****

**FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO**

**ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

**CURSO:**

**TÓPICOS AVANZADOS EN INGENIERÍA DE SISTEMAS**

**TÍTULO: “DESARROLLO DE UN PROGRAMA PARA LA ARQUITECTURA DE TECNOLOGÍAS DE INFORMACIÓN EN LA EMPRESA ENFOQUE SALUD”**

**DOCENTE**:

**Mg**. JESUS MANUEL CALDAS NUÑEZ

**INTEGRANTES:**

Leyva Cruz Silvana Yaoskelliney

Maquen Mujica, Miguel Ángel

López Vallejos Rober Yubelder

**CICLO:**

X

**Pimentel, 2023 - I**

1. **ARQUITECTURA - DISEÑO As Is**

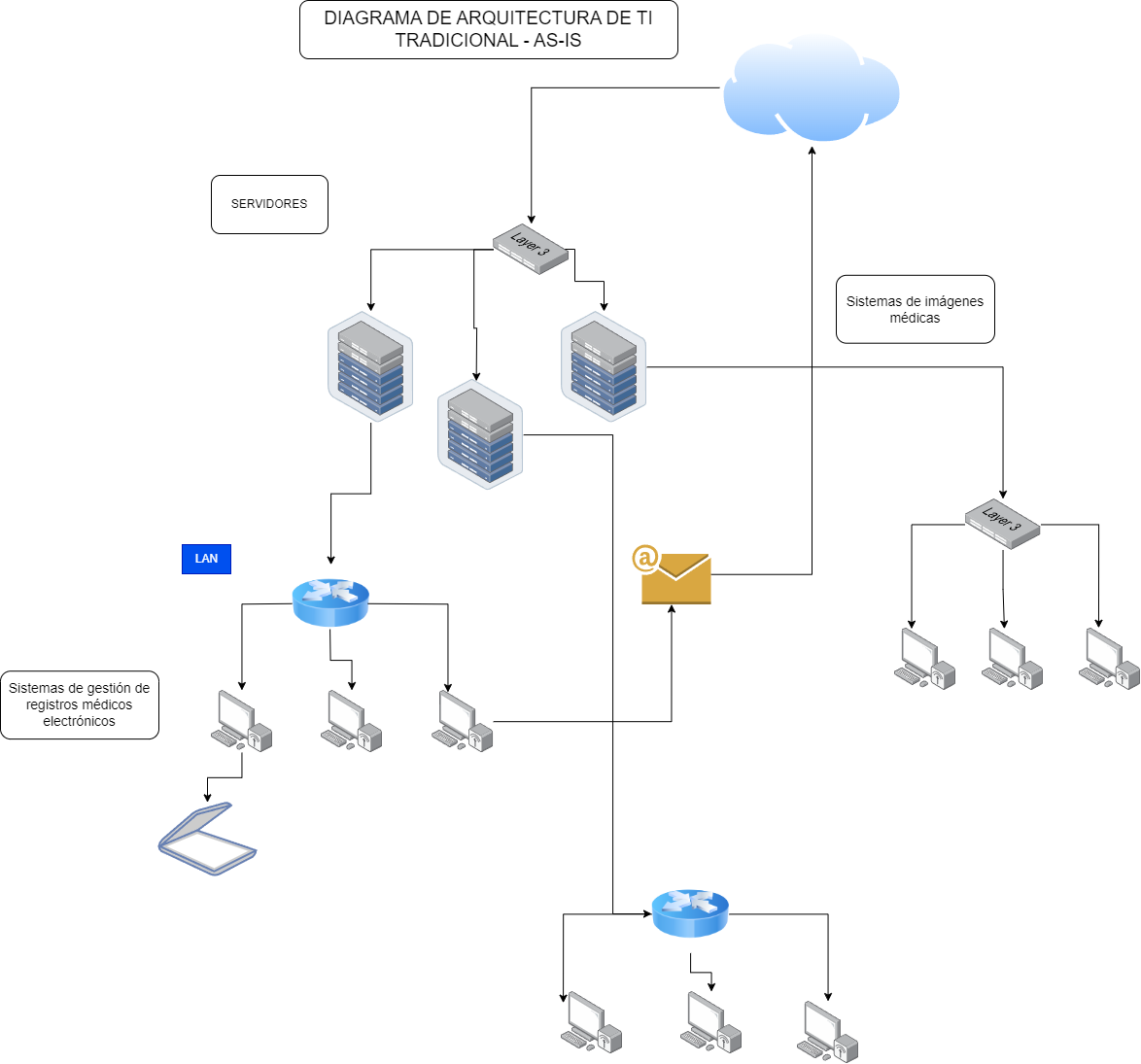
****

Fig. : Arquitectura actual de diseño AS IS.

**DESCRIPCIÓN AQUITECTURA DISEÑO As Is:**

La arquitectura de TI representada en el gráfico muestra una organización que ha implementado una infraestructura para el almacenamiento de información, comunicación y colaboración en sus diferentes áreas. Los componentes principales de esta arquitectura son los servidores, switches, routers y computadoras utilizadas por los colaboradores.

La organización cuenta con tres servidores que desempeñan un papel vital en el almacenamiento de la información generada en las diferentes áreas. Estos servidores pueden estar configurados para distintos propósitos, como almacenamiento de archivos, bases de datos o incluso servicios de aplicaciones.

Para facilitar la conexión y el intercambio de datos entre las computadoras de los colaboradores y los servidores, se han implementado dos switches. Estos switches actúan como puntos de enlace, permitiendo que las computadoras se conecten a los servidores utilizando los protocolos de comunicación de Internet. Los switches aseguran una transmisión eficiente de datos al dirigir los paquetes a los destinos correctos, evitando congestiones y optimizando el rendimiento de la red.

Además, se han utilizado dos routers para habilitar la comunicación inicial entre las computadoras y los servidores. Estos routers son responsables de enrutar los paquetes de datos dentro de la red, asegurando que los mensajes se envíen correctamente a su destino final. Los routers también pueden proporcionar funciones adicionales, como la traducción de direcciones de red (NAT) y la implementación de políticas de seguridad, para garantizar la confiabilidad y la protección de la red.

En la infraestructura, un total de nueve computadoras se conectan a la red para ser utilizadas por los colaboradores de la organización. Estas computadoras son herramientas clave para llevar a cabo las tareas diarias, permitiendo a los colaboradores acceder a la información almacenada en los servidores, comunicarse entre sí y realizar diversas actividades relacionadas con su trabajo. Además, una de las áreas de la organización utiliza un scanner para digitalizar documentos y también hace comunicaciones por correo directo a través de Internet.

Además de los componentes mencionados anteriormente, la organización utiliza una conectividad a Internet proporcionada por la empresa Movistar con una velocidad de 20 Mbps. Esta conexión a Internet es vital para permitir el acceso a recursos en línea, comunicación externa, servicios en la nube y otros servicios basados en Internet que pueden ser necesarios para las operaciones diarias de la organización.

**Internet:** Internet funciona debido al estándar abierto de interconectividad entre redes donde cualquiera puede ofrecer servicios sin permisos de una autoridad central. La arquitectura abierta de Internet, basada en protocolos estándar como TCP/IP (Protocolo de Control de Transmisión/Protocolo de Internet), proporciona un marco común para la comunicación y el intercambio de información entre diferentes dispositivos y redes en todo el mundo. Esto significa que los usuarios de Internet tienen la capacidad de comunicarse y acceder a servicios independientemente de su ubicación geográfica, dispositivo o proveedor de servicios de Internet [1].

**Modelo OSI:**

Los protocolos son un conjunto de reglas que permiten la conexión entre dispositivos a través de la red global. Los protocolos más importantes son TCP/IP [2], el modelo OSI organiza la familia de protocolos en capas de red como las siguientes.

**Protocolos de Capa Física:**

* USB: Siglas de Universal Serial Bus es un estándar de hardware para la transferencia de datos.
* Ethernet: Siglas de Ethernet Physical Layer, utiliza señales eléctricas para la transmisión de datos y es un estándar de comunicación para redes de área local (LAN).

**Protocolos capa de Enlace de Datos:**

* FDDI: Utiliza la topología en anillo y una interfaz de distribución de datos en fibra para redes LAN.
* HDLC: Utilizado para proporcionar un enlace de comunicación seguro entre dos dispositivos en redes locales y amplias.

**Protocolos capa de Transporte:**

* SPX: Permite la entrega de paquetes en orden utilizado para la transmisión de audio y video en tiempo real, gradualmente reemplazado por UDP.
* TCP: Permite la transmisión de paquetes hasta que se complete correctamente, utilizado en transferencia de archivos, etc.
* UDP: Permite enviar información sin conexión y sin garantía de entrega, utilizado en servicios donde la pérdida de datos no es de impacto.

**Protocolos de capa Aplicación:**

* **FTP:** Permite la transferencia de archivos, utiliza comandos como “put” o “get” además de codificación de caracteres.
* **DHCP:** Permite la asignación dinámica de direcciones IP, máscaras de subred, permitiendo una mejor administración de la red.

**Servidores:** Un servidor es un equipo de hardware o software que proporciona servicios, recursos o funcionalidades a otros dispositivos o programas conocidos como "clientes"

**Switch:** dispositivo de red utilizado en arquitecturas de redes locales (LAN) para interconectar múltiples dispositivos, como computadoras, servidores, impresoras, teléfonos IP, entre otros. Actúa como un punto central de conexión, permitiendo que los dispositivos se comuniquen entre sí dentro de la red.

El switch opera en la capa 2 del modelo OSI (capa de enlace de datos) y funciona como un conmutador de paquetes. Su función principal es recibir, analizar y dirigir los paquetes de datos a través de los puertos adecuados hacia su destino final. Almacenará direcciones MAC (Media Access Control) en su tabla de direcciones, lo que le permite determinar a qué puerto debe enviar los paquetes según la dirección MAC de destino.

Los switches ofrecen varias ventajas en comparación con los hubs, que eran utilizados anteriormente. Estas ventajas incluyen:

* **Segmentación de red:** Un switch divide una red en dominios de colisión separados, lo que mejora el rendimiento y la seguridad de la red.
* **Mayor ancho de banda:** Cada puerto del switch tiene su propio ancho de banda dedicado, lo que permite una mayor capacidad de transmisión de datos y evita congestiones.
* **Conmutación rápida:** El switch envía los paquetes directamente a su destino, sin necesidad de enviarlos a todos los dispositivos de la red como lo haría un hub.
* **Mayor seguridad:** Al almacenar direcciones MAC, el switch puede filtrar o bloquear el tráfico no autorizado en la red.

**Routers:** Dispositivo de red que se utiliza para interconectar diferentes redes y dirigir el tráfico de datos entre ellas. Actúa como un punto central que permite la comunicación entre computadoras y otros dispositivos en una red, ya sea dentro de una red local (LAN) o entre redes diferentes, como una red local y la Internet

1. **ARQUITECTURA DE TI QUALYS - DISEÑO To Be**

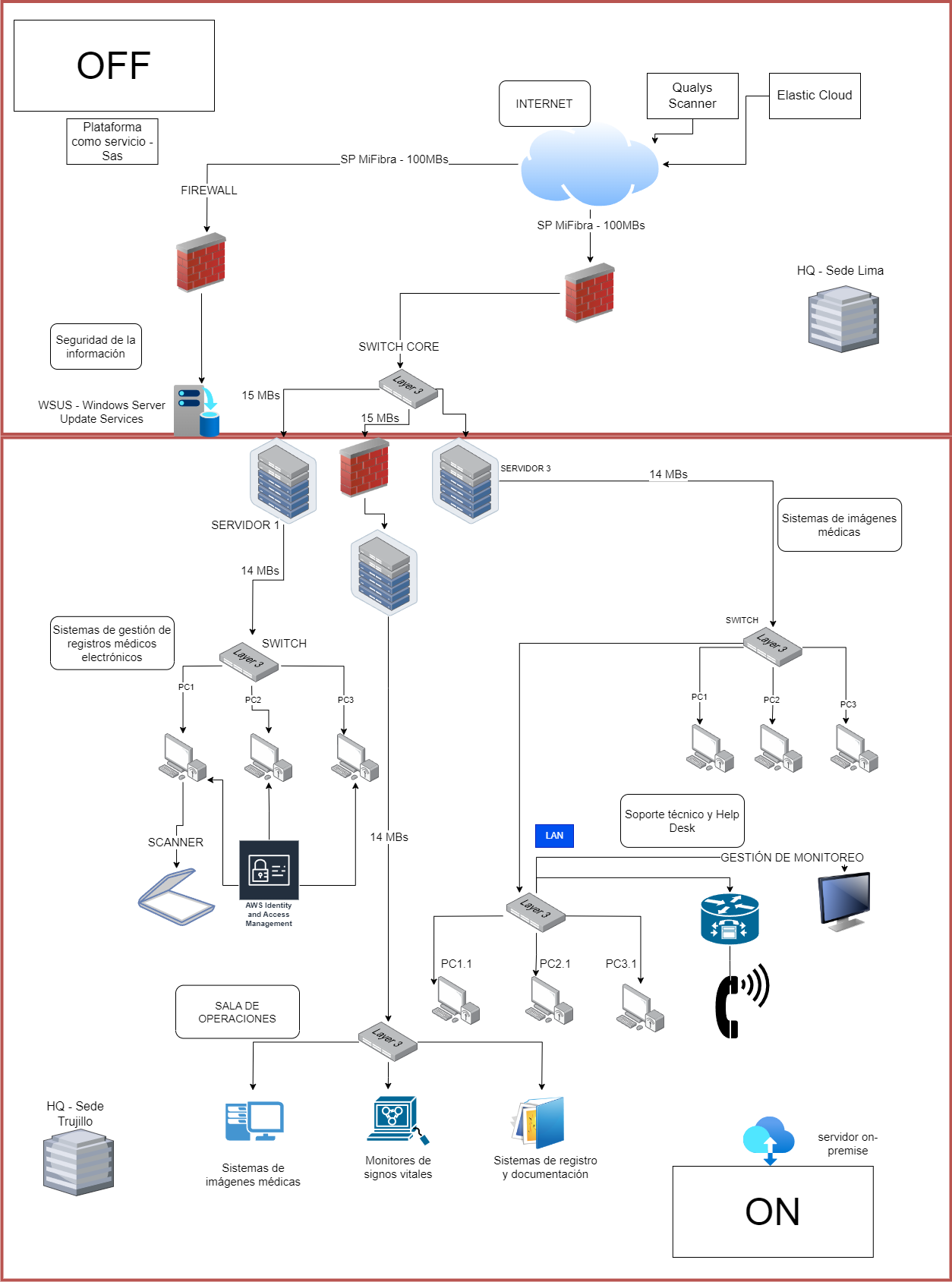
****

Fig. : Arquitectura de TI Qualys, diseño ToBe

**DESCRIPCIÓN ARQUITECTURA DE TI QUALYS - DISEÑO To Be:**

En el diseño "To Be" de la arquitectura de TI descrita, se prioriza la mejora en el tratamiento, transporte y seguridad de la información. Para lograr esto, se incorporan tres firewalls estratégicamente ubicados que interactúan con los switches antes de permitir el acceso a la red de Internet. Estos firewalls desempeñan un papel crucial en la protección de la infraestructura y los datos, permitiendo un control y filtrado efectivo del tráfico de red.

El diagrama de la arquitectura se divide en dos partes: OFF (Plataforma como servicio - SaaS) y ON (servidor on-premise). En la parte OFF, se utiliza un proveedor externo que ofrece servicios SaaS, lo que significa que las aplicaciones y servicios se entregan a través de la nube. El proveedor externo, con sede en Lima, proporciona servicios SaaS y también ofrece servicios complementarios de Qualys y Elastic Cloud. Qualys se utiliza para llevar a cabo análisis de seguridad y evaluaciones de vulnerabilidades, mientras que Elastic Cloud se utiliza para el monitoreo y análisis de datos.

En la sede de la empresa en Lima, se encuentra un servidor dedicado para la gestión de parches y actualizaciones. Este servidor es responsable de garantizar que los sistemas y aplicaciones estén actualizados con los últimos parches de seguridad y actualizaciones necesarias. Esto es esencial para mantener un nivel adecuado de seguridad y protección contra vulnerabilidades conocidas.

La incorporación de firewalls, el uso de servicios SaaS y la gestión centralizada de parches y actualizaciones en el servidor on-premise reflejan un enfoque integral para garantizar la seguridad y confiabilidad de la infraestructura de TI. Al enfocarse en mejorar el tratamiento, transporte y seguridad de la información, la organización puede fortalecer su postura de seguridad y proteger sus activos críticos contra amenazas cibernéticas.

Cabe destacar que este es solo un resumen del diseño "To Be" descrito y que la implementación y configuración específica dependerán de los requisitos y necesidades de la organización, así como de las tecnologías y soluciones seleccionadas. Es fundamental realizar un análisis detallado y consultas con expertos en seguridad y arquitectura de TI para asegurar una implementación eficiente y efectiva.

En la sección ON de la arquitectura "To Be", se incluyen tres servidores on-premise que desempeñan un papel fundamental en el funcionamiento de la empresa. Estos servidores pueden estar configurados para diferentes propósitos, como almacenamiento de datos, alojamiento de aplicaciones internas o servicios específicos de la empresa.

Además de los servidores, se tienen nueve dispositivos conectados a la red. Estos dispositivos pueden ser computadoras utilizadas por los colaboradores de la empresa para llevar a cabo sus tareas diarias. Cada uno de estos dispositivos está conectado a través de tres switches, que actúan como puntos de enlace para proporcionar conectividad y enlace de datos entre los dispositivos y los servidores.

Las cuatro LANs dedicadas a las oficinas principales, incluida la sede en Trujillo, permiten una segmentación lógica de la red y una administración más eficiente de los recursos y la seguridad. Cada LAN puede estar configurada para atender a un grupo específico de usuarios o para brindar servicios especializados, según las necesidades de la empresa.

Además de las funciones de oficina, se menciona que en la sede de Trujillo se encuentran registros de maquinarias utilizadas para obtener datos de los clientes. Estos registros pueden almacenar información relevante sobre los equipos utilizados en el proceso de obtención de datos, como registros de mantenimiento, registros de uso y datos técnicos relacionados. La gestión de estos registros es crucial para garantizar el mantenimiento adecuado de las maquinarias y ofrecer un servicio de calidad a los clientes.

Por último, se menciona un router dedicado al flujo de información del teléfono. Esto indica que existe una infraestructura de comunicación telefónica implementada en la organización, y el router desempeña un papel central en la gestión de las comunicaciones telefónicas internas y externas.

**Qualys:**

Qualys Scanner es una herramienta de seguridad de red y vulnerabilidad desarrollada por Qualys, Inc. Se utiliza para realizar análisis de seguridad y evaluaciones de vulnerabilidad en redes, sistemas y aplicaciones. El Qualys Scanner identifica y escanea activos de red en busca de posibles vulnerabilidades, como configuraciones incorrectas, fallos de seguridad o falta de parches de seguridad.

La función principal de Qualys Scanner es analizar y evaluar la seguridad de una infraestructura de TI. Realiza exploraciones automatizadas en busca de vulnerabilidades conocidas y proporciona informes detallados sobre las posibles brechas de seguridad encontradas. Estos informes permiten a los administradores de seguridad tomar medidas correctivas para fortalecer la seguridad de la red y proteger los activos de la organización.

La empresa Qualys, ofrece su aplicación con el servicio del escaneo web con el objetivo de ayudar a las organizaciones a identificar y contrarrestar las vulnerabilidades relacionadas con una amenaza que se considera como una de las más inquietantes de la última década denominadas Log4Shell [3].

**Virtual scanner:** Es una versión virtual del Qualys Scanner. En lugar de ser una solución basada en hardware, el Virtual Scanner se ejecuta como una máquina virtual en entornos virtuales o en la nube. Proporciona las mismas capacidades de escaneo y evaluación de seguridad que el scanner físico, pero con la flexibilidad adicional de poder implementar y escalar fácilmente en entornos virtualizados.

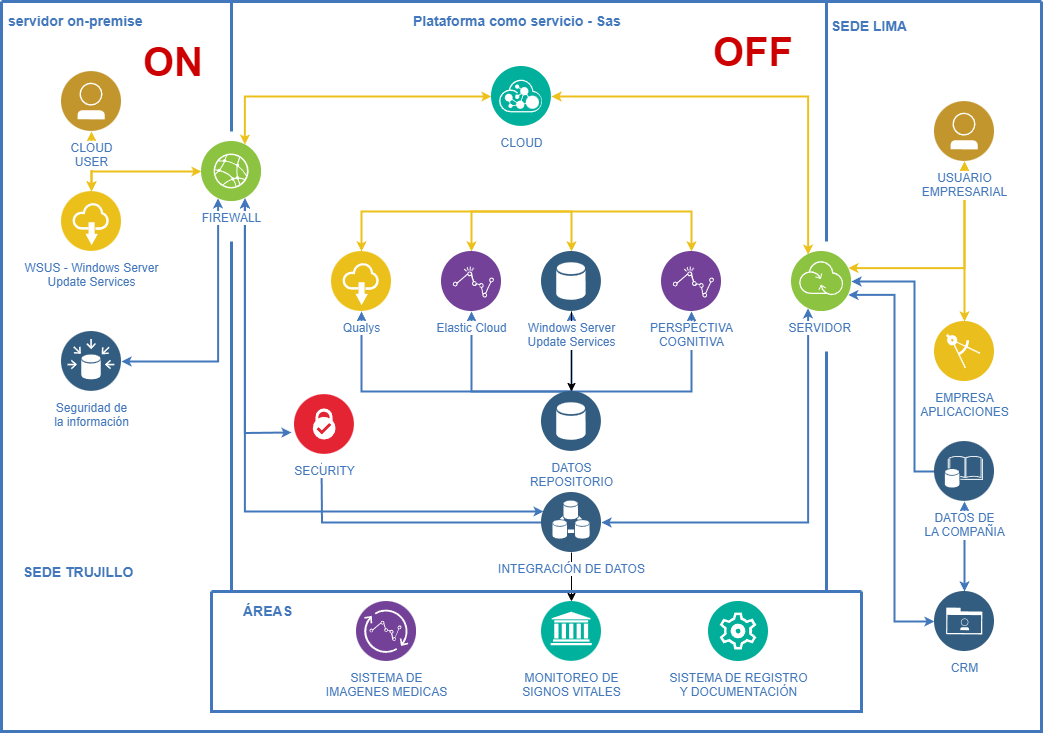
Ofrece ventajas como la fácil implementación, la capacidad de escalar según las necesidades y la capacidad de ejecutarse en plataformas virtualizadas, lo que lo hace especialmente adecuado para organizaciones que utilizan infraestructuras virtuales que cuenta con integración nativa de Amazon Web Services [4].

**Virtual Gateway:** El Virtual Gateway (puerta de enlace virtual) es un componente de seguridad proporcionado por Qualys. Actúa como un punto centralizado para administrar y controlar el tráfico de red entre los sistemas y las herramientas de seguridad de Qualys, como el scanner y otros módulos de seguridad.

Permite una comunicación segura y encriptada entre los diferentes componentes de seguridad de Qualys, facilitando la transferencia de datos y la gestión centralizada de la seguridad. También proporciona funciones adicionales de seguridad, como el filtrado de tráfico y la prevención de ataques, ayudando a proteger la infraestructura de la organización contra amenazas cibernéticas.

Los scanner de contenido son probablemente incapaces de decodificar la conexión SSL, por ello es necesario utilizar tecnologías tales como Redes Privadas Virtuales (VPN) para proteger los datos, que utilizan el protocolo de Internet v6 como un ‘túnel’ protegido entre dos Routers Gateway [5].

1. **ARQUITECTURA DE TI ELASTIC CLOUD - DISEÑO To Be:**



**DESCRIPCIÓN ARQUITECTURA DE TI ELASTIC CLOUD - DISEÑO TO BE:**

En el diseño "To Be" de la arquitectura de TI que incorpora Elastic Cloud, se busca lograr un manejo eficiente y cuidado de la información en la empresa. En el centro del diagrama se encuentra el servicio SaaS que incluye Qualys, Elastic Cloud, el servidor de actualizaciones y el servidor de copias de seguridad. Estos servicios son visualizados a través de una perspectiva continua, que evalúa y genera gráficas para mostrar cómo se maneja la información en la empresa.

La información se integra con el módulo de seguridad de acceso, el cual limita el acceso a ciertas áreas según los permisos otorgados por la empresa. Además, se utiliza un sistema de imágenes, monitoreo de signos vitales y un sistema de registro y documentación para asegurar un manejo adecuado de la información.

La sede de Lima está interconectada a través de un servidor, donde se realiza la integración de datos y se solicita un firewall antes de exponer la información. Dependiendo de los permisos otorgados, se accede a la información del servidor on-premise. Además, se mantiene una comunicación constante con el servidor de parches y actualizaciones para asegurar que los sistemas estén al día.

En la sede de Lima, se utiliza un sistema de gestión de relaciones con clientes (CRM) que asigna privilegios a los usuarios y se integra con las aplicaciones de la empresa. Esto permite llevar un registro de los procesos llevados a cabo en la empresa y gestionar eficientemente las interacciones con los clientes.

La solicitud de firewall antes de exponer la información desde la sede de Lima agrega una capa adicional de seguridad. Esto asegura que cualquier tráfico entrante o saliente se someta a un control riguroso y solo se permita el acceso a recursos autorizados. De esta manera, se minimiza el riesgo de posibles ataques o fugas de información.

El servidor de parches y actualizaciones desempeña un papel crucial en el mantenimiento de un entorno seguro y actualizado. Este servidor se encarga de aplicar las últimas actualizaciones y parches de seguridad en los sistemas, aplicaciones y servicios utilizados en la empresa. Esto ayuda a mitigar vulnerabilidades conocidas y a mantener la infraestructura protegida contra amenazas emergentes.

**Elastic Clouds:**  Elastic Cloud es una plataforma de servicios en la nube proporcionada por Elastic. Elastic es una empresa conocida por desarrollar soluciones de búsqueda y análisis de datos, como Elasticsearch, Logstash y Kibana (ELK stack). Elastic Cloud permite a los usuarios implementar y gestionar estas soluciones en la nube, ofreciendo escalabilidad, disponibilidad y flexibilidad. Permite a las organizaciones ampliar o reducir fácilmente su capacidad de almacenamiento y procesamiento según sea necesario, sin la necesidad de invertir en infraestructura adicional [6].

el diseño "To Be" de la arquitectura de TI con Elastic Cloud se enfoca en garantizar un eficiente manejo y cuidado de la información. Incorpora capacidades de monitoreo y análisis, seguridad de acceso, solicitud de firewall y mantenimiento actualizado. Estas medidas trabajan en conjunto para crear un entorno robusto, seguro y optimizado para la gestión de la información en la empresa

# Bibliografía

|  |  |
| --- | --- |
| [1] | Internetsociety, «www.internetsociety.org,» 2017. [En línea]. Available: https://www.internetsociety.org/es/about-the-internet/how-it-works/. |
| [2] | KIO, «www.kionetworks.com,» 2021. [En línea]. Available: https://www.kionetworks.com/blog/data-center/protocolos-de-comunicaci%C3%B3n-de-redes. |
| [3] | Qualys, «www.qualys.com/company,» 2021. [En línea]. Available: https://www.qualys.com/company/newsroom/news-releases/es/qualys-ofrece-gratuitamente-su-tecnologia-para-mitigar-la-vulnerabilidad/. [Último acceso: 2023]. |
| [4] | B. Villora, «Evaluación y gestión de vulnerabilidades: Cómo sobrevivir en el,» 2018. [En línea]. Available: https://m.riunet.upv.es/bitstream/handle/10251/106947/VILLORA%20-%20Evaluaci%C3%B3n%20y%20gesti%C3%B3n%20de%20vulnerabilidades%3A%20C%C3%B3mo%20sobrevivir%20en%20el%20mundo%20de%20los%20ciberataques.pdf. [Último acceso: 2023]. |
| [5] | OWASP, «Una Guía para Construir Aplicaciones y Servicios Web Seguros,» The open web Application Security Proyect, 2005. [En línea]. Available: https://owasp.org/www-pdf-archive/OWASP\_Development\_Guide\_2.0.1\_Spanish.pdf. [Último acceso: 2023]. |
| [6] | E. Cloud, «www.elastic.co/,» Elasticsearch hospedado, 2023. [En línea]. Available: www.elastic.co/es/cloud/. [Último acceso: 2023]. |