

**FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO**

**ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

**TÍTULO DEL INFORME**

**DOCENTE**

Jesus Manuel Caldas Nuñez

**CURSO**

TÓPICOS AVANZADOS EN INGENIERÍA DE SISTEMAS

**INTEGRANTES**

Delgado Farro Javier Manuel  
More Villegas Fiorella Jhajaira  
Sanchez Pardo Samuel

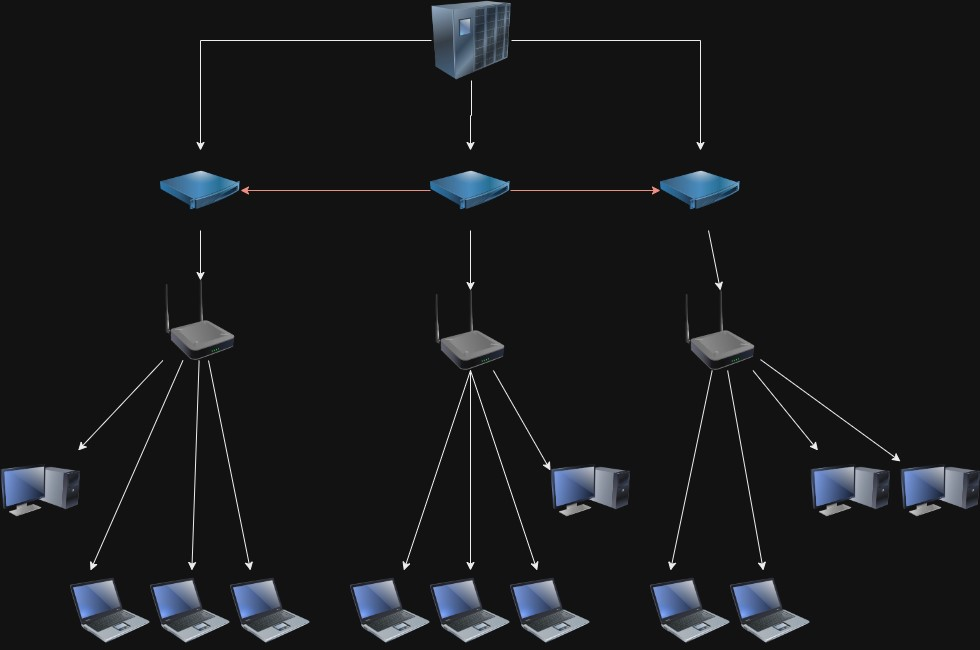
**SEMESTRE**

2023-I

**PIMENTEL, JULIO DEL 2023**

**ÍNDICE**

* **ASIS (gráfico + descripción)**

****

El gráfico representa la infraestructura de tecnología de la información (TI) de una organización local, la cual ha desarrollado un sistema completo para el almacenamiento de información, comunicación y colaboración en todas sus áreas. La arquitectura de TI está compuesta por varios componentes esenciales, incluyendo un servidor central, switches, routers y computadoras utilizadas por los colaboradores.

El servidor central desempeña un papel vital en el almacenamiento de la información generada en las distintas áreas de la organización. Este servidor puede ser configurado para satisfacer diversas necesidades, como el almacenamiento de archivos, bases de datos o servicios de aplicaciones, adaptándose así a los requerimientos específicos de la organización.

Para facilitar la conectividad y el intercambio de datos entre las computadoras de los colaboradores y el servidor central, se ha implementado un switch principal. Este switch actúa como un punto de conexión central, permitiendo que las computadoras se conecten al servidor utilizando los protocolos de comunicación de Internet. De esta manera, los switches aseguran una transmisión eficiente de datos al dirigir los paquetes hacia los destinos correctos, evitando congestiones y optimizando el rendimiento de la red.

Además, se han utilizado tres routers para habilitar la comunicación inicial entre las computadoras y el servidor central. Estos routers son responsables de dirigir los paquetes de datos dentro de la red, garantizando que los mensajes sean enviados correctamente a su destino final. Los routers también ofrecen funciones adicionales, como la traducción de direcciones de red (NAT) y la implementación de políticas de seguridad, para asegurar la confiabilidad y protección de la red.

En cuanto a las computadoras utilizadas por los colaboradores, un total de trece están conectadas a la red. Estas computadoras son herramientas clave para llevar a cabo las tareas diarias, permitiendo que los colaboradores accedan a la información almacenada en el servidor, se comuniquen entre sí y realicen diversas actividades relacionadas con su trabajo. Además, en una de las áreas de la organización, se utiliza un escáner para digitalizar documentos, y también se realizan comunicaciones directas a través de Internet.

Adicionalmente a los componentes mencionados anteriormente, la organización cuenta con una conexión a Internet proporcionada por la empresa Movistar, con una velocidad de 100 Mbps. Esta conexión a Internet es crucial para permitir el acceso a recursos en línea, la comunicación externa, los servicios en la nube y otras herramientas basadas en Internet que son necesarias para las operaciones diarias de la organización. Esta conexión rápida y confiable es fundamental para el funcionamiento eficiente de la infraestructura de TI y para respaldar las actividades de la organización en un entorno digital cada vez más conectado.

Internet se sustenta en su arquitectura abierta, la cual se basa en un estándar de interconectividad entre redes. Esta arquitectura permite que cualquier entidad pueda ofrecer servicios sin requerir permisos de una autoridad central. Los protocolos estándar, como TCP/IP (Protocolo de Control de Transmisión/Protocolo de Internet), son fundamentales en esta arquitectura, ya que proporcionan un marco común para la comunicación e intercambio de información entre dispositivos y redes en todo el mundo. Esto significa que los usuarios de Internet tienen la capacidad de comunicarse y acceder a servicios sin importar su ubicación geográfica, el dispositivo que utilicen o el proveedor de servicios de Internet.

El modelo OSI (Interconexión de Sistemas Abiertos) organiza los protocolos en capas de red, y algunos de los protocolos más importantes son los siguientes:

· En la capa física, se encuentran protocolos como USB (Bus Universal en Serie), que es un estándar de hardware para la transferencia de datos, y Ethernet, que utiliza señales eléctricas para la transmisión de datos y es ampliamente utilizado en redes de área local (LAN).

· En la capa de enlace de datos, se utilizan protocolos como FDDI (Interfaz de Datos Distribuidos por Fibra), que utiliza una topología en anillo y una interfaz de distribución de datos en fibra para redes LAN, y HDLC (Control de Enlace de Datos de Alto Nivel), utilizado para establecer enlaces seguros de comunicación entre dispositivos en redes locales y amplias.

· En la capa de transporte, se encuentran protocolos como SPX (Intercambio de Paquetes Secuenciados), utilizado para la entrega ordenada de paquetes y la transmisión de audio y video en tiempo real (actualmente reemplazado gradualmente por UDP), TCP (Protocolo de Control de Transmisión), que permite la transmisión de paquetes asegurándose de que se completen correctamente (utilizado, por ejemplo, en transferencia de archivos), y UDP (Protocolo de Datagramas de Usuario), que permite el envío de información sin conexión y sin garantía de entrega (utilizado en servicios donde la pérdida de datos no es crítica).

· En la capa de aplicación, se encuentran protocolos como FTP (Protocolo de Transferencia de Archivos), que permite la transferencia de archivos y utiliza comandos como "put" o "get" y codificación de caracteres, y DHCP (Protocolo de Configuración Dinámica de Host), que permite la asignación dinámica de direcciones IP y máscaras de subred para una mejor administración de la red.

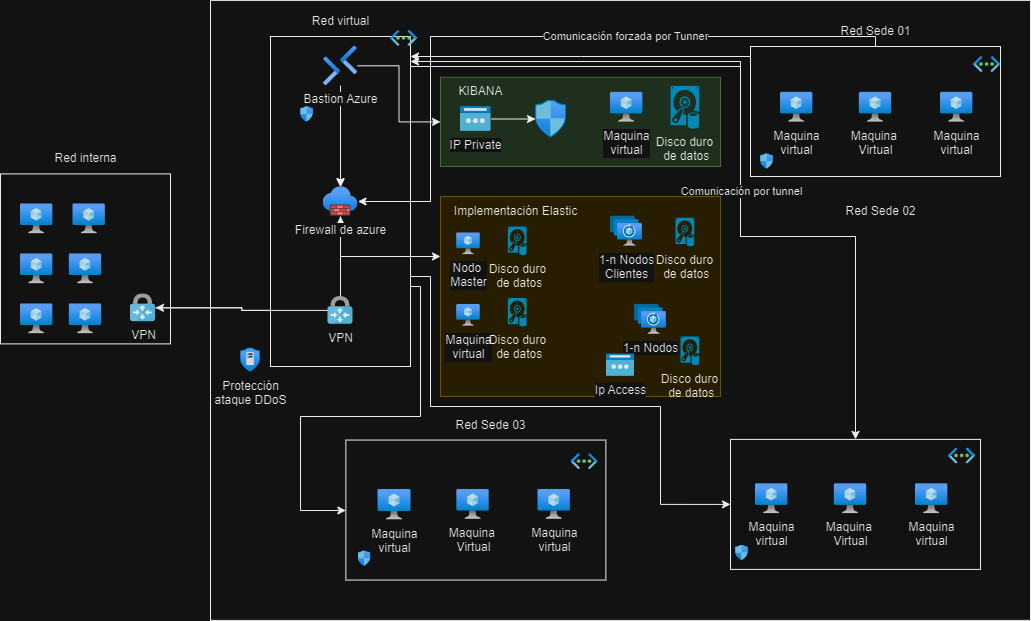
Los servidores son dispositivos de hardware o software que brindan servicios, recursos o funcionalidades a otros dispositivos o programas conocidos como "clientes". Estos servidores pueden ofrecer una amplia gama de servicios, como almacenamiento de archivos, administración de bases de datos, hosting de sitios web, servicios de correo electrónico, entre otros.

Los switches son dispositivos de red utilizados en redes locales (LAN) para interconectar múltiples dispositivos, como computadoras, servidores, impresoras y teléfonos IP. Actúan como puntos centrales de conexión, permitiendo que los dispositivos se comuniquen entre sí dentro de la red. Los switches operan en la capa 2 del modelo OSI (capa de enlace de datos) y funcionan como conmutadores de paquetes. Su principal función es recibir, analizar y dirigir los paquetes de datos hacia los puertos adecuados para su destino final. Almacenan direcciones MAC (Control de Acceso al Medio) en una tabla, lo que les permite determinar a qué puerto enviar los paquetes según la dirección MAC de destino.

Los switches ofrecen diversas ventajas en comparación con los hubs, que se utilizaban anteriormente. Estas ventajas incluyen la segmentación de la red en dominios de colisión separados, lo que mejora el rendimiento y la seguridad de la red, un mayor ancho de banda dedicado a cada puerto, permitiendo una mayor capacidad de transmisión de datos y evitando congestiones, una conmutación rápida que envía los paquetes directamente a su destino sin enviarlos a todos los dispositivos de la red, y una mayor seguridad al poder filtrar o bloquear el tráfico no autorizado en la red [1].

Los routers son dispositivos de red utilizados para interconectar diferentes redes y dirigir el tráfico de datos entre ellas. Actúan como puntos centrales que permiten 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. Los routers se encargan de enrutar los paquetes de datos dentro de la red, asegurándose de que los mensajes sean enviados correctamente a su destino final. Además, los routers pueden ofrecer funciones adicionales como la traducción de direcciones de red (NAT) y la implementación de políticas de seguridad para garantizar la confiabilidad y protección de la red [2]

* **ARQUITECTURA DE TI DISEÑÓ To Be**

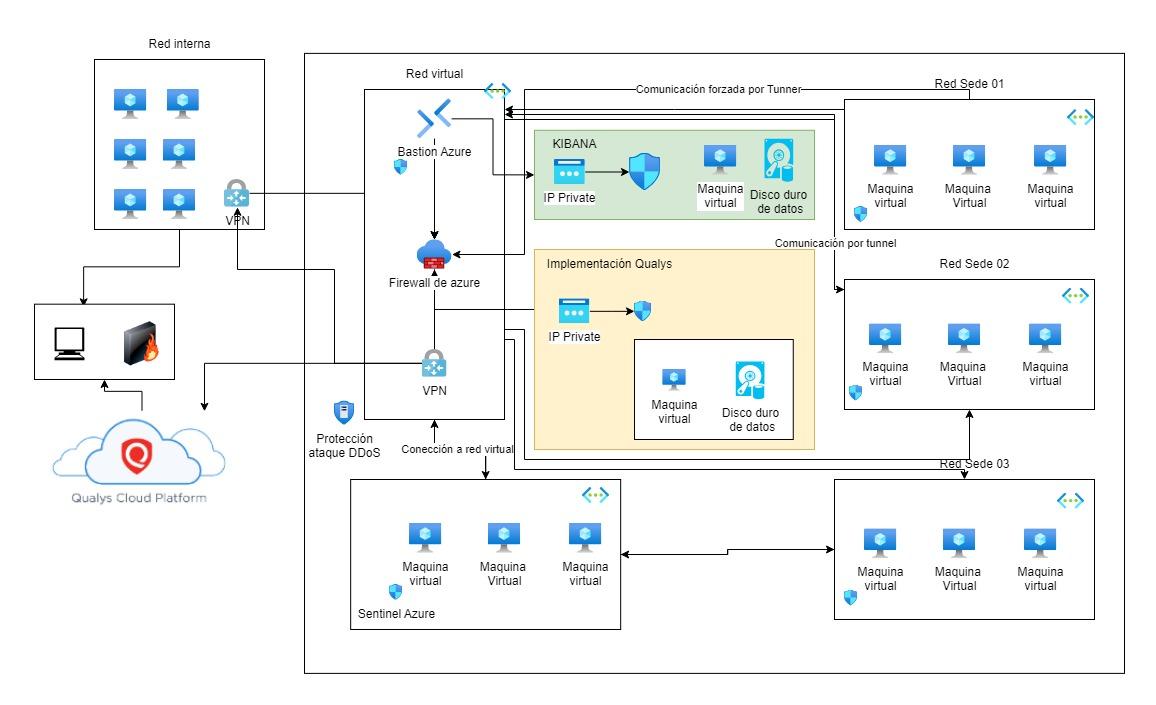
****

Dentro del marco de la arquitectura de TI descrita en el diseño "To Be", se otorga una prioridad significativa a la mejora en el procesamiento, transporte y salvaguarda de la información. Con el fin de alcanzar estos objetivos, se integran estratégicamente tres firewalls que interactúan con los switches antes de permitir el acceso a la red de Internet. Estos firewalls desempeñan un papel fundamental en la protección de la infraestructura y los datos, al facilitar un control y filtrado efectivos del tráfico de la red.

Se propone como solución la implementación de una infraestructura de tecnología de la información (TI) más compleja, en la cual la red interna se conectará a través de una red virtual utilizando una VPN. Esta VPN estará equipada con un Firewall de Azure y Bastion Azure. Además, se establecerá un entorno compuesto por Kibana con una dirección IP privada y una máquina virtual con un disco duro de datos.

Por otro lado, la implementación de Elastic contará con un nodo Master, una máquina virtual y uno o varios nodos (1-n) para los clientes, así como otro conjunto de nodos (1-n) con direcciones IP de acceso. Con el fin de garantizar una comunicación segura, se emplea la comunicación forzada por Tunner a través de tres redes distintas para cada sede.

* **TOBE 2 PARA MONITOREO Y ARTICLOUD**

****

En la propuesta del TO BE 2, se integra el servicio de Qualys la cual brinda diferentes servicios que ayudan a mejorar la seguridad y monitoreo. Primero el servicio de Qualys para gestionar el ingreso a los servicios de la empresa, lo cual le permitira analizar los recursos en busca que

**SERVICIOS PÚBLICOS QUALYS AZURE**

Qualys Azure es una solución de seguridad basada en la nube que se integra con el entorno Microsoft Azure. Qualys, una reconocida empresa de seguridad de la información, proporciona una plataforma de gestión de vulnerabilidades y cumplimiento normativo que ayuda a las organizaciones a identificar y abordar las posibles amenazas y riesgos en sus entornos de Azure [3]

**La integración de Qualys Azure en un entorno en la nube es importante por varias razones:**

* **Descubrimiento y visibilidad:** Qualys Azure ofrece una visibilidad exhaustiva de los recursos de Azure en una organización. Esto permite identificar y rastrear los activos y servicios de Azure existentes, incluso en entornos de escala empresarial y dinámicos.
* **Evaluación de vulnerabilidades:** La solución de Qualys permite realizar evaluaciones de vulnerabilidades en los recursos de Azure para identificar debilidades y brechas de seguridad. Utilizando técnicas como el escaneo de puertos, la detección de servicios y las pruebas de penetración, Qualys ayuda a identificar y priorizar las vulnerabilidades que podrían ser explotadas por atacantes.
* **Cumplimiento normativo**: Qualys Azure ofrece herramientas para evaluar y cumplir con los requisitos de cumplimiento normativo en entornos de Azure. Esto es especialmente importante para las organizaciones que operan en sectores altamente regulados, como la industria financiera o la atención médica, donde el cumplimiento de las normativas y estándares de seguridad es crucial.
* **Gestión continua de la seguridad:** Qualys Azure permite realizar un seguimiento continuo de la seguridad en entornos de Azure. Esto incluye la capacidad de realizar escaneos y evaluaciones periódicas, así como la monitorización de eventos de seguridad en tiempo real para detectar y responder rápidamente a posibles amenazas.

**Las ventajas de utilizar Qualys Azure incluyen:**

* **Escalabilidad:** Al ser una solución basada en la nube, Qualys Azure se puede escalar fácilmente para adaptarse a los entornos en constante crecimiento de Azure. Puede manejar grandes volúmenes de recursos y proporcionar una cobertura efectiva para organizaciones de todos los tamaños.
* **Automatización:** Qualys Azure ofrece capacidades de automatización que permiten agilizar las tareas de seguridad y reducir la carga de trabajo manual. Esto incluye la programación de escaneos automáticos, la generación de informes personalizados y la integración con flujos de trabajo y herramientas existentes.
* **Accesibilidad y facilidad de uso:** La interfaz intuitiva de Qualys Azure facilita su uso y permite a los equipos de seguridad acceder rápidamente a la información necesaria. También proporciona paneles de control y métricas visuales para una mejor comprensión de la postura de seguridad de los entornos de Azure.
* **Integración con otros servicios:** Qualys Azure se puede integrar con otras soluciones de seguridad y herramientas de administración de Azure. Esto proporciona una vista unificada de la seguridad y permite una mayor eficiencia operativa al centralizar la gestión de la seguridad.

**SERVICIOS PRIVADOS QUALYS AZURE**

La plataforma de Qualys proporciona una amplia gama de funcionalidades de seguridad en la nube. Permite a las organizaciones tener una visibilidad completa de su infraestructura en los servicios privados de Azure, así como implementar medidas de seguridad proactivas y gestionar los riesgos de manera eficiente.

La integración de Qualys en los servicios privados de Azure brinda diversas ventajas:

* **Visibilidad y control:** La integración permite tener una visibilidad completa de la infraestructura en los servicios privados de Azure. Esto incluye la capacidad de descubrir y rastrear los recursos, así como tener una comprensión detallada de la postura de seguridad de la infraestructura en la nube.
* **Evaluación de vulnerabilidades:** El Virtual Scanner de Qualys permite escanear los recursos y activos en los servicios privados de Azure para identificar vulnerabilidades. Esto ayuda a las organizaciones a comprender los riesgos y las debilidades de seguridad presentes en su infraestructura, permitiendo tomar medidas para mitigarlos.
* **Cumplimiento normativo:** La plataforma de Qualys proporciona funcionalidades para evaluar y cumplir con los requisitos de cumplimiento normativo en los servicios privados de Azure. Esto es especialmente relevante para las organizaciones que operan en sectores altamente regulados y deben cumplir con estándares de seguridad específicos.
* **Automatización y escalabilidad:** Qualys ofrece capacidades de automatización que permiten programar escaneos de forma regular, generación de informes automatizados y tareas de administración de seguridad. Esto facilita la gestión y escalabilidad en entornos en constante crecimiento.
* **Gestión centralizada:** La integración de Qualys en los servicios privados de Azure brinda una plataforma centralizada para gestionar la seguridad de la infraestructura. Proporciona paneles de control y métricas visuales para una mejor comprensión de la postura de seguridad y facilita la coordinación entre los equipos de seguridad.
* **CONCLUSIONES Y RECOMENDACIONES**

Elastic Cloud es una solución poderosa y conveniente para implementar y gestionar Elasticsearch y Kibana, y se utiliza ampliamente para el análisis y la búsqueda de datos en tiempo real. Su facilidad de uso y capacidad de escalabilidad lo convierten en una opción atractiva para empresas de diversos tamaños y sectores que buscan una forma eficiente de administrar y analizar grandes volúmenes de datos.

La infraestructura implementada, que combina servidores físicos y servicios en la nube de Azure, ofrece una base sólida para respaldar las operaciones empresariales y aprovechar los beneficios de la escalabilidad, flexibilidad y seguridad. La integración de servicios públicos y privados, la comunicación segura a través de VPN, los servidores de bases de datos, el equilibrador de carga, el proxy NGINX, Kibana y Elastic Cloud con Elasticsearch proporcionan una infraestructura sólida, adaptable y eficiente para respaldar sus necesidades empresariales actuales y futuras.

Se deben aprovechar las capacidades proactivas de Qualys en la gestión de parches para identificar y aplicar las actualizaciones necesarias en los servicios privados de Azure. Esto garantizará que los sistemas estén protegidos contra vulnerabilidades conocidas y amenazas.

Es importante evaluar la posibilidad de aprovechar las soluciones integrales de Qualys, que abarcan la gestión de vulnerabilidades, el cumplimiento normativo, la detección de amenazas y la respuesta a incidentes. Estas soluciones combinadas pueden fortalecer las defensas de seguridad de la empresa y prepararla para enfrentar los desafíos de seguridad de manera efectiva.

* **REFERENCIAS**

[1] C. Barrera, M. R. Cansino, y G. C. del C. E. de las redes de voz y datos de la DGB, “ISSN: 0187-750X public@dgb.unam.mx”, Redalyc.org. [En línea]. Disponible en: https://www.redalyc.org/pdf/285/28580115.pdf. [Consultado: 17-jul-2023].

[2] “¿Qué es un router?”, *Cisco*, 17-oct-2021. [En línea]. Disponible en: <https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html>.

[[3] sikovatc, «Aplicación de Confianza cero principios a máquinas virtuales en Azure», 24 de mayo de 2023. https://learn.microsoft.com/es-es/security/zero-trust/azure-infrastructure-virtual-machines](https://www.zotero.org/google-docs/?sIYYRa)