administrador". Esto permitirá restringir los permisos del usuario.
- Se selecciona "Aceptar" para guardar los cambios.
- Finaliza el proceso de configuración siguiendo las instrucciones en pantalla.

9. OBJETIVOS DE FUNCIONALIDAD DEL SISTEMA ELTHON

Los sistemas de ELTHON manejan un papel crucial para cualquier organización, ya que permite identificar, evaluar y controlar los riesgos que pueden afectar su operación.

Para lograr una gestión efectiva, es necesario contar con un sistema que permita generar reportes y servicios de respuesta en tiempo real, además de mantener una comunicación continua con los clientes. En este sentido, es importante destacar las ventajas que puede ofrecer una plataforma tecnológica, tales como la automatización de procesos, la reducción de errores y la toma de decisiones informada y oportuna. A continuación, se describen con más detalle las ventajas que ELTHON reúne para desarrollar los sistemas.

- **Monitoreo en tiempo real:** Al tener un sistema en tiempo real, se pueden monitorear los datos y las tendencias en tiempo real, lo que permite a los usuarios tomar decisiones informadas y oportunas, esto es especialmente importante para la gestión de riesgos, donde los datos deben ser actualizados y precisos para tomar decisiones importantes.

- **Servicios de respuesta rápida:** Los sistemas en tiempo real permiten a los usuarios responder rápidamente a las necesidades del cliente y del mercado. Esto es particularmente importante en el caso de un sistema de gran escala, donde las respuestas rápidas y precisas pueden ayudar a minimizar el riesgo y proteger a la empresa.

- **Reportes y análisis precisos:** Los sistemas permiten la generación de reportes precisos, cálculos y análisis de datos en tiempo real. Esto puede ser útil para tomar decisiones informadas y basadas en datos, así como para cumplir con los requisitos reglamentarios y las necesidades de informes de los clientes.

- **Conexión continua con los clientes:** Los sistemas en tiempo real permiten una conexión continua con los clientes, lo que puede mejorar la experiencia del usuario y fomentar la lealtad del cliente. Esto es particularmente importante en el caso de

un sistema de gestión de riesgos, donde la transparencia y la comunicación abierta son esenciales para mantener la confianza de los clientes.

- **Escalabilidad y flexibilidad:** Los sistemas en tiempo real pueden ser escalables y flexibles, lo que significa que pueden manejar grandes volúmenes de datos y adaptarse a los cambios en el mercado y las necesidades del negocio. Esto puede ser especialmente importante en el caso de un sistema de gestión de riesgos, donde los riesgos y las amenazas pueden cambiar rápidamente y el sistema debe ser capaz de adaptarse y responder en consecuencia.

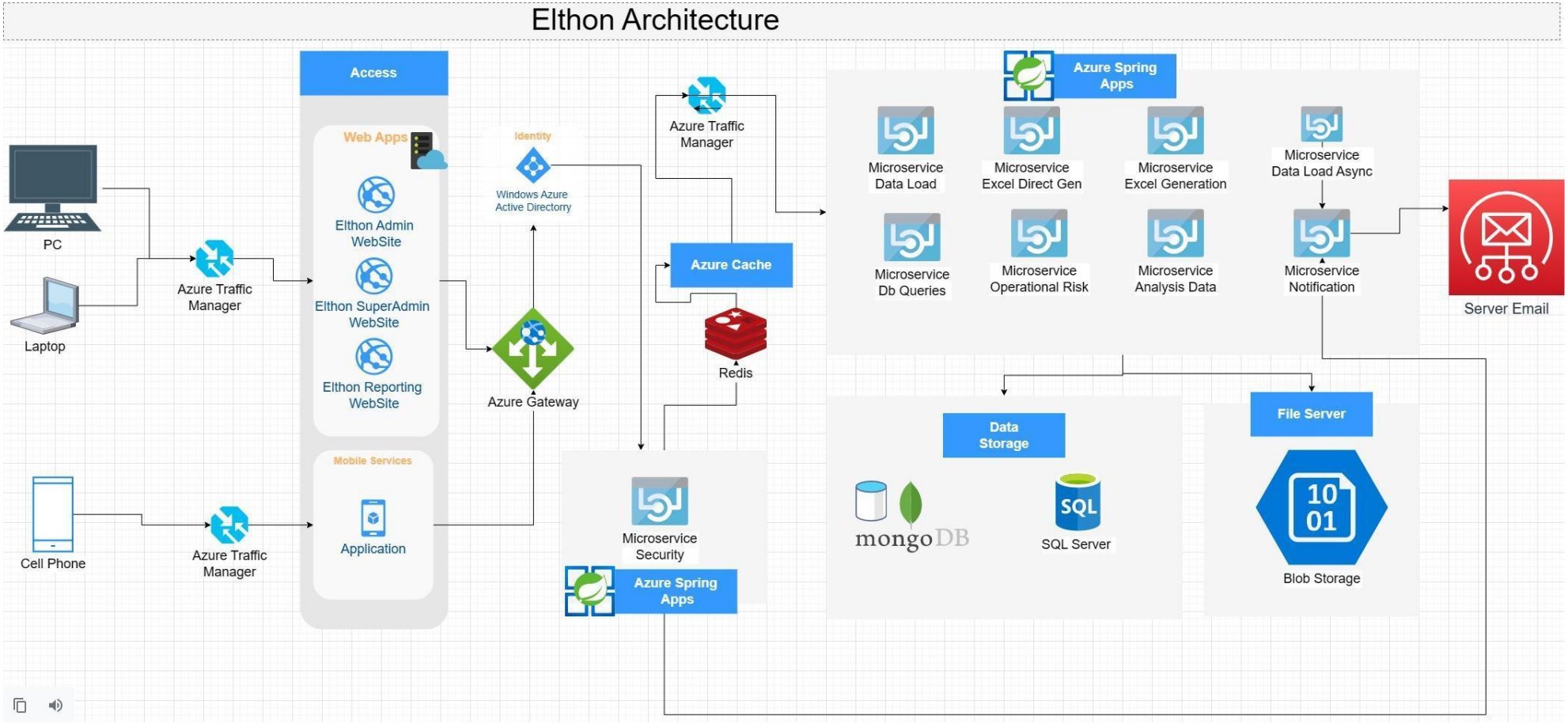
10. ARQUITECTURA ELTHON CEO CON AZURE

ELTHON CEO utiliza la arquitectura de AZURE y la arquitectura interna guiada a microservicios en el sistema de gestión de riesgos para tener una mayor flexibilidad, seguridad y escalabilidad, lo que permite adaptarse a las necesidades cambiantes de los clientes y el mercado.

La seguridad de la arquitectura se basa en la implementación de medidas de seguridad a nivel de red y de datos en línea con los estándares de seguridad provistos por AZURE. Además, la arquitectura interna guiada a microservicios ha permitido una mayor flexibilidad y escalabilidad en el manejo de peticiones, lo que se traduce en una mejor calidad de servicio y una mayor capacidad de adaptación a los cambios del entorno.

Al utilizar la infraestructura y servicios de AZURE, no se tienen limitaciones de tecnología o infraestructura, lo que ha permitido una mayor agilidad en la implementación y mejora continua de la arquitectura.

10.1. ARQUITECTURA DE ELTHON CEO



Diseño de Arquitectura ELTHON.

La arquitectura de ELTHON CEO está compuesta por varios servicios en la nube de AZURE. Para la implementación de microservicios, se utiliza Spring Cloud Apps, lo que permite una gestión centralizada de la configuración y la escalabilidad de los microservicios. Para el desarrollo de la interfaz de usuario, se utiliza Web Apps de AZURE, lo que permite una implementación rápida y sencilla del Frontend. Para el almacenamiento de archivos, se utiliza Blobs AZURE, lo que permite un almacenamiento seguro y escalable de los archivos. Finalmente, para la gestión de sesiones, se utiliza REDIS, lo que permite una gestión rápida y eficiente de las sesiones de usuario.

10.1.1. DESCRIPCIÓN DE LOS COMPONENTES DE LA ARQUITECTURA DE ELTHON

En la arquitectura de ELTHON CEO se utilizan diferentes componentes de AZURE que se comunican entre sí para hacer funcionar los sistemas de gestión de riesgos, administración de usuarios y seguridad. Los componentes principales son:

- **AZURE Traffic Manager:** se encarga de distribuir el tráfico entre las diferentes instancias de Web Apps.
- **Web Apps:** se utilizan para desarrollar y alojar los sitios web Sistemas de ELTHON SuperAdmin, Administración y Reportería.
- **AZURE Gateway:** se utiliza como puerta de enlace para conectar diferentes servicios y aplicaciones.
- **Aplicación móvil de ELTHON:** se comunica con los diferentes servicios y aplicaciones para proporcionar una experiencia de usuario integrada.
- **AZURE Active Directory:** se utiliza para la gestión de identidades y accesos de los usuarios de ELTHON CEO.
- **Microservicio de seguridad con REDIS:** se utiliza para almacenar y gestionar las sesiones basadas en caché de los usuarios de ELTHON CEO.
- **Microservicios AZURE Spring Apps:** se utilizan para desarrollar y alojar los microservicios de ELTHON CEO.
- **Microservicio como servidor de emails y notificaciones:** se utiliza para enviar correos electrónicos y notificaciones a los usuarios de ELTHON CEO.
- **Bases de datos como SQL Server y MongoDB:** se utilizan para almacenar y gestionar los datos de los diferentes servicios y aplicaciones de ELTHON CEO.

10.1.2. DESCRIPCIÓN CAPAS DE LA ARQUITECTURA DE ELTHON

Se describirá las capas lógicas, física y de acceso de la arquitectura de ELTHON es una sección esencial para comprender la estructura y el funcionamiento de esta solución tecnológica.

La capa lógica de la arquitectura de ELTHON se refiere a la estructura conceptual y abstracta que define los procesos y las interacciones de la solución. Esta capa incluye la definición de los microservicios y las funcionalidades que se proporcionarán a los usuarios, y cómo estos servicios interactúan entre sí para satisfacer las necesidades y los requisitos del negocio.

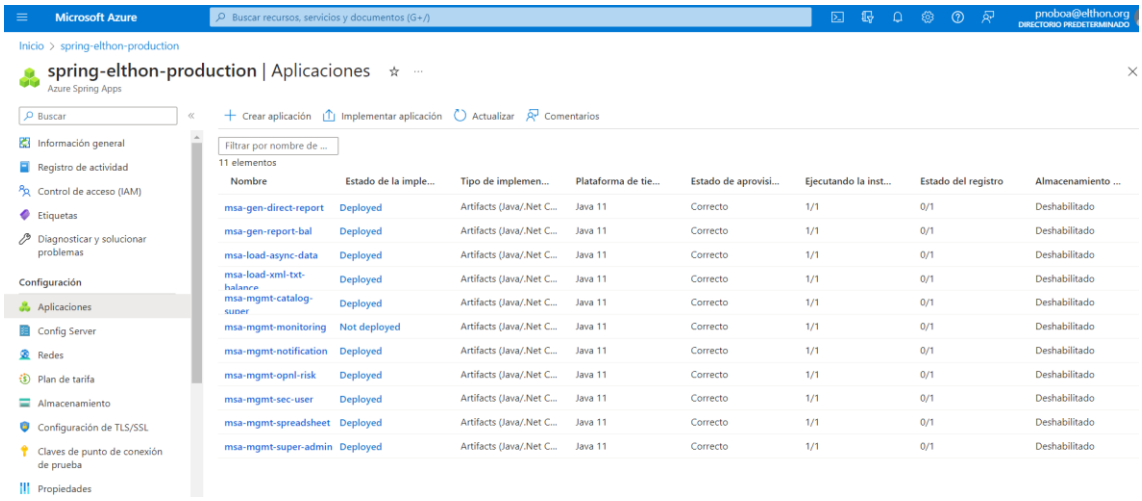
La capa física de la arquitectura de ELTHON se refiere a la infraestructura tecnológica subyacente que soporta la solución. En este caso, la capa física de ELTHON está alojada en la nube utilizando AZURE, esto significa que el hardware, el software, la red y otros componentes físicos que soportan la solución están ubicados en centros de datos en la nube, proporcionados y administrados por AZURE. La infraestructura en la nube ofrece ventajas como la escalabilidad, la disponibilidad y la seguridad, lo que permite que la solución se adapte a las necesidades cambiantes del negocio.

10.1.2.1. CAPA LÓGICA

La capa lógica de la arquitectura de ELTHON es la estructura abstracta que define los procesos y las interacciones de la solución, en el caso de ELTHON, la capa lógica se aloja en AZURE Spring Apps, una plataforma de aplicaciones en la nube que permite alojar microservicios en Java 11 con tecnología Gradle.

Los servicios alojados en la capa lógica de ELTHON están diseñados para realizar diversas tareas, como cargar datos, realizar cálculos, generar informes y proporcionar soluciones para necesidades genéricas, metodologías reglamentarias y necesidades específicas de los clientes.

El uso de microservicios en la capa lógica permite que los servicios sean altamente escalables y modulares, esto significa que cada microservicio se puede desarrollar, probar e implementar de manera independiente, lo que facilita la gestión y el mantenimiento de la solución en su conjunto. Además, el uso de tecnologías de última generación, como Java 11 y Gradle, garantiza un alto rendimiento y una alta eficiencia en la ejecución de los servicios.



Instancia Microservicios.

10.1.2.2. CAPA FÍSICA

El uso de AZURE para la capa física de la arquitectura de ELTHON tiene las principales ventajas siguientes:

- En primer lugar, permite una alta escalabilidad, lo que significa que la solución puede crecer o disminuir según las necesidades del negocio.
- En términos de seguridad, AZURE ofrece una variedad de medidas de seguridad para proteger los datos y los servicios alojados en la nube, como son firewalls de red, control de acceso y autenticación multifactor, así como encriptación de datos en tránsito y en reposo.
- AZURE como plataforma, cuenta con una infraestructura altamente escalable y segura, lo que nos permite adaptarnos a las necesidades de nuestros clientes en tiempo real y garantizar la privacidad y seguridad de los datos.

En resumen, la utilización de AZURE Spring Apps, SQL Server, REDIS, AZURE Blobs y Web Apps en la capa física de nuestra arquitectura nos proporciona una serie de ventajas significativas en términos de escalabilidad, seguridad, eficiencia y experiencia del usuario, lo que nos permite ofrecer un servicio de gestión de riesgos altamente efectivo y satisfactorio para los clientes.

10.1.2.3. CAPA SEGURIDAD

La capa de seguridad en ELTHON se enfoca en garantizar la protección de los datos y sistemas críticos de la empresa, y para ello se utilizan varias medidas de seguridad, en primer lugar, se hace uso de la seguridad nativa que proporciona AZURE para los servicios de AZURE Spring Apps, SQL Server, REDIS, AZURE Blobs y Web Apps, significa que estos servicios ya cuentan con medidas de seguridad implementadas por defecto, como autenticación y encriptación de datos.

Además, en ELTHON se implementa la seguridad de acceso en los sistemas, basada en perfiles y claves seguras. Esto significa que cada usuario tiene un perfil de acceso por entidad definido que le permite realizar únicamente las acciones necesarias para su trabajo el acceso a los módulos está limitado en el contrato de la entidad, evitando así que se acceda a información o funcionalidades que no le corresponden. Además, se utilizan claves seguras, encriptación y transporte de peticiones seguras en la red para proteger la información de acceso y se exige el cambio periódico de las mismas para evitar el acceso no autorizado.

Todas estas medidas de seguridad se combinan para garantizar un entorno seguro y protegido para los datos y sistemas de ELTHON. De esta manera, se minimiza el riesgo de exposición de datos y se protege la información crítica de la empresa. Además, al utilizar la seguridad nativa de AZURE, se aprovechan las ventajas que ofrece esta plataforma en términos de seguridad y se cuenta con un equipo de expertos en seguridad de la información respaldando la infraestructura.

10.1.2.4. CAPA ACCESO

La capa de acceso en la arquitectura de ELTHON se enfoca en proporcionar a los usuarios la manera de interactuar con los servicios y sistemas que se alojan en la nube de AZURE. Para ello, se han implementado diversas soluciones tecnológicas que permiten el acceso a los sistemas desde distintos dispositivos y plataformas.

Una de las principales herramientas que se utiliza en la capa de acceso es el uso de Web Apps, que son aplicaciones web alojadas en AZURE y que permiten a los usuarios acceder a los sistemas a través de un navegador web. Esta solución ofrece una gran flexibilidad ya que se puede acceder a los sistemas desde cualquier dispositivo que tenga conexión a internet y un navegador web.

Además, también se ha desarrollado una aplicación móvil para acceder a los sistemas de ELTHON. Esta aplicación está basada en Flutter y consume los mismos microservicios

que el sistema web, alojados en AZURE Spring Apps. De esta forma, los usuarios pueden acceder a los mismos servicios y funcionalidades desde su dispositivo móvil.

En cuanto a la seguridad en la capa de acceso, se han implementado medidas para garantizar la autenticación y autorización de los usuarios, interviene la capa de seguridad vista en el anterior punto.

10.1.2.5. CAPA NOTIFICACIONES Y MONITOREO

La capa de notificaciones y monitoreo en la arquitectura de ELTHON es de vital importancia para el correcto funcionamiento del sistema y la satisfacción del usuario. Para lograr esto, se utiliza un microservicio genérico que se encarga de enviar mensajes informativos al usuario a través de correo electrónico y de registrar los logs del sistema para su posterior análisis y monitoreo. Este microservicio es altamente escalable y está alojado en AZURE Spring Apps, lo que nos permite tener una capacidad de procesamiento adecuada para el manejo de grandes volúmenes de datos. Además, contamos con un sistema de alertas que nos notifica de cualquier incidencia en el sistema para poder tomar acciones inmediatas y minimizar los tiempos de inactividad. Todo esto nos permite tener un control total sobre la salud del sistema y brindar un servicio de calidad y confiable a nuestros clientes.

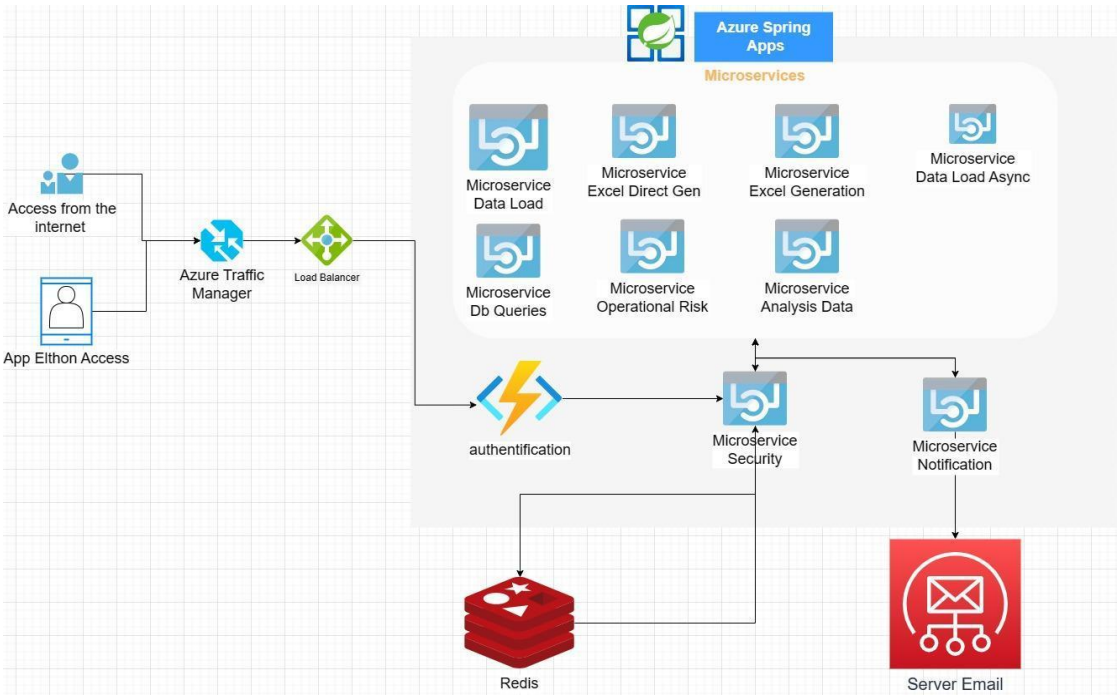
10.2. DESCRIPCIÓN SEGURIDAD, GESTIÓN CONTRASEÑAS Y SESIONES DE ELTHON CON COMPONENTES AZURE

La seguridad de ELTHON, se han utilizado diferentes componentes de AZURE para garantizar la protección de la información. En primer lugar, se ha utilizado AZURE Active Directory para la autenticación y autorización de usuarios en el sistema, lo que permite una gestión centralizada de las credenciales de acceso. Se han implementado políticas de seguridad y permisos a nivel de aplicación y base de datos, con el fin de controlar el acceso a la información en función de los roles y responsabilidades de los usuarios.

Otro aspecto importante de la seguridad de ELTHON es la gestión de contraseñas y sesiones. Para ello, se ha utilizado AZURE REDIS como manejo de sesiones por cache, lo que permite almacenar y gestionar de forma segura y eficiente las sesiones de los usuarios en la aplicación.

Se implementan políticas y buenas prácticas para la gestión de contraseñas, tales como la obligatoriedad de contraseñas seguras y el cambio periódico de las mismas. De esta

manera, se garantiza que la información de los usuarios esté protegida de accesos no autorizados.



Diseño de Comunicación Microservicios.

10.3. DESCRIPCIÓN MICROSERVICIO DE SEGURIDADES DE ELTHON

Un microservicio basado en AZURE Spring Apps para la gestión de seguridad en ELTHON se enfoca en utilizar componentes de autenticación y autorización robustos y escalables. En este caso, se utiliza el protocolo OAuth2 para manejar la autenticación de los usuarios en la aplicación. Además, se emplea Spring Security para proporcionar medidas de seguridad adicionales en el microservicio, como proteger endpoints, validar permisos y roles, y restringir el acceso a recursos sensibles.

Enfoque General

Para garantizar la seguridad de las contraseñas, se utiliza el método de encriptación de contraseñas BCrypt en combinación con Spring Security. De esta forma, las contraseñas de los usuarios se almacenan en una forma irreversible y segura en la base de datos. Para la gestión de tokens JWT, se utiliza la biblioteca de JSON Web Tokens de Spring, lo que permite la emisión, validación y renovación de tokens de acceso para los usuarios autenticados.

Para la gestión de sesiones, se emplea AZURE REDIS como almacenamiento de caché para guardar las sesiones de los usuarios por un periodo de dos horas. Al usar REDIS, se puede garantizar una alta disponibilidad y escalabilidad del sistema, lo que permite manejar un gran volumen de sesiones concurrentes.

Además, al establecer un tiempo de vida para las sesiones, se puede garantizar que las sesiones no se almacenan indefinidamente en la memoria, lo que ayuda a mejorar el rendimiento y la seguridad del sistema.

COMPONENTES INDIVIDUALES

a) Auth2:

Es un protocolo de autorización que permite a las aplicaciones obtener acceso limitado a una cuenta de usuario en un servicio, como Facebook o Google. Auth2 es una solución de seguridad robusta y ampliamente utilizada en el desarrollo de aplicaciones web y móviles, ya que permite a los usuarios autorizar el acceso a su información personal sin compartir su contraseña. Algunas ventajas de usar Auth2 son:

- Mejora la experiencia del usuario al evitar que tenga que crear una nueva cuenta y contraseña para acceder a una nueva aplicación.
- Aumenta la seguridad de la aplicación al no requerir que los usuarios compartan su contraseña con la aplicación.
- Facilita el manejo de permisos y roles de usuarios.

VENTAJAS DEL ENFOQUE ELTHON:

- Simplifica la implementación de autenticación y autorización, ya que permite delegar estas funciones a un servidor de autorización.
- Permite el acceso a recursos protegidos por medio de tokens de acceso, los cuales se pueden renovar sin necesidad de pedir las credenciales del usuario nuevamente.
- Proporciona un mecanismo seguro para compartir recursos entre aplicaciones, ya que no se comparten credenciales de usuario.
- Permite la autenticación de usuarios a través de varias plataformas de forma segura y unificada.
- Ofrece una gestión de tokens granular y configurable, lo que permite personalizar la duración de los tokens y los permisos de acceso.

b) Spring Security:

Es un framework de seguridad que proporciona una capa de seguridad en el nivel de la aplicación para proteger las aplicaciones de posibles vulnerabilidades y ataques. Spring Security es fácil de configurar y personalizar, y tiene una amplia gama de funciones de seguridad, incluyendo autenticación, autorización y prevención de ataques CSRF y XSS. Algunas ventajas de usar Spring Security son:

- Proporciona una capa de seguridad en el nivel de la aplicación, lo que significa que la aplicación está protegida incluso si la red o la infraestructura subyacente son vulnerables.
- Es fácil de personalizar para cumplir con los requisitos específicos de la aplicación.
- Proporciona una variedad de funciones de seguridad para proteger la aplicación contra vulnerabilidades y ataques.

VENTAJAS DEL ENFOQUE ELTHON:

- **Facilidad de integración:** Spring Security se integra fácilmente con otros componentes de Spring, lo que facilita su implementación en proyectos basados en este framework.
- **Amplia funcionalidad:** Spring Security ofrece una amplia variedad de funcionalidades de seguridad, desde autenticación y autorización hasta protección contra ataques comunes como cross-site scripting (XSS) y cross-site request forgery (CSRF).
- **Configuración flexible:** Spring Security ofrece una gran flexibilidad en cuanto a su configuración, permitiendo a los desarrolladores personalizar su funcionamiento según las necesidades específicas de cada proyecto.
- **Comunidad activa:** Spring Security es un proyecto de código abierto con una comunidad de desarrolladores activa, lo que significa que se mantiene actualizado y recibe continuamente mejoras y actualizaciones de seguridad.
- **Integración con otras herramientas de seguridad:** Spring Security se integra con otras herramientas de seguridad como OAuth y OpenID Connect, lo que permite a los desarrolladores implementar autenticación y autorización basadas en estándares abiertos de manera sencilla y eficiente.

c) Método de encriptación Bcrypt:

Bcrypt es un algoritmo de hashing de contraseñas seguro y ampliamente utilizado que ayuda a proteger las contraseñas de los usuarios. Algunas ventajas de usar Bcrypt son:

- Proporciona un nivel de seguridad adicional para las contraseñas de los usuarios.
- Es difícil de descifrar para los atacantes.
- Es ampliamente utilizado y probado en la industria.

VENTAJAS DEL ENFOQUE ELTHON:

- **Seguridad mejorada:** Bcrypt es uno de los algoritmos de encriptación de contraseñas más seguros disponibles. Utiliza técnicas como la Hash y el hashing iterativo para dificultar los ataques de fuerza bruta y reducir la probabilidad de que los hackers puedan descifrar las contraseñas almacenadas.
- **Fácil de usar:** Bcrypt es fácil de usar e implementar en aplicaciones web y en bases de datos. La mayoría de los framework de desarrollo web, como Spring Boot, ofrecen soporte integrado para el uso de Bcrypt en la encriptación de contraseñas.
- **Amplia compatibilidad:** Bcrypt es compatible con una amplia variedad de lenguajes de programación y plataformas, lo que lo hace una opción versátil para ELTHON en su arquitectura de seguridad.
- **Escalabilidad:** Bcrypt es escalable y puede manejar grandes volúmenes de contraseñas de manera eficiente. Esto es especialmente importante para ELTHON, ya que puede tener una gran cantidad de usuarios y contraseñas que deben ser encriptadas y almacenadas de manera segura.

d) Email_Auth

Este método genera un código de un solo uso (OTP, One-Time Password) que se envía al correo electrónico registrado del usuario. El OTP se crea utilizando un algoritmo criptográfico seguro (HMAC-SHA256) y tiene una validez configurable (por defecto, 5 minutos). El envío del código se realiza a través de un servicio de correo electrónico integrado, utilizando conexiones seguras (TLS 1.3). Una vez recibido, el usuario ingresa el OTP en la interfaz de la aplicación, y el backend valida su autenticidad contra un valor almacenado temporalmente en una base de datos cifrada (AES-256).

VENTAJAS DEL ENFOQUE ELTHON:

- **Facilidad de uso:** No requiere que el usuario instale aplicaciones adicionales, ya que el correo electrónico es un canal accesible para la mayoría de los usuarios.
- **Compatibilidad universal:** Funciona en cualquier dispositivo con acceso al correo electrónico, sin dependencias de hardware específico.

- **Rápida implementación:** Se integra fácilmente con servicios de correo existentes, aprovechando infraestructuras SMTP estándar.
- **Flexibilidad de configuración:** Permite personalizar el tiempo de validez del OTP y el número de reintentos, adaptándose a los requisitos de cada cliente.

e) TOTP_Auth

Este método implementa un código de autenticación basado en el tiempo (TOTP, Time-based One-Time Password) conforme a la especificación RFC 6238. Los códigos TOTP son generados por aplicaciones autenticadoras móviles, como Google Authenticator o Microsoft Authenticator, utilizando una clave secreta compartida proporcionada por el servidor. Durante la configuración inicial, el usuario escanea un código QR que contiene la clave secreta y los parámetros TOTP. Los códigos generados tienen una validez de 30 segundos (estándar RFC 6238) y se validan en el backend.

VENTAJAS DEL ENFOQUE ELTHON:

- **Alta seguridad:** Los códigos TOTP son efímeros y cambian cada 30 segundos, reduciendo significativamente el riesgo de interceptación o reutilización.
- **Independencia de conectividad:** Funciona sin conexión a internet una vez configurada la aplicación autenticadora, ideal para entornos con conectividad limitada.
- **Estándar ampliamente adoptado:** Compatible con múltiples aplicaciones autenticadoras, garantizando interoperabilidad y facilidad de uso.
- **Resistencia a ataques de phishing:** Al no depender de un canal de comunicación como el correo, reduce la exposición a ataques de suplantación.

f) Gestión de tokens JWT:

JWT (JSON Web Token) es un estándar abierto que define un formato compacto y autocontenido para transmitir información de forma segura entre partes como un objeto JSON. JWT se utiliza ampliamente en aplicaciones web y móviles como un medio para autenticar y autorizar solicitudes de API. Algunas ventajas de usar JWT son:

- Es fácil de implementar y usar.
- Proporciona un método seguro para transmitir información de forma segura entre partes.
- Es compatible con varios lenguajes de programación y plataformas.

VENTAJAS DEL ENFOQUE ELTHON:

- **Seguridad: J**WT permite la verificación de la integridad de los datos y la autenticación del remitente mediante la firma digital de los tokens. Esto proporciona una capa adicional de seguridad para las comunicaciones entre los servicios y las aplicaciones cliente.
- **Escalabilidad:** JWT es un estándar ampliamente adoptado y compatible con múltiples plataformas y lenguajes de programación. Esto permite a ELTHON implementar una solución de autenticación escalable y de alta disponibilidad para satisfacer las necesidades de su creciente base de usuarios.
- **Flexibilidad:** JWT permite incluir información adicional en los tokens, como los permisos de usuario, que pueden ser útiles para la autorización de usuarios en diferentes servicios y microservicios.
- **Eficiencia:** Al ser un formato compacto y seguro, JWT reduce la sobrecarga de la comunicación y el procesamiento de datos en comparación con otros métodos de autenticación y autorización.

g) REDIS para el guardado de sesiones por 2 horas:

REDIS es una base de datos en memoria de código abierto ampliamente utilizada para el almacenamiento en caché y la sesión de gestión. REDIS es rápido y escalable, y proporciona funciones avanzadas para la gestión de caché, como la expiración automática y la gestión de transacciones. Algunas ventajas de usar REDIS para el almacenamiento de sesiones son:

- Proporciona un almacenamiento de sesiones rápido y escalable.
- Permite la configuración de expiración automática para sesiones inactivas.
- Proporciona una gestión avanzada de transacciones y una fácil integración con otras aplicaciones.

Estructura

El microservicio basado en AZURE Spring Apps de seguridad para ELTHON proporciona medidas de seguridad y autenticación robustas y escalables para proteger los datos sensibles de la aplicación. Al utilizar componentes de autenticación y autorización confiables, y almacenar las sesiones por medio de REDIS, se puede garantizar un alto nivel de seguridad y disponibilidad para la aplicación.

11. ARQUITECTURA DE AZURE

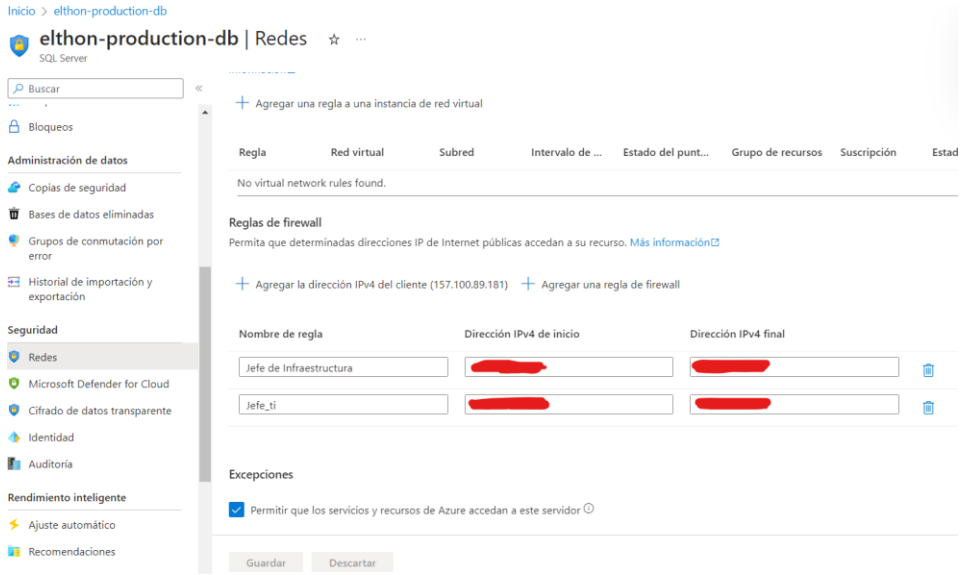
La arquitectura de AZURE se describe como una plataforma en la nube altamente escalable y segura que ofrece una amplia gama de servicios cloud para ayudar a construir, implementar y administrar aplicaciones y servicios en línea. Se basa en una estructura de centros de datos en todo el mundo, conectados por redes privadas de alta velocidad, lo que permite una disponibilidad global y una alta escalabilidad. Además, AZURE proporciona una amplia gama de servicios de seguridad y cumplimiento, incluyendo el cifrado de datos en reposo y en tránsito, la autenticación de usuarios, el control de acceso y la gestión de identidades

Diseño de arquitectura de seguridad de AZURE.
Recuperado de https://learn.microsoft.com/es-es/azure/architecture/guide/security/security-start-here

11.1. FUNCIONALIDADES DE SEGURIDAD DE LA ARQUITECTURA DE AZURE

AZURE FIREWALL

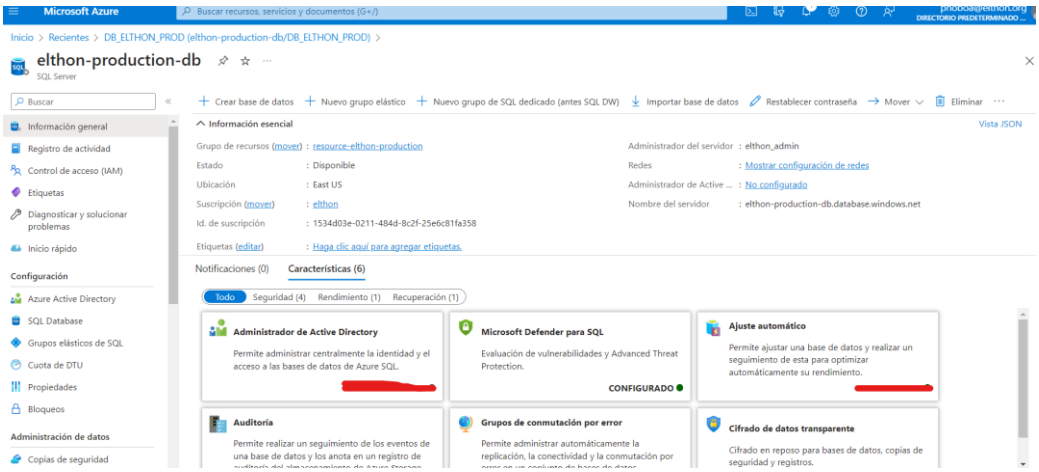
Servicio nativo de seguridad en la nube proporcionado por Microsoft AZURE, que permite implementar una arquitectura de seguridad de red robusta y altamente escalable. Al usar AZURE Firewall, ELTHON puede proteger su infraestructura de red y recursos en la nube mediante la creación de reglas y políticas de seguridad personalizadas, controlando el tráfico de entrada y salida, y filtrando amenazas conocidas y desconocidas. Con la integración de AZURE Firewall en su arquitectura de red, ELTHON puede reducir el tiempo y los costos asociados con la administración y el mantenimiento de una solución de seguridad de red on-premises.



Firewall por IP de ELTHON en AZURE.

MICROSOFT DEFENDER FOR CLOUD

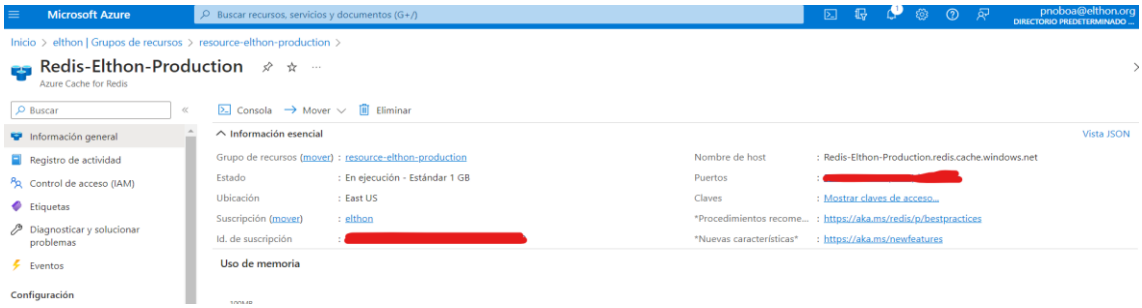
Seguridad en la nube que proporciona protección avanzada contra amenazas para los servicios y recursos de AZURE. Utiliza tecnologías de inteligencia artificial y aprendizaje automático para analizar y detectar amenazas en tiempo real, lo que ayuda a proteger la infraestructura y los datos críticos de la organización en la nube. Al incorporar Microsoft Defender for Cloud en la arquitectura de la nube de ELTHON, se puede mejorar la seguridad y la protección de los servicios y recursos en la nube de la empresa, garantizando así la continuidad del negocio y la satisfacción del cliente.



Microsoft Defender for Cloud de ELTHON en AZURE.

AZURE KEY VAULT

Con Key Vault, se pueden proteger las claves de cifrado, los secretos de autenticación y otros datos sensibles, manteniéndolos seguros y accesibles solo por los usuarios autorizados y aplicaciones en la nube. Además, Key Vault permite controlar y auditar el acceso a los secretos, y cumple con los estándares de cumplimiento y seguridad de la industria.

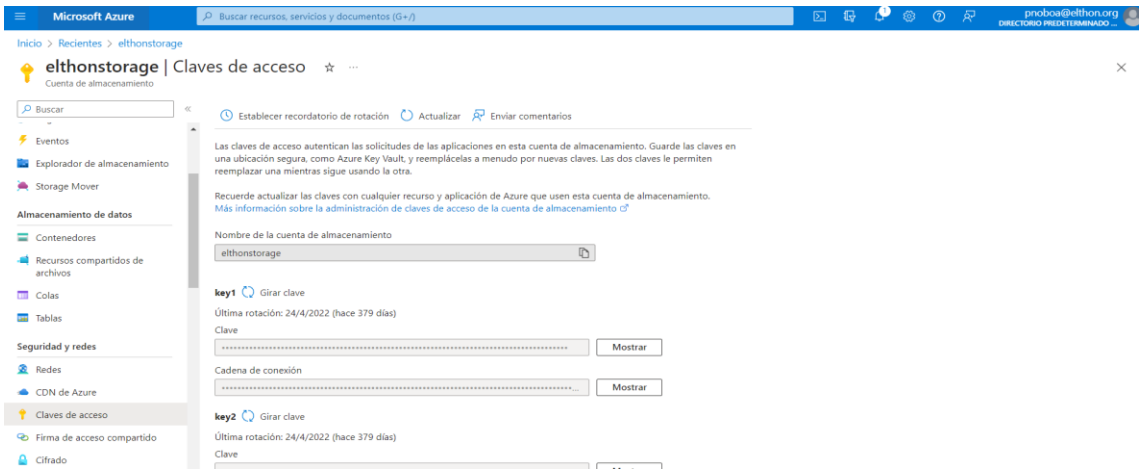


AZURE Key (Claves de Acceso) ELTHON en AZURE.

PRIVATE LINK

Con Private Link, ELTHON CEO puede exponer servicios en la nube de forma segura a sus clientes y socios, sin exponer la dirección IP pública. Esto se logra mediante la creación de una conexión privada entre la red virtual de AZURE de ELTHON CEO y las claves otorgadas a los cliente o socio mediante los sistemas de acceso, lo que proporciona una conectividad privada y de baja latencia.

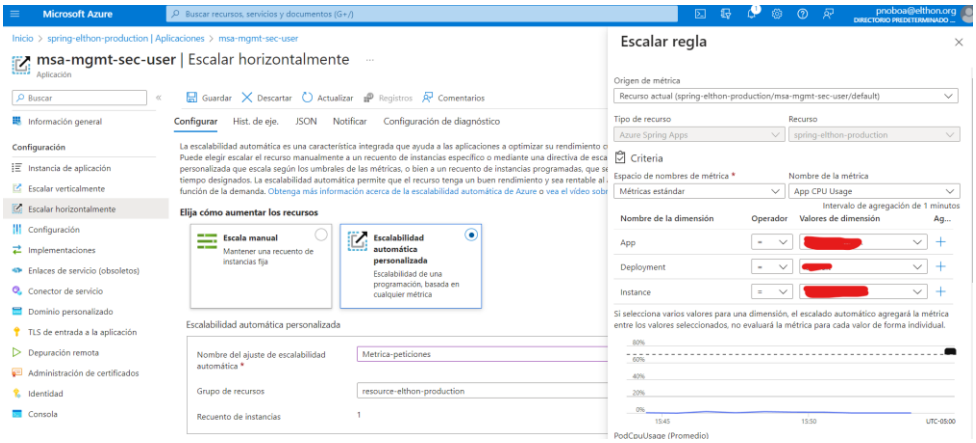
Además, Private Link también ayuda a proteger los datos de la empresa al permitir el control de acceso y la segmentación de redes para limitar el acceso a los recursos solo a usuarios autorizados.



Tokens ELTHON en AZURE.

AZURE APPLICATION GATEWAY

Servicio de balanceo de carga de nivel de aplicación que permite enrutar el tráfico basado en criterios como la URL, la dirección IP de origen y el contenido HTTPS. Esto facilita la distribución eficiente del tráfico a diferentes servicios web, mejorando la escalabilidad y disponibilidad del sistema. Además, el servicio proporciona funciones avanzadas de seguridad, como protección contra ataques DDoS, terminación SSL/TLS y capacidades de firewall de aplicaciones web. Al utilizar AZURE Application Gateway en la arquitectura de ELTHON, se mejora la eficiencia y seguridad del sistema.

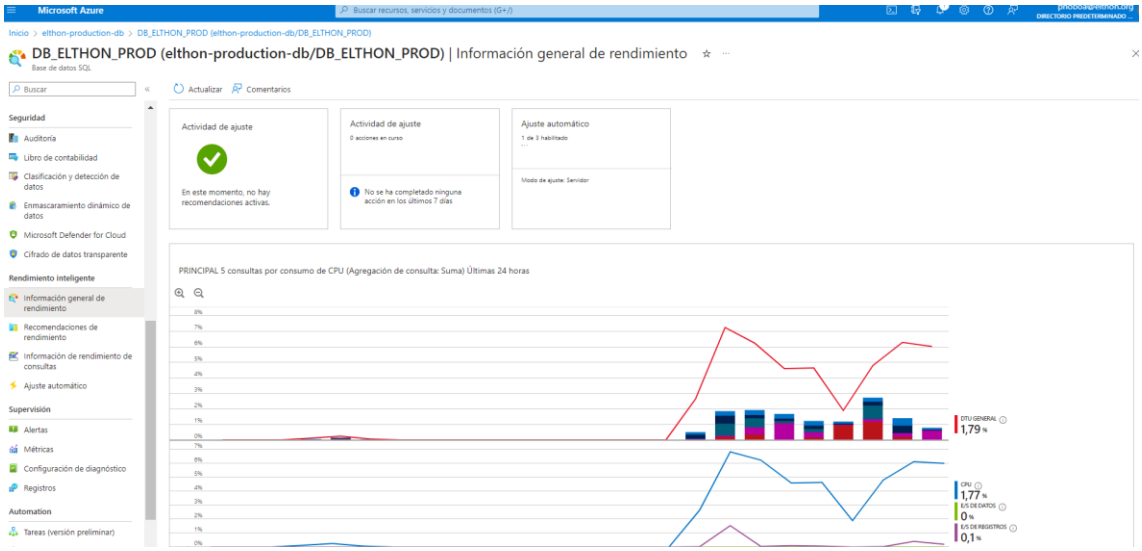


Métricas por solicitudes para Escalabilidad y disponibilidad de ELTHON con AZURE.

AZURE POLICY

Servicio de AZURE que permite definir y aplicar políticas de cumplimiento y seguridad en la nube. Estas políticas se pueden aplicar a recursos individuales o a grupos de recursos en AZURE y permiten garantizar que los recursos se creen y se administren de acuerdo con las normas de la organización.

Se establecen restricciones en la creación de recursos, definir reglas de etiquetado y monitorear el cumplimiento de las políticas. Además, se pueden integrar las políticas de AZURE Policy con otras herramientas de administración de la nube, como AZURE Security Center. Todo esto permite garantizar la seguridad y el cumplimiento de los requisitos legales y normativos en el entorno de la nube de ELTHON CEO.



Administración de Recursos de ELTHON con AZURE.

11.2. ARQUITECTURA INDIVIDUAL DE SERVICIOS ELTHON EN AZURE

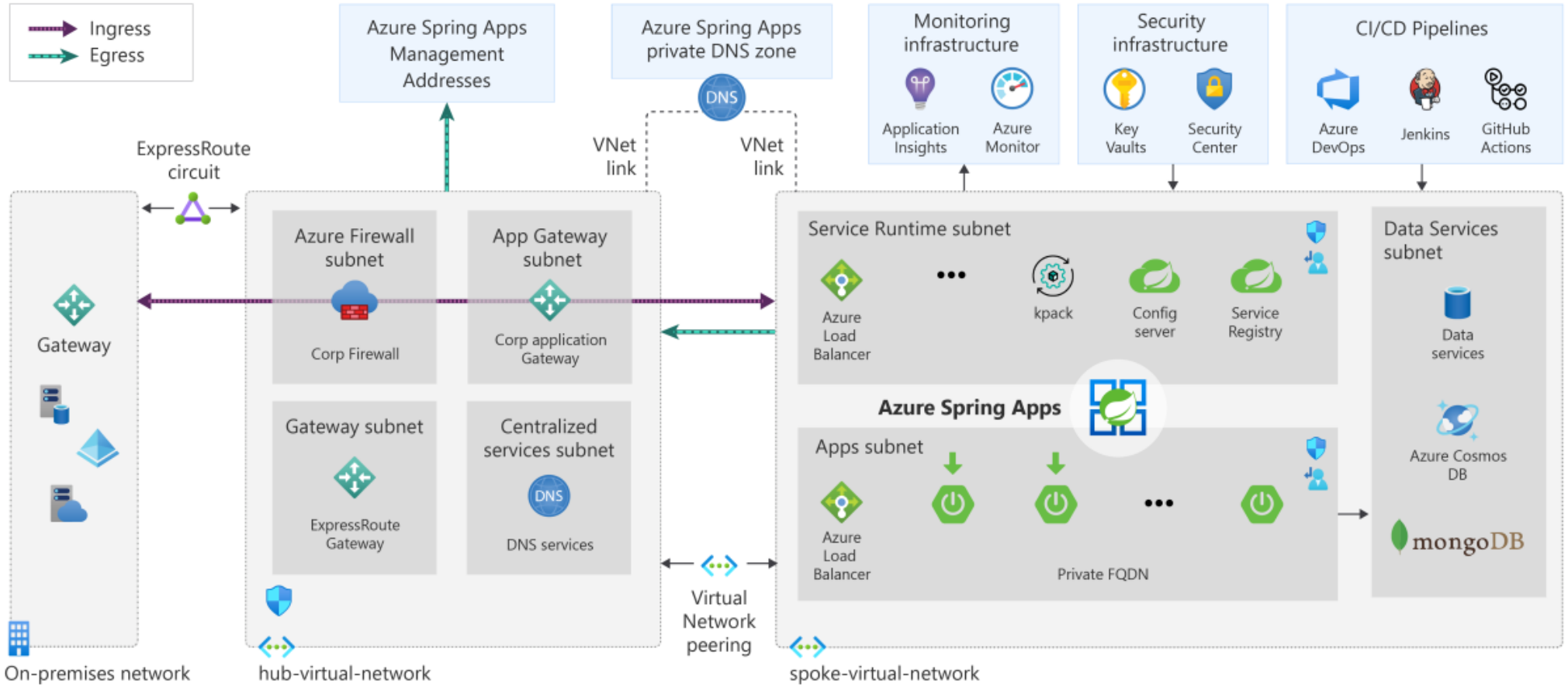
La arquitectura individual de servicios de ELTHON en AZURE se enfoca en la utilización de microservicios a través de la plataforma AZURE Spring Cloud, permitiendo una mayor escalabilidad y modularidad del sistema. Además, se cuenta con una aplicación web en el Frontend para la interacción del usuario con los diferentes servicios. En cuanto a la gestión de bases de datos, se han implementado distintos sistemas según las necesidades de cada servicio, incluyendo bases de datos SQL Server, REDIS y MongoDB, todos alojados en AZURE.

La combinación de estas tecnologías permite una alta disponibilidad del sistema y una mayor eficiencia en el procesamiento y gestión de la información. La arquitectura tanto individual como total de ELTHON CEO está diseñada para cumplir con los estándares de seguridad y protección de datos de AZURE, garantizando así la confidencialidad, integridad, disponibilidad y privacidad de los usuarios, a continuación, se menciona de manera individual la arquitectura manejada por AZURE de cada Servicio de ELTHON.

11.2.1. ARQUITECTURA AZURE SPRING APPS (MICROSERVICIOS DE ELTHON)

La arquitectura de AZURE Spring Apps proporciona un enfoque basado en microservicios para el desarrollo y la implementación de aplicaciones empresariales en la nube. ELTHON usa el framework Spring Boot para crear y gestionar fácilmente los microservicios en AZURE, mientras beneficia la escalabilidad y fiabilidad de la nube de AZURE.

La arquitectura de referencia de AZURE Spring Apps proporciona una guía detallada para la implementación de una arquitectura de microservicios segura y altamente disponible en AZURE. Con el presente análisis, ELTHON implementa una arquitectura de microservicios que cumpla con los requisitos de rendimiento, seguridad y escalabilidad de sus aplicaciones empresariales en la nube.



Diseño de arquitectura de AZURE Spring Apps (microservicios).

Recuperado de https://learn.microsoft.com/es-es/azure/spring-apps/media/reference-architecture/architecture-private-standard.png

ELTHON CEO CON AZURE SPRING APPS

La arquitectura de microservicios de ELTHON está basada en AZURE Spring Apps, una solución de AZURE que proporciona una plataforma completamente administrada para la creación y despliegue de aplicaciones basadas en Spring. Con AZURE Spring Apps, los desarrolladores de ELTHON implementan rápidamente y escalan sus microservicios, lo que les permite responder rápidamente a las necesidades del negocio. Además, la arquitectura de AZURE Spring Apps proporciona una alta disponibilidad, escalabilidad y seguridad para los servicios de ELTHON, lo que garantiza una experiencia confiable para los usuarios finales.

A continuación, se presentan los requisitos de infraestructura de ELTHON CEO considerados para los microservicios que forman parte de los sistemas:

- Una subred solo debe tener una instancia de AZURE Spring Apps.
- Se debe cumplir al menos una prueba comparativa de seguridad.
- Los registros del servicio de nombres de dominio (DNS) del host de aplicación se deben almacenar en el DNS privado de AZURE (el DNS es obtenido directamente de AZURE con los parámetros de la cuenta ELTHON y sus normativas para el nombre y objetivo del microservicio).
- Las dependencias de los servicios de AZURE se deben comunicar a través de puntos de conexión de servicio o Private Link solo entre ellos.
- Los datos en reposo deben estar cifrados.
- Los datos en tránsito deben estar cifrados.
- Se pueden usar canalizaciones de implementación de DevOps (AZURE DevOps con librería personalizada de ELTHON) y requerir conectividad de red a AZURE Spring Apps.
- El tráfico de salida debe viajar a través de una aplicación virtual de red (NVA) central (AZURE Firewall).
- Al usar Config Server de AZURE Spring Apps para cargar las propiedades de configuración desde un repositorio, el repositorio debe ser privado.
- El enfoque de seguridad de Confianza cero de Microsoft requiere que los secretos, los certificados y las credenciales se conserven en un almacén seguro.
- Los grupos de recursos administrados por la implementación de AZURE Spring Apps no se deben modificar.
- Las subredes administradas por la implementación de AZURE Spring Apps no se deben modificar.

DESCRIPCIÓN DE LA ARQUITECTURA

- **API Gateway:** es un punto de entrada para las solicitudes de los Sistemas de ELTHON a los microservicios. Proporciona una capa de seguridad, como autenticación y autorización (controlados por ELTHON y la gestión de claves), y puede manejar la transformación de protocolos y la traducción de mensajes. En la arquitectura de AZURE Spring Apps, el API Gateway se ubica en una subred separada para permitir un mayor control de seguridad.

- **AZURE Firewall Subnet:** es una subred que contiene la instancia de AZURE Firewall, un servicio de seguridad que protege la red de AZURE de amenazas externas. El firewall puede filtrar el tráfico entrante y saliente proporcionando una capa adicional de seguridad para la red.

- **Gateway Subnet:** es una subred que contiene la instancia de AZURE Virtual Network Gateway, que proporciona conectividad segura y privada entre la red de AZURE y las redes locales.

- **AZURE Spring Apps Private DNS Zone:** es una zona de DNS privada que se utiliza para resolver nombres de dominio de AZURE Spring Apps (base a los nombres por normativa según el objetivo del funcionamiento que da ELTHON al Microservicio) en la red virtual de AZURE. Proporciona una forma fácil y segura de acceder a las aplicaciones de Spring en la red de AZURE.

- **Service Runtime Subnet:** es una subred que contiene el servicio de tiempo de ejecución de AZURE Spring Apps. Este servicio aloja los microservicios de ELTHON y proporciona características como escalabilidad automática, equilibrio de carga y administración de versiones de la aplicación.

- **Apps Subnet:** es una subred que contiene las instancias de las aplicaciones de Spring. Cada instancia se ejecuta en su propia máquina virtual y está aislada de las demás instancias de la aplicación.

- **AZURE Load Balance:** es un servicio que distribuye el tráfico de red a través de múltiples instancias de aplicaciones de Spring en una misma subred. Proporciona alta disponibilidad y escalabilidad para las aplicaciones.

- **Security Infrastructure:** se refiere a los servicios de seguridad que se utilizan en la arquitectura de AZURE Spring Apps, como AZURE Firewall, AZURE Active Directory y el cifrado de datos en reposo y en tránsito.

- **Virtual Network Peering:** es una conexión de red privada y segura entre dos redes virtuales de AZURE. Se utiliza para permitir la comunicación entre diferentes redes virtuales en la misma región de AZURE, lo que es útil para conectar diferentes componentes de la arquitectura interna de ELTHON alojada en AZURE.

ANÁLISIS DE ELTHON CEO POR VENTAJAS DE ARQUITECTURA AZURE SPRING APPS

Conectividad local de AZURE Spring Apps

Las aplicaciones pueden comunicarse con varios recursos locales, externos y de AZURE. Permite enrutar el tráfico externamente o a la red local mediante ExpressRoute o una red privada virtual (VPN) de sitio a sitio.

Marco de arquitectura de AZURE

- **Optimización de costos:** AZURE Spring Apps cuenta con componentes escalables y admite el escalado automático de aplicaciones, lo que puede mejorar el uso y la rentabilidad. Además, puede usar Application Insights y AZURE Monitor para reducir los costos operativos.
- **Excelencia operativa:** AZURE Spring Apps ofrece diferentes herramientas, como AZURE Pipelines, AZURE Monitor, Application Insights y Microsoft Defender for Cloud, que permiten una operación eficaz y segura del servicio.
- **Confiabilidad:** AZURE Spring Apps está diseñado para aumentar la disponibilidad de la aplicación en caso de error mediante servicios y consideraciones arquitectónicas. Se puede implementar en varias regiones y utiliza DNS privado de AZURE o AZURE Front Door y AZURE Application Gateway para garantizar la disponibilidad.
- **Seguridad:** La arquitectura cumple con controles y pruebas comparativas definidos por el sector, y se enfoca en los principios de diseño de seguridad para la gobernanza, las conexiones de red y seguridad de las aplicaciones. Además, permite la segregación a través del aislamiento de los recursos de red.

Ventajas de la Arquitectura para Misión y Visión de ELTHON CEO

- **Integración nativa con el ecosistema de AZURE:** Se integra perfectamente con otros servicios y herramientas de AZURE, como AZURE Monitor, AZURE SQL Database,

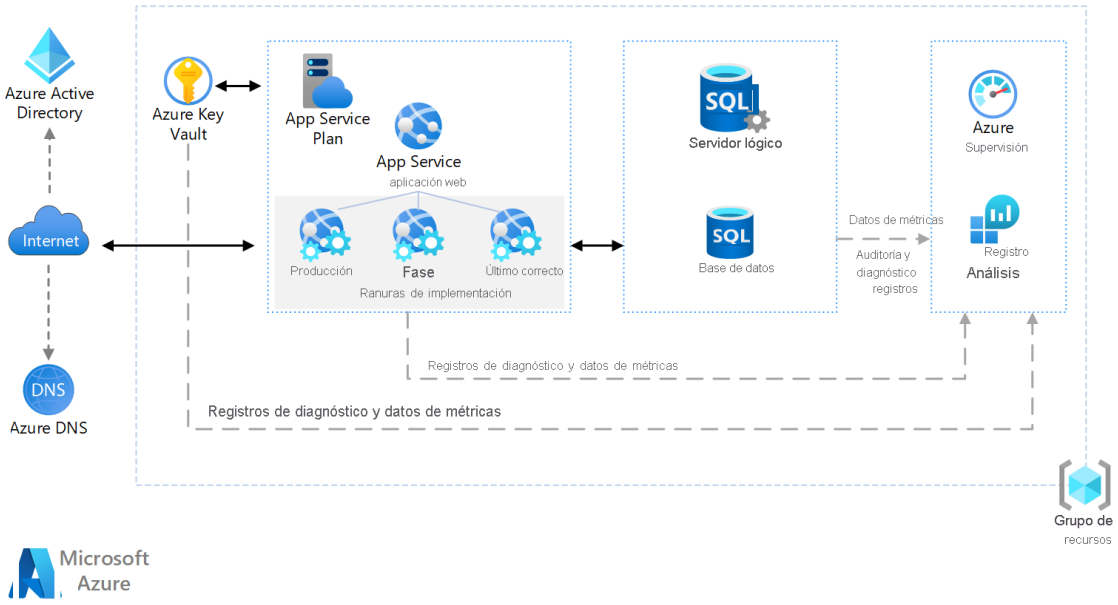
REDIS y MongoDb. Esto significa compatibilidad y manejo eficiente entre diferentes instancias y tecnologías de ELTHON para aprovechar fácilmente la funcionalidad de estos servicios en los microservicios y componentes que forman parte de la Arquitectura Interna a los Sistemas.

- **Escalabilidad y elasticidad:** La arquitectura de AZURE Spring Apps versión estándar permite escalar horizontal y verticalmente la aplicación para manejar aumentos repentinos en la carga de trabajo o aumentos necesarios de infraestructura para funcionalidades que requieren más recursos. Se puede ajustar el número de instancias de la aplicación para adaptarte a la demanda y reducir los costos cuando la demanda disminuye.
- **Seguridad y cumplimiento:** AZURE Spring Apps cumple con los estándares de seguridad y cumplimiento más estrictos, incluyendo ISO 27001, SOC 1, SOC 2 y PCI DSS.
- **Soporte de Microsoft:** Al elegir AZURE Spring Apps, ELTHON tiene acceso al soporte de clase empresarial de Microsoft. Esto incluye soporte técnico 24/7, asistencia en la resolución de problemas y actualizaciones de seguridad regulares.
- **Desarrollo más ágil:** La arquitectura de AZURE Spring Apps permite centrar el desarrollo de ELTHON y sus microservicios Spring en lugar de en la infraestructura. Puede implementar, escalar y actualizar el microservicio con facilidad y rapidez, lo que te permite llevar las ideas al mercado más rápido.

11.2.2. ARQUITECTURA AZURE WEB APPS (SISTEMAS VISUALES FRONTEND)

Arquitectura de AZURE Web Apps para los sistemas visuales Frontend de ELTHON. AZURE Web Apps es una plataforma de alojamiento de aplicaciones web en la nube que ofrece escalabilidad, alta disponibilidad y seguridad, la arquitectura de AZURE Web Apps se basa en una serie de componentes, como los planes de alojamiento, las instancias de la aplicación, los servicios de aplicaciones, los grupos de recursos y los servicios de AZURE. Prioriza aspectos importantes como la seguridad, el rendimiento y la escalabilidad de la arquitectura.

En cuanto a la arquitectura específica para los sistemas visuales Frontend de ELTHON, se describe cómo se puede utilizar AZURE Web Apps para alojar las aplicaciones web que proporcionan la interfaz de usuario a los clientes. Las presentes características son importantes para este propósito, como la capacidad de alojar múltiples aplicaciones web en una sola instancia de la aplicación, la integración con Visual Code y otras herramientas de desarrollo y la capacidad de escalar horizontalmente en respuesta a picos de tráfico.



Diseño de arquitectura de AZURE Web Apps (Frontend).
Recuperado de https://learn.microsoft.com/es-es/azure/architecture/reference-architectures/app-service-web-app/images/basic-webapp-v2.png

DESCRIPCIÓN DE LA ARQUITECTURA AZURE WEB APPS

AZURE App Service es una plataforma completamente administrada para crear e implementar aplicaciones en la nube.

- **Una ranura de implementación:** permite almacenar provisionalmente una implementación y, posteriormente, intercambiarla con la implementación de producción. De este modo, evita realizar la implementación directamente en producción. Consulte la sección de ingeniería e implementación de versiones a continuación para obtener recomendaciones específicas.

- **Dirección IP:** la aplicación de App Service tiene una dirección IP pública y un nombre de dominio. El nombre de dominio es un subdominio, según la normativa de ELTHON el sistema reportería es ELTHON-production-report.azurewebsites.net.

- **AZURE DNS:** es un servicio de hospedaje para dominios DNS que permite resolver nombres mediante la infraestructura de Microsoft AZURE. Al hospedar dominios en AZURE, puede administrar los registros DNS con las mismas credenciales, API, herramientas y facturación que con los demás servicios de AZURE. Para usar un nombre de dominio personalizado, como contoso.com, cree registros DNS que asignen el nombre de dominio personalizado a la dirección IP. Para más información, consulte Configurar un nombre de dominio personalizado en AZURE App Service.

- **AZURE Active Directory:** es un servicio de administración de identidades y acceso basado en la nube que permite a los empleados acceder a aplicaciones en la nube desarrolladas para su organización.

- **AZURE Monitor:** es una solución para recopilar, analizar y actuar sobre registros y métricas en todos los entornos.

- **AZURE Key Vault:** admite la administración de secretos, la administración de claves y la administración de certificados. Puede almacenar secretos de aplicación como cadenas de conexión de base de datos.

ANÁLISIS DE ELTHON CEO POR VENTAJAS DE ARQUITECTURA DE AZURE WEB APPS

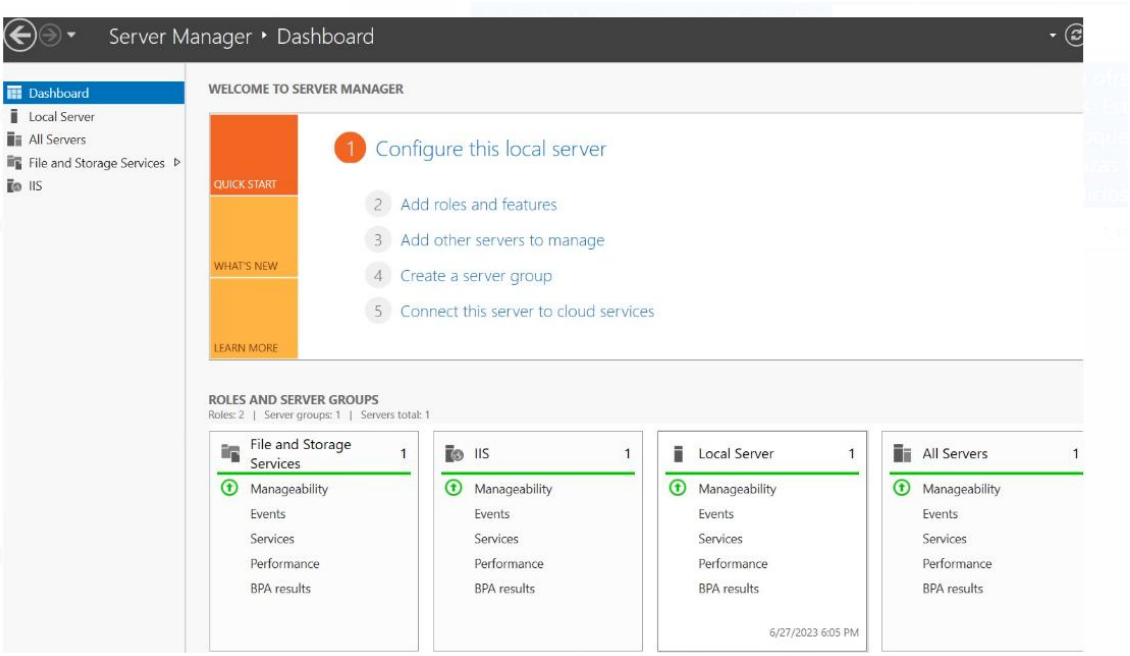
La arquitectura presente da a ELTHON CEO soporte y funcionamiento de una plataforma confiable, escalable y segura para alojar sistemas visuales Frontend. Con esta arquitectura, ELTHON CEO puede centrarse en la innovación y el desarrollo de nuevas funcionalidades para sus usuarios, mientras Microsoft AZURE se encarga de la gestión y mantenimiento de la infraestructura subyacente, entre los puntos más importantes resaltan los siguientes:

- **Escalabilidad:** AZURE Web Apps permite a ELTHON CEO escalar sus sistemas visuales Frontend de manera horizontal o vertical según la demanda de los usuarios. El uso de AZURE Web Apps permite a ELTHON CEO aumentar o disminuir la capacidad de sus aplicaciones en tiempo real, sin necesidad de preocuparse por la infraestructura subyacente.
- **Disponibilidad y fiabilidad:** AZURE Web Apps garantiza alta disponibilidad y fiabilidad de las aplicaciones web de ELTHON CEO. Esto se debe a que las aplicaciones se ejecutan en servidores redundantes, lo que asegura que el servicio esté disponible incluso en caso de que uno o varios servidores fallen.
- **Integración con otros servicios de AZURE:** AZURE Web Apps se integra perfectamente con otros servicios de AZURE, lo que significa que ELTHON CEO utiliza una amplia gama de servicios adicionales (microservicios- bases de datos entre otros), AZURE Blob Storage y AZURE Cosmos DB, para proporcionar capacidades adicionales a sus aplicaciones web.
- **Seguridad:** AZURE Web Apps proporciona seguridad de nivel empresarial para las aplicaciones web de ELTHON CEO. La plataforma ofrece diversas medidas de seguridad, como autenticación y autorización, protección DDoS, cifrado de datos y seguimiento de actividades de usuario, entre otros.

- **Facilidad de gestión:** AZURE Web Apps permite a ELTHON CEO administrar sus aplicaciones web de manera fácil y eficiente, ya que la plataforma proporciona herramientas de gestión intuitivas y amigables para el usuario. Esto incluye la capacidad de configurar, monitorizar y depurar aplicaciones web, así como la gestión de certificados SSL y la implementación continua.

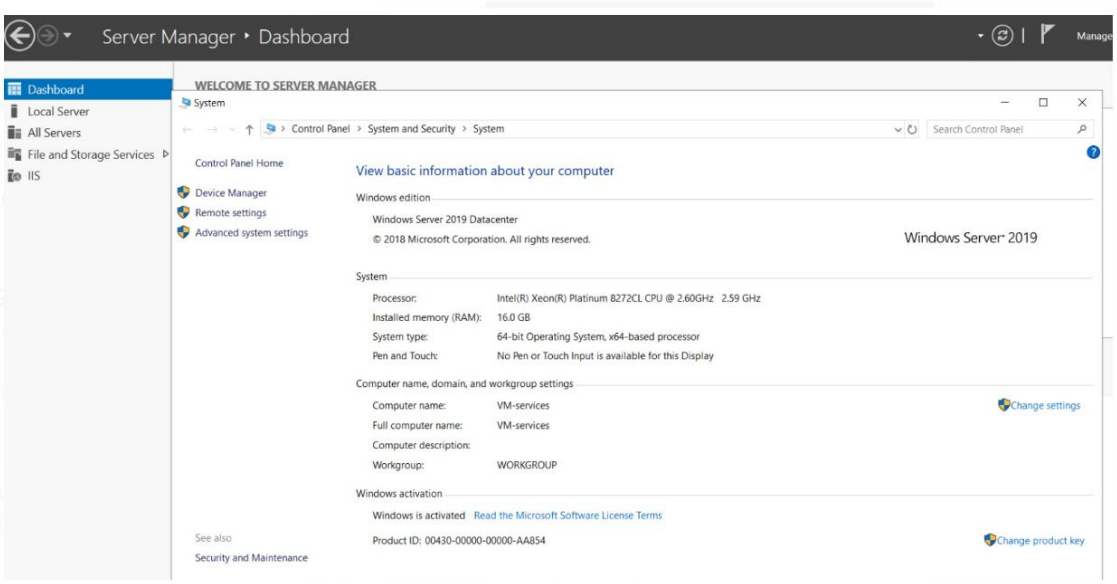
11.2.3. ARQUITECTURA DE RESPALDOS ELTHON: SERVIDOR

Para garantizar la integridad y disponibilidad de los datos, servicios y demás componentes de ELTHON CEO se ha implementado una arquitectura de respaldos adecuada a base de un servidor físico. La siguiente figura presenta un enfoque para respaldar y proteger los datos en el servidor ELTHON en caso de contingencia con el proveedor principal AZURE:



Servidor Físico

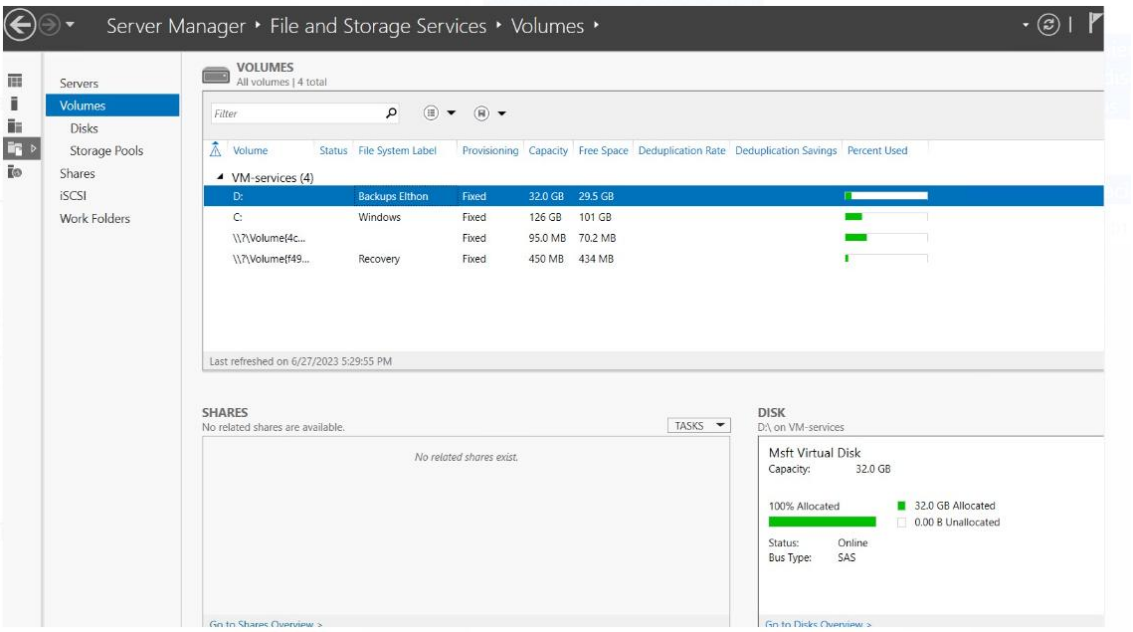
La siguiente muestra las especificaciones del software físico. Windows (Windows Server 2019 Datacenter)



Especificaciones de Software físico

ELTHON CEO define una estrategia clara de almacenamiento de respaldos que determinan la frecuencia, el tipo y la ubicación de los respaldos.

- Se ingresa la VPN
- Seguido de información crítica a respaldar (desarrollo y backups de elton)
- Se cifran los archivos a transmitir en el servidor.
- Se establece comunicación mediante el RDP
- Se transmiten los archivos cifrados al disco D: (BACKUPS ELTHON), la siguiente figura muestra las particiones del servidor.



Particiones del servidor

El servidor físico se usa para:

- respaldos de código,
- backup mensual,
- stack tecnológico y
- documentación de ELTHON CEO.

12. SEGURIDAD DE RED

La seguridad de red física es un aspecto fundamental para proteger los recursos y datos del servidor de ELTHON CEO contra amenazas internas y externas. Una solución efectiva para fortalecer la seguridad de la red es utilizar un firewall de próxima generación (NG Firewall), como NG Firewall Complete, junto con la implementación de una red privada virtual (VPN).

NG Firewall Complete es una solución integral que ofrece un conjunto de funciones avanzadas de seguridad de red, diseñadas para proteger y controlar el tráfico que entra y sale de la red del servidor. Estas características incluyen la inspección profunda de paquetes, filtrado de contenidos, prevención de intrusiones, control de aplicaciones y más.

Una de las funcionalidades más importantes de NG Firewall Complete es su capacidad para establecer y administrar conexiones VPN (Virtual Private Network). Una VPN permite crear una conexión segura y encriptada entre redes o dispositivos remotos a través de una red pública, como Internet. Esto garantiza la confidencialidad e integridad de la información transmitida a través de la VPN.

Los datos transmitidos a través de la VPN están protegidos mediante encriptación, lo que reduce el riesgo de interceptación o manipulación por parte de terceros no autorizados. Además de la funcionalidad VPN, NG Firewall Complete también ofrece otras capas de seguridad de red, como el control de aplicaciones. Esto permite a los administradores definir políticas para permitir o bloquear el acceso a aplicaciones específicas, lo que ayuda a prevenir amenazas y proteger la red de posibles ataques basados en aplicaciones maliciosas.

13. INFRAESTRUCTURA DE BASES DE DATOS EN AZURE

La infraestructura de bases de datos juega un papel crucial en el almacenamiento y procesamiento de la información relacionada con la gestión de riesgos y la administración de usuarios. Para lograr una alta disponibilidad, escalabilidad y rendimiento, se han utilizado múltiples bases de datos, cada una diseñada para una función específica. En esta sección, se describirán brevemente las bases de datos utilizadas en la arquitectura de ELTHON, así como su función y cómo se relacionan con otros componentes de la arquitectura.

INFRAESTRUCTURA GLOBAL DE AZURE

- Cada región de AZURE está conformada por uno o más centros de datos (Datacenter).
- Los centros de datos de AZURE están diseñados para ser altamente redundantes y escalables.
- Cada centro de datos de AZURE cuenta con múltiples capas de seguridad física y lógica para proteger la infraestructura y los datos de los clientes.
- AZURE utiliza una red global de fibra óptica para conectar los centros de datos y regiones entre sí, lo que permite una alta velocidad y baja latencia en la comunicación de los servicios y datos de AZURE.
- AZURE ofrece diversas opciones de almacenamiento de datos, incluyendo bases de datos relacionales como SQL Server y MySQL, almacenamiento de objetos como AZURE Blob Storage, almacenamiento de archivos como AZURE Files, y bases de datos NoSQL como AZURE Cosmos DB.
- AZURE cuenta con herramientas de administración y monitoreo para permitir a los usuarios visualizar y controlar su infraestructura y aplicaciones en tiempo real.
- AZURE tiene un enfoque de sostenibilidad y responsabilidad social, y busca utilizar energías renovables y reducir la huella de carbono de sus operaciones.

VENTAJAS DE LA INFRAESTRUCTURA PARA ELTHON

- **Alta disponibilidad:** AZURE garantiza una alta disponibilidad y escalabilidad, lo que permite que los sistemas de ELTHON estén siempre disponibles y puedan adaptarse a la demanda.
- **Seguridad:** AZURE proporciona múltiples capas de seguridad, incluyendo la autenticación, el control de acceso y la protección de datos, lo que ayuda a proteger los sistemas y datos de ELTHON contra posibles amenazas.
- **Integración con herramientas de desarrollo:** AZURE se integra con diversas herramientas de desarrollo, como Visual Code y GitLab, lo que facilita la implementación y el mantenimiento de los sistemas de ELTHON.
- **Flexibilidad:** AZURE ofrece una amplia gama de servicios y herramientas, lo que permite a ELTHON personalizar su infraestructura y adaptarla a sus necesidades específicas.
- **Escalabilidad**: AZURE permite a ELTHON escalar sus sistemas de forma horizontal o vertical, lo que permite ajustar la capacidad de los sistemas en función de la demanda en tiempo real.

- **Automatización:** AZURE ofrece diversas herramientas de automatización, como AZURE Automation y AZURE Function, lo que permite a ELTHON automatizar tareas repetitivas y mejorar la eficiencia de sus sistemas.
- **Analytics:** AZURE ofrece herramientas de análisis de datos, como AZURE Stream Analytics y AZURE Machine Learning, lo que permite a ELTHON obtener información valiosa sobre sus sistemas y usuarios, y mejorar su toma de decisiones.

13.1. BASE DE DATOS SQL SERVER DENTRO DE AZURE (INFORMACIÓN PRIVADA)

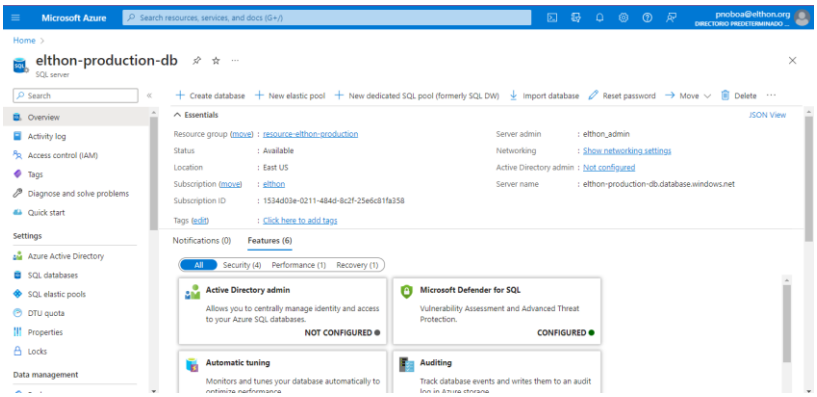
Es un servicio de base de datos relacional, que se ejecuta en una plataforma de computación en la nube y el acceso a ella se proporciona como un servicio. Además, para una base de datos administrada, el proveedor de servicios se ocupa de las necesidades operativas, como la escalabilidad, la copia de seguridad y la alta disponibilidad.

ELTHON

ELTHON utiliza la base de datos SQL Server para almacenar información privada, incluyendo datos de clientes y de la propia empresa. SQL Server es una base de datos relacional de Microsoft que ofrece un alto rendimiento y escalabilidad para aplicaciones empresariales de gran tamaño. Con SQL Server, ELTHON puede administrar grandes cantidades de datos (no Bigdata) de forma eficiente y confiable, y garantizar la integridad de los datos con sus características de seguridad integradas.

La replicación permite a ELTHON copiar y distribuir los datos en varias bases de datos en tiempo real, lo que permite la escalabilidad horizontal y la disponibilidad de los datos en caso de fallo del servidor. La copia de seguridad permite a ELTHON hacer copias periódicas de la base de datos y restaurar los datos en caso de un desastre.

Otra ventaja de SQL Server es su compatibilidad con herramientas y lenguajes de programación populares, lo que permite a los desarrolladores de ELTHON utilizar sus habilidades existentes y herramientas familiares para trabajar con la base de datos. Además, SQL Server también admite la integración con AZURE, lo que permite a ELTHON aprovechar la infraestructura de nube de Microsoft para administrar y escalar su base de datos de manera más eficiente.



Instancia Sql Server ELTHON.

INFRAESTRUCTURA

AZURE SQL Database se basa en la base de datos del servidor SQL y, por lo tanto, se mantiene sincronizada con la última versión mediante el uso de la base de código común. Dado que la versión en la nube de la tecnología de la base de datos se esfuerza por desvincularla de la infraestructura informática subyacente, no es compatible con algunas de las funciones de T-SQL específicas del contexto disponibles en el servidor SQL tradicional. Sin embargo, el resto de las características son las mismas con las incompatibilidades explicadas por Microsoft. AZURE SQL Database también es similar a la oferta de instancias administradas de SQL de Microsoft.

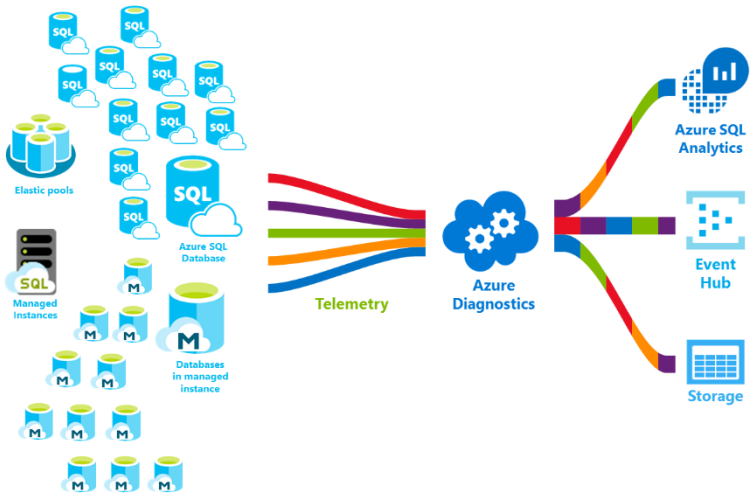


Diagrama de escalabilidad de Base de Datos Sql Server por Dtu.
Recuperado de https://learn.microsoft.com/es-es/azure/azure-sql/database/media/sql-database-paas-overview/architecture.png?view=azuresql

Características

- Aprendizaje continuo de los patrones de acceso a datos de la aplicación host, ajuste de rendimiento adaptativo y mejoras automáticas en la confiabilidad y protección de datos.
- Escalado bajo demanda.
- Gestión y supervisión de aplicaciones multiusuario con beneficios de aislamiento de un cliente por base de datos.
- Integración con herramientas de código abierto como Cheetah, sql-cli, Visual Studio Code, AZURE Management Portal, PowerShell, SQL Server Management Studio y REST API.
- Protección de datos con encriptación, autenticación, limitación del acceso del usuario al subconjunto de datos, monitoreo y auditoría continuos para ayudar a detectar amenazas potenciales y proporcionar un registro de eventos críticos en caso de una infracción.

13.1.1. BASE DE DATOS MONGODB (INFORMACIÓN PÚBLICA Y BIGDATA)

Es una base de datos “no SQL” de código abierto y escrito en C++ más utilizada en todo el mundo. Se trata de un sistema orientado a los documentos, es decir, los datos se almacenan en documentos. Esto significa que los campos presentes en los documentos pueden variar de unos a otros, así como la estructura de los datos puede cambiar con el tiempo. No obstante, este gestor ofrece una alta escalabilidad, flexibilidad y rapidez que lo diferencia del resto.

ELTHON

En el caso de ELTHON, el uso de MongoDB como base de datos para su información pública permite un manejo eficiente de grandes volúmenes de datos. Al ser una base de datos no relacional, permite una mayor flexibilidad en el diseño y estructura de los datos, lo que se adapta perfectamente a las necesidades de la aplicación. Además, MongoDB es altamente escalable y puede manejar grandes cantidades de datos, lo que lo convierte en una excelente opción para ELTHON, que maneja billones de datos en su plataforma.

Una de las ventajas de MongoDB es su capacidad para realizar consultas complejas en grandes conjuntos de datos. MongoDB utiliza un lenguaje de consulta muy poderoso que permite realizar consultas complejas y filtrar los datos de manera eficiente.

Además, MongoDB ofrece una serie de herramientas de análisis y agregación que permiten analizar y resumir grandes conjuntos de datos de manera eficiente. Esto hace

que MongoDB sea una excelente opción para aplicaciones que requieren un alto nivel de análisis de datos, como es el caso de ELTHON.

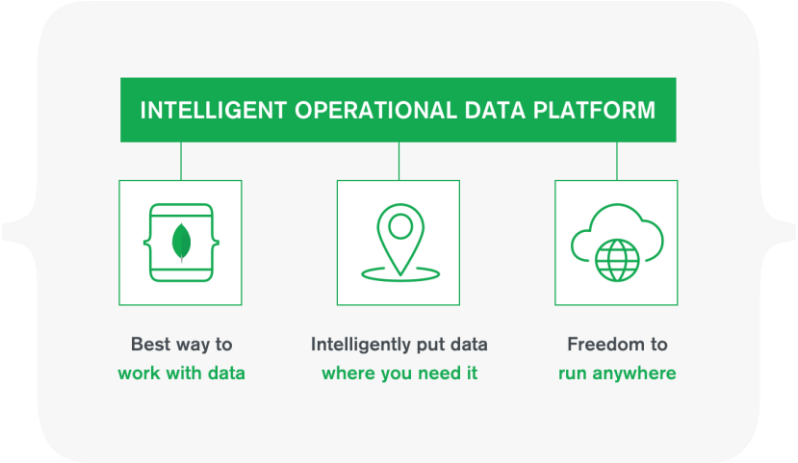


Diagrama Manejo de MongoDB
Recuperado de https://learn.microsoft.com/es-es/azure/azure-sql/database/media/sql-database-paas-overview/architecture.png?view=azuresql

Características

- MongoDB es una base de datos no relacional (NoSQL) que permite almacenar y procesar grandes cantidades de datos de forma escalable y distribuida.
- Ofrece una gran flexibilidad en cuanto al esquema de datos, lo que permite adaptarse fácilmente a cambios en los requerimientos de la aplicación.
- Es una base de datos documental, lo que significa que los datos se almacenan en documentos BSON (JSON binario) que pueden contener diferentes tipos de datos y estructuras anidadas.
- Ofrece herramientas de consulta avanzadas, incluyendo búsquedas textuales, geoespaciales y por expresiones regulares.

Ventajas de Infraestructura MongoDB instanciado en AZURE para ELTHON

- MongoDB es altamente escalable, permitiendo aumentar la capacidad de almacenamiento y procesamiento de datos de manera horizontal a través de la creación de clústeres.
- AZURE ofrece servicios gestionados de MongoDB que se encargan de la instalación, configuración y mantenimiento de la base de datos, liberando a ELTHON CEO de la necesidad de administrar la infraestructura subyacente.

- La integración de MongoDB con AZURE permite aprovechar las capacidades de la plataforma en términos de seguridad, disponibilidad y rendimiento.
- La flexibilidad en el esquema de datos de MongoDB permite una rápida adaptación a cambios en los requerimientos de la aplicación, lo que puede acelerar el desarrollo y lanzamiento de nuevas funcionalidades.
- La capacidad de procesar grandes cantidades de datos de forma eficiente permite a ELTHON CEO analizar y obtener insights valiosos de su información, lo que puede llevar a mejoras en la toma de decisiones y el desempeño del negocio.

13.1.2. BASE DE DATOS REDIS AZURE (GESTIÓN DE SESIONES)

La infraestructura de AZURE REDIS es una solución de almacenamiento en memoria basada en caché de alta velocidad y durabilidad que ofrece una forma eficiente de almacenar y recuperar datos en aplicaciones web y móviles. En el caso de ELTHON, se utiliza REDIS para gestionar las sesiones de los usuarios en su plataforma, permitiendo una experiencia de usuario más fluida y rápida. En este apartado se describirán las características y ventajas de usar AZURE REDIS como solución de almacenamiento en caché para las sesiones de los usuarios en la plataforma ELTHON.

El uso de REDIS para la gestión de sesiones en ELTHON ha permitido la persistencia de datos de sesión en la caché de REDIS, lo que significa que los usuarios pueden mantener su sesión incluso si se producen fallos de servidor. Esto se debe a que la información de sesión se guarda en caché en REDIS y no en la memoria del servidor, lo que reduce el riesgo de pérdida de datos y aumenta la disponibilidad de la aplicación. Además, REDIS también ofrece una amplia gama de funciones, como la gestión de listas, mapas y conjuntos de datos, que se han integrado en la aplicación de ELTHON para mejorar la funcionalidad y la eficiencia.

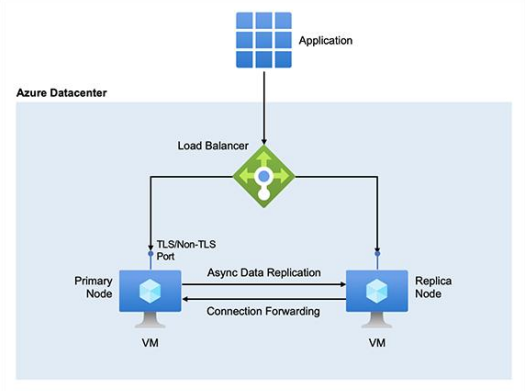


Diagrama Disponibilidad en Tiempo Real REDIS.
Recuperado de https://learn.microsoft.com/es-es/azure/azure-cache-for-redis/media/cache-high-availability/replication.png

Características

- REDIS es una base de datos en memoria, lo que significa que los datos se almacenan en la memoria RAM, lo que permite una alta velocidad en el acceso y recuperación de los datos.
- REDIS soporta varios tipos de estructuras de datos, incluyendo cadenas, listas, conjuntos, mapas hash y más. Esto proporciona una gran flexibilidad en el almacenamiento de datos.
- REDIS ofrece una funcionalidad de pub/sub (publicación y suscripción) que permite a las aplicaciones enviar y recibir mensajes de forma asincrónica. Esto es especialmente útil para la construcción de aplicaciones en tiempo real o para procesos de notificación.
- REDIS también soporta la persistencia de datos, lo que significa que los datos pueden ser almacenados en disco y recuperados en caso de un fallo en el sistema o un reinicio del servidor, a menos que pase el tiempo de duración del registro en ese caso se elimina automáticamente.

Ventajas

- El uso de REDIS como manejo de sesiones por cache puede mejorar significativamente el rendimiento de las aplicaciones web de ELTHON, ya que reduce la carga en el servidor y mejora el tiempo de respuesta para los usuarios.
- REDIS es altamente escalable, lo que significa que puede manejar grandes cantidades de datos y usuarios sin sacrificar la velocidad y el rendimiento.
- Al estar alojado en AZURE, REDIS ofrece una gran disponibilidad y redundancia para garantizar que los datos estén siempre accesibles y seguros.
- REDIS es una tecnología de código abierto y tiene una gran comunidad de desarrolladores que constantemente están trabajando en mejoras y nuevas funcionalidades. Esto significa que hay una gran cantidad de recursos y herramientas disponibles para ELTHON en caso de necesitar soporte o ayuda en el uso de REDIS.

13.1.3. INFRAESTRUCTURA DE RED INTERNA ELTHON

La infraestructura de red interna de ELTHON es una parte fundamental de nuestra estructura tecnológica que nos permite garantizar la conectividad y el intercambio de información eficiente dentro de nuestra organización. Nuestra infraestructura de red interna está diseñada para cumplir con los más altos estándares de seguridad y

confiabilidad, con el objetivo de proteger la integridad y la confidencialidad de la información que circula a través de ella.

Se formula los siguientes puntos como bases de la construcción de la red:

- Contar con una arquitectura de red robusta y escalable que nos permite satisfacer las necesidades de comunicación de nuestros empleados, departamentos y sistemas. Utilizamos una combinación de tecnologías cableadas e inalámbricas para asegurar una cobertura completa y una conectividad confiable en todas nuestras instalaciones.
- Implementamos una serie de medidas de seguridad en nuestra infraestructura de red interna. Esto incluye el uso de firewalls de última generación que controlan y filtran el tráfico de red, permitiendo únicamente el acceso autorizado y previniendo cualquier intento de intrusión o acceso no autorizado a nuestros sistemas.
- Utilizar tecnologías de detección y prevención de intrusiones para monitorear y proteger nuestra red contra posibles amenazas externas.
- En cuanto a la segmentación de la red, implementar una estructura de red jerárquica que divida nuestra infraestructura en subredes más pequeñas y seguras.
- Cada departamento o área de la organización tiene su propia subred, lo que permite aplicar políticas de acceso y control de manera más granular. Esto nos ayuda a minimizar el riesgo de propagación de amenazas y limitar el acceso no autorizado a la información sensible.

13.1.3.1. NG FIREWALL COMPLETE

NG Firewall proporciona una interfaz intuitiva, receptiva y basada en navegador que le permite obtener rápidamente visibilidad del tráfico en la red. Desde el filtrado de contenido hasta la protección avanzada contra amenazas, la conectividad VPN y la configuración basada en aplicaciones para la optimización del ancho de banda, NG Firewall ofrece una plataforma de seguridad de red integral y de nivel empresarial para organizaciones de cualquier industria.

13.1.3.2. BANDWIDTH CONTROL

ELTHON utiliza la aplicación Bandwidth Control que es parte del conjunto de herramientas de NG Firewall, esto permite a los administradores:

- Garantizar la calidad del servicio (QoS), permitiendo utilizar los recursos de ancho de banda de manera eficiente y ahorre dinero.
- Priorizar el ancho de banda lejos del uso recreativo y hacia aplicaciones críticas para el negocio como VOIP, aplicaciones comerciales basadas en la nube o videoconferencias.

- Supervisar y realizar un seguimiento de los abusadores de ancho de banda por usuario, aplicación, protocolo, sitio web, etc. para determinar el origen de los problemas de ancho de banda.
- Establecer cuotas para la cantidad de datos que se pueden usar durante un tiempo determinado. Se combina con reglas para tomar automáticamente una acción (como bloquear) cuando se exceda esa cuota.
- Responder automáticamente a los abusadores de ancho de banda a través de una variedad de técnicas que incluyen bloqueo, cuotas u otras sanciones.

13.1.3.3. WAN BALANCER

ELTHON utiliza la aplicación WAN Balancer que es parte del conjunto de herramientas de NG Firewall, esto permite a los administradores:

- Maximizar el rendimiento y el rendimiento acumulados de su red al distribuir el tráfico según reglas simples.
- Lograr el rendimiento de las líneas dedicadas de alto costo al equilibrar las conexiones a Internet de menor costo.
- Múltiples conexiones a Internet también brindan el beneficio de proporcionar capacidad de conmutación por error en caso de que falle una o más de sus conexiones.
- Nota: Requiere una tarjeta de red dedicada y un espacio de dirección IP único para cada conexión a Internet. WAN Balancer equilibra el rendimiento agregado, pero no aumenta el rendimiento de ninguna conexión a Internet individual.

13.1.3.4. WAN FAILOVER

ELTHON utiliza la aplicación WAN Failover que es parte del conjunto de herramientas de NG Firewall, esto permite a los administradores:

- Definir los criterios de conmutación por conexión, brindándole un control total.
- Registrar todo el tiempo de inactividad de cada conexión.
- Nota: Requiere una tarjeta de red dedicada y un espacio de dirección IP único para cada conexión a Internet. WAN Balancer aumenta el rendimiento agregado, pero no aumenta el rendimiento de ninguna conexión a Internet individual.

13.1.3.5. WEB CACHE

ELTHON utiliza la aplicación Web Caché que es parte del conjunto de herramientas de NG Firewall, esto permite a los administradores:

- Mejorar el rendimiento de carga de la página.
- Reducir la latencia de la red y mejorar las velocidades percibidas.
- Eliminar las solicitudes repetidas de contenido de uso frecuente, liberando recursos para otras solicitudes.

13.1.3.6. CAPTIVE PORTAL

ELTHON utiliza la aplicación Captive Portal que es parte del conjunto de herramientas de NG Firewall, esto permite a los administradores:

- Requerir que los usuarios vean y/o acepten una Política de uso aceptable antes de acceder a Internet.
- Autentique a los usuarios contra el directorio local de NG Firewall, RADIUS o Microsoft Active Directory (requiere Directory Connector). Autenticar a los usuarios a través de cuentas de Google, Facebook u Office 365 directamente.
- Configurar el portal cautivo para que se muestre solo en un subconjunto de su red.
- Separar los dispositivos móviles en un rack diferente con diferentes políticas para entornos BYOD (traiga su propio dispositivo). Las páginas cautivas se pueden mostrar por sistema operativo y/o tipo de dispositivo. Muestre diferentes páginas del portal cautivo a usuarios inalámbricos y con cable.
- Personalizar la apariencia de la página del portal cautivo.
- Mostrar una página de advertencia cuando el usuario supera la cuota o se agrega al cuadro de penalización por mal comportamiento.
- Diseñar integraciones personalizadas en Python.
- Usar direcciones MAC para rastrear dispositivos, eliminando la necesidad de volver a autenticar los dispositivos.
- Bloquear sitios SS

13.1.3.7. IPSEC VPN

ELTHON utiliza la aplicación Ipsec VPN que es parte del conjunto de herramientas de NG Firewall, esto permite a los administradores:

- Proporcionar comunicaciones seguras de Protocolo de Internet (IP) al autenticar y cifrar cada paquete IP de una sesión de comunicación
- Utilizar tecnología de seguridad de vanguardia, compatible con túnel completo o túnel dividido, integrado con L2TP y XAUTH.
- Utilizar L2TP que proporciona autenticación simple sin necesidad de software de terceros.
- Utilizar túnel de malla completa sin licencias por túnel.

- Utilizar túneles GRE a sitios remotos.
- Forzar VPN bajo demanda con autenticación basada en certificación.
- Detectar los estados del túnel VPN inmediatamente y reinicie automáticamente un túnel en caso de que se corte la conexión.

13.1.3.8. DIRECTORY CONNECTOR

ELTHON utiliza la aplicación Directory Connector que es parte del conjunto de herramientas de NG Firewall, esto permite a los administradores:

- Omitir la creación de nuevos usuarios y grupos cuando puede heredarlos directamente de su Active Directory, RADIUS o el directorio local de NG Firewall.
- Inicio de sesión de usuario opcional a través de la secuencia de comandos de inicio de sesión de notificación de usuario; una vez que los usuarios inician sesión en su PC, inician sesión automáticamente en la red.
- Generar informes y la gestión de políticas con nombres de usuario y grupos que provienen directamente del directorio.
- Conectarse a varios servidores de Active Directory.

13.1.3.9. POLICY MANAGER

ELTHON utiliza la aplicación Police Manager que es parte del conjunto de herramientas de NG Firewall, esto permite a los administradores:

- Personalizar la red en función del tiempo: horario de oficina, después del horario de atención, horario de tareas, horario de almuerzo y más.
- Configurar diferentes políticas para distintas horas/días de la semana.
- Registrar e informar automáticamente sobre el comportamiento del sistema y del usuario, lo que le permite monitorear y controlar su red.

13.1.3.10. REPORTS

ELTHON utiliza la aplicación reports que es parte del conjunto de herramientas de NG Firewall, esto permite a los administradores:

- Informes resumidos, detallados y por usuario
- Envío automatizado de informes por correo electrónico / Archivo de informes
- Informe datos disponibles en formato CSV
- Informes para identificar datos para hosts, usuarios u otros criterios de interés

13.1.3.11. FIREWALL

ELTHON utiliza la aplicación Firewall de código abierto y gratuito bajo la Licencia Pública General GNU que es parte del conjunto de herramientas de NG Firewall, esto permite a los administradores:

- Bloquear sesiones fácilmente según reglas simples que se basan en una variedad de atributos.

13.1.3.12. INTRUSION PREVENTION

ELTHON utiliza la aplicación Intrusion Prevention de código abierto y gratuito bajo la Licencia Pública General GNU que es parte del conjunto de herramientas de NG Firewall, esto permite a los administradores:

- Miles de firmas para una variedad de ataques.
- Valores predeterminados cuidadosamente seleccionados ajustados continuamente para una protección óptima.
- Nuevas firmas de ataque se descargan automáticamente en su servidor.

13.1.3.13. PHISH BLOCKER

ELTHON utiliza la aplicación Phish Blocker de código abierto y gratuito bajo la Licencia Pública General GNU que es parte del conjunto de herramientas de NG Firewall, esto permite a los administradores:

- Bloquear el correo electrónico de phishing en SMTP.
- Bloquear sitios web "pharming" maliciosos.
- Registro de eventos de phish capturado.
- Los informes muestran cuántos correos electrónicos fraudulentos se detuvieron, a quién se dirigían y desde dónde se enviaron.

13.1.3.14. THREAT PREVENTION

ELTHON utiliza la aplicación Threat Prevention que es parte del conjunto de herramientas de NG Firewall, esto permite a los administradores:

- Bloquear el acceso a las direcciones IP según el índice de reputación de IP de Webroot BightCloud®.
- Revisar y escanear todo el tráfico cifrado.

13.1.3.15. VIRUS BLOCKER

ELTHON utiliza la aplicación Virus Blocker que es parte del conjunto de herramientas de NG Firewall, esto permite:

- Utilizar Bitdefender premiado como "Mejor protección" y "Mejor rendimiento" por AV-Test.
- Detiene más malware que cualquier otro software (tasa de detección del 99,8%).
- Protege contra toda la gama de tráfico de Internet: HTTP, FTP y SMTP.
- Descomprime y escanea archivos y archivos comprimidos: Zip, RAR, Tar, Gzip, Bzip2, MS OLE2, MS Cabinet Files, MS CHM y MS SZDD; incluso protegiendo contra complejas bombas de archivo.
- Menos falsos positivos significa menos interrupción del flujo de datos y de los usuarios.
- Usted define cómo se maneja el correo electrónico infectado (eliminar, bloquear, transferir) y cualquier notificación (remitente y/o destinatario).
- Detecta clientes infectados que se unen a su red y evita que llamen a casa.

13.1.3.16. AD BLOCKER

A través de esta herramienta ELTHON realiza lo siguiente:

- Se bloquea la mayoría del contenido publicitario que se entrega a los usuarios en las páginas web que solicitan.
- Se usa suscripciones de filtro descargables de una variedad de fuentes que contienen listas de sitios web y extensiones que normalmente se usan para entregar publicidad.

13.1.3.17. APPLICATION CONTROL Y APPLICATION CONTROL LITE

Para mejorar la productividad ELTHON utiliza las aplicaciones de Application Control y Application Control Lite Control, estas son sus funcionalidades:

- Estas herramientas ayudan a controlar los drenajes de productividad, los acaparadores de ancho de banda y las aplicaciones ágiles de protocolo utilizadas para la omisión de filtros.
- Funciona en conjunto con Web Filter, SSL Inspector, Bandwidth Control y Policy Manager para brindar las herramientas que necesita para hacer cumplir la política de uso y ver dónde se gastan recursos de red.

- Con esto nos aseguramos que los usuarios puedan acceder a aplicaciones basadas en la nube de misión crítica, mientras mantienen las aplicaciones recreativas o inapropiadas fuera de la red.
- Se realiza una inspección profunda de paquetes (DPI) y de flujo profundo (DFI) del tráfico de la red, lo que le permite identificar con precisión miles de aplicaciones comunes, como redes sociales, P2P, mensajería instantánea, transmisión de video, uso compartido de archivos, aplicaciones empresariales y mucho más.

13.1.3.18. SPAM BLOCKER Y SPAM BLOCKER LITE

Debido a que el 80% de todo el correo electrónico es spam, phishing o fraude por correo electrónico. ELTHON utiliza la aplicación Spam Blocker y Spam Blocker Lite que es parte del conjunto de herramientas de NG Firewall, esto permite a los administradores:

- Evitar que los usuarios desperdicien un promedio de 100 horas al año limpiando la bandeja de entrada.
- Reducir frustraciones y las pérdidas financieras reales causadas por correos electrónicos maliciosos.

13.1.3.19. SSL INSPECTOR

ELTHON utiliza la aplicación SSL Inspector con los siguientes propósitos:

- Analizar el tráfico, identificar amenazas o manejar violaciones de políticas.
- Colocar a NG Firewall en medio del tráfico cifrado, con la capacidad de descifrar y analizar los datos a medida que pasan.
- Crear un certificado especializado en cada cliente. Este certificado se comunica directamente con la puerta de enlace, que luego puede descifrar el tráfico HTTPS y SMTP, procesarlo y volver a cifrarlo sobre la marcha, todo desde NG Firewall, sin exponer nunca el tráfico descifrado a la red.
- Inspeccionar el tráfico HTTPS de la misma manera que el tráfico HTTP normal, lo que significa que se pueden aplicar todas las aplicaciones de NG Firewall y sus reglas

13.1.3.20. WEB FILTER

ELTHON utiliza la aplicación de Web Filter que es parte del conjunto de herramientas de NG Firewall para permitir a los administradores lo siguiente:

- Garantizar la seguridad web y del contenido en toda la red.
- Crear políticas fácil y rápidamente para bloquear el acceso a pornografía, juegos de apuestas, videos, redes sociales, sitios de compras u otro contenido y aplicaciones indeseables o inapropiados.
- Monitorear o controlar fácilmente las búsquedas en los motores de búsqueda populares, incluidos Google, YouTube, Ask, Bing y Yahoo.
- Aplicar búsquedas seguras en YouTube, así como búsquedas de registros, lo que le brinda un grado de visibilidad y control sin precedentes, ideal para entornos sensibles al contenido, como escuelas, bibliotecas públicas y organizaciones de servicios sociales.
- Permitir el acceso a contenido inapropiado puede reducir la productividad, crear distracciones o incluso dar lugar a acciones legales. Web Filter es una forma rápida, fácil y eficaz de asegurarse de que los usuarios no abusen de sus políticas de uso de la red.

13.1.3.21. WEB MONITOR

ELTHON utiliza la aplicación de Web Monitor que es parte del conjunto de herramientas de NG Firewall, esto permite a los administradores:

- Categorizar las solicitudes de sitios web, brindándoles una visibilidad completa del tráfico web.
- Incluye una clasificación con la base de datos de URL más grande de su tipo en 79 categorías, incluidas las categorías de alto riesgo, con más de 750 millones de dominios y más de 32 mil millones de URL clasificadas en más de 45 idiomas.
- Web Monitor evalúa 6 millones de IP peligrosas correlacionadas con URL. A medida que se visitan los sitios, se categorizan dinámicamente mediante búsquedas basadas en la nube para la categorización en tiempo real
- categoriza el tráfico HTTPS usando SNI y/o cualquier información de certificado.
- Es perfecto para organizaciones que necesitan monitorear, no controlar, la actividad web. Para controlar el tráfico web o la actividad del motor de búsqueda (bloqueo, marca, alerta), se requiere el filtro web

14. MODELADO DE DATOS Y CREACIÓN DE LA BASE DE DATOS DE ELTHON

En esta sección, se detallará el proceso de creación del modelo de datos relacional, scripts SQL y la creación de la base de datos de ELTHON en el entorno de AZURE. Este proceso es fundamental para el correcto funcionamiento de las aplicaciones y servicios de ELTHON, ya que es la base sobre la cual se construyen y almacenan los datos.

Para la creación del modelo de datos, se ha utilizado un enfoque relacional, lo que permite establecer relaciones entre las diferentes tablas de la base de datos. Además, se ha tenido en cuenta el rendimiento y la escalabilidad de la base de datos, para garantizar que pueda manejar grandes cantidades de datos de manera eficiente y sin comprometer el rendimiento de las aplicaciones. Una vez definido el modelo de datos, se han creado los scripts SQL necesarios para la creación de la base de datos en AZURE. Estos scripts incluyen la creación de tablas, índices, claves foráneas y otros objetos necesarios para el correcto funcionamiento de la base de datos. Además, se han definido políticas de retención de datos y de backup para garantizar la disponibilidad y la integridad de los datos almacenados en la base de datos.

14.1. MODELADO CDM

El modelado de la base de datos es una etapa fundamental en el desarrollo de cualquier sistema informático, ya que permite establecer la estructura y organización de los datos que se van a manejar. En el caso de ELTHON, se ha optado por utilizar un modelo conceptual de datos (CDM, por sus siglas en inglés) para representar la estructura de su base de datos. El CDM es una representación gráfica de alto nivel que describe las entidades, atributos y relaciones que componen la base de datos.

Para construir el CDM de ELTHON, se parte de una tabla de Excel que contiene la información relevante sobre las tablas, relaciones, atributos compartidos y sus atributos individuales. A partir de esta información, se procede a identificar las entidades y las relaciones entre ellas, lo que permite construir un diagrama que representa el esquema de la base de datos.

El modelo CDM es una herramienta de gran utilidad para el equipo de desarrollo de ELTHON, ya que permite tener una visión clara y estructurada de la base de datos y facilita la tarea de definir las tablas y los campos correspondientes en el sistema de gestión de bases de datos (DBMS).

Es importante destacar que el proceso de modelado de la base de datos es una tarea que requiere una cuidadosa planificación y un análisis detallado de los requisitos del sistema.

Por lo tanto, es necesario contar con un equipo de profesionales experimentados en el diseño y la implementación de bases de datos. Además, es necesario contar con herramientas adecuadas para el modelado, como software especializado en la creación

de diagramas de entidad-relación (ERD) y CDM. En este sentido, el uso de herramientas de software especializado, combinado con la experiencia y el conocimiento del equipo de desarrollo de ELTHON, ha sido fundamental para el éxito en el modelado de su base de datos.

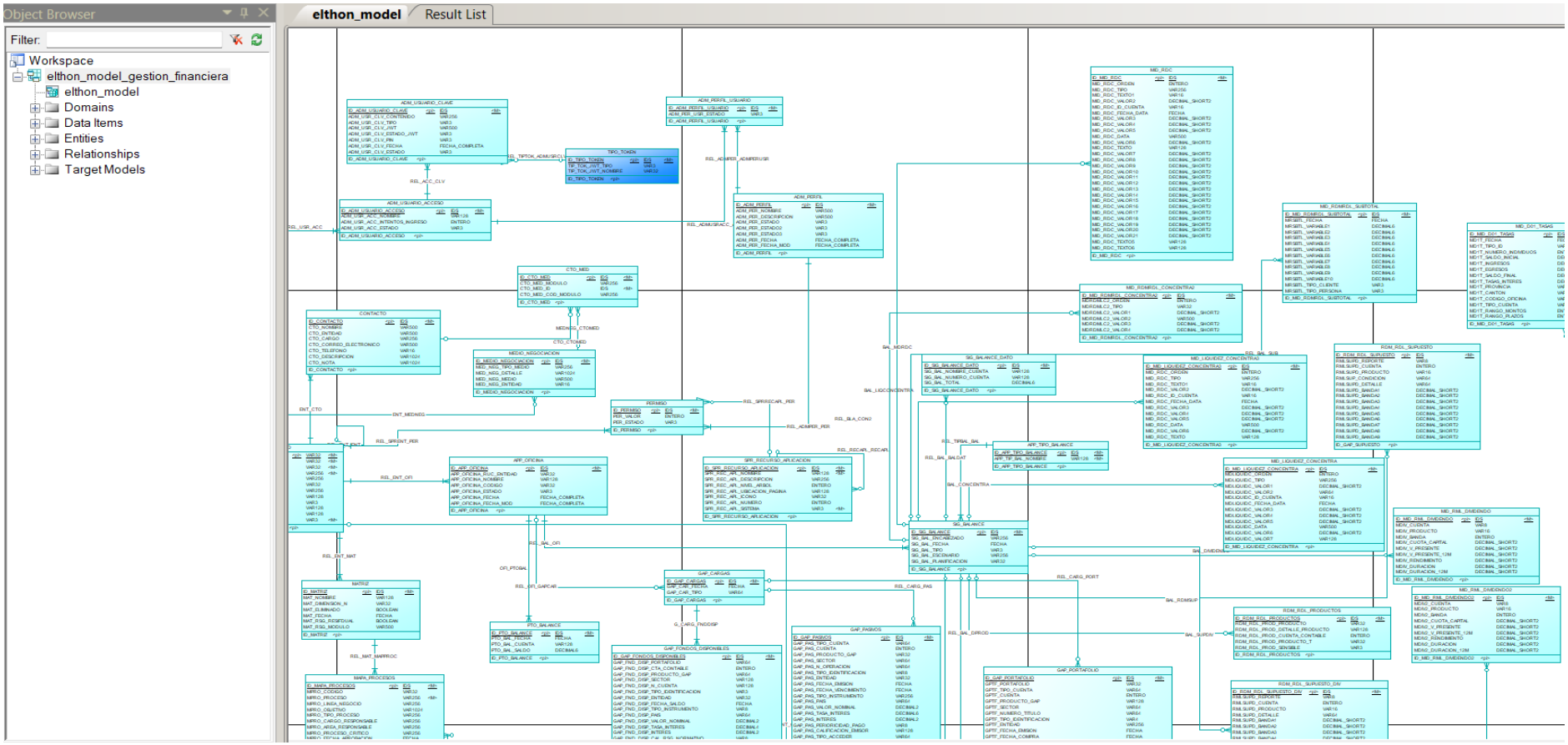


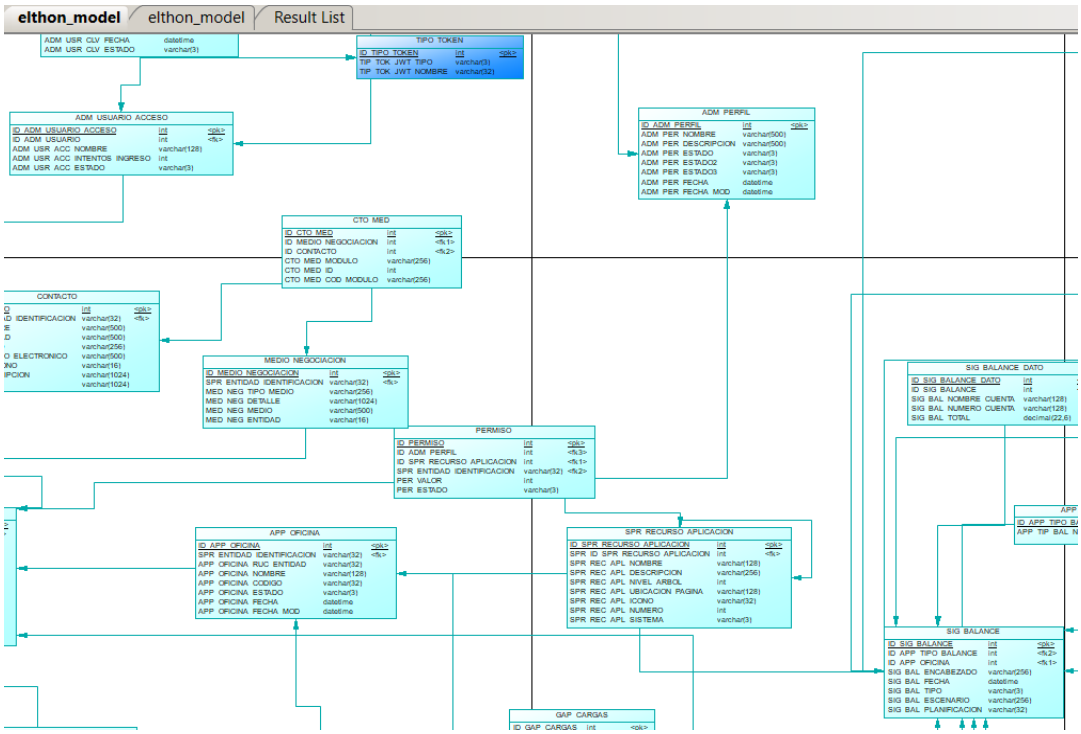
Diagrama CDM de ELTHON

14.2. MODELADO FÍSICO

Una vez que se ha completado la fase de modelado lógico de la base de datos, el siguiente paso es llevar a cabo el modelado físico. El modelado físico implica la implementación concreta de la base de datos utilizando un sistema de gestión de bases de datos específico. En este caso, el sistema de gestión de bases de datos utilizado por ELTHON es Microsoft SQL Server.

Durante el modelado físico, se definirán los detalles técnicos de la implementación de la base de datos, tales como la definición de las tablas, la creación de índices, la definición de las restricciones de integridad referencial y la creación de procedimientos almacenados. Además, también se definirán las opciones de configuración específicas del sistema de gestión de bases de datos que se utilizará.

El objetivo principal del modelado físico es garantizar que la base de datos implementada sea eficiente, escalable y esté optimizada para su uso en el sistema específico en el que se integrará. Para lograr esto, se deben tener en cuenta factores como la cantidad de datos que se manejarán, la frecuencia de las consultas y el rendimiento del hardware disponible. Además, también se debe garantizar que la base de datos sea segura y cumpla con los estándares de seguridad de la organización.



Ejemplo Diagrama Modelado Físico de ELTHON.

14.3. GENERACIÓN SCRIPT DATABASE

La generación de scripts es un paso crucial en el proceso de creación y mantenimiento de una base de datos. Una vez que se ha completado el modelado físico de la base de datos, se pueden generar scripts que contengan las instrucciones necesarias para crear la estructura de la base de datos, incluyendo las tablas, los índices y los atributos. Estos scripts son esenciales para garantizar que la base de datos se cree de manera consistente y confiable en diferentes entornos.

En el caso de ELTHON, la generación de scripts se realiza utilizando herramientas especializadas para la gestión de bases de datos. Estas herramientas permiten crear scripts personalizados que se ajusten a las necesidades específicas de la base de datos de ELTHON, como la inclusión de nuevas tablas, atributos y restricciones. Una vez que se ha generado el script, se puede utilizar para crear la base de datos en un nuevo entorno o para actualizar una base de datos existente.

La generación de scripts también es útil para el mantenimiento continuo de la base de datos. Cuando se realizan cambios en la estructura de la base de datos, como la adición de nuevas tablas o la modificación de los índices, se pueden generar nuevos scripts para garantizar que los cambios se implementen de manera consistente en todos los entornos. Además, la generación de scripts permite a los desarrolladores y administradores de bases de datos documentar y controlar los cambios en la base de datos, lo que puede ser útil para la auditoría y el cumplimiento de normas.

Name	Last commit
Indexes	GAP model
Scripts-Datos	update model
Scripts	Merge branch 'main' of gitlab.com-risk:elthon/resourc...
elthon-model-db	update model
resources-elthon	GAP model

Distribución Scripts de ELTHON.

IMPORTANCIA DEL BUEN MANEJO DE SCRIPTS PARA ELTHON

- **Facilita la gestión de versiones:** al guardar los scripts en el CDM, se puede tener un control sobre las diferentes versiones de la base de datos y de los cambios realizados. Esto es importante para mantener la coherencia y consistencia en la estructura y contenido de la base de datos.
- **Permite la colaboración y trabajo en equipo:** al tener los scripts de creación y modificación en el CDM, diferentes equipos pueden trabajar en la misma base de datos y colaborar en la gestión de cambios y mejoras de manera más eficiente y coordinada.
- **Mejora la documentación y la trazabilidad:** los scripts guardados en el CDM son una fuente de documentación sobre la estructura y evolución de la base de datos. Esto permite una mayor trazabilidad y comprensión de la historia y los cambios realizados en la base de datos.
- **Facilita la automatización y despliegue:** al tener los scripts guardados en el CDM, es posible automatizar la creación y modificación de tablas, índices y atributos, lo que facilita el despliegue y la gestión de la base de datos en diferentes ambientes.
- **Facilita el mantenimiento:** Al tener los scripts de creación de tablas y cambios de atributos guardados en el CDM, se facilita el mantenimiento de la base de datos. En caso de que sea necesario modificar algún atributo o añadir una nueva tabla, se puede acceder al script correspondiente y realizar los cambios necesarios sin tener que empezar desde cero.
- **Permite replicar la base de datos:** Los scripts de creación de tablas y cambios de atributos son esenciales para replicar la base de datos en diferentes entornos, como el de desarrollo, prueba o producción. Al contar con los scripts actualizados y guardados en el CDM, se puede replicar la estructura de la base de datos de manera rápida y eficiente en cualquier entorno.
- **Ayuda a mantener la consistencia:** El uso de scripts de creación de tablas y cambios de atributos en la base de datos permite mantener la consistencia en la estructura de la base de datos. Esto evita errores en la manipulación de la información y asegura que la información esté organizada de la manera adecuada para su uso.

14.4. PROCESO DE GESTIÓN DEL MODELADO DE BASE DE DATOS ELTHON

El proceso de modelado de bases de datos de ELTHON, basado en el uso de archivos Excel y la posterior creación de scripts de tablas y atributos, es una de las mejores prácticas que se pueden llevar a cabo para garantizar la calidad, coherencia y consistencia de los datos que maneja la empresa. Este enfoque permite que los especialistas en la materia puedan diseñar y modelar las tablas y relaciones de forma precisa, y que los jefes de TI puedan supervisar y validar el trabajo de los especialistas para garantizar que se cumplan los objetivos del proyecto.

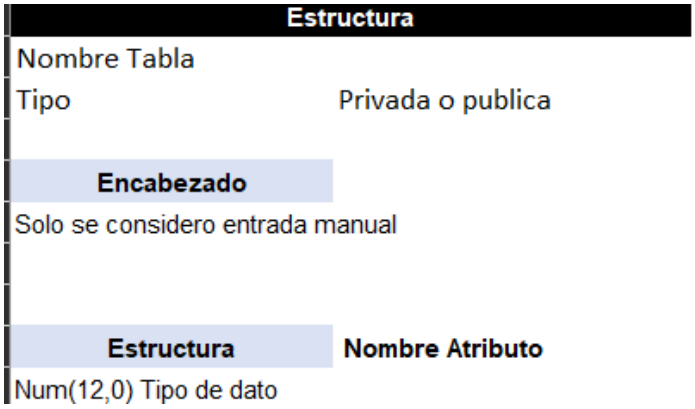
El proceso de modelado de bases de datos de ELTHON se puede describir en los siguientes pasos:

- **Diseño y construcción del archivo Excel:** en este paso, el especialista en la materia del sistema y módulo correspondiente se encarga de analizar, resolver y armar el archivo Excel con las tablas, atributos y relaciones necesarios para el proyecto. Este paso es crucial ya que una buena planificación y diseño en este punto pueden ahorrar tiempo y recursos en las fases posteriores del proceso.
- **Análisis del archivo Excel:** en este paso, el jefe de TI se encarga de analizar y validar el archivo Excel para garantizar que se cumplen los estándares y requisitos de la empresa. Además, se revisa la coherencia y consistencia de los datos para evitar problemas posteriores en la fase de implementación.
- **Creación del modelo conceptual y físico:** Pasos detallados en anteriores puntos, este modelo incluye información detallada sobre los tipos de datos, las restricciones de integridad y las relaciones entre las tablas.
- **Creación del script de la base de datos:** con el modelo físico de la base de datos listo, se procede a la creación del script de la base de datos. Este script incluye todas las instrucciones necesarias para crear las tablas, índices, atributos y relaciones en la base de datos.
- **Implementación del modelo de la base de datos:** finalmente, se implementa el modelo de la base de datos en el sistema de la empresa.

Ventajas

- El uso de Excel como herramienta de modelado permite una visualización clara y estructurada de la información que se desea incluir en la base de datos, lo que facilita la comunicación y el entendimiento entre los miembros del equipo.
- La revisión del Excel por parte del jefe de TI asegura que la estructura de la tabla y las relaciones entre atributos sean consistentes con los estándares del sistema, lo que mejora la calidad y la integridad de los datos.
- La creación de un script único para cada tabla asegura que los cambios sean controlados y trazables, lo que minimiza el riesgo de errores y garantiza la consistencia en la base de datos.
- La asociación de microservicios con cada tabla facilita la implementación de funcionalidades específicas para cada módulo del sistema, lo que permite una mayor flexibilidad y escalabilidad del sistema.

En resumen, el proceso de manejo de base de datos de ELTHON se destaca por su rigurosidad y atención a los detalles en cada etapa del ciclo de vida de la base de datos. Desde la creación del modelo de datos, hasta la generación de los scripts para la creación de tablas y conexión con los microservicios, cada paso es cuidadosamente planificado y ejecutado. Esto asegura que la base de datos se ajuste perfectamente a las necesidades de la empresa y sea fácil de mantener y actualizar en el futuro.



Estructura del Excel para Modelado de Tablas de ELTHON.

DESCRIPCIÓN EXCEL

- La estructura en el Excel permite definir el nombre de la tabla y su tipo de información, lo que facilita la comprensión de la información que se va a almacenar y su clasificación como pública o privada. Esto es importante para garantizar el cumplimiento de las normativas de privacidad y seguridad de la información.
- El encabezado que se liga a un tipo de estructura permite relacionar tablas entre sí, lo que es fundamental para el correcto funcionamiento del sistema y la gestión de la información. Además, esta relación se puede definir en el modelo CDM, lo que facilita la visualización de las relaciones entre las diferentes tablas y su integración en el modelo físico.
- Los atributos que se especifican en el Excel incluyen información importante como el tipo de dato, el tamaño y el nombre descriptivo. Esta información es fundamental para el correcto diseño de la base de datos, ya que permite definir la estructura de cada tabla y la información que se va a almacenar. Además, esta información se puede utilizar para la generación de scripts de creación de tablas y atributos, lo que ahorra tiempo y reduce la posibilidad de errores humanos en la creación de la base de datos.

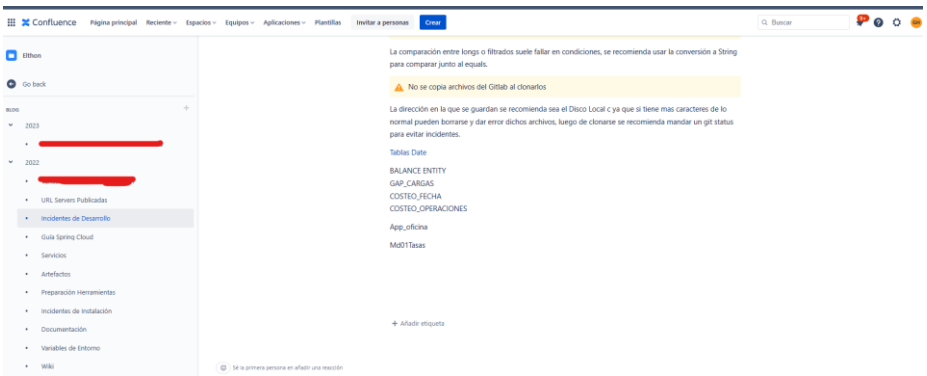
15. HERRAMIENTAS DE SOPORTES TÉCNICO

Para el correcto desarrollo y mantenimiento de los proyectos en ELTHON, se hace uso de diferentes herramientas de soporte técnico. Estas herramientas están diseñadas para facilitar la colaboración y comunicación entre los miembros del equipo, mejorar la eficiencia del proceso de desarrollo y garantizar la calidad del software desarrollado.

A continuación, se describirán las herramientas más utilizadas por el equipo de desarrollo de ELTHON y sus principales ventajas:

CONFLUENCE

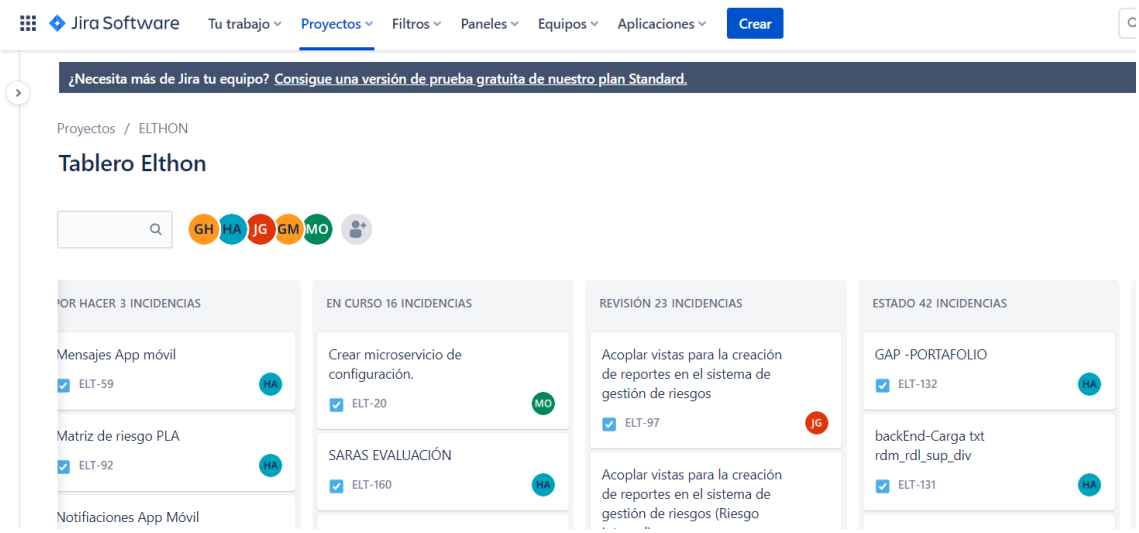
Esta herramienta se utiliza para crear, compartir y colaborar en la documentación del proyecto. Confluence permite crear páginas web con información de proyecto, documentación, especificaciones técnicas, entre otros, de manera fácil y organizada. Además, Confluence permite la colaboración en tiempo real y la gestión de versiones de los documentos, lo que facilita el trabajo en equipo y garantiza la actualización de la documentación.



Confluence ELTHON.

JIRA

Esta herramienta se utiliza para la gestión de tareas, seguimiento de errores y seguimiento de la evolución del proyecto. Jira permite la creación y asignación de tareas, la programación de entregas y la planificación del proyecto. Además, Jira permite la gestión y seguimiento de errores y problemas, lo que permite un enfoque proactivo en la identificación y resolución de problemas.



Jira ELTHON.

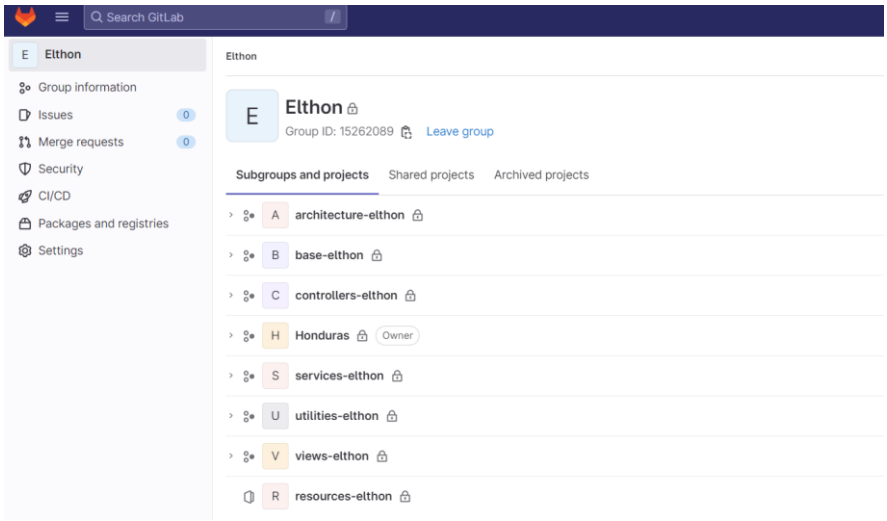
STACK

Esta herramienta se utiliza para la monitorización y análisis de los servidores y aplicaciones del proyecto. Stack permite la visualización en tiempo real del estado del servidor y aplicaciones, lo que facilita la detección temprana de problemas y la toma de medidas para solucionarlos.

GITLAB

Herramienta de control de versiones de software y una plataforma de colaboración de desarrollo de software, proporciona una manera de rastrear y administrar los cambios en el código fuente, así como también facilita la colaboración entre desarrolladores en un mismo proyecto. Además, GitLab también ofrece herramientas de integración y entrega continuas, lo que permite a los equipos automatizar las pruebas, la compilación y la implementación de software.

En el caso de ELTHON, GitLab es una herramienta de soporte fundamental para el desarrollo y mantenimiento de los sistemas. Permite a los desarrolladores trabajar en equipo en un mismo código fuente y mantener un historial de los cambios realizados en el código. Esto les permite colaborar de manera efectiva en la resolución de problemas y errores, y asegurarse de que el código se encuentre en un estado consistente y sin conflictos. Además, con las herramientas de integración continua y entrega continua de GitLab, los desarrolladores pueden asegurarse de que los cambios de código se prueben y se implementen automáticamente, lo que acelera el proceso de desarrollo y mejora la calidad del software entregado.



GitLab ELTHON.

16. AZURE DEVOPS DE ELTHON

AZURE DevOps es una plataforma integral de servicios en la nube diseñada para soportar todo el ciclo de vida del desarrollo de software, desde la planificación y el seguimiento hasta la entrega y el monitoreo. La plataforma incluye una serie de herramientas integradas como repositorios de código, seguimiento de problemas, compilación e implementación automatizadas, pruebas y monitoreo de rendimiento, entre otras.

El objetivo principal de AZURE DevOps es brindar una solución completa y escalable para la gestión del ciclo de vida de aplicaciones de software, permitiendo una mayor colaboración entre los equipos de desarrollo y operaciones. Además, su integración con otras herramientas de Microsoft, como AZURE Boards y AZURE Repos, permite a los desarrolladores trabajar de manera más eficiente en proyectos de cualquier tamaño.

ELTHON ha adoptado AZURE DevOps como su herramienta principal para la gestión de proyectos de software. Esto se debe en gran parte a las ventajas que ofrece la plataforma, como la integración continua, la implementación continua, la automatización de pruebas y la gestión de versiones de código. Además, el uso de AZURE DevOps ha permitido a ELTHON mejorar la colaboración y la comunicación entre los equipos de desarrollo y operaciones, lo que ha llevado a una mayor eficiencia en el desarrollo y la implementación de soluciones de software.

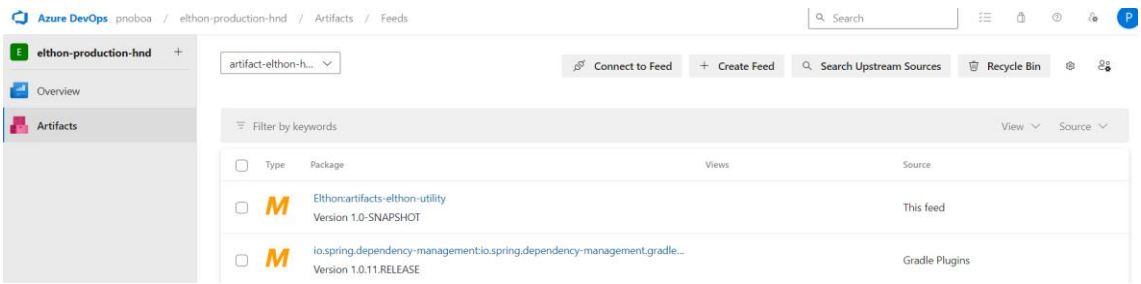
16.1. ARTIFACTS

Artifacts es una herramienta de AZURE DevOps que tiene como objetivo la gestión de paquetes de software y artefactos para el desarrollo de aplicaciones. Con esta herramienta, los equipos de desarrollo pueden compartir y reutilizar paquetes de código, bibliotecas, plantillas y otros artefactos de forma centralizada, lo que ayuda a simplificar la gestión de dependencias y aumentar la eficiencia en el desarrollo de software. Una de las principales características de Artifacts es su capacidad para gestionar paquetes de diferentes tipos y formatos, incluyendo NuGet, npm, Maven, Python, Gradle y otros. Además, esta herramienta permite la creación y publicación de paquetes, la gestión de versiones y la implementación de políticas de seguridad para controlar el acceso y la distribución de artefactos.

16.1.1. ARTIFACTS ELTHON

ELTHON utiliza Artifacts como una librería centralizada para compartir y reutilizar código entre diferentes microservicios, esto facilita la comunicación entre los diferentes servicios ya que pueden consumir artefactos de forma segura mediante el consumo de URL, lo que reduce la complejidad en el desarrollo y permite una mayor eficiencia en el tiempo de implementación. Además, el uso de Artifacts permite una mejor gestión y control de versiones del código, lo que garantiza la calidad y estabilidad de los servicios.

También ayuda a la prevención de errores al tener una gestión más controlada de las dependencias y actualizaciones de librerías, Artifacts es una herramienta fundamental para el desarrollo de ELTHON y ayuda a garantizar una mejor calidad de software y una mayor eficiencia en el tiempo de implementación.



Artifacts ELTHON.

17. SLA DE AZURE COMO PROVEEDOR

Los acuerdos de nivel de servicio (SLA) son contratos que establecen los términos y condiciones para el uso de los servicios en la nube y describen los niveles de servicio que los proveedores deben cumplir. Microsoft AZURE ofrece un SLA completo para sus servicios en la nube, lo que garantiza una alta disponibilidad y un rendimiento confiable

de sus servicios. Para ELTHON, una empresa que proporciona sistemas a gran escala y de gran potencia para análisis y reportes es fundamental contar con una infraestructura de alta disponibilidad y un rendimiento confiable para sus clientes. Por lo tanto, el SLA de AZURE es de gran importancia para garantizar que los servicios que ofrece ELTHON estén disponibles para sus clientes y que cumplan con normativas de seguridad en todo momento.

AZURE actualiza su certificado SLA mensualmente, se puede evidenciar en el siguiente link https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services?lang=1. A continuación, se redacta las partes de fundamental importancia para la arquitectura y cumplimiento de objetivos, contratos y necesidades de los clientes de ELTHON.

17.1. INTRODUCCIÓN DEL DOCUMENTO

Este Acuerdo de nivel de servicio para Microsoft Online Services es parte de su acuerdo de licencias por volumen de Microsoft. Los términos en mayúscula utilizados, pero no definidos en este SLA tendrán el significado que se les asigna en el Acuerdo. Este SLA se aplica a los Servicios en línea de Microsoft enumerados en este documento (un "Servicio" o los "Servicios"), pero no se aplica a los servicios de marca por separado que están disponibles con los Servicios o están conectados a ellos o a cualquier software local que sea parte de cualquier Servicio.

Si no se logra ni mantiene los Niveles de Servicio para cada Servicio como se describe en este SLA, entonces usted puede ser elegible para un crédito para una parte de sus tarifas de servicio mensuales. No modificaremos los términos de su SLA durante el período inicial de su suscripción; sin embargo, si renueva su suscripción, la versión de este SLA vigente en el momento de la renovación se aplicará durante todo el plazo de renovación. Proporcionaremos un aviso con al menos 90 días de anticipación para cambios materiales adversos a este SLA. Puede revisar la versión más reciente de este SLA en cualquier momento visitando https://aka.ms/CSLA. Las vistas previas y los servicios en línea y/o los niveles de servicio proporcionados sin cargo no están incluidos ni son elegibles para reclamos o créditos de SLA.

Aclaraciones y Resumen de Cambios a este Documento

A continuación, se muestran las adiciones, eliminaciones y otros cambios recientes a este SLA. A continuación, también se enumeran aclaraciones de la política de Microsoft en respuesta a preguntas comunes de los clientes.

Adiciones/Actualizaciones	Eliminaciones
API de AZURE para FHIR	
Nivel Premium de AZURE Files	
Servicios de datos de AZURE Health	
Servicio de tecnología médica	
Servicio Open AI de AZURE	
ámbito de Microsoft	
Centinela de Microsoft	

17.2. TÉRMINOS GENERALES

DEFINICIONES

- **Período Mensual Aplicable:** significa, para un mes calendario en el que se adeuda un Crédito de Servicio, la cantidad de días que usted es suscriptor de un Servicio.
- **Tiempo de inactividad**: se define para cada Servicio en los Términos específicos de los Servicios a continuación. A excepción de los servicios de Microsoft AZURE, el tiempo de inactividad no incluye el tiempo de inactividad programado. El tiempo de inactividad no incluye la falta de disponibilidad de un Servicio debido a las limitaciones que se describen a continuación y en los Términos específicos de los Servicios.
- **Tarifas de servicio mensuales aplicables:** hace referencia a las tarifas totales que realmente pagó por un Servicio que se aplican al mes en el que se adeuda un Crédito de servicio.
- **Código de error**: significa una indicación de que una operación ha fallado, como un código de estado HTTP en el rango 5xx.
- **Conectividad externa**: es el tráfico de red bidireccional a través de protocolos admitidos, como HTTP y HTTPS, que se puede enviar y recibir desde una dirección IP pública.
- **Incidente:** significa (i) cualquier evento individual, o (ii) cualquier conjunto de eventos, que resultan en Tiempo de Inactividad.
- **Portal de administración:** hace referencia a la interfaz web, proporcionada por Microsoft, a través de la cual los clientes pueden administrar el Servicio.
- **Tiempo de inactividad programado**: se refiere a los períodos de tiempo de inactividad relacionados con el mantenimiento o las actualizaciones de la red, el hardware o el Servicio. Publicaremos un aviso o le notificaremos al menos cinco (5) días antes del comienzo de dicho tiempo de inactividad.
- **Crédito de servicio:** es el porcentaje de las Tarifas de servicio mensuales aplicables que se le acreditan luego de la aprobación de la reclamación de Microsoft.

- **Nivel de servicio:** hace referencia a las métricas de rendimiento establecidas en este SLA que Microsoft acepta cumplir en la prestación de los Servicios.
- **Recurso de servicio:** significa un recurso individual disponible para su uso dentro de un Servicio.
- **Código de éxito:** significa una indicación de que una operación ha tenido éxito, como un código de estado HTTP en el rango 2xx.
- **Ventana de soporte:** se refiere al período de tiempo durante el cual se admite una característica del Servicio o la compatibilidad con un producto o servicio separado.
- **Minutos de Usuario:** significa el número total de minutos en un mes, menos todo el Tiempo de Inactividad Programado, multiplicado por el número total de usuarios.

RECLAMOS

Para que Microsoft considere un reclamo, debe enviar el reclamo al servicio de atención al cliente de Microsoft Corporación, incluida toda la información necesaria para que Microsoft valide el reclamo, incluidos, entre otros:

1. Una descripción detallada del Incidente
2. Información sobre el tiempo y la duración del tiempo de inactividad
3. El número y la(s) ubicación(es) de los usuarios afectados (si corresponde
4. descripciones de sus intentos de resolver el Incidente en el momento en que ocurrió.

Para un reclamo relacionado con Microsoft AZURE, debemos recibir el reclamo dentro de los dos meses posteriores al final del mes de facturación en el que ocurrió el Incidente objeto del reclamo. Para los reclamos relacionados con todos los demás Servicios, debemos recibir el reclamo al final del mes calendario siguiente al mes en que ocurrió el Incidente. Por ejemplo, si el Incidente ocurrió el 15 de febrero, debemos recibir el reclamo y toda la información requerida antes del 31 de marzo.

Se evalúa toda la información razonablemente disponible para nosotros y haremos una determinación de buena fe de si se debe un Crédito de servicio. Haremos todos los esfuerzos comercialmente razonables para procesar las reclamaciones durante el mes siguiente y dentro de los cuarenta y cinco (45) días posteriores a la recepción. Debe cumplir con el Acuerdo para ser elegible para un Crédito de servicio. Si determinamos que se le debe un Crédito de servicio, aplicaremos el Crédito de servicio a sus Tarifas de servicio mensuales aplicables.

Si compró más de un Servicio (no como una suite), entonces puede presentar reclamos de conformidad con el proceso descrito anteriormente como si cada Servicio estuviera

cubierto por un SLA individual. Por ejemplo, si compró Exchange Online y SharePoint Online (no como parte de una suite), y durante el plazo de la suscripción un Incidente causó Tiempo de inactividad para ambos Servicios, entonces podría ser elegible para dos Créditos de servicio separados (uno para cada Servicio), mediante la presentación de dos reclamaciones en virtud de este SLA. En el caso de que no se alcance más de un Nivel de Servicio para un Servicio en particular debido al mismo Incidente, debe elegir solo un Nivel de Servicio bajo el cual hacer un reclamo basado en el Incidente. A menos que se indique lo contrario en un SLA específico, solo se permite un Crédito de servicio por Servicio durante un Período mensual aplicable.

CRÉDITOS DE SERVICIO

Los Créditos de servicio son su único y exclusivo recurso para cualquier problema de rendimiento o disponibilidad de cualquier Servicio en virtud del Acuerdo y este SLA. No puede compensar unilateralmente sus tarifas de servicio mensuales aplicables por problemas de rendimiento o disponibilidad.

Los Créditos de servicio se aplican solo a las tarifas pagadas por el Servicio, Recurso de servicio o nivel de Servicio en particular para el cual no se ha alcanzado un Nivel de servicio. En los casos en que los Niveles de servicio se aplican a Recursos de servicio individuales o a niveles de Servicio separados, los Créditos de servicio se aplican solo a las tarifas pagadas por el Recurso de servicio afectado o el nivel de Servicio, según corresponda. Los Créditos de servicio otorgados en cualquier mes de facturación para un Servicio o Recurso de servicio en particular no excederán, en ninguna circunstancia, sus tarifas de servicio mensuales para ese Servicio o Recurso de servicio, según corresponda, en el mes de facturación.

Si se compró Servicios como parte de una suite u otra oferta única, las Tarifas de servicio mensuales aplicables y el Crédito de servicio para cada Servicio se prorratearán.

Si se compró un Servicio de un revendedor, recibirá un crédito de servicio directamente de su revendedor y el revendedor recibirá un Crédito de servicio directamente de nosotros. El Crédito de servicio se basará en el precio minorista estimado para el Servicio aplicable, según lo determinemos a nuestra discreción razonable.

LIMITACIONES

Este SLA y cualquier Nivel de servicio aplicable no se aplican a ningún problema de rendimiento o disponibilidad:

- Debido a factores fuera de nuestro control razonable (desastres naturales, guerras, actos de terrorismo, disturbios, acciones gubernamentales o una falla de red o dispositivo externo a nuestros centros de datos, incluso en su sitio o entre su sitio y nuestro centro de datos)
- Que resulten del uso de servicios, hardware o software no proporcionados por nosotros, incluidos, entre otros, problemas que resulten de un ancho de banda inadecuado o relacionados con software o servicios de terceros
- Eso resulta de fallas en una sola ubicación de Microsoft Datacenter, cuando la conectividad de su red depende explícitamente de esa ubicación de una manera no georresistente
- Causado por su uso de un Servicio después de que le aconsejáramos que modificara su uso del Servicio, si no modificó su uso como se le aconsejó
- Durante o con respecto a versiones preliminares, preliminares, beta o de prueba de un Servicio, función o software (según lo determinemos nosotros) o compras realizadas con créditos de suscripción de Microsoft
- Que resulten de su acción no autorizada o falta de acción cuando sea necesario, o de sus empleados, agentes, contratistas o proveedores, o cualquier persona que obtenga acceso a nuestra red por medio de sus contraseñas o equipo, o que resulten de otra manera de su incumplimiento de las medidas de seguridad adecuadas. Prácticas
- Eso resulta de su incumplimiento de las configuraciones requeridas, uso de plataformas compatibles, seguimiento de cualquier política para un uso aceptable o su uso del Servicio de una manera inconsistente con las características y la funcionalidad del Servicio (intentos de realizar operaciones que no son compatibles) o son incompatibles con nuestra guía publicada
- Que resulten de entradas, instrucciones o argumentos defectuosos (solicitudes para acceder a archivos que no existen)
- Que resulten de intentos de realizar operaciones que excedan las cuotas prescritas o que resulten de la regulación de sospechas de comportamiento abusivo
- Debido a su uso de funciones del Servicio que están fuera de las Ventanas de soporte asociadas
- Para licencias reservadas, pero no pagadas, en el momento del Incidente.
- Sus operaciones iniciadas, como reiniciar, detener, iniciar, conmutación por error, computación a escala y almacenamiento a escala que generan tiempo de inactividad, se excluyen del cálculo del tiempo de actividad.
- La ventana de mantenimiento mensual que incurre en un tiempo de inactividad para parchear su servidor e infraestructura se excluye del cálculo del tiempo de actividad.

Los servicios comprados a través de contratos de licencia por volumen Open, Open Value y Open Value Subscription, y los servicios en un paquete de Office 365 Small Business Premium comprados en forma de clave de producto no son elegibles para Créditos de servicio basados en tarifas de servicio. Para estos Servicios, cualquier Crédito de servicio para el que pueda ser elegible se acreditará en forma de tiempo de servicio (es decir, días) en lugar de tarifas de servicio, y cualquier referencia a "Cargos de servicio mensuales aplicables" se elimina y reemplaza por "Comisiones de servicio aplicables". Período mensual."

17.3. AZURE ACTIVE DIRECTORY AD

- **Tiempo de inactividad**: cualquier período de tiempo en el que los usuarios no puedan iniciar sesión en el servicio de AZURE Active Directory, o AZURE Active Directory no pueda emitir correctamente los tokens de autenticación y autorización necesarios para que los usuarios inicien sesión en las aplicaciones conectadas al servicio
- **Porcentaje de tiempo de actividad mensual:** el porcentaje de tiempo de actividad mensual se calcula mediante la siguiente fórmula:

$$\frac{User\ Minutes\ -Downtime}{User\ Minutes}\ x\ 100$$

donde el tiempo de inactividad se mide en minutos de usuario; es decir, para cada mes, el Tiempo de Inactividad es la suma de la duración (en minutos) de cada Incidente que ocurre durante ese mes multiplicada por la cantidad de usuarios afectados por ese Incidente.

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,99%	10%
<99,9%	25%
<99%	50%
<95%	100%

17.4. SERVICIOS DE DOMINIO DE AZURE ACTIVE DIRECTORY

- **Dominio administrado:** hace referencia a un dominio de Active Directory que está aprovisionado y administrado por AZURE Active Directory Domain Services.
- **Máximo de Minutos Disponibles:** es el número total de minutos que el Cliente ha implementado un Dominio Administrado determinado en Microsoft AZURE

durante un mes de facturación en una suscripción de Microsoft AZURE determinada.

- **Tiempo de inactividad:** es el total de minutos acumulados durante un mes de facturación para una determinada suscripción de Microsoft AZURE durante el cual un Dominio administrado determinado no está disponible. Se considera que un minuto no está disponible si todas las solicitudes de autenticación de dominio de las cuentas de usuario que pertenecen al dominio administrado, LDAP se vinculan a la DSE raíz o la búsqueda de registros de DNS, realizadas desde dentro de la red virtual donde está habilitado el dominio administrado, devuelven un error Código o no devolver un Código de éxito dentro de los 30 segundos.
- **Porcentaje de tiempo de actividad mensual:** el porcentaje de tiempo de actividad mensual se calcula mediante la siguiente fórmula:

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,9%	10%
<99%	25%

17.5. SERVICIOS DE ANÁLISIS

- **Servidor:** hace referencia a cualquier servidor de AZURE Analysis Services.
- **Máximo de Minutos Disponibles:** es el número total de minutos que un Servidor determinado ha estado implementado en Microsoft AZURE durante un mes de facturación en una suscripción de Microsoft AZURE determinada.
- **Operaciones de cliente:** es el conjunto de todas las operaciones documentadas admitidas por AZURE Analysis Services.
- **Tiempo de inactividad:** es el total de minutos acumulados durante un mes de facturación para una determinada suscripción de Microsoft AZURE durante el cual un servidor determinado no está disponible. Se considera que un minuto no está disponible para un servidor determinado si más del 1% de todas las operaciones del cliente completadas durante el minuto arrojan un código de error.
- **Porcentaje de tiempo de actividad mensual**: el porcentaje de tiempo de actividad mensual para un servidor determinado se calcula utilizando la siguiente fórmula:

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,9%	10%
<99%	25%

17.6. SERVICIOS DE ADMINISTRACIÓN DE API

- **Minutos de implementación:** es la cantidad total de minutos que una instancia de API Management determinada se ha implementado en Microsoft AZURE durante un mes de facturación.
- **Máximo de Minutos Disponibles:** es la suma de todos los Minutos de Implementación en todas las instancias de API Management implementadas por usted en una determinada suscripción de Microsoft AZURE durante un mes de facturación.
- **Proxy:** es el componente del Servicio de administración de API responsable de recibir solicitudes de API y reenviarlas a la API dependiente configurada.
- **Tiempo de inactividad:** el total de Minutos de implementación acumulados, en todas las instancias de API Management implementadas por usted en una determinada suscripción de Microsoft AZURE, durante el cual el Servicio de API Management no está disponible. Se considera que un minuto no está disponible para una instancia de API Management determinada si todos los intentos continuos de realizar operaciones a través del Proxy durante el minuto dan como resultado un Código de error o no devuelven un Código de éxito en cinco minutos.
- **Porcentaje de tiempo de actividad mensual:** el porcentaje de tiempo de actividad mensual se calcula mediante la siguiente fórmula:

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Crédito de servicio para implementaciones de nivel premium escaladas en dos o más regiones:

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,99%	10%
<99%	25%

17.7. CENTRO DE APLICACIONES

- **Servicio de compilación:** es una función que permite a los clientes crear sus aplicaciones móviles en Visual Studio App Center.

- **Servicio de prueba:** es una función que permite a los clientes cargar y ejecutar pruebas para sus aplicaciones móviles en dispositivos físicos que se ejecutan en Visual Studio App Center.
- **Servicio de notificaciones push:** es una función que permite a los clientes enviar mensajes a dispositivos específicos configurados para recibir dichos mensajes mediante Visual Studio App Center.

Cálculo del Tiempo de Actividad Mensual y Niveles de Servicio para Visual Studio App Center Build Service

- **Máximo de Minutos Disponibles:** es el número total de minutos para los cuales el Cliente implementó el Servicio de Compilación para una determinada suscripción de Microsoft AZURE durante un mes de facturación.
- **Tiempo de inactividad:** es el número total de minutos dentro del Máximo de minutos disponibles durante los cuales el Servicio de compilación no está disponible. Un minuto se considera no disponible si todas las solicitudes HTTP continuas al Servicio de compilación para realizar operaciones iniciadas por el Cliente a lo largo del minuto resultan en un Código de error o no devuelven una respuesta dentro de un minuto.
- **Porcentaje de tiempo de actividad mensual:** el porcentaje de tiempo de actividad mensual para Visual Studio App Center Build Service se calcula como el máximo de minutos disponibles menos el tiempo de inactividad dividido por el máximo de minutos disponibles multiplicado por 100. El porcentaje de tiempo de actividad mensual se representa mediante la siguiente fórmula:

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Los siguientes Niveles de Servicio y Créditos de Servicio se aplican al uso del Cliente del Servicio de Compilación de Visual Studio App Center.

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,9%	10%
<99%	25%

Cálculo del tiempo de actividad mensual y niveles de servicio para el servicio de prueba de Visual Studio App Center

- **Máximo de Minutos Disponibles:** es el número total de minutos para los cuales el Cliente implementó el Servicio de Prueba para una determinada suscripción de Microsoft AZURE durante un mes de facturación.
- **Tiempo de inactividad:** el número total de minutos dentro del Máximo de minutos disponibles durante los cuales el Servicio de prueba no está disponible. Un minuto se considera no disponible si todas las solicitudes HTTP continuas al Servicio de prueba para realizar operaciones iniciadas por el Cliente a lo largo del minuto resultan en un Código de error o no devuelven una respuesta dentro de un minuto.
- **Porcentaje de tiempo de actividad mensual:** el porcentaje de tiempo de actividad mensual para el servicio de prueba de Visual Studio App Center se calcula como el máximo de minutos disponibles menos el tiempo de inactividad dividido por el máximo de minutos disponibles multiplicado por 100. El porcentaje de tiempo de actividad mensual se representa mediante la siguiente fórmula:

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Los siguientes Niveles de Servicio y Créditos de Servicio se aplican al uso del Servicio de Prueba del Centro de Aplicaciones de Visual Studio por parte del Cliente.

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,9%	10%
<99%	25%

Cálculo del tiempo de actividad mensual y niveles de servicio para el servicio de notificaciones PUSH de Visual Studio App Center

- **Máximo de Minutos Disponibles:** es el número total de minutos para los cuales el Cliente implementó el Servicio de Notificación Push para una determinada suscripción de Microsoft AZURE durante un mes de facturación.
- **Tiempo de inactividad:** la cantidad total de minutos dentro de los minutos máximos disponibles durante los cuales el servicio de notificaciones automáticas no está disponible. Un minuto se considera no disponible si todas las solicitudes HTTP continuas al Servicio de notificaciones push para realizar operaciones iniciadas por el Cliente a lo largo del minuto resultan en un Código de error o no devuelven una respuesta dentro de un minuto.
- **Porcentaje de tiempo de actividad mensual:** el porcentaje de tiempo de actividad mensual para el servicio de notificaciones push de Visual Studio App Center se calcula como el máximo de minutos disponibles menos el tiempo de inactividad

dividido por el máximo de minutos disponibles multiplicado por 100. El porcentaje de tiempo de actividad mensual se representa mediante la siguiente fórmula:

-

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Los siguientes Niveles de Servicio y Créditos de Servicio se aplican al uso del Cliente del Servicio de Notificación Push de Visual Studio App Center.

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,9%	10%
<99%	25%

17.8. CONFIGURACIÓN DE APLICACIÓN

- **Almacén de configuración:** se refiere a una única implementación de AZURE App Configuration creada por el Cliente, de modo que se enumera en la pestaña Configuración de la aplicación en el Portal de administración.

Cálculo del tiempo de actividad mensual y niveles de servicio para AZURE App Configuration

- **Minutos de implementación:** es la cantidad total de minutos que un Almacén de configuración determinado se ha implementado en Microsoft AZURE durante un mes de facturación.
- **Máximo de Minutos Disponibles:** es la suma de todos los Minutos de Implementación en todos los Almacenes de Configuración implementados por el Cliente en una determinada suscripción de Microsoft AZURE durante un mes de facturación.
- **Tiempo de inactividad:** es el total de minutos acumulados dentro del Máximo de minutos disponibles, durante los cuales el Almacén de configuración no está disponible. Se considera que un minuto no está disponible para un Almacén de configuración dado cuando no hay conectividad durante el minuto entre el Almacén de configuración y la puerta de enlace de Internet de Microsoft.
- **Porcentaje de Tiempo de Actividad Mensual:** para la Configuración de la Aplicación de AZURE se calcula como el Máximo de Minutos Disponibles menos el Tiempo de Inactividad dividido por el Máximo de Minutos Disponibles en un mes de facturación para una determinada suscripción de Microsoft AZURE. El porcentaje de tiempo de actividad mensual se representa mediante la siguiente fórmula:

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,9%	10%
<99%	25%

17.9. SERVICIO DE APLICACIONES

- **Minutos de implementación:** es la cantidad total de minutos que se ha configurado para ejecutar una aplicación determinada en Microsoft AZURE durante un mes de facturación. Los minutos de implementación se miden desde el momento en que se creó la aplicación o el cliente inició una acción que daría lugar a la ejecución de la aplicación hasta el momento en que el cliente inició una acción que daría lugar a la detención o eliminación de la aplicación.
- **Máximo de Minutos Disponibles:** es la suma de todos los Minutos de Implementación en todas las Aplicaciones implementadas por el Cliente en una determinada suscripción de Microsoft AZURE durante un mes de facturación.
- **Aplicación:** es una aplicación web, aplicación móvil, aplicación API, aplicación lógica, implementada por el Cliente dentro del Servicio de aplicaciones. El SLA es compatible cuando se ejecuta en una sola instancia y en varias instancias.
- **Tiempo de Inactividad:** es el total de Minutos de Implementación acumulados, en todas las Aplicaciones implementadas por el Cliente en una determinada suscripción de Microsoft AZURE, durante los cuales la Aplicación no está disponible. Se considera que un minuto no está disponible para una aplicación determinada cuando no hay conectividad entre la aplicación y la puerta de enlace de Internet de Microsoft.
- **Porcentaje de tiempo de actividad mensual:** el porcentaje de tiempo de actividad mensual se calcula mediante la siguiente fórmula:

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,95%	10%
<99%	25%
<95%	100%

Términos adicionales: Los Créditos de servicio se aplican solo a las tarifas atribuibles a su uso de Aplicaciones web, Aplicaciones móviles, Aplicaciones API o Aplicaciones lógicas y no a tarifas atribuibles a otros tipos de aplicaciones disponibles a través del Servicio de aplicaciones, que no están cubiertas por este SLA.

17.10. PUERTA DE ENLACE DE APLICACIONES

- **Servicio en la nube de Application Gateway:** se refiere a una colección de dos o más instancias o implementaciones de Application Gateway medianas o más grandes capaces de admitir escalabilidad automática o redundancia de zona, configuradas para realizar servicios de equilibrio de carga HTTP.
- **Máximo de Minutos Disponibles:** es el total de minutos acumulados durante un mes de facturación durante el cual se implementó un Servicio en la Nube de Application Gateway en una suscripción de Microsoft AZURE.
- **Tiempo de inactividad:** es el total de Minutos disponibles máximos acumulados durante un mes de facturación para un Servicio en la nube de Application Gateway determinado durante el cual el Servicio en la nube de Application Gateway no está disponible. Un minuto determinado se considera no disponible si todos los intentos de conectarse al servicio en la nube de Application Gateway durante el minuto no tienen éxito.
- **Porcentaje de tiempo de actividad mensual:** el porcentaje de tiempo de actividad mensual se calcula mediante la siguiente fórmula:

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,95%	10%
<99%	25%

17.11. PERSPECTIVAS DE LA APLICACIÓN

- **Recurso de Application Insights:** es el contenedor de Application Insights que recopila, procesa y almacena los datos para una única clave de instrumentación.
- **Minutos Máximos Disponibles:** es la cantidad total de minutos que el Cliente ha implementado un Recurso de Application Insights determinado dentro de una suscripción de Microsoft AZURE durante un mes de facturación.

- **Tiempo de inactividad:** es el número total de minutos dentro del Máximo de minutos disponibles en los que los datos dentro de un recurso de Application Insights no están disponibles. Se considera que un minuto no está disponible para un recurso específico de Application Insights durante el cual ninguna operación HTTP dio como resultado un código de éxito.
- **Porcentaje de disponibilidad de consultas mensuales:** para un recurso de Application Insights determinado se calcula como el máximo de minutos disponibles menos el tiempo de inactividad dividido por el máximo de minutos disponibles multiplicado por 100.

El Porcentaje de Disponibilidad de Consulta Mensual se calcula utilizando la siguiente fórmula:

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Porcentaje de disponibilidad de consulta mensual	Crédito de servicio
<99,9%	10%
<99%	25%

17.12. SERVICIOS DE IA APLICADA DE AZURE

- **Total, de Intentos de Transacción:** es el número total de solicitudes de API autenticadas por parte del Cliente durante un mes de facturación para una API de Servicios de IA Aplicada dada. El total de intentos de transacción no incluye las solicitudes de API que devuelven un código de error que se repite continuamente dentro de una ventana de cinco minutos después de que se recibe el primer código de error.
- **Transacciones fallidas:** es el conjunto de todas las solicitudes a la API de servicios de inteligencia artificial aplicada dentro de los intentos de transacciones totales que devuelven un código de error. Los intentos de transacción fallidos no incluyen las solicitudes de API que devuelven un código de error que se repite continuamente en un período de cinco minutos después de recibir el primer código de error.

CÁLCULO DE TIEMPO DE ACTIVIDAD MENSUAL

Porcentaje de Tiempo de Actividad Mensual: para cada Servicio de API se calcula como Intentos de Transacción Totales menos Transacciones Fallidas dividido por Intentos de

Transacción Totales en un mes de facturación para una suscripción de API determinada. El porcentaje de tiempo de actividad mensual se representa mediante la siguiente fórmula:

$$\frac{Total\ Transaction\ Attempts - Failed\ Transactions}{Total\ Transaction\ Attempts}\ x\ 100$$

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,9%	10%
<99%	25%

17.13. AUTOMATIZACIÓN

- **Minutos de implementación:** es la cantidad total de minutos que una cuenta de Automatización determinada se ha implementado en Microsoft AZURE durante un mes de facturación.
- **Servicio de agente de DSC:** es el componente del Servicio de automatización responsable de recibir y responder a las solicitudes de extracción, registro e informes de los nodos de DSC.
- **Máximo de minutos disponibles:** es la suma de todos los minutos de implementación en todas las cuentas de automatización implementadas en una suscripción de Microsoft AZURE determinada durante un mes de facturación.
- **Servicio de automatización:** configuración de estado deseado (DSC).
- **Tiempo de inactividad:** el total de Minutos de implementación acumulados, en todas las cuentas de Automatización implementadas en una determinada suscripción de Microsoft AZURE, durante los cuales el Servicio de agente de DSC no está disponible. Se considera que un minuto no está disponible para una cuenta de Automatización dada si todas las solicitudes continuas de extracción, registro y generación de informes de los nodos de DSC asociados con la cuenta de Automatización al Servicio de agente de DSC durante el minuto resultan en un Código de error o no devuelven un Código de éxito dentro de cinco minutos.
- **Porcentaje de tiempo de actividad mensual:** el porcentaje de tiempo de actividad mensual se calcula mediante la siguiente fórmula:

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,9%	10%
<99%	25%

Términos adicionales: los Créditos de servicio se aplican solo a las tarifas atribuibles a su uso de la funcionalidad DSC dentro del Servicio de automatización.

17.14. SERVICIO DE AUTOMATIZACIÓN – AUTOMATIZACIÓN DE PROCESOS

- **Trabajos retrasados:** es el número total de trabajos, para una suscripción de Microsoft AZURE determinada, que no se inician dentro de los treinta (30) minutos de sus Horas de inicio planificadas.
- **Trabajo:** significa la ejecución de un Runbook.
- **Hora de inicio planificada:** es una hora a la que está programado que un trabajo comience a ejecutarse.
- **Runbook:** significa un conjunto de acciones especificadas por usted para ejecutar dentro de Microsoft AZURE.
- **Trabajos totales:** es el número total de trabajos programados para ejecutarse durante un mes de facturación determinado, para una suscripción de Microsoft AZURE determinada.
- **Porcentaje de tiempo de actividad mensual:** el porcentaje de tiempo de actividad mensual se calcula mediante la siguiente fórmula:

$$\frac{Total\ Jobs - Delayed\ Jobs}{Total\ Jobs}\ x\ 100$$

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,9%	10%
<99%	25%

Términos adicionales: los Créditos de servicio se aplican solo a las tarifas atribuibles a su uso de la funcionalidad de Automatización de procesos dentro del Servicio de automatización.

17.15. COPIAS DE SEGURIDAD DE AZURE

- **Copia de seguridad:** es el proceso de copiar datos de la computadora desde un servidor registrado a una Bóveda de copia de seguridad.
- **Agente de copia de seguridad:** hace referencia al software instalado en un servidor registrado que permite que el servidor registrado realice una copia de seguridad o restaure uno o más elementos protegidos.
- **Bóveda de copia de seguridad:** se refiere a un contenedor en el que puede registrar uno o más elementos protegidos para la copia de seguridad.

- **Fallo:** significa que el Agente de copia de seguridad o el Servicio no completan por completo una operación de copia de seguridad o recuperación configurada correctamente debido a la falta de disponibilidad del Servicio de copia de seguridad.
- **Elemento protegido:** hace referencia a una colección de datos, como un volumen, una base de datos o una máquina virtual que se ha programado para realizar una copia de seguridad en el Servicio de copia de seguridad, de modo que se enumera como un Elemento protegido en la pestaña Elementos protegidos en la sección Servicios de recuperación. del Portal de Gestión.
  La " recuperación " o " restauración " es el proceso de restauración de datos informáticos desde una bóveda de copia de seguridad a un servidor registrado.

CÁLCULO DEL TIEMPO DE ACTIVIDAD MENSUAL Y NIVELES DE SERVICIO PARA EL SERVICIO DE COPIA DE SEGURIDAD

- **Minutos de implementación:** es la cantidad total de minutos durante los cuales se programó la copia de seguridad de un elemento protegido en una bóveda de copia de seguridad.
- **Máximo de Minutos Disponibles:** es la suma de todos los Minutos de Implementación en todos los Elementos Protegidos para una determinada suscripción de Microsoft AZURE durante un mes de facturación.
- **Tiempo de Inactividad:** El total de Minutos de Implementación acumulados en todos los Elementos Protegidos programados para la Copia de Seguridad por usted en una determinada suscripción de Microsoft AZURE durante la cual el Servicio de Copia de Seguridad no está disponible para el Elemento Protegido. Se considera que el Servicio de copia de seguridad no está disponible para un Elemento protegido dado desde la primera falla en la copia de seguridad o restauración del elemento protegido hasta el inicio de una copia de seguridad o recuperación exitosa de un elemento protegido, siempre que los reintentos se intenten continuamente con una frecuencia no inferior a una vez cada treinta minutos.
- **Porcentaje de tiempo de actividad mensual:** el porcentaje de tiempo de actividad mensual se calcula mediante la siguiente fórmula:

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,9%	10%
<99%	25%

17.16. LOTE

- **Tasa de error promedio:** para un mes de facturación es la suma de las tasas de error para cada hora en el mes de facturación dividida por la cantidad total de horas en el mes de facturación.
- **Tasa de error:** es el número total de solicitudes fallidas dividido por el total de solicitudes durante un intervalo de una hora determinado. Si el total de solicitudes en un intervalo de una hora dado es cero, la tasa de error para ese intervalo es 0%.
- **Solicitudes excluidas:** son solicitudes que dan como resultado un código de estado HTTP 4xx, que no sea un código de estado HTTP 408.
- **Solicitudes fallidas:** es el conjunto de todas las solicitudes dentro de Total de solicitudes que devuelven un Código de error o un código de estado HTTP 408 o no devuelven un Código de éxito en 5 segundos.
- **Solicitudes totales:** es la cantidad total de solicitudes de API REST autenticadas, distintas de las Solicitudes excluidas, para realizar operaciones en cuentas de Batch intentadas dentro de un intervalo de una hora dentro de una suscripción de AZURE determinada durante un mes de facturación.
- **Porcentaje de tiempo de actividad mensual:** para el Servicio por lotes se calcula restando del 100 % la Tasa de error promedio para una suscripción de Microsoft AZURE dada en un mes de facturación. La "tasa de error promedio" para un mes de facturación es la suma de las tasas de error para cada hora en el mes de facturación dividida por la cantidad total de horas en el mes de facturación.

$$Monthly\ Uptime\ \% = 100\% - Average\ Error\ Rate$$

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,9%	10%
<99%	25%

17.17. CACHÉ DE AZURE PARA REDIS

- **Caché:** se refiere a una implementación del Servicio de caché creada por el Cliente, de modo que sus Puntos finales de caché se enumeran en la pestaña Caché en el Portal de administración.

- **Puntos finales de caché:** se refiere a los puntos finales a través de los cuales se puede acceder a un caché.
- **Zona de disponibilidad:** es un área aislada por fallas dentro de una región de AZURE, que proporciona alimentación, refrigeración y redes redundantes.

Cálculo del tiempo de actividad mensual y niveles de servicio para el servicio de caché

- **Minutos de implementación:** es la cantidad total de minutos que se ha implementado un caché determinado en Microsoft AZURE durante un mes de facturación.
- **Máximo de Minutos Disponibles:** es la suma de todos los Minutos de Implementación en todos los Cachés implementados por el Cliente en una determinada suscripción de Microsoft AZURE durante un mes de facturación.
- **Tiempo de Inactividad:** El total de Minutos de Implementación acumulados, en todos los Cachés implementados por el Cliente en una determinada suscripción de Microsoft AZURE, durante los cuales el Caché no está disponible. Un minuto se considera no disponible para un Caché dado cuando no hay conectividad durante el minuto entre uno o más Puntos finales de Caché asociados con el Caché y la puerta de enlace de Internet de Microsoft.
- **Porcentaje de tiempo de actividad mensual:** el porcentaje de tiempo de actividad mensual se calcula mediante la siguiente fórmula:

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Los Niveles de Servicio y los Créditos de Servicio aplicables al uso del Servicio de Caché por parte del Cliente varían según las condiciones de implementación y el nivel del Servicio de Caché. A menos que se indique lo contrario anteriormente, los Niveles de Servicio y los Créditos de Servicio se aplican al uso del Servicio de Caché por parte del Cliente, que incluye el Servicio de Caché Administrado de AZURE o los niveles Estándar, Premium, Empresarial y Flash Empresarial del Servicio de Caché de AZURE para REDIS. El nivel Básico de AZURE Cache for REDIS Cache no está cubierto por este SLA.

Crédito de servicio:

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,9%	10%
<99%	25%

Para cualquier Caché de nivel Enterprise o Enterprise Flash implementada en tres o más Zonas de Disponibilidad en la misma región de AZURE, los siguientes Niveles de Servicio y Créditos de Servicio se aplican al uso del Servicio de Caché por parte del Cliente:

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,99%	10%
<99%	25%

Para cualquier caché de nivel Enterprise y Enterprise Flash implementada (1) en al menos tres regiones de AZURE y tres o más zonas de disponibilidad en cada una de esas regiones y (2) con replicación geográfica activa habilitada para todas las instancias de caché cuando la característica de replicación geográfica activa está habilitado y generalmente disponible (es decir, no en vista previa), los siguientes Niveles de Servicio y Créditos de Servicio son aplicables al uso del Servicio de Caché por parte del Cliente:

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,999 %	10%
<99%	25%

17.18. SERVICIOS EN LA NUBE

- **Servicios en la nube:** hace referencia a un conjunto de recursos informáticos utilizados para funciones web y de trabajo.
- **Conectividad de la instancia de rol:** es el tráfico de red bidireccional entre la instancia de rol y otras direcciones IP que utilizan protocolos de red TCP o UDP en los que la instancia de rol está configurada para el tráfico permitido. Las direcciones IP pueden ser direcciones IP en el mismo Servicio en la Nube que la máquina virtual, direcciones IP dentro de la misma red virtual que la máquina virtual o direcciones IP públicas enrutables.
- **Inquilino:** representa uno o más roles, cada uno de los cuales consta de una o más instancias de roles que se implementan en un solo paquete.
- **Dominio de actualización:** se refiere a un conjunto de instancias de Microsoft AZURE a las que se aplican actualizaciones de plataforma simultáneamente.
- **Rol web:** es un componente de servicios en la nube que se ejecuta en el entorno de ejecución de AZURE que se personaliza para la programación de aplicaciones web con el respaldo de IIS y ASP.NET.
- **Rol del trabajador:** es un componente de servicios en la nube que se ejecuta en el entorno de ejecución de AZURE que es útil para el desarrollo generalizado y puede realizar un procesamiento en segundo plano para un rol web.

Cálculo del tiempo de actividad mensual y niveles de servicio para servicios en la nube

- **Máximo de minutos disponibles:** es el total de minutos acumulados durante un mes de facturación para todos los roles orientados a Internet que tienen dos o más instancias implementadas en diferentes dominios de actualización.
- El máximo de minutos disponibles se mide desde el momento en que se implementó el Arrendatario y se iniciaron sus roles asociados como resultado de una acción iniciada por el Cliente hasta el momento en que el Cliente inició una acción que resultaría en la detención o eliminación del Arrendatario.
- **Tiempo de inactividad:** el total de minutos acumulados que forman parte del máximo de minutos disponibles que no tienen conectividad de instancia de rol.
- **Porcentaje de tiempo de actividad mensual:** el porcentaje de tiempo de actividad mensual se representa mediante la siguiente fórmula:

$$Monthly\ Uptime\ \% = \frac{(Maximum\ Available\ Minutes - Downtime)}{Maximum\ Available\ Minutes}\ X\ 100$$

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,95%	10%
<99%	25%

17.19. BÚSQUEDA COGNITIVA DE AZURE

- **Tasa de error promedio:** para un mes de facturación es la suma de las tasas de error para cada hora en el mes de facturación dividida por la cantidad total de horas en el mes de facturación.
- **Tasa de error:** es el número total de solicitudes fallidas dividido por el total de solicitudes, en todas las instancias del servicio de búsqueda en una suscripción de AZURE determinada, durante un intervalo de una hora determinado. Si el total de solicitudes en un intervalo de una hora es cero, la tasa de error para ese intervalo es 0%.
- **Solicitudes excluidas:** son todas las solicitudes que se limitan debido al agotamiento de los recursos asignados para una Instancia de servicio de búsqueda, como lo indica un código de estado HTTP 503 y un encabezado de respuesta que indica que la solicitud se limitó.
- **Solicitudes fallidas:** es el conjunto de todas las solicitudes dentro de Total de solicitudes que no devuelven un código de éxito o una respuesta HTTP 4xx.

- **Réplica:** es una copia de un índice de búsqueda dentro de una instancia de servicio de búsqueda.
- **Instancia de servicio de búsqueda:** es una instancia de servicio de búsqueda de AZURE que contiene uno o más índices de búsqueda.
- **Solicitudes totales:** es el conjunto de (i) todas las solicitudes para actualizar una instancia de servicio de búsqueda que tiene tres o más réplicas, más (ii) todas las solicitudes para consultar una instancia de servicio de búsqueda que tiene dos o más réplicas, distintas de las solicitudes excluidas, dentro de un intervalo de una hora dentro de una suscripción de AZURE determinada durante un mes de facturación.
- **Porcentaje de tiempo de actividad mensual:** el porcentaje de tiempo de actividad mensual se calcula mediante la siguiente fórmula:

$$100\% - Average\ Error\ Rate$$

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,9%	10%
<99%	25%

17.20. PUERTA DE ENLACE DE COMUNICACIÓN DE AZURE

- **Número de teléfono asignado:** es un número de teléfono que cumple con todos los siguientes criterios:
  - Se ha aprovisionado dentro de los entornos Operator Connect o Teams Phone Mobile.
  - El número de teléfono está configurado para la conectividad a través de AZURE Communications Gateway.
  - El estado del número de teléfono es "asignado" en los entornos de Operator Connect o Teams Phone Mobile. Esto incluye (pero no se limita a) la asignación a usuarios, puentes de conferencia, aplicaciones de voz y aplicaciones de terceros.
- **Tiempo de inactividad:** es cualquier período de tiempo en un mes de facturación para una Suscripción de Microsoft AZURE determinada cuando los Números de teléfono asignados no pueden iniciar o recibir llamadas de voz a través de AZURE Communications Gateway.

- **Número de minutos de tiempo de inactividad:** es la suma de todo el Tiempo de inactividad, multiplicado por la cantidad de Números de teléfono asignados que

no pueden iniciar o recibir llamadas a través de AZURE Communications Gateway durante el Tiempo de inactividad determinado.

- **Número máximo de minutos disponibles:** es el número total de minutos en un mes de facturación que AZURE Communications Gateway se ha implementado correctamente (es decir, el estado de aprovisionamiento está marcado como completo) multiplicado por el número máximo de números de teléfono asignados en cualquier momento dentro de ese mes de facturación.
- **Porcentaje de tiempo de actividad mensual:** El porcentaje de tiempo de actividad mensual se calcula utilizando la siguiente fórmula:

$$\frac{Maximum\ Available\ Number\ Minutes - Downtime\ Number\ Minutes}{Maximum\ Available\ Number\ Minutes}\ x\ 100$$

Este SLA no se aplica a interrupciones causadas por fallas de software, equipos o servicios de terceros que no están controlados por Microsoft, o software de Microsoft que no se ejecuta como parte de este Servicio.

Los siguientes Niveles de Servicio y Créditos de Servicio se aplican al uso del Cliente de AZURE Communications Gateway:

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,99%	25%
<98%	50%
<95	100%

17.21. SERVICIOS DE COMUNICACIÓN DE AZURE

- **Tiempo de inactividad:** Cualquier período de tiempo en el que los usuarios finales no pueden iniciar una llamada PSTN o no pueden acceder al audio de la conferencia a través de la PSTN.
- **Minutos de Usuario:** significa el número total de minutos en un mes, menos todo el Tiempo de Inactividad Programado, multiplicado por el número total de usuarios. SLA de llamadas de audio y video
- **Porcentaje de tiempo de actividad mensual:** el porcentaje de tiempo de actividad mensual se calcula mediante la siguiente fórmula:

$$\frac{User\ Minutes - Downtime}{User\ Minutes}\ x\ 100$$

donde el tiempo de inactividad se mide en minutos de usuario; es decir, para cada mes, el tiempo de inactividad es la suma de la duración (en minutos) de cada incidente que ocurre durante ese mes multiplicado por la cantidad de usuarios afectados por ese incidente.

Tarifa Mensual de Buena Llamada	Crédito de servicio
<99,9%	10%
<99%	25%

Servicios sin llamadas

Todos los demás servicios basarán el cálculo del SLA en el tiempo de actividad de la puerta de enlace del servicio. Esto se aplicará a cada una de las siguientes ofertas individuales dentro de AZURE Communication Services:

- Charlar
- SMS
- Proveedor de recursos
- Autenticación (UTM)

Tiempo de actividad: se calcula con la siguiente fórmula:

$$\frac{Total\ Requests - Unavailable\ Requests}{Total\ Requests}\ x\ 100$$

donde Solicitudes no disponibles son solicitudes que dan como resultado errores 5xx.

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,9%	10%
<99%	25%

- **Términos adicionales:** el crédito de servicio se aplicará al servicio individual que no estaba disponible. Si el Cliente está utilizando los servicios de SMS y Chat, y el servicio de SMS no cumple con el SLA, el Cliente recibirá un crédito por el uso de SMS, no por el uso de chat.

  Los minutos disponibles se basan únicamente en los servicios que están bajo el control de AZURE Communication Services; esto excluye servicios de terceros como proveedores de telecomunicaciones y operadores.

17.22. AZURE SPRING APPS

- **Aplicación:** es una aplicación Spring Boot implementada por el Cliente dentro de AZURE Spring Apps. Excluyendo Apps en el Nivel Básico.

- **Spring Apps Service Runtime:** es una colección de componentes de Spring Apps (Spring Apps Config Server, Spring Apps Registry) alojados por Microsoft.

Cálculo del tiempo de actividad mensual y niveles de servicio para AZURE Spring Apps

- **Minutos de implementación:** es la cantidad total de minutos que se ha configurado para ejecutar una aplicación determinada en Microsoft AZURE durante un mes de facturación. Los minutos de implementación se miden desde el momento en que se creó la aplicación o el cliente inició una acción que daría lugar a la ejecución de la aplicación hasta el momento en que el cliente inició una acción que daría lugar a la detención o eliminación de la aplicación.
- **Máximo de Minutos Disponibles:** es la suma de todos los Minutos de Implementación en todas las Aplicaciones implementadas por el Cliente en una determinada suscripción de Microsoft AZURE durante un mes de facturación.
- **Tiempo de Inactividad:** es la suma de todos los Minutos de Implementación, en todas las Aplicaciones implementadas por el Cliente en una determinada suscripción de Microsoft AZURE, durante un mes de facturación durante el cual la Aplicación no está disponible. Se considera que un minuto no está disponible para una aplicación determinada si todos los intentos continuos de conexión entre la aplicación y la puerta de enlace de Internet de Microsoft o el tiempo de ejecución del servicio AZURE Spring Apps durante el minuto dan como resultado un código de error o no devuelven un código de éxito en cinco minutos.
- **Porcentaje de tiempo de actividad mensual:** El porcentaje de tiempo de actividad mensual se calcula mediante la siguiente fórmula:
-

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,95%	10%
<99%	25%

17.23. AZURE SQL SERVER

- **Zona de disponibilidad:** es un área aislada por fallas dentro de una región de AZURE, que proporciona alimentación, refrigeración y redes redundantes.
- **Base de datos:** se refiere a cualquier Base de datos SQL de Microsoft AZURE creada en cualquiera de los niveles de Servicio e implementada como una base de datos única o en un Grupo Elástico.
- **Implementación redundante de zona:** es una base de datos que se implementa en varias zonas de disponibilidad.
- **Principal:** hace referencia a cualquier Base de datos que tenga una relación de replicación geográfica activa con una Base de datos en otras regiones de AZURE. El primario puede procesar solicitudes de lectura y escritura desde la aplicación.
- **Secundaria:** hace referencia a cualquier base de datos que mantenga una relación de replicación geográfica asincrónica con una principal en otra región de AZURE y que se pueda usar como destino de conmutación por error. El secundario puede procesar solicitudes de solo lectura de las aplicaciones.
- **Secundario compatible:** significa cualquier Secundario que se crea con la misma configuración y en el mismo nivel de servicio que el Primario. Si el secundario se crea en un grupo elástico, se considera compatible si tanto el primario como el secundario se crean en grupos elásticos con configuraciones coincidentes y con una densidad que no supere las 250 bases de datos para una configuración compatible.

CÁLCULO DEL TIEMPO DE ACTIVIDAD MENSUAL Y NIVELES DE SERVICIO PARA AZURE SQL DATABASE SERVICE

- **Minutos de implementación:** es el número total de minutos que una base de datos determinada ha estado operativa en Microsoft AZURE durante un mes de facturación.
- **Máximo de Minutos Disponibles:** es la suma de todos los Minutos de Implementación para una determinada suscripción de Microsoft AZURE durante un mes de facturación.
- **Tiempo de inactividad:** es el total de minutos de implementación acumulados en todas las bases de datos en una determinada suscripción de Microsoft AZURE durante el cual la base de datos no está disponible. Se considera que un minuto no está disponible para una Base de datos dada si fallan todos los intentos continuos del Cliente de establecer una conexión a la Base de datos dentro del minuto.
- **Porcentaje de tiempo de actividad mensual:** para una base de datos dada se calcula como el máximo de minutos disponibles menos el tiempo de inactividad

dividido por el máximo de minutos disponibles en un mes de facturación para una determinada suscripción de Microsoft AZURE.

El porcentaje de tiempo de actividad mensual se calcula utilizando la siguiente fórmula:

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,99%	10%
<99%	25%
<95%	100%

Objetivo de punto de recuperación (RPO)

- **Geo-Replication Link:** es un objeto programático que representa una conexión entre un Primario específico y el Secundario.
- **Retraso de replicación geográfica:** es un lapso desde el punto de compromiso de la transacción en el principal y el reconocimiento por parte del secundario de que la actualización del registro de transacciones se ha mantenido.
- **Comprobación de retraso de replicación:** es un método programático para obtener el valor de retraso de replicación geográfica para un enlace de replicación geográfica específico.
- **Objetivo de punto de recuperación (RPO):** significa un retraso de replicación geográfica que no debe exceder los 5 segundos.

  N: es el número de verificación de retraso de replicación para un enlace de replicación geográfica determinado en una hora determinada.

  S: es el conjunto clasificado por retraso de los resultados de Verificación de retraso de replicación en orden ascendente para un Vínculo de replicación geográfica determinado en una hora determinada.
- **Rango ordinal:** es el percentil 99 usando el método de rango más cercano representado por la siguiente fórmula:

$$\frac{99}{100}\ x\ N$$

  P99 Replication Lag: es el valor en el rango ordinal de S.
- **Horas de implementación:** es la cantidad total de horas que una Secundaria compatible determinada ha estado operativa para una suscripción de Microsoft AZURE determinada durante un mes de facturación.
- **Horas de retraso excesivas:** es el número total de intervalos de una hora durante los cuales la comprobación de retraso de replicación resultó en un retraso de

replicación P99 mayor o igual a RPO para una suscripción de Microsoft AZURE determinada durante un mes de facturación. Si el número de comprobaciones de retraso de replicación en un intervalo de una hora determinado es cero, las horas de retraso excesivo para ese intervalo son 0.

- **Porcentaje de cumplimiento de RPO mensual:** para una implementación de base de datos determinada se calcula mediante la siguiente fórmula:

$$100\% - \frac{Excessive\ Lag\ Hours}{Deployment\ Hours}\ x\ 100$$

Los siguientes Niveles de Servicio y Créditos de Servicio se aplican al uso por parte del Cliente de la función de replicación geográfica activa con el nivel Business Critical del servicio AZURE SQL Database con un Secundario Compatible:

Operación	RPO	Porcentaje de consecución de RPO mensual	Crédito de servicio
Geo-Replicación	5 segundos	<100%	10% del costo mensual total de Secundario Conforme

OBJETIVO DE TIEMPO DE RECUPERACIÓN (RTO)

- **Conmutación por error no planificada:** es una acción iniciada por el Cliente cuando el Principal está fuera de línea para habilitar un Secundario compatible como Principal.
- **Tiempo de recuperación:** es el tiempo transcurrido desde la conmutación por error no planificada hasta que el secundario actúa como principal.
- **Objetivo de Tiempo de Recuperación (RTO):** significa un Tiempo de Recuperación máximo permitido que no exceda los 30 segundos.
- **Conmutación por error no planificada no conforme:** es una conmutación por error no planificada que no se pudo completar dentro del RTO.
- **Porcentaje de consecución de RTO mensual:** para una implementación de base de datos determinada, en un mes de facturación para una suscripción determinada, se representa mediante la siguiente fórmula:

$$\frac{Total\ Number\ of\ Unplanned\ Failovers\ -\ Total\ Number\ of\ Non-Compliant\ Unplanned\ Failovers}{Total\ Number\ of\ Unplanned\ Failovers}\ x\ 100$$

Los siguientes Niveles de servicio y Créditos de servicio se aplican al uso que hace el Cliente de la característica de replicación geográfica activa con el nivel de servicio Crítico para la empresa del servicio SQL Database con un Secundario compatible:

Operación	RTO	Porcentaje de consecución de RTO mensual	Crédito de servicio
Conmutación por error no planificada de una sola base de datos	30 segundos	<100%	100% del costo mensual total de Secundario Conforme

17.24. APLICACIONES WEB ESTÁTICAS

- **Minutos de implementación:** es la cantidad total de minutos que se ha configurado para ejecutar una aplicación determinada en Microsoft AZURE durante un mes de facturación. Los minutos de implementación se miden desde el momento en que se creó la aplicación o el cliente inició una acción que daría lugar a la ejecución de la aplicación hasta el momento en que el cliente inició una acción que daría lugar a la detención o eliminación de la aplicación.
- **Máximo de Minutos Disponibles:** es la suma de todos los Minutos de Implementación en todas las Aplicaciones implementadas por el Cliente en una determinada suscripción de Microsoft AZURE durante un mes de facturación.
- **Aplicación:** es una aplicación web implementada por el Cliente dentro de las aplicaciones web estáticas.
- **Tiempo de Inactividad:** El total de Minutos de Implementación acumulados, en todas las Aplicaciones implementadas por el Cliente en una determinada suscripción de Microsoft AZURE, durante los cuales la Aplicación no está disponible. Se considera que un minuto no está disponible para una aplicación determinada cuando no hay conectividad entre la aplicación y la puerta de enlace de Internet de Microsoft.
- **Porcentaje de tiempo de actividad mensual:** el porcentaje de tiempo de actividad mensual se calcula mediante la siguiente fórmula:

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,95%	10%
<99%	25%

17.25. AZURE BLOBS

- **Tasa de error promedio:** para un mes de facturación es la suma de las tasas de error de cada hora del mes de facturación dividida por el número total de horas del mes de facturación.
- **Cuenta de almacenamiento de blobs:** es una cuenta de almacenamiento especializada para almacenar datos como blobs y brinda la capacidad de especificar un nivel de acceso que indica la frecuencia con la que se accede a los datos de esa cuenta.
- **Cuenta de almacenamiento de blobs en bloques:** es una cuenta de almacenamiento especializada para almacenar datos como blobs en bloques o adjuntos en unidades de estado sólido.
- **Nivel de acceso esporádico:** es un atributo de un blob o cuenta que indica que se accede a él con poca frecuencia y tiene un nivel de servicio de disponibilidad más bajo que los blobs en el nivel de acceso frecuente.
- **Nivel de acceso activo:** es un atributo de un blob o cuenta que indica que se accede con frecuencia.
- **Transacciones excluidas:** son transacciones de almacenamiento que no cuentan ni para las Transacciones totales de almacenamiento ni para las Transacciones de almacenamiento fallidas. Las transacciones excluidas incluyen fallas de autenticación previa; fallas de autenticación; intentos de transacciones para cuentas de almacenamiento por encima de sus cuotas prescritas; creación o eliminación de contenedores, archivos compartidos, tablas o colas; limpieza de colas; y copiar blobs o archivos entre cuentas de almacenamiento.

  La " tasa de error " es el número total de transacciones de almacenamiento fallidas dividido por el total de transacciones de almacenamiento durante un intervalo de tiempo establecido (establecido actualmente en una hora). Si el total de transacciones de almacenamiento en un intervalo de una hora determinado es cero, la tasa de error para ese intervalo es 0%.
- **Transacciones de almacenamiento fallidas:** es el conjunto de todas las transacciones de almacenamiento dentro de las Transacciones de almacenamiento totales que no se completan dentro del Tiempo máximo de procesamiento asociado con su tipo de transacción respectivo, como se especifica en la tabla a continuación. El Tiempo máximo de procesamiento incluye solo el tiempo dedicado a procesar una solicitud de transacción dentro del Servicio de almacenamiento y no incluye el tiempo dedicado a transferir la solicitud hacia o desde el Servicio de almacenamiento.

Tipos de transacciones	Tiempo máximo de procesamiento
PutBlob y GetBlob (incluye bloques y páginas) Obtener intervalos de blobs en páginas válidos	Dos (2) segundos multiplicados por la cantidad de MB transferidos en el curso del procesamiento de la solicitud
PutFile y GetFile	Dos (2) segundos multiplicados por la cantidad de MB transferidos en el curso del procesamiento de la solicitud
Copiar blob	Noventa (90) segundos (donde los blobs de origen y destino están dentro de la misma cuenta de almacenamiento)
Copiar archivo	Noventa (90) segundos (donde los archivos de origen y destino están dentro de la misma cuenta de almacenamiento)
PonerBlockList ObtenerBlockList	Sesenta (60) segundos
Consulta de tabla Operaciones de lista Buscar operaciones	Diez (10) segundos (para completar el procesamiento o devolver una continuación)
Operaciones de tabla por lotes	Treinta (30) segundos
Todas las operaciones de tabla de una sola entidad	Dos (2) segundos
Todas las demás operaciones de blobs, archivos y mensajes	

Estas cifras representan los tiempos máximos de procesamiento. Se espera que los tiempos reales y promedio sean mucho más bajos. Las transacciones de almacenamiento fallidas no incluyen:

- Solicitudes de transacciones que son limitadas por el Servicio de almacenamiento debido a que no se obedecen los principios de interrupción apropiados.
- Solicitudes de transacciones que tienen tiempos de espera establecidos más bajos que los respectivos Tiempos máximos de procesamiento especificados anteriormente.
- Leer solicitudes de transacciones a cuentas RA-GRS para las que no intentó ejecutar la solicitud en la región secundaria asociada con la cuenta de almacenamiento si la solicitud a la región principal no tuvo éxito.
- Leer solicitudes de transacciones a cuentas RA-GRS que fallan debido a un retraso en la replicación geográfica.

- **Retraso de replicación geográfica:** para las cuentas GRS y RA-GRS es el tiempo que tardan los datos almacenados en la región principal de la cuenta de almacenamiento en replicarse en la región secundaria de la cuenta de almacenamiento. Debido a que las cuentas GRS y RA-GRS se replican de forma asíncrona en la región secundaria, los datos escritos en la región principal de la cuenta de almacenamiento no estarán disponibles inmediatamente en la región secundaria. Puede consultar el Retraso de replicación geográfica para una cuenta de almacenamiento, pero Microsoft no ofrece ninguna garantía en cuanto a la duración de cualquier Retraso de replicación geográfica bajo este SLA.
- **Cuenta de almacenamiento con redundancia geográfica (GRS):** es una cuenta de almacenamiento para la cual los datos se replican de forma síncrona dentro de una región principal y luego se replican de forma asíncrona en una región secundaria. No puede leer o escribir datos directamente en la región secundaria asociada con las cuentas GRS.
- **Cuenta de almacenamiento redundante localmente (LRS):** es una cuenta de almacenamiento para la cual los datos se replican de forma síncrona solo dentro de una región principal.
- **Región principal:** es una región geográfica en la que se encuentran los datos dentro de una cuenta de almacenamiento, según lo seleccionado por usted al crear la cuenta de almacenamiento. Puede ejecutar solicitudes de escritura solo en datos almacenados dentro de la región principal asociada con cuentas de almacenamiento.
- **Cuenta de almacenamiento con redundancia geográfica** con acceso de lectura (RA-GRS) " es una cuenta de almacenamiento para la cual los datos se replican de forma síncrona dentro de una región principal y luego se replican de forma asíncrona en una región secundaria. Puede leer datos directamente, pero no puede escribir datos en la región secundaria asociada con las cuentas RA-GRS.
- **Región secundaria:** es una región geográfica en la que los datos dentro de una cuenta GRS o RA-GRS se replican y almacenan, según lo asignado por Microsoft AZURE en función de la región principal asociada con la cuenta de almacenamiento. No puede especificar la región secundaria asociada con las cuentas de almacenamiento.
- **Total de Transacciones de Almacenamiento:** es el conjunto de todas las transacciones de almacenamiento, distintas de las Transacciones Excluidas, intentadas dentro de un intervalo de una hora en todas las cuentas de almacenamiento en el Servicio de Almacenamiento en una suscripción determinada.
- **Cuenta de almacenamiento con redundancia de zona (ZRS):** es una cuenta de almacenamiento para la cual los datos se replican en varias instalaciones. Estas

instalaciones pueden estar dentro de la misma región geográfica o en dos regiones geográficas.

- **Porcentaje de tiempo de actividad mensual:** el porcentaje de tiempo de actividad mensual se calcula mediante la siguiente fórmula:

$$100\% - Average\ Error\ Rate$$

Crédito de servicio: hot blobs en LRS, ZRS, GRS y RA-GRS (solicitudes de escritura) Cuentas y blobs en LRS Block Blob Storage Cuentas:

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,9%	10%
<99%	25%

Crédito de servicio – RA-GRS (solicitudes de lectura) Cuentas :

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,99%	10%
<99%	25%

Crédito de servicio: LRS, GRS y RA-GRS (solicitudes de escritura) Cuentas de almacenamiento de blobs (nivel de acceso esporádico):

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99%	10%
<98%	25%

Crédito de servicio: RA-GRS (solicitudes de lectura) Cuentas de almacenamiento de blobs (nivel de acceso esporádico):

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,9%	10%
<98%	25%

17.26. SEGURIDAD DE APLICACIONES EN LA NUBE DE MICROSOFT

- **Tiempo de inactividad:** cualquier período de tiempo en el que el administrador de TI del Cliente o los usuarios autorizados por el Cliente no puedan iniciar sesión con las credenciales adecuadas. El tiempo de inactividad programado no excederá las 10 horas por año calendario.

- **Porcentaje de tiempo de actividad mensual:** el porcentaje de tiempo de actividad mensual se calcula mediante la siguiente fórmula:

$$\frac{User\ Minutes\ -\ Downtime}{User\ Minutes}\ x\ 100$$

Donde el tiempo de inactividad se mide en minutos de usuario; es decir, para cada mes, el Tiempo de Inactividad es la suma de la duración (en minutos) de cada Incidente que ocurre durante ese mes multiplicada por la cantidad de usuarios afectados por ese Incidente.

Porcentaje de tiempo de actividad mensual	Crédito de servicio
<99,9%	10%
<99%	25%

17.27. APÉNDICE A: COMPROMISO DE NIVEL DE SERVICIO PARA LA DETECCIÓN Y EL BLOQUEO DE VIRUS, LA EFICACIA DEL CORREO NO DESEADO O LOS FALSOS POSITIVOS

Con respecto a Exchange Online y EOP con licencia como un Servicio independiente o a través de la suite ECAL, o Exchange Enterprise CAL con Servicios, puede ser elegible para Créditos de Servicio si no alcanzamos el Nivel de Servicio descrito a continuación para: (1) Detección y Bloqueo de Virus, (2) Eficacia del spam o (3) Falso positivo. Si no se alcanza alguno de estos Niveles de servicio individuales, puede presentar una reclamación de Crédito de servicio. Si un Incidente hace que fallemos en más de una métrica de SLA para Exchange Online o EOP, solo puede realizar un reclamo de Crédito de servicio para ese incidente por Servicio.

NIVEL DE SERVICIO DE DETECCIÓN Y BLOQUEO DE VIRUS

- "Detección y bloqueo de virus" se define como la detección y el bloqueo de virus por parte de los filtros para prevenir infecciones. "Virus" se define ampliamente como programa maligno conocido, que incluye virus, gusanos y caballos de Troya.
- Un virus se considera conocido cuando los motores comerciales de detección de virus ampliamente utilizados pueden detectar el virus y la capacidad de detección está disponible en toda la red EOP.
- Debe ser el resultado de una infección no intencionada.
- El virus debe haber sido escaneado por el filtro de virus EOP.
- Si EOP le entrega un correo electrónico que está infectado con un virus conocido, EOP le notificará y trabajará con usted para identificarlo y eliminarlo. Si esto

resulta en la prevención de una infección, no será elegible para un Crédito de servicio bajo el Nivel de servicio de detección y bloqueo de virus.

- El Nivel de Servicio de Detección y Bloqueo de Virus no se aplicará a:
    - Formas de abuso de correo electrónico no clasificadas como malware, como spam, phishing y otras estafas, adware y formas de spyware, que debido a su naturaleza dirigida o uso limitado no son conocidas por la comunidad antivirus y, por lo tanto, no son rastreadas por antivirus. productos de virus como un virus.
    - Virus corruptos, defectuosos, truncados o inactivos contenidos en NDR, notificaciones o correos electrónicos rebotados.
- El Crédito de Servicio disponible para el Servicio de Detección y Bloqueo de Virus es: 25% de Crédito de Servicio de la Tarifa de Servicio Mensual Aplicable si ocurre una infección en un mes calendario, con un máximo de un reclamo permitido por mes calendario.

NIVEL DE SERVICIO DE EFECTIVIDAD DE SPAM

- La “efectividad del spam” se define como el porcentaje de spam entrante detectado por el sistema de filtrado, medido diariamente.
- Las estimaciones de la eficacia del correo no deseado excluyen los falsos negativos en los buzones de correo no válidos.
- El mensaje de spam debe ser procesado por nuestro servicio y no estar corrupto, malformado o truncado.
- El nivel de servicio de efectividad de correo no deseado no se aplica al correo electrónico que contiene la mayoría del contenido que no está en inglés.
- Usted reconoce que la clasificación del correo no deseado es subjetiva y acepta que haremos una estimación de buena fe de la tasa de captura de correo no deseado en función de las pruebas que usted proporcione oportunamente.

El Crédito de Servicio disponible para el Servicio de Efectividad de Spam es:

% del mes calendario en que la efectividad del spam está por debajo del 99 %	Crédito de servicio
>25%	25%
> 50%	50%
100%	100%

NIVEL DE SERVICIO FALSO POSITIVO

- Falso positivo" se define como la proporción de correos electrónicos comerciales legítimos identificados incorrectamente como spam por el sistema de filtrado con respecto a todos los correos electrónicos procesados por el servicio en un mes calendario.
- Los mensajes completos y originales, incluidos todos los encabezados, deben informarse al equipo de abuso.
- Se aplica únicamente al correo electrónico enviado a buzones de correo válidos.
- Usted reconoce que la clasificación de los falsos positivos es subjetiva y comprende que haremos una estimación de buena fe de la proporción de falsos positivos en función de las pruebas que usted proporcione oportunamente.
- Este Nivel de Servicio de Falso Positivo no se aplicará a:
    - correo electrónico masivo, personal o pornográfico
    - correo electrónico que contiene la mayoría del contenido que no está en inglés
    - correo electrónico bloqueado por una regla de política, filtrado de reputación o filtrado de conexión SMTP
    - correo electrónico enviado a la carpeta de correo no deseado

18. COMUNICACIONES ENTRE SERVICIOS AZURE

Los sistemas nativos en la nube adoptan microservicios para construir aplicaciones modernas. La arquitectura de microservicios es distribuida y ligeramente acoplada, por lo que un error en un componente no interrumpe toda la aplicación. Por lo tanto, los servicios deben interactuar mediante un protocolo de comunicación entre procesos como HTTP, AMQP o un protocolo binario como TCP, en función de la naturaleza de cada servicio.

18.1. MICROSERVICIOS

Los microservicios son componentes independientes construidos como un conjunto distribuido de servicios pequeños que interactúan a través de un tejido compartido y se comunican con contratos de API bien definidos. Las aplicaciones basadas en microservicios se utilizan para satisfacer las necesidades empresariales que cambian rápidamente y comercializar las nuevas características más rapidez.

Características

- Cada uno implementa una capacidad de negocio específica dentro de un contexto de dominio más amplio.

- Cada uno se desarrolla de forma autónoma y puede desplegarse independientemente.
- Cada uno es autónomo y encapsula su propia tecnología de almacenamiento de datos, dependencias y plataforma de programación.
- Cada una se ejecuta en su propio proceso y se comunica con las demás mediante protocolos de comunicación estándar, como HTTP/HTTPS, gRPC, WebSockets o AMQP.
- Se componen juntos para formar una aplicación.
- Normalmente los diversos microservicios que componen una aplicación de un extremo a otro se establecen mediante comunicaciones REST y comunicaciones flexibles controladas por eventos en lugar de orquestadores de procesos de negocios centralizados.
- Los dos protocolos que se usan habitualmente son respuesta-solicitud HTTP con API de recurso y mensajería asincrónica ligera al comunicar actualizaciones en varios microservicios.

18.2. TIPOS DE COMUNICACIÓN

El cliente y los servicios pueden comunicarse a través de muchos tipos de comunicación, cada uno de ellos se encuentra destinado a distintos escenarios y objetivos. Inicialmente, esos tipos de comunicaciones se pueden clasificar en dos ejes.

18.2.1. PRIMER EJE

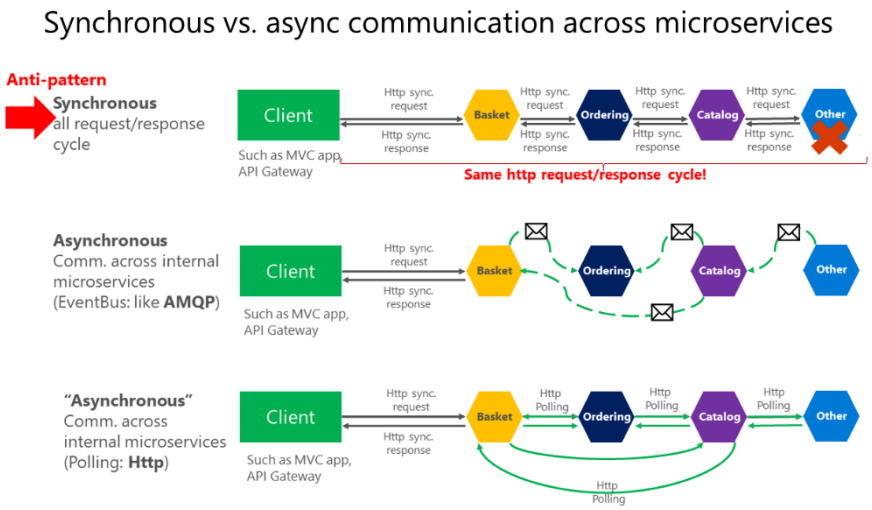
El primer eje define si el protocolo es sincrónico o asincrónico:

18.2.1.1. PROTOCOLO SINCRÓNICO

HTTP es un protocolo sincrónico. El cliente envía una solicitud y espera una respuesta del servicio. Eso es independiente de la ejecución de código de cliente, que puede ser sincrónica o asincrónica. El protocolo (HTTP/HTTPS) es sincrónico y el código de cliente solo puede continuar su tarea cuando recibe la respuesta del servidor HTTP.

18.2.1.2. PROTOCOLO ASINCRÓNICO

Normalmente el código de cliente o el remitente del mensaje no espera ninguna respuesta. Simplemente envía el mensaje al igual que cuando se envía un mensaje a una cola o a cualquier otro agente de mensajes.



Protocolo sincrónico o asincrónico

18.2.2. SEGUNDO EJE

El segundo eje define si la comunicación tiene un único receptor o varios:

18.2.2.1. RECEPTOR ÚNICO

Cada una de las solicitudes deben ser procesadas por un receptor o servicio exactamente.

18.2.2.2. VARIOS RECEPTORES

Cada solicitud puede ser procesada por cero y varios receptores. Este tipo de comunicación debe ser asincrónica; se basa en una interfaz de bus de eventos para extender las actualizaciones de datos entre varios microservicios mediante eventos. Este tipo de eje se implementa a través de un bus de servicio o algún tipo de artefacto similar como AZURE Service Bus mediante temas y suscripciones. Una aplicación basada en microservicio suele usar una combinación de estos estilos de comunicación. El tipo más habitual es la comunicación de un único receptor con un protocolo sincrónico como HTTP/HTTPS al invocar a un servicio normal HTTP Web API.

18.3. DISEÑO DE COMUNICACIÓN

La comunicación entre los diferentes microservicios tiene que ser eficiente y sólida, debido a la gran cantidad de pequeños servicios interactuando para realizar una sola

actividad comercial. Hay varios enfoques ampliamente aceptados para implementar la comunicación entre servicios. A menudo, el tipo de interacción de la comunicación será lo que determine cuál es el mejor enfoque.

Los microservicios se comunican entre sí mediante API y tecnologías de mensajería. Las llamadas a métodos locales en proceso entre componentes se sustituyen ahora por llamadas de red. Cada microservicio debe comunicarse a través de protocolo de red, lo que le añade complejidad al sistema:

- La congestión de la red, la latencia y los fallos transitorios son una preocupación constante.
- La resiliencia (es decir, el reintento de peticiones fallidas) es esencial.
- Algunas llamadas deben ser idempotentes para mantener un estado coherente.
- Cada microservicio debe autenticar y autorizar las llamadas.
- Cada mensaje debe serializarse y luego deserializarse, lo que puede resultar costoso.
- El cifrado/descifrado de mensajes se vuelve importante.

Microsoft, proporciona una cobertura en profundidad de los patrones de comunicación para aplicaciones de microservicios.

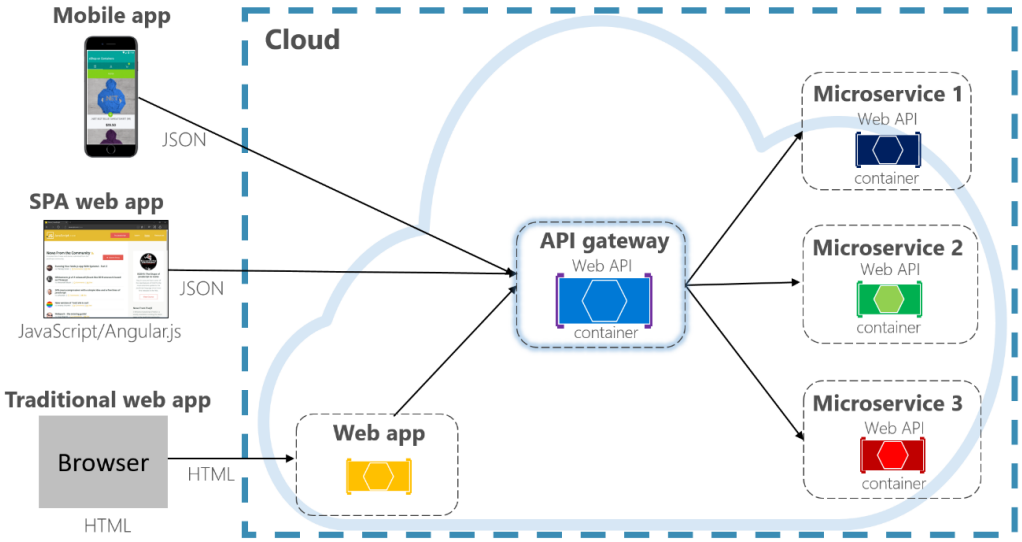
18.4. COMUNICACIÓN CON EL CLIENTE

En un sistema nativo en la nube, los clientes frontales (aplicaciones móviles, web y de escritorio) requieren un canal de comunicación para poder interactuar con los diversos microservicios back-end independientes. Un patrón de diseño de nube ampliamente aceptado es implementar un servicio de puerta de enlace API entre las aplicaciones de front-end y los servicios de back-end.

18.4.1. AZURE APPLICATION GATEWAY

El servicio API Gateway abstrae los microservicios principales de back-end. Implementado como una API web, actúa como un proxy inverso, enrutando el tráfico entrante a los microservicios internos. La puerta de enlace aísla al cliente de la partición y refactorización de servicios internos. Si cambia un servicio de back-end, lo acomoda en la puerta de enlace sin romper el cliente. Los sistemas más grandes a menudo exponen varias puertas de enlace API segmentadas por tipo de cliente (móvil, web,

escritorio) o funcionalidad de back-end. El patrón back-end for front-end proporciona instrucciones para implementar múltiples puertas de enlace.



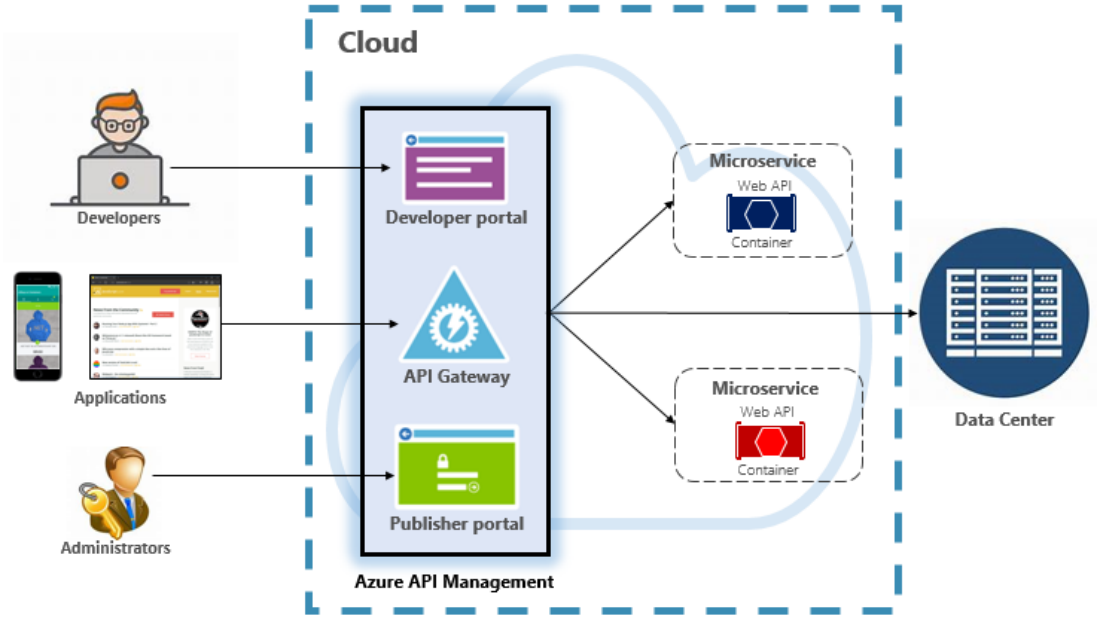
Patrón back-end for front-end

18.4.2. AZURE API MANAGEMENT

Es un servicio basado en la nube que no solo resuelve sus necesidades de API Gateway, sino que también proporciona una experiencia administrativa y de desarrollo con todas las funciones. El API Management expone un servidor de puerta de enlace que permite el acceso controlado a los servicios de back-end en función de reglas y políticas configurables.

Los administradores aplican políticas a cada punto final para afectar el comportamiento. Las políticas son declaraciones preconstruidas que se ejecutan secuencialmente para cada llamada de servicio. Adicionalmente se configuran para una llamada entrante, una llamada saliente o se invocan en caso de error.

AZURE API Management puede exponer los servicios de back-end que están alojados en cualquier lugar, en la nube o en su centro de datos. Para los servicios heredados que puede exponer en sus sistemas nativos de la nube, es compatible con las API REST y SOAP.



AZURE API Management

18.5. COMUNICACIÓN SERVICIO A SERVICIO

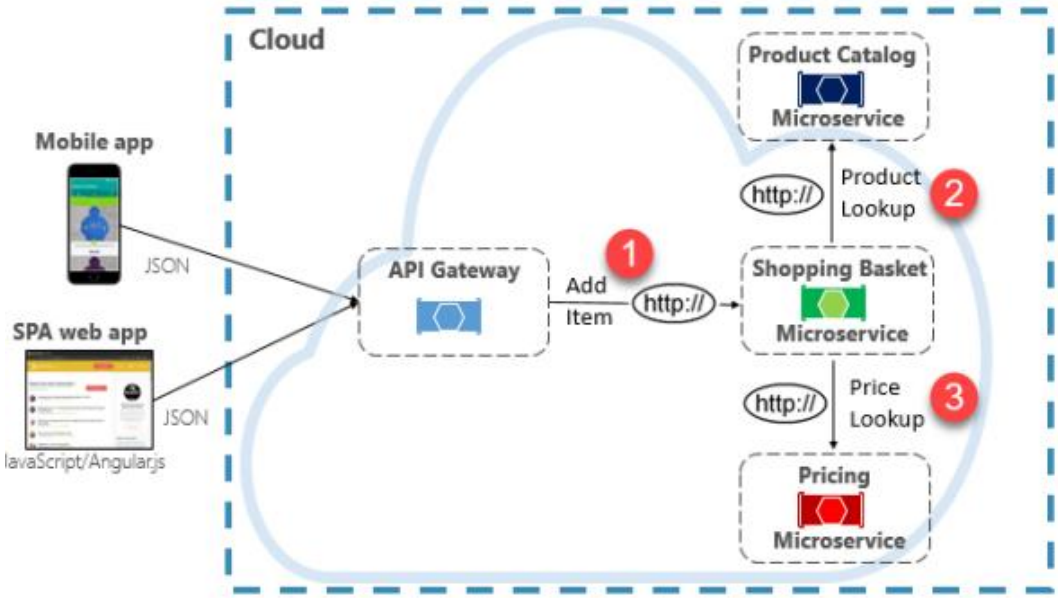
18.5.1. CONSULTAS

Es un enfoque que se centra en que un microservicio podría realizar una llamada a otro, lo que requiere una respuesta inmediata del microservicio para completar una operación. Hay muchos enfoques para implementar operaciones de consulta.

18.5.2. MENSAJERÍA DE SOLICITUD-RESPUESTA

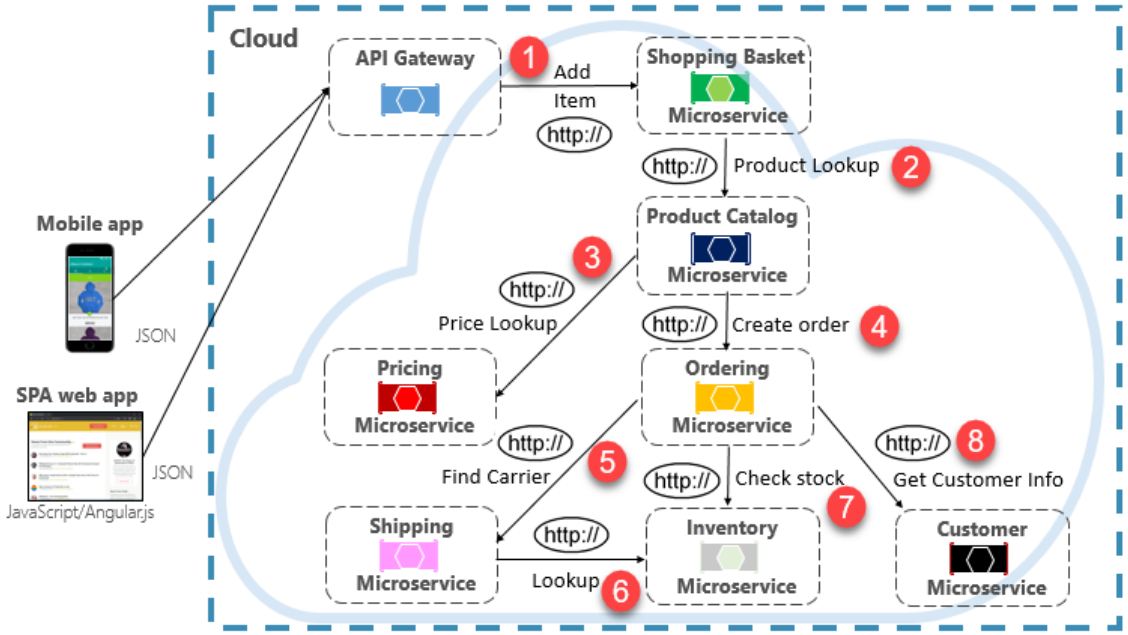
Cuando un cliente usa la comunicación solicitud-respuesta, envía una solicitud a un servicio, este la procesa y luego envía una respuesta. Este tipo de comunicación es especialmente idónea para consultar datos de una interfaz de usuario en tiempo real desde aplicaciones cliente.

En una arquitectura de microservicio probablemente se use este mecanismo de comunicación para la mayoría de las consultas



Mensajería de Solicitud – Respuesta

Una serie prolongada de comunicación HTTP directa puede desembocar en una concatenación profunda y compleja de llamadas a microservicios sincrónicos



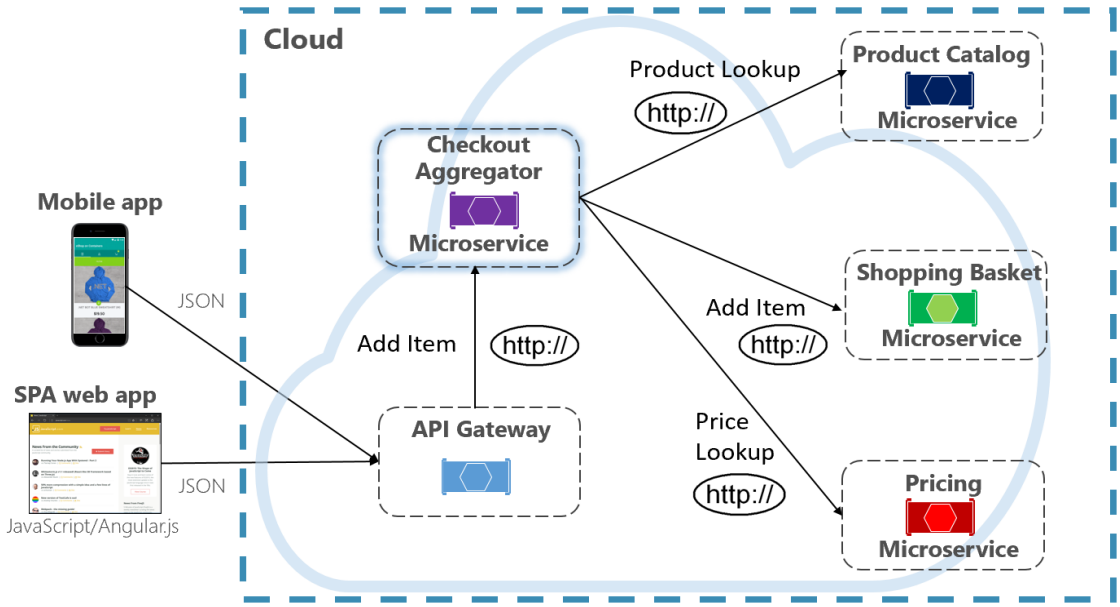
Llamada de microservicios sincrónicos

18.5.3. PATRÓN DE VISTA MATERIALIZADA

Una opción popular para eliminar el acoplamiento de microservicios es el patrón Materialized View. Con este modelo un microservicio almacena su propia copia local desnormalizada de los datos que pertenecen a otros servicios.

18.5.4. PATRÓN DE AGREGADOR DE SERVICIOS

Este patrón es otra opción que se utiliza para acabar con el acoplamiento de microservicios. Este esquema aísla una operación que permite realizar llamadas a distintos microservicios back-end, centralizando esta lógica en un microservicio especializado.

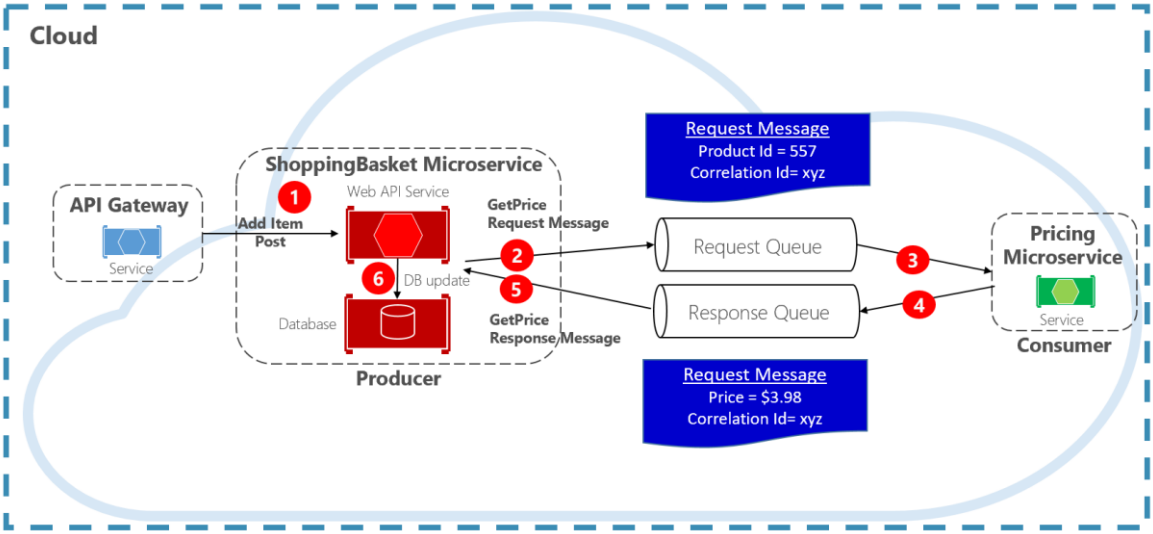


Patrón de agregador de servicios

En la figura anterior, el microservicio agregador de finalización de compra organiza el flujo de trabajo para la operación de finalización de compra. Este patrón incluye llamadas a diferentes microservicios back-end en un orden secuenciado. Los datos del flujo de trabajo se agregan y se devuelven al creador de la llamada. Aunque sigue implementando llamadas HTTP directas, el microservicio de agregador reduce las dependencias directas entre los microservicios back-end.

18.5.5. PATRÓN DE SOLICITUD/RESPUESTA

Es un enfoque para desacoplar mensajes HTTP sincrónicos que usa la comunicación de puesta en cola. La comunicación mediante una cola es continuamente un canal unidireccional, con un productor que envía el mensaje y un consumidor que lo recibe. Con este patrón, se implementan una cola de solicitudes y una cola de respuestas.



Patrón de solicitud - respuesta

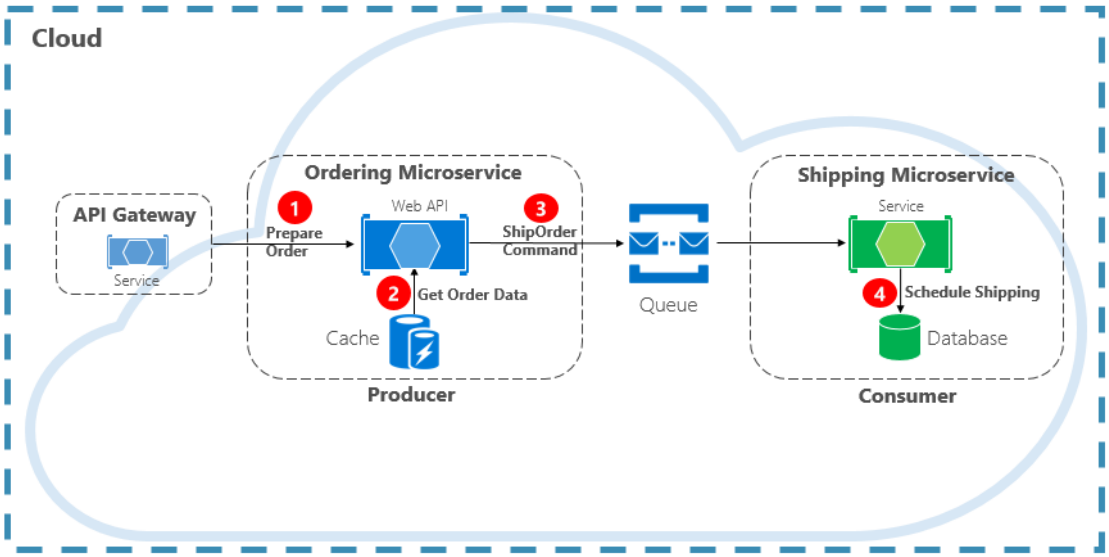
El productor del mensaje crea un mensaje basado en consultas que contiene un identificador de correlación único, y lo coloca en una cola de solicitudes. El servicio que consume quita el mensaje de la cola, lo procesa y coloca la respuesta en la cola de respuestas con el mismo identificador de correlación. El servicio productor quita el mensaje de la cola, lo coteja con el identificador de correlación y sigue procesando.

18.5.6. COMANDO

El comando es otro tipo de interacción de comunicación, en el cual un microservicio puede necesitar que otro microservicio realice una acción. En la siguiente figura, observamos como un microservicio (el productor) envía un mensaje a otro microservicio (el consumidor) y le ordena que haga algo, pero no requiere una respuesta.

La mayoría de las veces, el productor no requiere una respuesta, pero en el caso de que sí se necesite una réplica, el consumidor devuelve un mensaje independiente al productor en otro canal. La mejor forma de enviar un mensaje de comando es hacerlo de forma asincrónica con una cola de mensajes compatible con un agente de mensajes ligero.

Una cola es una construcción intermedia a través de la cual un productor y consumidor pasan un mensaje. Este tipo de comunicación implementa un patrón de mensajería asincrónica de punto a punto, en donde el productor sabe dónde se debe enviar un comando y lo enruta correctamente, garantizando que el mensaje sea procesado exactamente mediante una de las instancias de consumidor que leen el canal.



Comando

En este escenario, tanto el servicio productor como el consumidor pueden llegar escalar horizontalmente sin verse afectados entre sí, utilizando tecnologías que pueden ser distintas en cada lado.

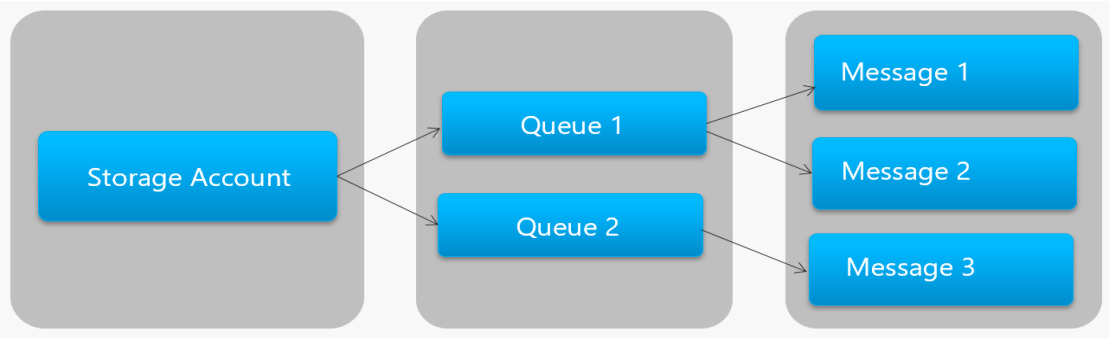
La nube de AZURE admite dos tipos de colas de mensajes que los sistemas nativos de nube pueden consumir para implementar la mensajería de comandos: colas de AZURE Storage y colas de AZURE Service Bus.

18.5.7. COLAS DE AZURE STORAGE

Las colas de AZURE Storage ofrecen una infraestructura de colas sencilla que es rápida y asequible y que está respaldada por las cuentas de AZURE Storage. Es un servicio para almacenar grandes cantidades de mensajes, a los que se puede acceder desde cualquier lugar del mundo a través de llamadas autenticadas mediante HTTP o HTTPS.

Las colas de AZURE Storage incluyen un mecanismo de puesta en cola basado en REST con una mensajería confiable y persistente, que puede escalar horizontalmente a un

gran número de clientes simultáneos para controlar los picos de tráfico. Proporcionan un conjunto de características mínimo, un solo mensaje puede tener un tamaño máximo de 64 KB.



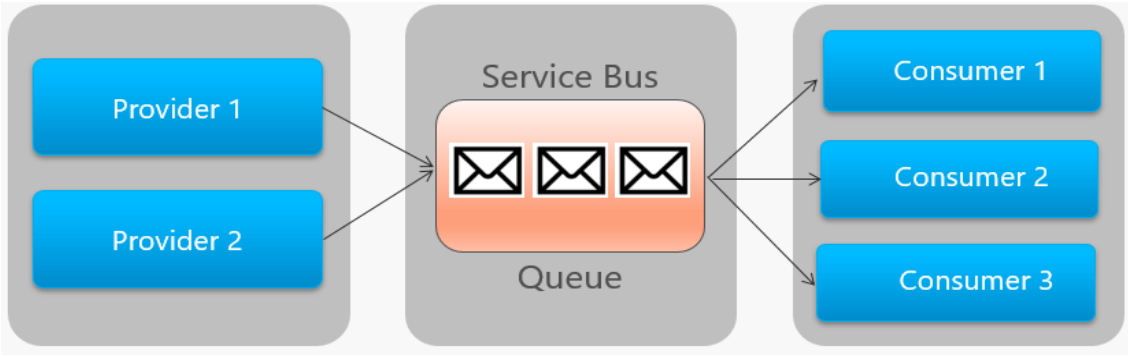
Colas de AZURE Store

18.5.8. LIMITACIONES

- El orden de los mensajes no está garantizado.
- Un mensaje se conserva solo siete días antes de que se quite automáticamente.
- No existe compatibilidad con la administración de estados, la detección de duplicados o las transacciones.

18.5.9. COLAS DE AZURE SERVICE BUS

AZURE Service Bus se establece dentro de una infraestructura de mensajes muy sólida, admite un modelo de mensajería asincrónica y los mensajes se almacenan de forma confiable en un agente (la cola) hasta que el consumidor los recibe. La cola de mensajes garantiza una entrega de mensajes de tipo FIFO (el primero en entrar es el primero en salir), respetando el orden en el que los mensajes se agregaron a la cola. Service Bus proporciona un amplio conjunto de características, incluida la compatibilidad con transacciones y una característica de detección de duplicados.



Service Bus

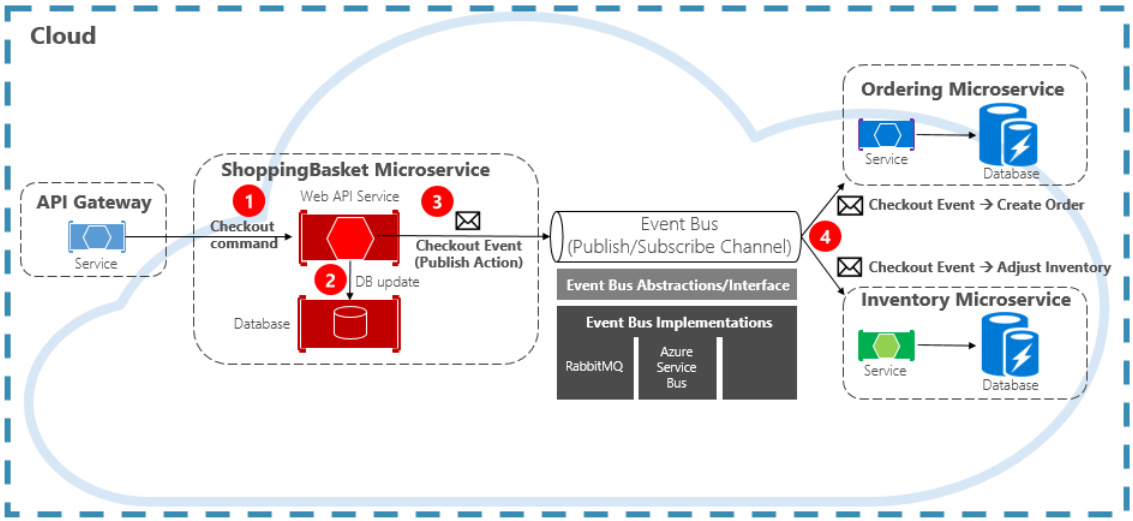
18.5.10. CARACTERÍSTICAS

- El tamaño de las colas de Service Bus está limitado a 80 GB y un mensaje puede tener un tamaño mucho mayor, hasta 256 KB.
- Los mensajes se conservan en la cola durante un período de tiempo ilimitado.
- Admite llamadas basadas en HTTP, sino que también proporciona plena compatibilidad con el protocolo AMQP (Estándar abierto que admite un protocolo binario).
- La cola garantiza "una entrega como máximo" por mensaje.
- La detección de duplicados nos libera de tener que crear más infraestructura.
- Una cola de mensajes de Service Bus al uso se controla por medio de un único agente de mensajes y se almacena en un único almacén de mensajes.
- El rendimiento general ya no está limitado por el rendimiento de un agente de mensajes o almacén de mensajería en concreto.
- Una interrupción temporal de un almacén de mensajería no hace que una cola particionada deje de estar disponible.

18.5.11. EVENTO

Este estilo arquitectónico controlado por eventos consiste en un proceso de dos pasos. El microservicio (publicador) genera un evento que indica que un estado ha cambiado o que se ha producido una acción. El microservicio interesado es notificado mediante la suscripción al evento en el agente de mensajes.

El publicador y los suscriptores no tienen conocimiento el uno de los otros y los sistemas de microservicios utilizan una combinación de estos tipos de interacción al realizar operaciones que requieren la interacción entre servicios. Para implementar la comunicación basada en eventos se usa el patrón publicador/suscriptor.



Eventos

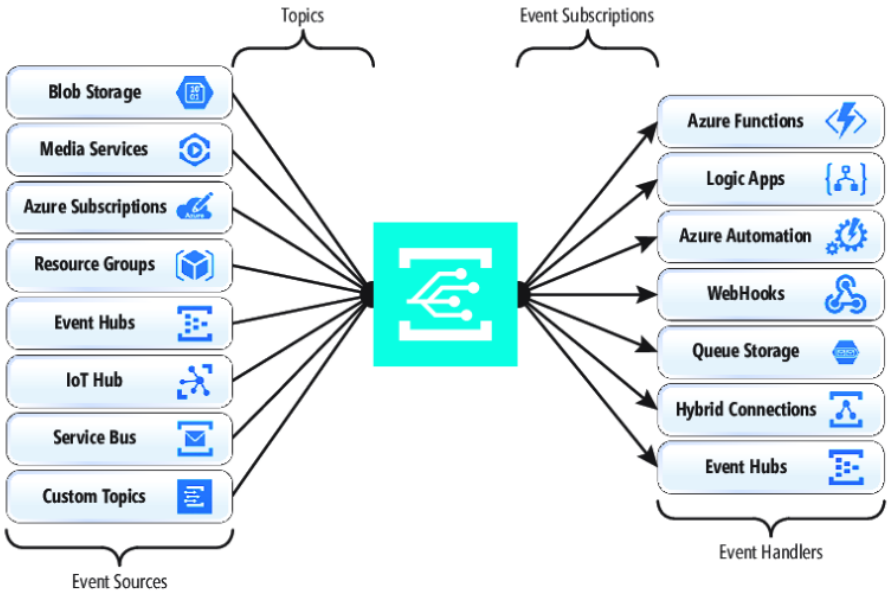
El componente de bus de eventos que se encuentra en el centro del canal de comunicación. Es una clase personalizada que encapsula el agente de mensajes y lo desacopla de la aplicación subyacente.

18.5.12. AZURE EVENT GRID

Se centra en las cargas de trabajo controladas por eventos, lo que permite el procesamiento de eventos en tiempo real, una profunda integración con AZURE y una infraestructura sin servidor de plataforma abierta.

18.5.12.1. CARACTERÍSTICAS

- Admite un modelo de suscriptor filtrado según el cual cada suscripción establece las reglas relativas a los eventos que quiere recibir.
- Tiene profunda integración en el tejido de la infraestructura de AZURE.
- Publica eventos desde una suscripción de AZURE, un grupo de recursos o un servicio, lo que confiere a los desarrolladores un control específico sobre el ciclo de vida de los recursos de nube.
- Consume eventos HTTP personalizados publicados desde aplicaciones o servicios de terceros, así como enrutar eventos a suscriptores externos.



AZURE Event Grid

18.5.12.2. GRPC

GRPC es un marco moderno de alto rendimiento que desarrolla el protocolo de llamada a procedimiento remoto (RPC) antiguo. A nivel de aplicación, gRPC simplifica la mensajería entre los clientes y los servicios back-end. En las aplicaciones nativas de la nube, los desarrolladores a menudo trabajan en lenguajes de programación, marcos y tecnologías. Esta interoperabilidad complica los contratos de mensajes necesaria para la comunicación entre plataformas. gRPC proporciona una "capa horizontal uniforme". Los desarrolladores codifican en su plataforma nativa enfocada en la funcionalidad comercial, mientras que gRPC maneja la plomería de comunicación.

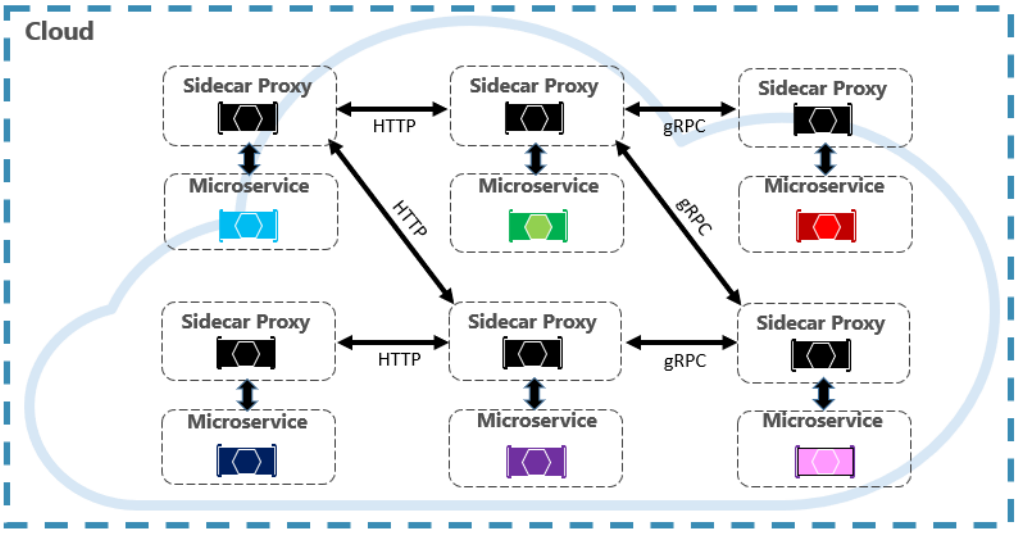
18.5.12.2.1. BENEFICIOS

- GRPC usa HTTP/2 para su protocolo de transporte. Si bien es compatible con HTTP 1.1, HTTP/2 presenta muchas capacidades avanzadas:
- Un protocolo de tramas binarias para el transporte de datos, a diferencia de HTTP 1.1, que se basa en texto.
- Compatibilidad de multiplexación para enviar varias solicitudes paralelas a través de la misma conexión: HTTP 1.1 limita el procesamiento a un mensaje de solicitud/respuesta a la vez.
- Comunicación bidireccional full-duplex para enviar solicitudes de clientes y respuestas del servidor simultáneamente.

- Transmisión integrada que permite solicitudes y respuestas para transmitir grandes conjuntos de datos de forma asíncrona.
- Compresión de encabezado que reduce el uso de la red.

18.6. INFRAESTRUCTURA DE COMUNICACIÓN SERVICE MESH

Es una capa de infraestructura configurable con capacidades integradas para manejar la comunicación de servicio a servicio, la capacidad de recuperarse y muchas preocupaciones transversales, además que transfiere la responsabilidad de estas preocupaciones fuera de los microservicios a la capa de malla de servicios. Un componente clave de una red de servicios es un proxy. En una aplicación nativa de la nube, normalmente se coloca una instancia de un proxy con cada microservicio. Si bien se ejecutan en procesos separados, los dos están estrechamente vinculados y comparten el mismo ciclo de vida.



Service Mesh

En la siguiente figura, se visualiza como un proxy que se ejecuta junto con cada microservicio intercepta los mensajes; cada proxy se puede configurar con reglas de tráfico específicas en donde entiende los mensajes y puede enrutarlos a través de sus servicios y el mundo exterior.

Una vez configurada, una red de servicios es altamente funcional. La malla recupera un grupo correspondiente de instancias de un punto final de detección de servicios, envía una solicitud a una instancia de servicio específica, registrando la latencia y el tipo de respuesta del resultado. Elige la instancia con más probabilidades de devolver una

respuesta rápida en función de diferentes factores, incluida la latencia observada para las solicitudes recientes.

19. CAPAS DE SEGURIDAD DE LOS SISTEMAS DE ELTHON

La capa de seguridad implementada en la empresa ELTHON CEO, está basada en tecnología Spring Boot y orientada a microservicios, utiliza varias tecnologías y enfoques para garantizar la seguridad y la arquitectura de la solución. A continuación, se describe cada uno de los componentes utilizados:

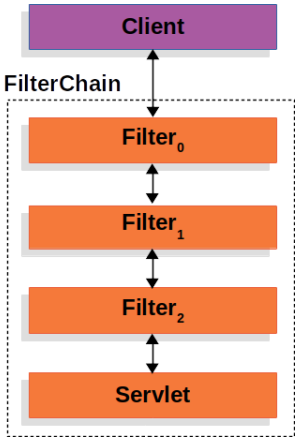
- **Spring Boot:** Spring Boot es un framework de desarrollo de aplicaciones Java que simplifica la configuración y la implementación de aplicaciones, proporcionando características de seguridad y facilitando la creación de microservicios.
- **Sesiones por REDIS:** REDIS es una base de datos en memoria de alta velocidad. En este caso, se utiliza para almacenar y gestionar las sesiones de los usuarios. Al utilizar REDIS, se obtiene un almacenamiento rápido y eficiente de las sesiones, lo que permite un manejo escalable y distribuido.
- **Spring Security:** Spring Security es un módulo de Spring que proporciona autenticación y control de acceso a las aplicaciones. Permite definir reglas de seguridad, como autenticación basada en contraseñas, tokens o certificados, y autorización basada en roles o permisos.
- **JWT (JSON Web Tokens):** Los JSON Web Tokens son una forma segura de transmitir información entre partes de manera compacta y autónoma como un objeto JSON. En este caso, se utilizan para autenticar y autorizar solicitudes en los microservicios. El token contiene información codificada, como roles o permisos, y se firma digitalmente para asegurar su integridad.
- **Encriptado por bcrypt:** bcrypt es un algoritmo de hash de contraseñas fuertemente resistente a ataques de fuerza bruta y diccionario. Se utiliza para cifrar y almacenar las contraseñas de los usuarios de manera segura. El bcrypt se caracteriza por su lenta velocidad de procesamiento, lo que dificulta los ataques de fuerza bruta y aumenta la seguridad.

19.1. ARQUITECTURA DE SEGURIDAD

En esta sección, se proporciona una visión general de la arquitectura de Spring Security en aplicaciones basadas en servlets. Se utiliza esta comprensión de alto nivel en las secciones posteriores, que abordan la Autenticación, la Autorización y la Protección contra exploits, para ofrecer una descripción detallada de cada aspecto.

19.1.1. FILTROS SERVLETS

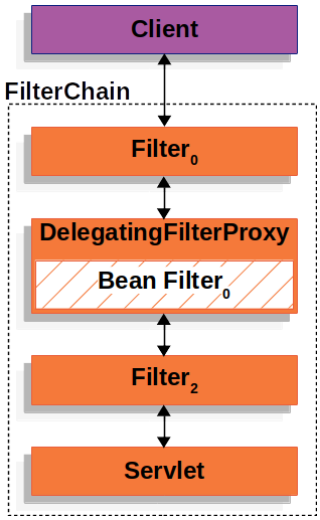
El cliente envía una solicitud a la aplicación y el contenedor crea un token, que contiene las instancias y que debe procesar el servicio, en función de la ruta de acceso del URI de solicitud. En una aplicación MVC de Spring, es una instancia de DispatcherServlet.



Filtros Servlets

19.1.2. DELEGATINGFILTERPROXY

Es clase proporcionada por Spring Framework que actúa como un filtro en la cadena de filtros de una aplicación web. Actúa como un punto de entrada para las solicitudes web, permitiendo el procesamiento de las mismas antes de que lleguen a la capa de aplicación.



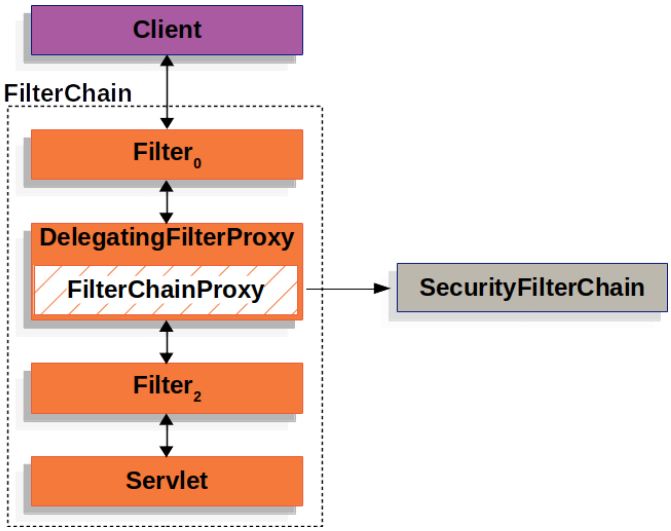
Delegatingfilterproxy

Cuando se utiliza Spring Security, se configura Delegating Filter Proxy en el archivo de configuración de la aplicación para interceptar las solicitudes web y aplicar las medidas

de seguridad necesarias. Delegating Filter Proxy delega el procesamiento de la solicitud a un filtro específico de Spring Security, denominado Filter Chain Proxy, que es responsable de aplicar la lógica de seguridad definida en la configuración.

19.1.3. FILTER CHAIN PROXY

Filter Chain Proxy contiene una serie de filtros, cada uno encargado de una tarea específica, como autenticación, autorización, protección contra ataques, entre otros. Estos filtros se ejecutan en orden secuencial y cada uno realiza su función correspondiente en el proceso de seguridad de la solicitud.

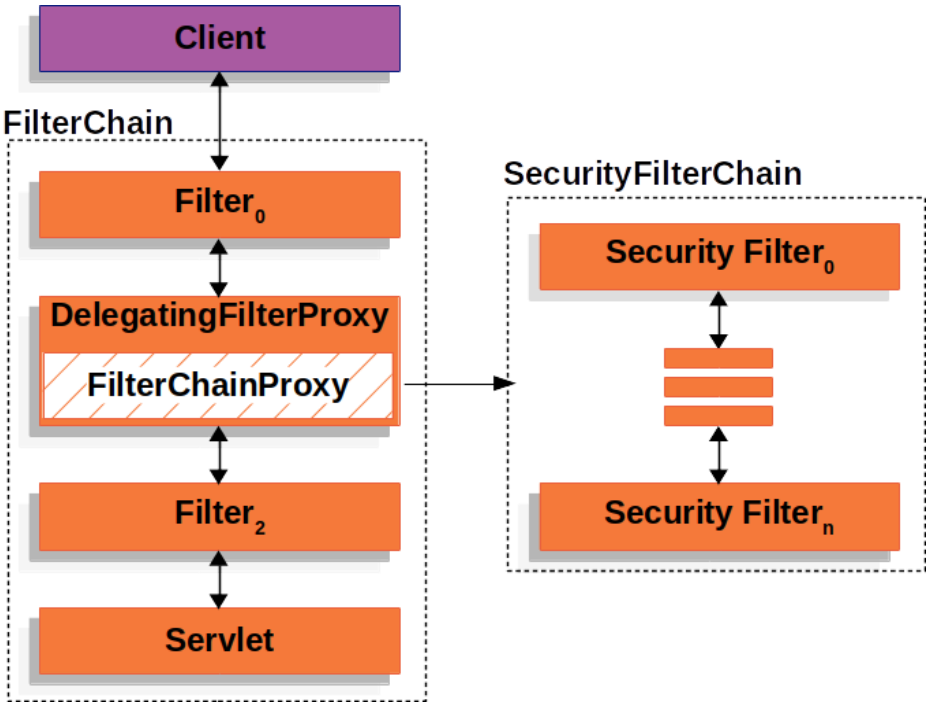


Filterchainproxy

Al configurar y utilizar DelegatingFilterProxy junto con FilterChainProxy, se establece una infraestructura sólida de seguridad en la aplicación basada en servlets. Spring Security se encarga de interceptar las solicitudes, aplicar los filtros adecuados y tomar las decisiones de autenticación y autorización necesarias para proteger los recursos de la aplicación.

19.1.4. SECURITYFILTERCHAIN

Dentro de la arquitectura de seguridad implementada en la empresa ELTHON CEO, otro componente importante de Spring Security es SecurityFilterChain. En el contexto de las aplicaciones basadas en servlets, SecurityFilterChain desempeña un papel clave en el procesamiento y la gestión de la seguridad.



Securityfilterchain

SecurityFilterChain es una interfaz que representa una cadena de filtros de seguridad configurados para una aplicación web. Cada instancia de SecurityFilterChain define un conjunto específico de filtros que se aplican a determinados patrones de URL o rutas en la aplicación.

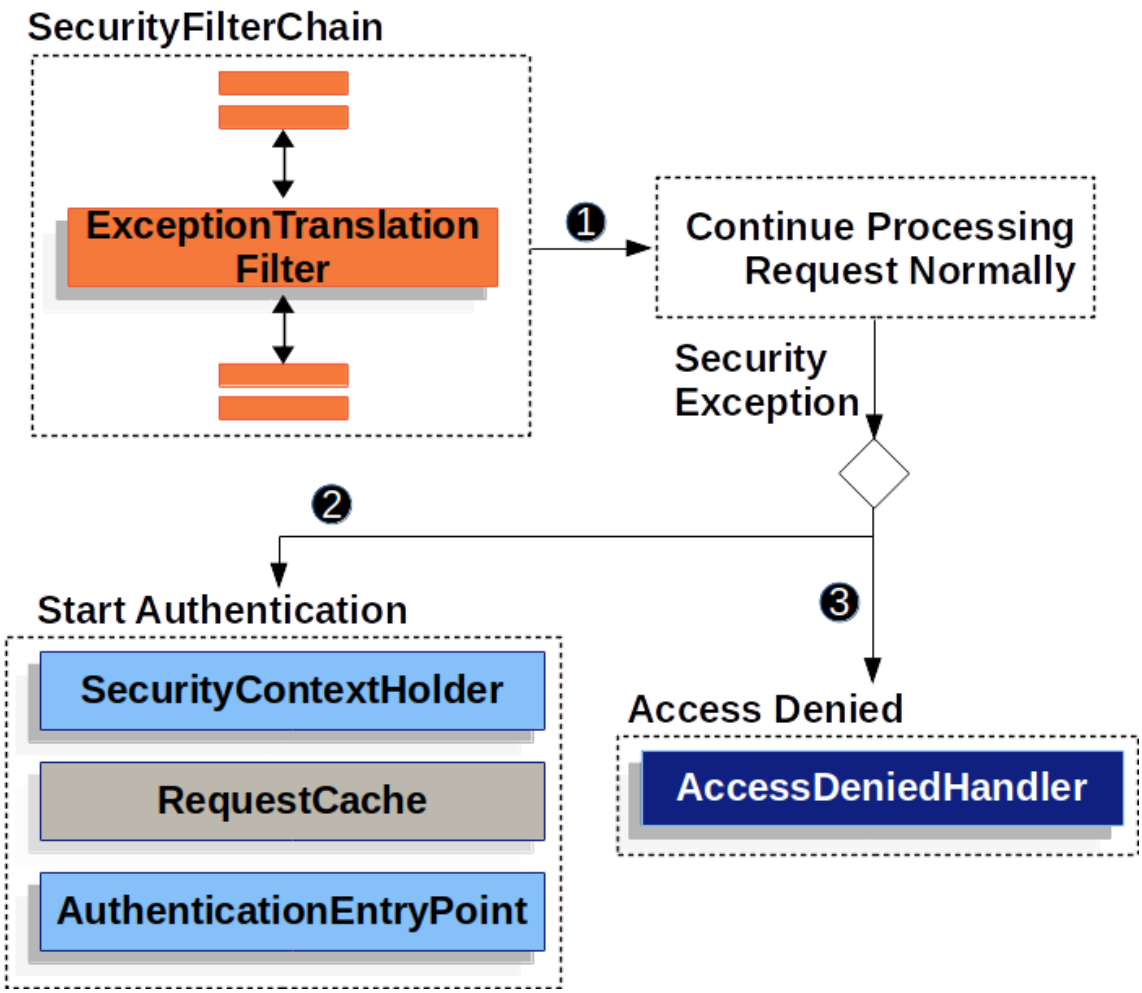
En el caso de ELTHON CEO, SecurityFilterChain se utiliza para definir y configurar la secuencia de filtros de seguridad que se aplicarán a las solicitudes web entrantes. Estos filtros pueden incluir acciones como autenticación, autorización, protección contra ataques y otras medidas de seguridad relevantes para la aplicación.

La configuración de SecurityFilterChain en la aplicación de ELTHON CEO permite establecer el orden y la funcionalidad de los filtros de seguridad, asegurando que las solicitudes sean procesadas adecuadamente. Cada filtro dentro de la cadena cumple una función específica en el proceso de seguridad, lo que contribuye a garantizar la integridad y protección de los recursos de la aplicación.

Es importante destacar que la configuración de SecurityFilterChain puede adaptarse y ajustarse según los requisitos y necesidades de seguridad específicas de ELTHON. Esto implica determinar los filtros necesarios, el orden de aplicación y las acciones a realizar en cada etapa del procesamiento de las solicitudes.

19.2. CONTROL DE EXCEPCIONES DE SEGURIDAD

Dentro de la arquitectura de seguridad implementada en la empresa ELTHON CEO, uno de los aspectos cruciales es el manejo de excepciones de seguridad. Esta funcionalidad permite gestionar de manera adecuada y controlada las situaciones en las que se producen violaciones de seguridad o errores relacionados con la autenticación y la autorización.



Securityfilterchain

El manejo de excepciones de seguridad en ELTHON CEO se realiza mediante Spring Security, que ofrece una serie de mecanismos para capturar y tratar estas excepciones de manera efectiva. Cuando ocurre una excepción de seguridad, Spring Security permite configurar cómo se debe manejar y responder a la misma, adaptándose a las necesidades específicas de ELTHON CEO.

En la perspectiva de ELTHON, el manejo de excepciones de seguridad permite controlar y gestionar adecuadamente las situaciones en las que los usuarios no están autorizados para acceder a determinados recursos o cuando se producen errores de autenticación. Esto contribuye a garantizar la integridad y la seguridad de los datos y recursos de la aplicación.

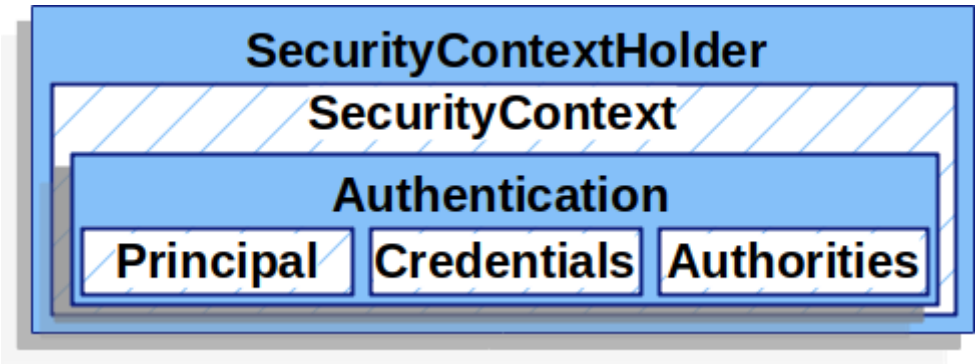
La configuración del manejo de excepciones de seguridad en ELTHON implica definir cómo se deben manejar diferentes tipos de excepciones, como AccessDeniedException, AuthenticationException y otros. Esto puede incluir redirigir al usuario a una página de error personalizada, mostrar mensajes de error específicos, realizar acciones de registro o notificar al administrador del sistema, según corresponda.

Además, ELTHON CEO puede aprovechar las capacidades de Spring Security para personalizar el manejo de excepciones según las necesidades de la aplicación. Esto puede implicar la implementación de clases personalizadas de excepción y su integración con los flujos de seguridad existentes para proporcionar una respuesta adecuada y específica a cada escenario de excepción.

19.3. AUTENTIFICACIÓN

En el contexto de ELTHON, la autenticación se basa en Spring Security, que ofrece diversas opciones y configuraciones para realizar el proceso de autenticación de manera segura y eficiente. La perspectiva de ELTHON en relación con la autenticación es garantizar que solo los usuarios autorizados y con credenciales válidas puedan acceder a la aplicación y a sus funcionalidades.

La configuración de la autenticación en ELTHON implica la definición de un proveedor de autenticación adecuado, que puede incluir opciones como autenticación basada en formularios, autenticación basada en tokens, autenticación mediante proveedores externos (como LDAP o proveedores de identidad) u otras estrategias personalizadas.
Además, ELTHON CEO puede implementar y personalizar los mecanismos de autenticación proporcionados por Spring Security, como el uso de algoritmos de cifrados seguros para almacenar las contraseñas de los usuarios, la configuración de políticas de bloqueo de cuentas por intentos fallidos de autenticación y la integración con servicios de directorio existentes.



Autenticación

Uno de los componentes clave es SecurityContextHolder, donde Spring Security almacena los detalles de autenticación del usuario actualmente autenticado. SecurityContext se obtiene de SecurityContextHolder y contiene la información del usuario autenticado actualmente.

Se menciona a continuación los siguientes componentes dentro de la autentificación:

- **SecurityContext:** se obtiene del SecurityContextHolder y contiene la información del usuario autenticado actualmente. Proporciona una representación del estado de autenticación y se utiliza para realizar verificaciones de autorización y controlar el acceso a recursos protegidos.
- **AuthenticationManager**: es la API que define cómo los filtros de Spring Security realizan el proceso de autenticación. Proporciona un mecanismo para autenticar a los usuarios utilizando diferentes proveedores de autenticación configurados en la aplicación.
- **ProviderManager**: es la implementación más común del AuthenticationManager. Es responsable de coordinar y ejecutar los AuthenticationProvider necesarios para realizar un tipo específico de autenticación. ELTHON CEO configura AuthenticationProvider personalizados para adaptarse a los requisitos de seguridad de la aplicación.
- **AuthenticationProvider**: se utilizan en conjunto con el ProviderManager para realizar un tipo específico de autenticación. Pueden integrarse con sistemas de autenticación externos o implementar lógica personalizada para verificar las credenciales de los usuarios y autenticarlos correctamente.
- **AuthenticationEntryPoint**: se utiliza para solicitar credenciales de un cliente cuando no se ha autenticado o se ha autenticado incorrectamente. Puede redirigir al cliente a una página de inicio de sesión personalizada o enviar una respuesta específica para solicitar las credenciales necesarias.

- **AbstractAuthenticationProcessingFilter**: es una clase base utilizada para la autenticación. Proporciona un punto de entrada para procesar y autenticar las solicitudes de los clientes. Se puede personalizar para adaptarse a las necesidades de autenticación específicas de ELTHON CEO y garantizar la seguridad adecuada de la aplicación.

19.4. COMUNICACIÓN DE LA CAPA POR HTTPS

Al utilizar Spring Security, ELTHON CEO puede habilitar y configurar el soporte de HTTPS en su aplicación. Esto implica la generación o adquisición de un certificado SSL/TLS válido y la configuración adecuada en el servidor de aplicaciones para habilitar la comunicación segura a través del protocolo HTTPS.

El uso de HTTPS en la comunicación entre los clientes y el servidor en ELTHON CEO proporciona varias ventajas en términos de seguridad:

- **Confidencialidad**: La comunicación a través de HTTPS cifra los datos transmitidos, lo que significa que solo el cliente y el servidor pueden acceder y entender la información intercambiada. Esto garantiza que los datos sensibles estén protegidos de posibles interceptaciones o ataques de escucha.
- **Integridad**: HTTPS utiliza técnicas criptográficas para garantizar la integridad de los datos. Los mensajes enviados a través de HTTPS están protegidos contra modificaciones no autorizadas durante la transmisión. Cualquier alteración en los datos será detectada, lo que garantiza que la información recibida sea confiable y no haya sido manipulada en tránsito.
- **Autenticidad**: HTTPS proporciona autenticación del servidor, lo que significa que los clientes pueden verificar la identidad del servidor con el que están interactuando. Esto evita los ataques de suplantación de identidad y garantiza que los clientes se comuniquen solo con servidores confiables y legítimos.

19.5. AUTENTICACIÓN JWT DE SPRING SECURITY

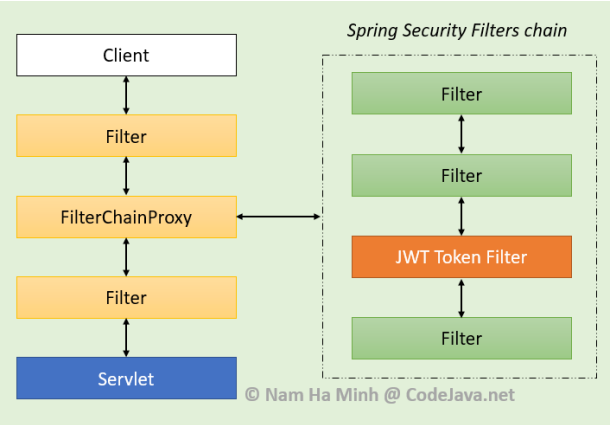
Se utiliza JSON Web Token (JWT) para asegurar las API REST, garantizando una transmisión segura de tokens junto con las solicitudes HTTP. Esto facilita una comunicación sin estado y segura entre los clientes REST y el backend de la API.

19.6. ARQUITECTURA DE JWT CON SPRING SECURITY

JSON Web Token (JWT) es un estándar abierto (RFC 7519) que ofrece una forma compacta y segura de transmitir información entre diferentes partes en forma de un objeto JSON. Un JWT se representa como una cadena que contiene un conjunto de notificaciones en formato JSON. Cada notificación está compuesta por un par de nombre y valor, donde el nombre es siempre una cadena y el valor puede ser cualquier valor válido en JSON.

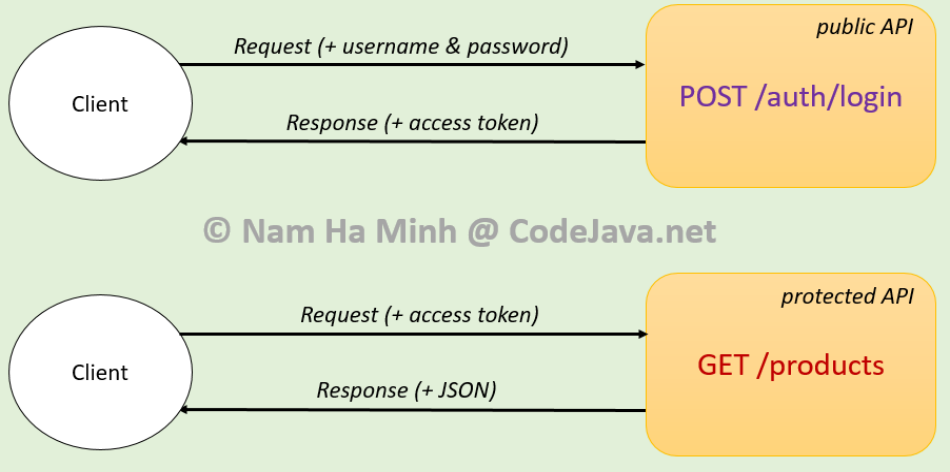
Los JWT son especialmente útiles en entornos con restricciones de espacio, como encabezados de autorización HTTP o parámetros de consulta URI, ya que su formato compacto facilita su uso en estas situaciones. Además, la información contenida en los JWT puede ser verificada y confiable, ya que está firmada digitalmente utilizando una clave secreta o un par de claves pública/privada RSA. La estructura de un JWT consta de tres partes separadas por puntos: el encabezado, la carga útil y la firma.

El encabezado describe las operaciones criptográficas aplicadas al conjunto de notificaciones del JWT, así como el tipo de algoritmo utilizado para firmar el token.



Spring Security Filters Chain

Tanto el encabezado como la carga útil se codifican en base64url antes de ser firmados digitalmente. La firma se genera utilizando el algoritmo especificado en el encabezado, como HS256 (HMAC SHA256). La firma se calcula combinando el encabezado y la carga útil codificados y utilizando una clave secreta.



Comunicación de peticiones y respuestas del servicio de seguridad

20. TRATAMIENTO DE LA INFORMACIÓN DENTRO DE LOS SISTEMAS DE ELTHON

El tratamiento de la información dentro de los sistemas de ELTHON es una tarea crítica que garantiza la seguridad y confidencialidad de los datos. En esta sección se describen las principales especificaciones técnicas y medidas implementadas para el tratamiento adecuado de la información.

Almacenamiento seguro de la información

ELTHON utiliza tecnologías de almacenamiento seguras para garantizar la protección de la información. Los datos se almacenan en bases de datos encriptadas y se utilizan mecanismos de autenticación y control de acceso para restringir el acceso a la información confidencial. Además, se establecen políticas de respaldo y recuperación de datos para asegurar la disponibilidad y continuidad del sistema en caso de fallos o incidentes.

Procesamiento eficiente y seguro

El procesamiento de la información se lleva a cabo de manera eficiente y segura en los sistemas de ELTHON. Se utilizan lenguajes de programación como Java y frameworks como Angular para el desarrollo de aplicaciones robustas y confiables. Se implementan buenas prácticas de codificación y se realizan pruebas exhaustivas para garantizar la calidad y seguridad del software. Asimismo, se establecen procedimientos de validación y verificación de datos para prevenir la introducción de información incorrecta o malintencionada.

Transferencia de datos segura

En ELTHON, se prioriza la seguridad en la transferencia de datos entre sistemas y entidades. Se utilizan protocolos seguros de comunicación, como HTTPS, que garantizan la encriptación de los datos durante la transmisión. Además, se implementan mecanismos de autenticación y autorización para asegurar que solo las partes autorizadas puedan acceder y manipular los datos transmitidos.

20.1. ALMACENAMIENTO DE LA INFORMACIÓN: AZURE BLOBS STORAGE

AZURE Storage es una plataforma completa y versátil de almacenamiento en la nube que brinda una amplia gama de servicios para satisfacer las diversas necesidades de almacenamiento de datos en entornos modernos de manera eficiente y segura. Algunos de los servicios clave que ofrece AZURE Storage son:

- **Blob Storage:** Es ideal para almacenar y gestionar objetos de datos no estructurados, como imágenes, videos o archivos de respaldo, que requieren una gran capacidad de almacenamiento y acceso rápido a los datos.
- **File Storage:** Proporciona almacenamiento compartido basado en el protocolo SMB (Server Message Block). Es adecuado para aplicaciones que necesitan compartir archivos entre diferentes sistemas operativos y requieren una estructura de directorios completa.
- **Queue Storage:** Posibilita la comunicación asincrónica entre los distintos componentes de aplicaciones distribuidas. Resulta especialmente útil en el manejo de colas de mensajes, donde los mensajes son enviados y recibidos secuencialmente para su procesamiento en un orden determinado.
- **Table Storage:** Ofrece una solución escalable y flexible de base de datos NoSQL. Permite almacenar cantidades extensas de datos tanto estructurados como semiestructurados, y resulta idóneo para aplicaciones web y móviles.
- **Disk Storage:** Permite el almacenamiento duradero de datos y sistemas operativos, y proporciona opciones de rendimiento optimizadas para adaptarse a diversas cargas de trabajo.

Cada uno de los servicios de AZURE Storage detallados en el apartado anterior ofrecen grandes beneficios dirigidos tanto para desarrolladores de aplicaciones como para profesionales de TI.

- **Durabilidad y alta disponibilidad:** Los distintos servicios de AZURE Storage garantizan la durabilidad de los datos y ofrecen redundancia para protegerlos contra errores de hardware.

- **Seguridad:** Permite un control sobre los permisos de acceso a los datos, garantizando que las personas con los permisos adecuados puedan acceder.
- **Escalabilidad:** Se encuentran diseñados para crecer de forma masiva y cumplir con las necesidades de rendimiento y capacidad de almacenamiento de las aplicaciones modernas.
- **Gestión simplificada:** AZURE storage se encarga de manera automática de las labores de mantenimiento, actualización y resolución de problemas críticos de hardware. Esto permite a los usuarios dedicarse al desarrollo de aplicaciones sin tener que preocuparse por la infraestructura subyacente, estableciendo la responsabilidad sobre AZURE.
- **Accesibilidad:** Los datos almacenados en AZURE Storage son accesibles desde cualquier parte del mundo a través de protocolos HTTP o HTTPS. El explorador de AZURE Storage brinda interfaces visuales intuitivas para trabajar con los datos almacenados.

20.2. GESTIÓN DE TRATAMIENTOS DE LA INFORMACIÓN: BACKEND

En ELTHON, la gestión de los tratamientos de la información en el backend es fundamental para garantizar la seguridad y confidencialidad de los datos. A continuación, se describen las principales consideraciones y especificaciones técnicas aplicadas en esta área.

Desarrollo de API seguras

En el desarrollo del backend, se utilizan tecnologías y prácticas seguras para la implementación de las API. Se emplea el framework Spring Boot junto con el lenguaje de programación Java, lo que permite desarrollar APIs robustas y confiables. Se aplican técnicas de encriptación y autenticación para asegurar la integridad y confidencialidad de los datos transmitidos.

Validación de datos y control de acceso

El tratamiento de la información en el backend incluye la validación de datos y el control de acceso. Se implementan mecanismos de validación de datos para garantizar la integridad de la información recibida y procesada. Además, se establecen políticas y reglas de acceso para controlar qué usuarios o roles tienen permiso para acceder a determinados datos o funcionalidades. Esto ayuda a prevenir accesos no autorizados y proteger la información sensible.

Seguridad en la lectura de objetos, archivos txt y XML

ELTHON utiliza técnicas seguras para la lectura de objetos y archivos en el backend. Se aplican validaciones de seguridad al procesar objetos, archivos txt y XML, evitando así posibles vulnerabilidades y manipulaciones no autorizadas. Se implementan medidas de control y validación de los datos leídos para garantizar su integridad y evitar posibles riesgos de seguridad.

Auditoría y registro de actividades

Para asegurar la trazabilidad y el control de las actividades realizadas en el backend, se lleva a cabo un registro de auditoría. Se registran las acciones realizadas por los usuarios y se almacenan en logs de auditoría. Esto permite identificar posibles incidentes de seguridad, detectar actividades sospechosas y tomar medidas correctivas oportunamente.

20.3. GESTIÓN DE TRATAMIENTOS DE LA INFORMACIÓN: FRONTEND

En ELTHON, la gestión de los tratamientos de la información en el frontend es crucial para proporcionar una experiencia segura y confiable a los usuarios. A continuación, se detallan las consideraciones y especificaciones técnicas aplicadas en esta área desde la perspectiva de ELTHON.

Desarrollo seguro con Angular y Kendo

En el frontend, utilizamos el framework Angular en combinación con la biblioteca Kendo UI para el desarrollo de aplicaciones web. Estas tecnologías nos permiten crear interfaces interactivas y seguras. Se siguen las mejores prácticas de seguridad en el desarrollo de componentes, servicios y módulos para garantizar la integridad y confidencialidad de los datos manipulados en el frontend.

Validación de datos y control de acceso

La validación de datos y el control de acceso son aspectos clave en el tratamiento de la información en el frontend. Se implementan mecanismos de validación de datos para garantizar que la información ingresada por los usuarios cumpla con los requisitos

establecidos. Además, se establecen políticas de control de acceso para determinar qué usuarios o roles tienen permisos para acceder a determinadas funcionalidades o datos sensibles. Esto nos permite prevenir accesos no autorizados y proteger la confidencialidad de la información.

Seguridad en la comunicación de datos

La comunicación de datos entre el frontend y el backend se realiza de manera segura. Se utilizan protocolos de comunicación encriptados, como HTTPS, para garantizar la confidencialidad e integridad de los datos transmitidos. Además, se aplican prácticas de seguridad en el manejo de tokens de autenticación y se establecen medidas de protección contra ataques de falsificación de solicitudes entre sitios (CSRF).

Pruebas de aceptación y aseguramiento de calidad

Antes de la implementación de nuevas funcionalidades o cambios en el frontend, se llevan a cabo pruebas de aceptación y aseguramiento de calidad. Estas pruebas nos permiten verificar que los tratamientos de la información se realicen correctamente y que no se introduzcan errores o vulnerabilidades en el sistema. Se realizan pruebas exhaustivas para garantizar la estabilidad, seguridad y funcionalidad adecuada del frontend.

20.4. GESTIÓN DE TRATAMIENTOS DE LA INFORMACIÓN: MEDIOS DE TRANSFERENCIA EXTERNA OWNCLOUD

ELTHON utiliza OwnCloud como solución para compartir archivos con otras personas, incluyendo auditores y personas que deseen validar la seguridad. OwnCloud es una plataforma segura y confiable que permite el intercambio seguro de archivos a través de diferentes canales de comunicación.

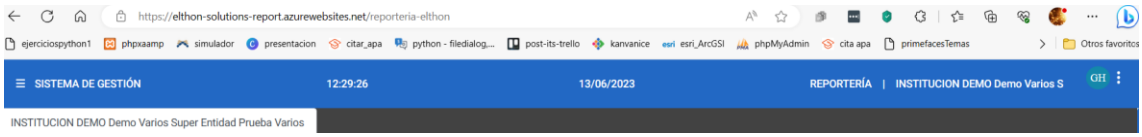
OwnCloud proporciona diversas características y funcionalidades que garantizan la confidencialidad, integridad y disponibilidad de los datos durante las transferencias externas. Algunos puntos clave que respaldan esta elección son:

- **Seguridad avanzada:** OwnCloud utiliza tecnologías de cifrado robustas para proteger los archivos durante la transferencia. Los datos se cifran en tránsito utilizando protocolos seguros como HTTPS, lo que garantiza que la información no sea interceptada ni alterada durante su envío.

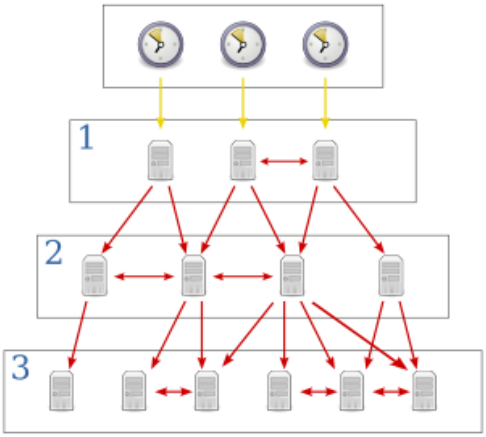
- **Control de acceso granular:** OwnCloud permite establecer permisos y restricciones específicas para cada usuario o grupo de usuarios. Esto asegura que solo las personas autorizadas tengan acceso a los archivos compartidos y que se respeten los niveles de confidencialidad requeridos.
- **Registro de actividades:** OwnCloud registra todas las actividades relacionadas con la transferencia de archivos, incluyendo quién accedió a qué archivos, cuándo y desde dónde. Esto proporciona una trazabilidad completa y ayuda en la auditoría de seguridad.
- **Gestión de versiones:** OwnCloud permite la gestión de versiones de archivos, lo que facilita el seguimiento de los cambios realizados y la recuperación de versiones anteriores en caso necesario.
- **Integración con otros sistemas:** OwnCloud se integra fácilmente con otros sistemas y aplicaciones utilizadas en ELTHON, lo que facilita el intercambio de archivos y la colaboración entre diferentes plataformas.

21. SINCRONIZACIÓN DE RELOJ

ELTHON, utiliza los servicios ofrecidos por Microsoft AZURE, por lo tanto, usa el servidor NTP (Network Time Protocol) predeterminado por Microsoft AZURE para sincronizar los relojes en todos sus sistemas. El NTP es un protocolo diseñado específicamente para lograr la sincronización precisa de los relojes en una red mediante el uso de clientes y servidores distribuidos. A continuación, se adjunta una imagen del sistema ELTHON con Fecha y Hora obtenidas.



Con este servidor NTP, ELTHON se beneficia de los mecanismos de protocolo proporcionados por esta tecnología para lograr una sincronización altamente precisa. El protocolo NTP permite la sincronización de relojes en diferentes sistemas con una precisión del orden de nanosegundos, lo que garantiza que todos los dispositivos y sistemas en la red de ELTHON estén ajustados a la misma hora. A continuación, se adjunta el esquema del protocolo NTP.



Además de su capacidad para mantener una sincronización precisa, el NTP también ofrece características adicionales para especificar la precisión y las fuentes de error potenciales en el reloj de un sistema local. Esto permite a ELTHON evaluar y comprender la calidad de la sincronización de sus sistemas, así como identificar posibles desviaciones y corregirlas en consecuencia.

El servidor NTP utilizado por ELTHON como parte de los servicios de Microsoft AZURE garantiza que los sistemas de la empresa estén sincronizados correctamente, lo que es esencial para una variedad de aplicaciones y servicios críticos. Al tener una base de tiempo común y precisa, ELTHON puede asegurarse de que los eventos, transacciones y registros en sus sistemas estén alineados temporalmente, lo que facilita el análisis de datos, la resolución de problemas y la auditoría.

Al aprovechar el servidor NTP que proporciona Microsoft AZURE como el estándar para la sincronización de relojes, ELTHON logra una coordinación precisa de tiempo en todos sus sistemas. Esto garantiza una base temporal común, facilita la detección y corrección de errores y contribuye a la eficiencia y la confiabilidad de las operaciones de la empresa.

22. MENSAJERIA OUTLOOK CON GMAIL

En ELTHON, la comunicación interna eficiente y segura es fundamental para el éxito de la organización. Para lograr esto, se ha optado por utilizar Outlook con cuentas de empresa Gmail como la solución de mensajería interna principal. A continuación, se presentan las razones por las cuales se ha seleccionado esta combinación de herramientas:

- **Interfaz intuitiva y familiar:** Outlook proporciona una interfaz de usuario intuitiva y familiar para la mayoría de los empleados. La familiaridad con la plataforma de

correo electrónico de Gmail facilita la adopción y el uso efectivo de las funciones de mensajería interna.

- **Integración con otras aplicaciones y servicios:** Outlook se integra de manera fluida con otras herramientas y servicios utilizados por ELTHON, como calendarios, contactos y tareas. Esta integración permite una mayor productividad y colaboración entre los empleados al centralizar la comunicación y la gestión de información en una sola plataforma.
- **Seguridad y privacidad:** Outlook con cuentas de empresa Gmail ofrece sólidas medidas de seguridad y privacidad para proteger la confidencialidad de la información transmitida. Los mensajes se envían a través de conexiones seguras y se implementan controles para prevenir el acceso no autorizado a los correos electrónicos.
- **Capacidad de almacenamiento y búsqueda:** La combinación de Outlook y cuentas de empresa Gmail proporciona una amplia capacidad de almacenamiento para los correos electrónicos, lo que permite a los empleados mantener un historial completo de sus comunicaciones. Además, la función de búsqueda avanzada facilita la recuperación rápida de correos electrónicos antiguos y la gestión eficiente de la información.
- **Acceso desde múltiples dispositivos:** Outlook y las cuentas de empresa Gmail permiten acceder a los correos electrónicos desde diferentes dispositivos, como computadoras de escritorio, laptops, tabletas y teléfonos móviles. Esto brinda flexibilidad a los empleados para mantenerse conectados y responder rápidamente a los mensajes, incluso cuando se encuentren fuera de la oficina.

ELTHON utiliza como gestor de correos electrónicos la herramienta Outlook el cual implementa características de seguridad en la nube.

21.1 ADMINISTRACIÓN SIMPLIFICADA

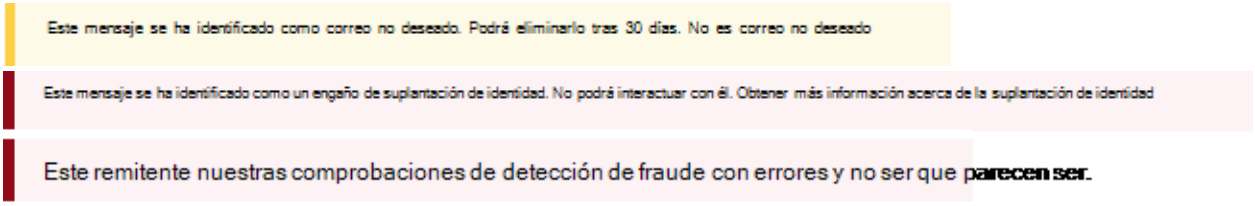
Conecta de forma segura a todos los usuarios, aplicaciones y dispositivos, y obtén una visibilidad completa y central.

21.2 PROTECCIÓN AUTOMATIZADA

Usa herramientas de inteligencia artificial y automatización para responder a las amenazas rápidamente, de forma efectiva y en tiempo real. Adicional ELTHON realiza la capacitación del personal en los siguientes temas que ayudan a mejorar la seguridad y no poner en riesgo la información compartida por correo electrónico.

- Buscar el icono de remitente de confianza en los nuevos mensajes

- Prestar atención a las barras de seguridad amarillas y rojas



- Agregar remitentes a las listas de remitentes bloqueados y seguros
- Comprobar la barra de dirección al iniciar sesión.
- Crear una contraseña segura.
- No responda nunca a correos electrónicos en los que se solicita su contraseña
- Activar la verificación en dos pasos
- Comprobar la actividad reciente de la cuenta
- Agregar un número de teléfono móvil y una dirección de correo electrónico alternativa a su cuenta

23. MANEJO DE ERRORES ELTHON

La gestión efectiva de errores es un componente crítico en la seguridad y estabilidad de los sistemas de información en ELTHON. Reconocemos que los errores pueden ocurrir en diversas situaciones, como a través de conexiones seguras (HTTPS), API u otras interfaces de comunicación, y es fundamental contar con un enfoque planificado para su identificación, resolución y mitigación.

En ELTHON, es importante la detección y reconocimiento de errores comunes que pueden afectar nuestros sistemas. A través de un riguroso proceso de auditoría y monitoreo continuo, identificamos patrones de errores que pueden surgir en nuestras operaciones diarias. Estos errores pueden incluir fallas de conexión, problemas de autenticación, incompatibilidad de versiones, entre otros.

Una vez identificados los errores comunes, nuestro equipo de especialistas en seguridad y desarrollo trabaja en estrecha colaboración para establecer un plan de acción. Este plan incluye la asignación de recursos necesarios, la priorización de las tareas de resolución y la implementación de medidas correctivas para mitigar su impacto en nuestros sistemas.

Además, reconocemos la posibilidad de falsos positivos, es decir, errores que se reportan erróneamente como resultado de falsas alarmas. Para abordar este desafío,

hemos implementado un proceso de verificación y validación exhaustivo para confirmar la autenticidad de cada error antes de emprender cualquier acción correctiva. Esto nos permite optimizar nuestra eficiencia y minimizar cualquier impacto innecesario en nuestras operaciones.

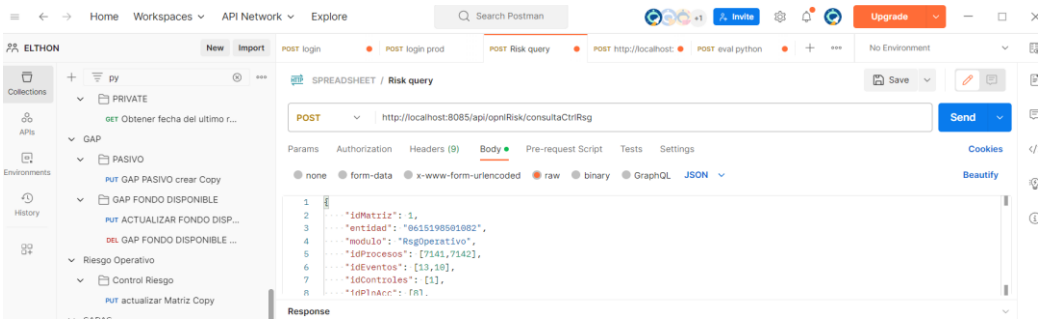
23.1. ERRORES

Es importante realizar estas pruebas en un entorno de desarrollo, donde se puedan simular las condiciones del sistema y tener mayor control sobre los componentes involucrados. Esto permite identificar y solucionar los problemas antes de que el microservicio se implemente en un entorno de producción o para resolver errores nuevos no contemplados.

23.1.1. API NO ENCONTRADA

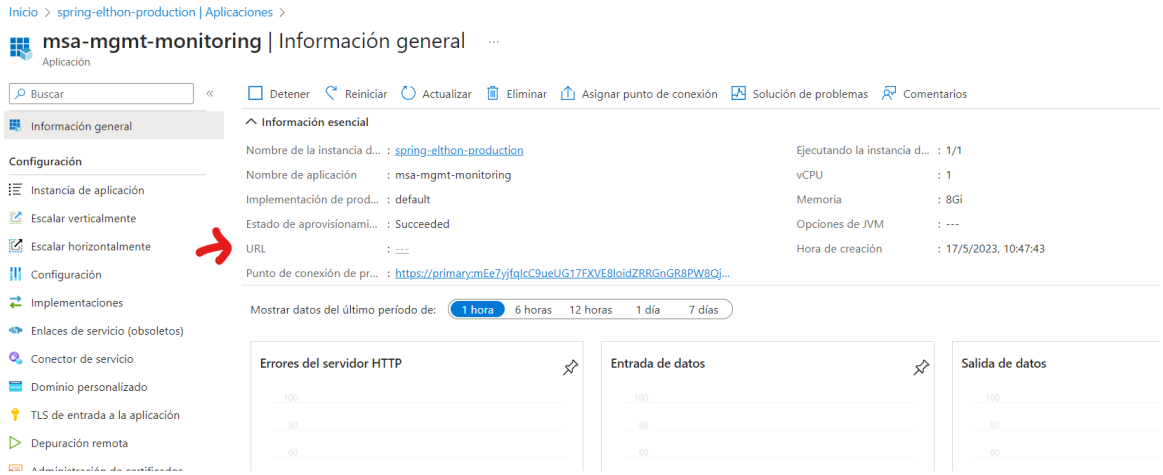
a. Descripción

Este problema se produce cuando un microservicio no se despliega correctamente, lo que puede deberse a diversos factores. También puede ocurrir cuando un servicio está desactualizado y no encuentra la función solicitada. Para verificar y comprobar la funcionalidad en estos casos, se recomienda utilizar Postman en un entorno de desarrollo.



Postman ELTHON con APIS relacionales

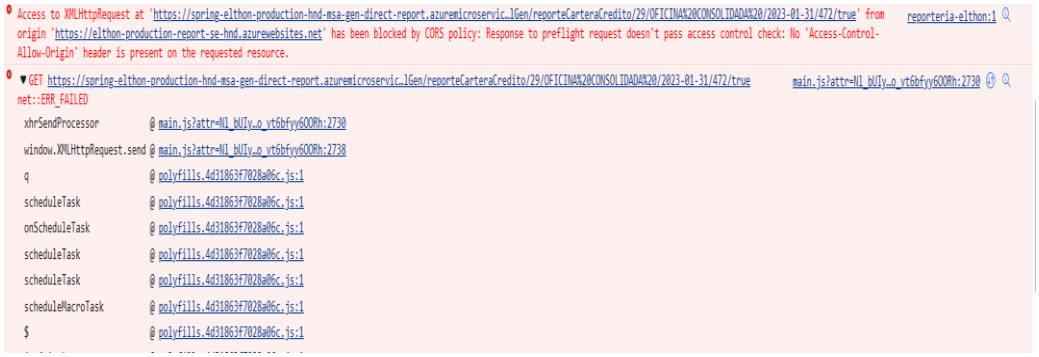
Cuando un microservicio no se sube adecuadamente, puede haber errores relacionados con la configuración, dependencias faltantes o problemas de conexión con otros componentes del sistema. Esto puede provocar que el microservicio no esté disponible para procesar las solicitudes y no pueda cumplir con su funcionalidad esperada.



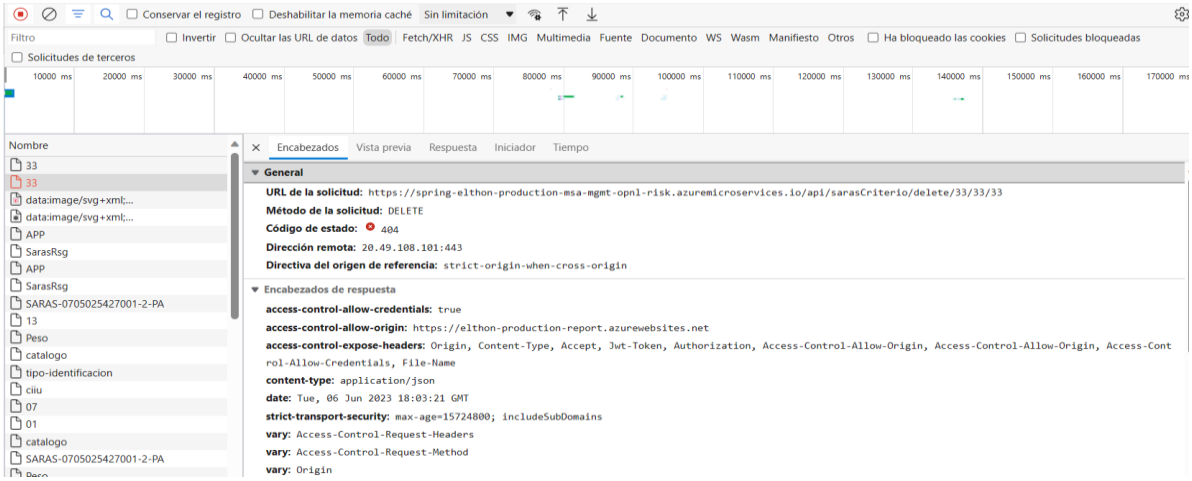
Error microservicio mal configurado

Por otro lado, si un servicio está desfasado, significa que la versión actual del servicio no es compatible con la función solicitada. Esto puede suceder cuando se actualizan las dependencias o se realiza una modificación en el código del servicio, lo que puede generar incompatibilidades con las solicitudes realizadas.

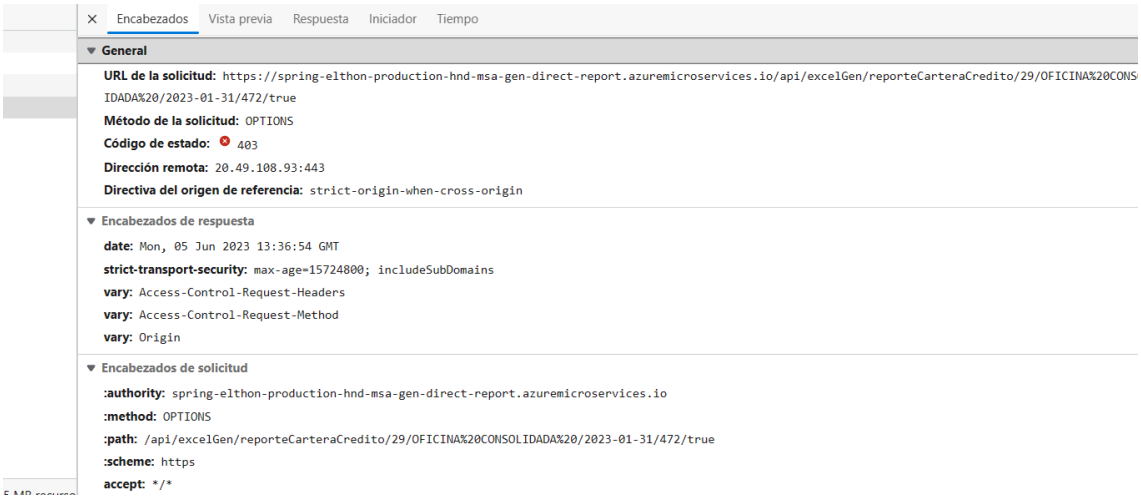
Error de consola



i. 404



ii. 403



iii. Falso Positivo (Errores no controlados)

b. Solución

Cuando nos enfrentamos a errores de la gama 403 y 404 en ELTHON, adoptamos un enfoque proactivo para su solución y mitigación. Estos errores pueden ocurrir debido a

diversas razones, como desfases en los servicios alojados en AZURE Spring Apps, problemas de versiones o incluso fallas en la carga correcta de una versión actualizada en el entorno.

Para resolver estos errores, seguimos un proceso estructurado que involucra la identificación precisa de la causa raíz y la implementación de medidas correctivas efectivas. Nuestro equipo de desarrollo y seguridad realiza un análisis exhaustivo de la situación, revisando cuidadosamente los registros y registros de auditoría para comprender la naturaleza exacta del problema.

Una vez identificada la causa subyacente, trabajamos en estrecha colaboración con nuestros equipos técnicos y de soporte para implementar las soluciones necesarias. Esto puede implicar la actualización de los servicios en AZURE Spring Apps, la corrección de la configuración de versiones, la realización de pruebas exhaustivas para asegurar la funcionalidad correcta y la sincronización adecuada de los componentes involucrados.

Además, para mitigar cualquier impacto negativo en la experiencia del usuario, contamos con un mecanismo de respaldo que nos permite recuperar la última versión funcional del servicio desde AZURE. Esto garantiza que, en caso de errores críticos o problemas con las versiones actualizadas, podamos restablecer rápidamente la funcionalidad operativa y minimizar cualquier interrupción en los servicios que brindamos.

24. GESTIÓN DE LA CAPACIDAD

ELTHON CEO proporciona la gestión de la capacidad de los Servicios y base de datos en la nube en el anexo 2 Gestión de capacidades de los activos de la información vinculado al Subproceso inventario y clasificación de activos.

25. ANEXOS

Anexo 1 Diagrama arquitectura general ELTHON CEO – AZURE
Anexo 2 Diagrama Arquitectura Crítica de Red Azure
Anexo 3 Diagrama Topología de red en estrella tipo HUB – AND – SPOKE en Azure
Anexo 4 Diagrama Azure Front Door
Anexo 5 Diagrama Topología Tradicional de Redes de Azure

26. REFERENCIAS

- Microsoft. (2021). Introducción a la seguridad en AZURE. Microsoft Learn. Recuperado el 8 de mayo de 2023, de
- Microsoft. (2021). AZURE Firewall. Recuperado el 8 de mayo de 2023, de https://azure.microsoft.com/es-es/products/azure-firewall/
- Microsoft. (2021). Microsoft Defender for Cloud. Recuperado el 8 de mayo de 2023, de https://azure.microsoft.com/es-es/products/defender-for-cloud/
- Microsoft. (2021). AZURE Key Vault. Recuperado el 8 de mayo de 2023, de https://azure.microsoft.com/es-es/products/key-vault/
- Microsoft. (2021). AZURE Private Link. Recuperado el 8 de mayo de 2023, de https://azure.microsoft.com/es-es/products/private-link/
- Microsoft. (s. f.). AZURE Application Gateway. Recuperado 8 de mayo de 2023, de https://azure.microsoft.com/es-es/products/application-gateway/
- Microsoft. (2021). AZURE Policy. https://azure.microsoft.com/es-es/products/azure-policy/
- Microsoft. (2021). Arquitectura de referencia de AZURE Spring Apps. Recuperado el 10 de mayo de 2023, de https://learn.microsoft.com/es-es/azure/spring-apps/reference-architecture?tabs=azure-spring-standard
- Microsoft. (s.f.). Basic web app. AZURE Architecture Center. Recuperado el 8 de mayo de 2023, de https://learn.microsoft.com/es-es/azure/architecture/reference-architectures/app-service-web-app/basic-web-app?tabs=cli
- Microsoft. (s.f.). Explore la infraestructura global de AZURE. AZURE. Recuperado el 9 de mayo de 2023, de https://azure.microsoft.com/es-mx/explore/global-infrastructure/
- MongoDB. (s. f.). MongoDB Architecture Guide. Recuperado el 10 de mayo de 2023, de https://www.mongodb.com/mongodb-architecture.
- Noelia L. (2023). Service Level Agreements (SLA) for Online Services. Microsoft. Retrieved from https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services?lang=1