

Universidad Cenfotec

Maestría en Ciberseguridad

Documento Final Proyecto de Investigación Aplicada 2

Tema:

Propuesta de Diseño para migración de Servicios Enterprise a Amazon Web Services

Aguilar Elizondo Aarón

Agosto, 2019

Declaratoria de derechos de autor

Yo Aarón David Aguilar Elizondo, autor de este documento de Tesis con título: "Propuesta de Diseño para migración de Servicios Enterprise a Amazon Web Services" solicito respetuosamente se mantenga bajo un perfil de Confidencial por un periodo máximo de cinco años.

El documento representa una propuesta real y aplicable a la empresa Teradyne Inc por lo cual contiene información sensible acerca de su infraestructura, aplicaciones mecanismos de seguridad y conectividad que requieren el debido resguardo de terceras partes.

Dedicatoria y Agradecimientos

Primero que todo quiero agradecerle a Dios quien me da la sabiduría y perseverancia para completar el proceso de Maestría, a mi esposa, por ser mi apoyo durante todo este proceso, a mis profesores y tutor, parte importante en la transferencia de conocimiento y experiencia.

A Teradyne Inc por autorizarme presentar esta propuesta y entrevistar a miembros clave de la organización en cada una de los grupos de infraestructura, aplicaciones y administración. Un especial agradecimiento para:

John Debella

Pankaj Desai

Javier Knudsen

Allan Ramírez

Christopher Herrera

Luis Jenkins

Francisco García

Quiero dedicar este trabajo a mis padres quienes siempre me inculcaron el deseo de mantenerme estudiando y aprendiendo a pesar de los obstáculos presentes en el camino.

Aprobación de Proyecto

Primero lector: Diego González

Segundo lector: Ignacio Trejos

Tutor: Carlos Manuel Calvo

Tabla de Contenido

Capítulo 1. Introducción 14

1.1 Generalidades 14

1.1.1 Historia de Teradyne inc. 14

1.1.2 Presencia global 17

1.2 Definición y Descripción del Problema 18

1.3 Justificación 18

1.3.1 ¿Por qué Amazon Web Services? 20

1.4 Objetivos 20

1.4.1 Objetivo General 20

1.4.2 Objetivos Específicos 20

1.5 Alcances y Limitaciones 21

1.5.1 Alcances 21

1.5.2 Limitaciones 21

1.6 Estado de la Cuestión 22

Capítulo 2. Marco Conceptual 29

2.1 ¿Qué es la nube? 29

2.2 Computación en la nube, ¿qué es? 30

2.3 ¿Cuáles son los tipos de informática en la nube? 30

2.4 Ventajas 31

2.5 Desventajas 33

2.6 Servicios de Amazon Web Services 34

2.6.1 Computación 34

2.6.2 Redes 35

2.6.3 Almacenamiento 35

2.6.4 Bases de Datos 36

2.6.5 Seguridad 36

2.6.6 Herramientas de Administración 37
2.7 Zonas de Disponibilidad y Regiones de AWS 37
Capítulo 3. Requerimientos 39
3.1 Requerimientos Generales 39
3.2 Requisitos Infraestructura 39
3.2.1 Network 39
3.2.2 Windows 40
3.2.3 Unix 40
3.2.4 Storage 40
3.2.5 Backup 41
3.2.6 Security 41
3.3 Requerimientos del Negocio 42
3.4 Requerimientos Generales Aplicaciones 42
3.5 Requerimientos Específicos aplicaciones Enterprise: 43
3.5.1 Active Directory 43
3.5.2 DNS interno 44
3.5.3 DNS Externo 45
3.5.4 SharePoint 46
3.5.5 Portal de Clientes internos y externos (Eknowledge) 48
3.5.6 Página Web (www.teradyne.com) 51
3.5.7 Carpetas Compartidas dentro del esquema DFS-R 51
3.5.8 LSF 52
3.5.9 Enterprise Backup 54
3.5.10 Team Center PLM 56
3.5.11 Servidor de administración de Antivirus 57
1.7 3.6 Modelo de Conectividad Actual 58
Capítulo 4. Propuesta 62

4.1 Modelo de Infraestructura propuesto 62
4.1.1 Regiones 62
4.1.2 Zonas de Disponibilidad 63
4.1.3 Direccionamiento.....63
4.1.4 Selección de Servidores y Sistema Operativo 64
4.1.5 Almacenamiento.....65
4.1.6 Distribución de Aplicaciones y servicios.....67
4.2 Modelo de Conectividad Propuesto 69
4.2.1 Enrutamiento 71
4.3 Aseguramiento de la infraestructura 71
4.3.1 Modelo de Responsabilidad Compartida AWS.....72
4.3.3 Security Groups y Network ACLs.....73
4.3.4 Seguridad en Sistema Operativo 73
4.3.5 Encriptación de Datos.....74
4.3.6 IAM (Identity and access management) 74
4.3.7 AWS Shield.....75
4.4 Monitoreo 75
4.5 Otras consideraciones.....76
4.5.1 Amazon Elastic Load Balancing 77
4.5.2 Amazon Route 53.....77
4.5.3 Amazon RDS.....77
4.5.4 Amazon CloudFront 78
4.5.5 Auto Scaling.....79
4.5.6 Certificaciones AWS 80
4.5.8 Implementación de requisitos en AWS.....80
4.6 Propuesta de migración 84
Capítulo 5. Conclusiones 87

Referencias.....89
Anexos.....93

Lista de Figuras, gráficos cuadros e ilustraciones

Figura 1. Teradyne D133. (Teradyne D133, s.f.) 15

Figura 2. Teradyne A500 (TERADYNE A500 - Analog VLSI Test System, s.f.) 15

Figura 3. Unidades de Negocio de Teradyne Inc. (Unidades de Negocio, 2019) 17

Figura 4. Distribución de empleados por país. (Distribucion de Empleados Teradyne, s.f.) 17

Figura 5. Aryaka POPs alrededor del mundo. (Aryaka Pop Locations, s.f.) 25

Figura 6. Aryaka POPs por zona geográfica. (Aryaka Pop Locations, s.f.) 25

Figura 7. Cuadrante Mágico de Gartner IasS 2017. (Barr, 2017) 27

Figura 8 Cuadrante Mágico de Gartner IasS 2018. (Gartner Magic Quadrant IaaS Providers 2018, s.f.) 28

Figura 9. IaaS, PaaS, SaaS. (¿Qué es PaaS?, s.f.) 31

Figura 10. Áreas de Servicios AWS. (Productos de la nube, s.f.) 34

Figura 11. Servicios Computación AWS. (Productos de la nube, s.f.) 34

Figura 12. Servicios Redes AWS. (Productos de la nube, s.f.) 35

Figura 13. Servicios Almacenamiento AWS. (Productos de la nube, s.f.) 35

Figura 14. Servicios Bases de Datos AWS. (Productos de la nube, s.f.) 36

Figura 15. Servicios Seguridad AWS. (Productos de la nube, s.f.) 36

Figura 16. Herramientas de Administración AWS. (Productos de la nube, s.f.) 37

Figura 17. Descripción Regiones y Zonas de Disponibilidad. (Regiones y zonas de disponibilidad, s.f.) 38

Figura 18. Regiones AWS. (Productos de la nube, s.f.) 38

Figura 19. Diagrama Lógico Active Directory. Basado en Documentación Interna 43

Figura 20. Diagrama Lógico DNS Interno. Basado en Documentación Interna 44

Figura 21. Diagrama Lógico DNS Externo. Basado en Documentación Interna 45

Figura 22. Diagrama Lógico SharePoint. Basado en Documentación Interna 46
Figura 23. Diagrama Lógico Eknowledge PROD / QAT. Basado en Documentación Interna 48
Figura 24. Diagrama Lógico Eknowledge DR. Basado en Documentación Interna.....50
Figura 25. Diagrama Lógico Pagina Web PROD/ DEV. Basado en Documentación Interna 51
Figura 26. Diagrama Lógico Esquema DFS. Basado en Documentación Interna 52
Figura 27. Diagrama lógico IBM LSF. Basado en Documentación Interna.....54
Figura 28. Diagrama Lógico de Enterprise Backup. Basado en Documentación Interna 55
Figura 29. Diagrama Lógico Team Center PLM. Basado en Documentación Interna ..56
Figura 30. Diagrama Lógico Servidor de administración Antivirus. Basado en Documentación Interna 57
Figura 31. Diagrama Lógico de conectividad en Data Center. Basado en Documentación Interna 59
Figura 32. Diagrama Lógico de Conectividad Sitio Ingeniería. Basado en Documentación Interna 60
Figura 33. Diagrama Lógico de conectividad sitios estándar. Basado en Documentación Interna 61
Figura 34. Amazon S3 Glacier. (AWS Cloud Practitioner Training, s.f.).....66
Figura 35. Diagrama Lógico VPC Propuesta. Región EE.UU (Norte de Virginia).....68
Figura 36. Diagrama Lógico VPC Propuesta. Región EE.UU. Oeste (Norte de California) 68
Figura 37. Diagrama Lógico VPC Propuesta. Región Asia Pacífico (Singapur) 69

Figura 38. Diagrama Lógico de Conectividad mediante Aryaka. (SD-WAN FOR AMAZON WEB SERVICES, s.f.)....70
Figura 39. Modelo de Responsabilidad Compartida de AWS. (Modelo de responsabilidad compartida, s.f.)....72
Figura 40. Ejemplos de configuración de alarmas. (AWS Cloud Practitioner Training, s.f.)....76
Figura 41. Diagrama Lógico Elastic Load Balancer. (AWS Cloud Practitioner Training, s.f.)....77
Figura 42. Motores Soportados y Distribución de responsabilidades Amazon RDS. (AWS Cloud Practitioner Training, s.f.)....78
Figura 43. Edge Locations AWS CloudFront. (Características clave de Amazon CloudFront, s.f.)....79
Figura 45. Descripción Amazon Glacier. (AWS Cloud Practitioner Training, s.f.)....79
Figura 46. Certificaciones y Acreditaciones AWS. (AWS Cloud Practitioner Training, s.f.)....80

Tabla 1. Inventario de Equipos Active Directory....43
Tabla 2. Inventario de Equipo DNS Interno....44
Tabla 3. Inventario de Equipos DNS Externo....45
Tabla 4. Inventario Equipos SharePoint....46
Tabla 5. Inventario Equipos Eknowledge PROD/ QAT....48
Tabla 6. Inventario Equipos Pagina Web PROD / DEV....51
Tabla 7. Inventario Equipos Principales Esquema de DFS....52
Tabla 8. Inventario equipos principales Enterprise Backup....55
Tabla 9. Inventario Equipos Team Center PLM....56
Tabla 10. Inventario Equipos Administración Antivirus....58

Tabla 11. Regiones AWS.....62
Tabla 12. Definición de Subnets a utilizar.....64
Tabla 13. Distribución de Aplicaciones en Regiones.....67
Tabla 14. Implementación de Requisitos Network.....80
Tabla 15. Implementación de Requisitos Windows.....81
Tabla 16. Implementación de Requisitos Unix.....82
Tabla 17. Implementación de Requisitos Storage.....82
Tabla 18. Implementación de Requisitos Backup.....83
Tabla 19. Implementación de Requisitos Security.....84

Resumen Ejecutivo

Teradyne Inc. es una empresa de alta tecnología con presencia en 12 países y 80 oficinas alrededor del mundo. Sus oficinas principales ubicadas en North Reading, Boston Massachusetts. Estados Unidos, también contienen su centro de datos principal desde donde se provee todos los servicios corporativos de tecnologías de información. Como sitio alterno su oficina en Agoura Hills, California, cuyo centro de datos es primordial para el esquema de recuperación ante desastres.

Históricamente en ambos sitios se presentan acontecimientos los cuales afectan parcial o totalmente la operación. Un ejemplo reciente que pone en evidencia puntos de mejora, sucede en noviembre del 2018, cuando un incendio forestal al sur de California alcanza pocos metros de edificio y pese a no haber daños específicamente en las instalaciones, provoca caídas en servicios de electricidad, internet y agua. Además, no es accesible por los caminos cerrados en los alrededores. En ese lapso, un evento completamente aislado en el Centro de Datos de North Reading con un breaker de un centro de carga principal, ocasiona la caída del fluido eléctrico del centro de datos completo.

Además de garantizar la disponibilidad de los servicios, es muy importante mantener un buen desempeño de ellos desde ubicaciones remotas y esto implica retos necesarios de solventar: la eficiente comunicación entre sitios, los tiempos de respuesta sobre todo en los sitios más remotos, las oficinas en el Continente Asiático, todo esto mientras se vela por la seguridad de las comunicaciones y los datos que se trasmiten.

En el presente documento se plantea una propuesta de diseño para la migración de los servicios dentro de la categoría Enterprise, también conocidos como “core services”, los cuales residen en los centros de datos principales y se utilizan y accesan desde las oficinas de Teradyne alrededor del mundo, a la nube de Amazon Web Services y de esta forma se aprovecha las características de replicación en diferentes zonas geográficas, se reduce los tiempos de respuesta de los sitios remotos, se mejora la experiencia del usuario y a la vez la disponibilidad de los sistemas y su desempeño. Además, se aborda en la propuesta cómo asegurar esta infraestructura, los datos que viajen y se almacenen en ella y como augurar el acceso desde las ubicaciones remotas.

Capítulo 1. Introducción

1.1 Generalidades

1.1.1 Historia de Teradyne inc.

Nicholas DeWolf y Alexander V. d'Arbeloff se conocen mientras hacen fila en sus unidades de ROTC[1] del MIT a finales de los años 40. Toman caminos separados después de graduarse, pero el destino los une de nuevo en 1960 para fundar Teradyne Inc., una empresa líder mundial en el mercado de equipos de testeo electrónico. La premisa es la siguiente: la velocidad de testeo de componentes electrónicos producidos en gran volumen alcanzaría un cuello de botella, a menos que las labores realizadas por técnicos y equipos de laboratorio pudiera de alguna forma automatizarse y así deciden crear un nuevo tipo de equipos de testeo de "grado industrial". Se llaman de esa manera por su desempeño, confiabilidad y retorno de inversión.

Teradyne inicia en un local en el centro de Boston y su nombre proviene de Tera, prefijo de 10 a la doceava potencia y dyne (dyn) o dina en español, una unidad de fuerza equivalente a 10μN en el Sistema Cegesimal de Unidades [2](Sistema CGS)

En 1961 se vende su primer producto llamado D133. Sirve para probar diodos de germanio. En poco tiempo los primeros clientes se dan cuenta que los resultados obtenidos en términos de rendimiento de la producción, resultan muy superiores al costo del tester.

[1] ROTC. Cuerpo de Entrenamiento de Oficiales de la Reserva, por sus siglas en inglés) Programa universitario, que prepara a adultos jóvenes para que se conviertan en oficiales de las Fuerzas Armadas de los Estados Unidos. (Programas del ROTC, s.f.)

[2] El Sistema Cegesimal de Unidades, también llamado sistema CGS, es un sistema de unidades basado en el centímetro, el gramo y el segundo. Su nombre es el acrónimo de estas tres unidades



Figura 1. Teradyne D133. (Teradyne D133, s.f.)

En la década de 1980, Teradyne expande su negocio de pruebas al adquirir Zehntel, un fabricante líder de sistemas de prueba de tarjetas de circuitos integrados. En 1987, la compañía introduce el A500, este lidera el mercado en la prueba de dispositivos integrados los cuales proporcionan la interfaz entre datos analógicos y digitales. Es el primer sistema de prueba analógico VLSI[3] (Very Large Scale Integration).

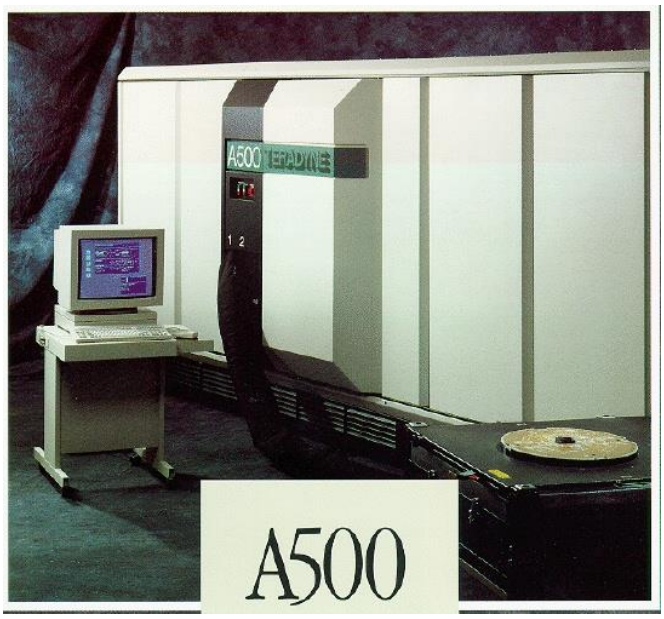


Figura 2. Teradyne A500 (TERADYNE A500 - Analog VLSI Test System, s.f.)

[3] La integración a escala muy grande o **VLSI** es el proceso de crear un circuito integrado compuesto por cientos de miles de transistores en un único chip.

En la década de 1990 la compañía adquiere Megatest Corporation, amplía su grupo Semi Test para incluir probadores más pequeños y menos costosos respecto de los disponibles actualmente. Teradyne también se convierte en un líder del mercado en la prueba de alto nivel System-on-a-Chip (SoC) con sus sistemas de prueba Catalyst y Tiger.

En el año 2000, Teradyne Connection Systems compra Herco Technologies y Synthane-Taylor, un año más tarde adquiere al líder de inspección y pruebas de tarjetas de circuitos, GenRad, y lo fusiona en la División de Pruebas de Ensamblaje. Las soluciones de diagnóstico de GenRad, que fabrican equipos de prueba para las industrias de fabricación y servicio automotriz, se convierten en un grupo de productos separado para Teradyne.

Posteriormente en el 2008, con la incorporación de Nextest para servir al mercado de pruebas de memoria flash e Eagle Test Systems al mercado de pruebas analógicas de alto volumen, Teradyne amplía su negocio de pruebas de semiconductores. Ese año, Teradyne ingresa al mercado de prueba de unidades de disco con el producto Neptune, desarrollado internamente y sirve al mercado de almacenamiento de datos de gran densidad.

Teradyne celebra su 50 aniversario en el 2010, con uno de sus años más fuertes. Al año siguiente, adquiere LitePoint Corporation, un proveedor líder de soluciones de prueba para productos inalámbricos, como computadoras portátiles, tabletas, redes domésticas y teléfonos celulares. Con la adición de LitePoint, la cartera de productos de Teradyne se extiende desde la prueba de chips de semiconductores, placas de circuitos y hasta productos listos para la venta.

Teradyne continúa brindando una ventaja competitiva a las compañías de electrónica líderes del mundo con sus principales unidades de negocios: Prueba de semiconductores, Prueba de sistemas, Prueba inalámbrica. Y con la adquisición más reciente por parte de la Compañía de Universal Robots, una compañía especializada en robots colaborativos, ingresa a la industria de la automatización industrial. (Historia de Teradyne, s.f.)

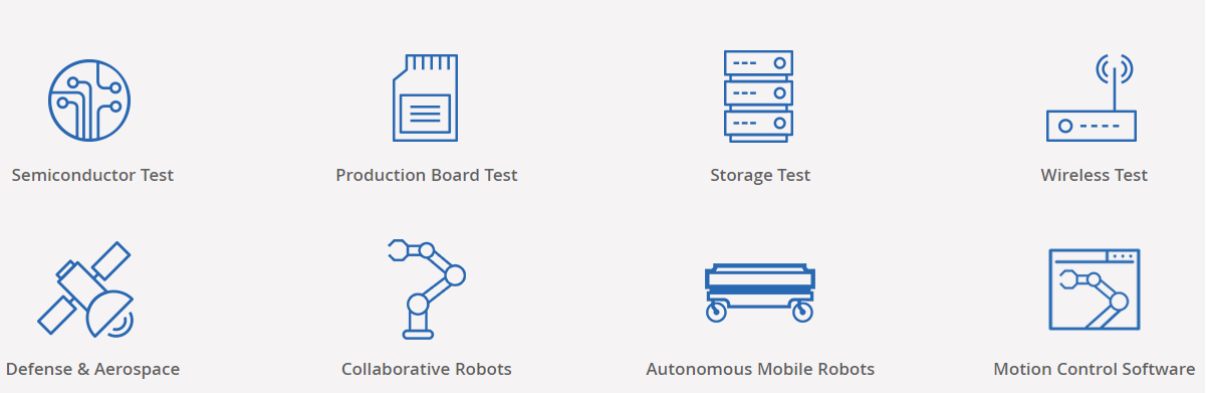


Figura 3. Unidades de Negocio de Teradyne Inc. (Unidades de Negocio, 2019)

1.1.2 Presencia global

Teradyne cuenta con 70 Oficinas alrededor del mundo y casi 5000 empleados distribuidos de la siguiente manera:



Figura 4. Distribución de empleados por país. (Distribucion de Empleados Teradyne, s.f.)

1.2 Definición y Descripción del Problema

Los servicios Core están hosteados en los Data Center de la empresa, siendo el de North Reading, Massachusetts el principal y el Disaster Recovery ubicado en Agoura Hills, California. Al tener presencia global existe la necesidad de acceder estos sistemas desde cualquier lugar del mundo, no necesariamente oficinas, pues muchos empleados trabajan de forma remota a través de un VPN.

El Diseño de los Data Centers se piensa para estar en dos sitios geográficamente separados, lo cual es recomendable, al ser menos probable que un evento catastrófico afecte ubicaciones tan distantes entre sí, a menos claro, se trate de un evento a nivel país.

La ubicación geográfica juega un papel importante en cuanto a tiempos de respuesta para el acceso a los servicios. La ubicación actual es conveniente para los sitios ubicados en América, donde se espera tiempos de respuesta bajos. Sin embargo, entre más remota sea la oficina, se espera los tiempos de respuesta tiendan a incrementar. Existen otros factores también capaces de afectar estos tiempos, e inclusive algunos a nivel país y de legislación propia, por cuanto regula las comunicaciones. Tal es el caso de China, más adelante se amplía al respecto.

Debido a esta necesidad de proveer acceso desde cualquier parte del mundo y además porque en el pasado ocurren eventos que afectan parcial o totalmente los servicios Core de la empresa, se plantea la necesidad de implementar estos servicios en una infraestructura donde se ofrezca mayor estabilidad y sea posible replicarlos en otras zonas geográficas.

1.3 Justificación

Con el fin de analizar si una infraestructura en la nube puede proveer un mayor nivel de redundancia, reducir tiempos de respuesta y por lo tanto bridar al usuario una mejor experiencia y eficiencia, el investigador tiene como tarea verificar, respecto de los servicios determinados como Enterprise, cuáles son sus requerimientos, dependencias y analizar si es posible una migración a una infraestructura en la nube.

Lo anterior representa un reto importante, pues algunos de estos servicios pueden enfrentar desafíos tecnológicos por el uso de versiones obsoletas de sistemas operativos, programas o componentes de ellos, los cuales a través del tiempo se mantienen por su dificultad para migrar a una plataforma más actualizada, su costo al hacerlo o simplemente por no haber una necesidad real. Además, pueden aparecer consideraciones por tomar en cuenta en términos de licenciamiento que se deba contemplar.

Tener un centro de datos en las instalaciones de la empresa representa, aparte de la limitación de espacio físico y ubicación geográfica otros gastos implícitos como lo son electricidad, UPS, aire acondicionado, sistemas de seguridad, control de acceso, detección de incendios, entre otros, con el nivel de redundancia definido, y para el caso particular de Teradyne mantener el centro de datos de Agoura Hills, como parte del esquema de recuperación ante desastres, con los equipos y servicios necesarios para mantener la operación en caso de un evento catastrófico en el centro de datos principal.

También existen gastos propiamente en equipos, ya sea de comunicación, almacenamiento, cableado, servidores. Para el caso de todo lo referente a hardware normalmente se compra con contratos de garantía y soporte, depende de la criticidad del equipo, En algunas ocasiones estos contratos se utilizan para el reemplazo de partes o en materia de soporte, pero, aun así, el tiempo de recuperación en caso de fallo puede extenderse hasta días. Otras veces simplemente no ocurre ninguna eventualidad con el hardware y no se requiere hacer uso de los contratos. Sin embargo, al llegar el equipo a un estado de obsolescencia es necesario realizar de nuevo una inversión para comprar el reemplazo.

Un motivo del porqué se quiere al migrar los servicios Enterprise a la nube de Amazon Web Services, en primer lugar, es eventualmente proveer acceso a algunos de los servicios a los sitios Asia desde una ubicación más cercana geográficamente hablando, con el propósito de ofrecer menores tiempos de respuesta y un nivel de redundancia superior. Pero, además, la intención de corto y mediano plazo es ir prescindiendo de los servidores físicos ubicados en los centros de datos de la empresa, que hostean los servicios críticos y conllevan gastos implícitos, por una versión en la nube la cual se pueda escalar cuando sea necesario, no dependa del hardware y se pague solamente los recursos por utilizar.

1.3.1 ¿Por qué Amazon Web Services?

Se escoge Amazon Web Services porque ejerce el liderazgo en el mercado para infraestructura, como servicio (IaaS) según el Cuadrante Mágico de Gartner en los últimos años (Ver Estado de la cuestión) y pese a mencionarse el crecimiento de sus principales competidores como son Azure de Microsoft y Google Cloud Platform de Google, todavía no alcanzan el nivel de madurez propio de AWS

1.4 Objetivos

1.4.1 Objetivo General

Elaborar una propuesta para migrar los servicios Enterprise de Teradyne. Inc a a la nube de Amazon Web.

1.4.2 Objetivos Específicos

- Identificar los servicios Enterprise por mover, sus dependencias y requerimientos.
- Analizar para cada uno de los servicios si es posible cumplir los requerimientos utilizando Amazon Web Services.
- Proponer la Infraestructura donde se migre los servicios.
- Diseñar la conectividad y mecanismos para acceder a los servicios.
- Definir los mecanismos para asegurar los servicios en la nube y el acceso a ellos por parte de los usuarios.
- Elaborar un plan para el proceso de migración en etapas.

1.5 Alcances y Limitaciones

1.5.1 Alcances

La propuesta descrita en esta investigación se formula con base en los requerimientos de cada una de las áreas de infraestructura, de tal forma, se apegue a la realidad de sus necesidades. Pero no necesariamente implica un compromiso por parte de Teradyne de implementarse a corto o largo plazo. La intención es primero conocer si es posible migrar sus servicios Enterprise a una infraestructura en la nube, donde se cumpla los requerimientos planteados por las partes y segundo, proponer una alternativa de cómo hacerlo.

El alcance de la investigación es exploratorio: pretende obtener la mayor cantidad de información de los servicios por migrar, así como de la infraestructura de Amazon Web Services, para que al utilizar sus servicios y características se pueda garantizar la correcta y eficiente operación de los servicios Enterprise migrados.

Esta investigación permite a futuro ser una base para un proyecto de implementación de servicios adicionales.

1.5.2 Limitaciones

Teradyne cuenta con más de 1900 Servidores Físicos y más de 400 Servidores Virtuales en el centro de datos principal. A cada server se le asigna una categorización de severidad, esta va de uno a cuatro, siendo uno los equipos más críticos para la operación, por ello, cualquier problema debe ser resuelto lo más rápido posible, con el fin de no afectar la continuidad del negocio. (Reporte de Inventario, Sistema Platinum, 2019)

La propuesta se limita a algunos de los servicios considerados como críticos, también llamados Enterprise y toda la infraestructura necesaria para su funcionamiento. Esta categoría se le da a servicios y aplicaciones de uso general como herramientas de trabajo utilizadas por empleados de Teradyne, clientes externos y partners, en cualquier parte del mundo. No todos los servicios Enterprise se consideran en este documento por diferentes circunstancias, algunas son razones del negocio, pues se decide esperar a que la implementación de los servicios contemplados en esta propuesta se complete, se tenga

un cierto nivel de madurez en la administración de la infraestructura en la nube y se alcance un nivel de confianza sobre la seguridad de la infraestructura.

Un caso particular es el servicio de Correo Electrónico, el cual se considera en esta propuesta porque actualmente migra de IBM Lotus Notes, hosteado en el Data Center principal, con un plan de recuperación de desastres en Agoura Hills y un esquema de replicación en Cebú, Filipinas para los usuarios de Asia hacia Exchange Online, junto con Office 365. Dos componentes adicionales vinculados con el correo electrónico son el Chat interno (IBM Sametime) y servidor de reuniones (IBM Meetings), en sus versiones para PC y dispositivos móviles, por lo tanto, estos servicios tampoco se contemplan. Por lo tanto, esta propuesta se limita a las siguientes aplicaciones y servicios:

- Active Directory
- DNS interno
- DNS Externo
- SharePoint (Intranet)
- Portal de Clientes internos y externos (Eknowledge)
- Página Web (www.teradyne.com)
- Carpetas Compartidas dentro del esquema DFS-R
- LSF
- Enterprise Backup
- Team Center (PLM)
- Servidor de administración de Antivirus

1.6 Estado de la Cuestión

El investigador al ser parte del grupo de infraestructura de Teradyne, está al tanto del diseño actual, tecnologías y herramientas utilizadas, además las necesidades actuales y planes a futuro de primera mano. Para ello consulta a los líderes de cada grupo de infraestructura y aplicaciones, una lista de requerimientos desde el punto de vista del equipo al cual representan. Además, sostiene una reunión con los managers, el fin es expresar de igual forma sus necesidades y preocupaciones a la hora de migrar los servicios a la nube.

A través del tiempo Teradyne utiliza diferentes tecnologías para mejorar la conectividad entre sus oficinas, así como el acceso a los recursos. Originalmente la conectividad es solamente de las oficinas remotas hacia los Data Center principales en Boston y Agoura Hills, por lo tanto, la conectividad entre dos oficinas remotas solo se hace en casos excepcionales, después de un análisis de la necesidad y de la cantidad de tráfico. En la mayoría de los casos dos oficinas remotas deben pasar a través de Boston para comunicarse entre sí, lo cual no resulta para nada eficiente. Por ejemplo, dos sitios, ambos en China, para hablarse entre sí deben ir hasta Boston, lo cual por supuesto tiene un tiempo de respuesta alto y tasas de transferencia de datos más bajas.

Para las oficinas más importantes se utiliza enlaces MPLS, tanto de Verizon como de AT&T para manejar el tráfico crítico. Estos ofrecen mayor estabilidad, la posibilidad de comunicación entre sitios directamente; pero con el agravante de precio considerablemente más elevado que un enlace regular de internet, por ello se cuenta con anchos de banda limitados.

Con el tiempo se incorpora dos tecnologías adicionales para mejorar la conectividad a través de la WAN. La primera utiliza Optimizadores WAN de la marca Riverbed. Esta básicamente hace compresión de paquetes al eliminar la necesidad de confirmación de entrega en todos los paquetes, es decir, no se espera a recibir los paquetes ACK para continuar enviando tráfico, además guarda en cache "tráfico", el cual más bien son secuencias de bits, alguna vez transmitidas y les coloca un puntero, así una segunda vez en lugar de retransmitirlo, utiliza la copia local del sitio de destino, esto es muy similar a lo conocido en almacenamiento como de-duplicación. (Como funciona un Steelhead Wan Accelerator, s.f.)

La segunda tecnología implementada con dispositivos de la marca Talari, se conoce como Link Aggregation. Permite unir dos o más enlaces de internet y generar un único canal con la sumatoria de los anchos de banda y un muy eficiente control de la salud de cada uno de los enlaces que lo componen, por ello, problemas de pérdida de paquetes en alguno de los enlaces no afecta la transmisión de datos. Esto además de servir para hacer un failover automático permite utilizar una funcionalidad adicional, se llama Path Replication. La idea es que, para tráfico crítico, se envíen los paquetes por dos o más enlaces en igual tiempo y el primero en llegar al destino se utiliza, con esto un paquete

perdido es poco probable y se reduce el número de retransmisiones al optimizar el uso del ancho de banda. (Talari WAN Aggregation, s.f.)

Estas dos tecnologías en mención solo se implementan en sitios de ingeniería, por ello, el resto de los sitios tienen los problemas originales. En 2016 se decide implementar túneles IPSec dinámicos, una tecnología de Cisco conocida en Cisco como DMVPN (Dynamic Multipoint VPN). (Salazar, 2016) Esta tecnología permite a los sitios remotos consultar en un dispositivo conocido como Hub, la información necesaria para construir un túnel directo con el sitio al cual se trata de llegar sin necesidad de interacción o configuración adicional, por parte de un administrador de red, de esa manera, cuando un sitio trata de contactar otro por primera vez, al no tener una ruta más directa consulta en el Hub, este le provee la información necesaria y en menos de un segundo se crea un túnel directo entre el sitio de origen y el de destino, el cual se mantendrá habilitado mientras exista tráfico entre ellos, en la configuración se define cuánto tiempo después de no observarse el tráfico se mantiene al túnel activo antes de desconectarse.

En 2017 Teradyne decide empezar a utilizar al proveedor de SD WAN llamado Aryaka, un proveedor líder mundial en esta tecnología. La ofrece alrededor del mundo, ello se conoce como Puntos de Presencia o POP, los cuales son puntos de entrada a la red de Aryaka, dentro de la cual se obtiene una calidad de conexión muy buena, y además ofrece compresión, optimización, calidad de servicio, herramientas de monitoreo, y funcionalidades como Path Replication. En otras palabras, con Aryaka se obtiene implícitamente los beneficios ofrecidos por Riverbed y Talari. Desde el sitio donde se inicia la conexión hacia el POP de Aryaka se establece un túnel IPSec al utilizar enlaces regulares de internet, por lo tanto, no hace falta invertir en enlaces dedicados. Como parte del servicio, Aryaka monitorea estos enlaces "última milla" para garantizar su salud y en caso de ser necesario se ponen en contacto con los proveedores de servicio para corregir cualquier problema detectado. (SD WAN as a Service (Aryaka), s.f.)

Todas las oficinas de Teradyne migran a esta tecnología y pese a estar todavía en proceso se espera completar el 100% en 2019



Figura 5. Aryaka POPs alrededor del mundo. (Aryaka Pop Locations, s.f.)

AMERICAS:	APAC:	EMEA:
San Jose, CA, USA	Sydney, Australia	London, England
Dallas, TX, USA		Tel Aviv, Israel
Chicago, IL, USA	Beijing, China	Frankfurt, Germany
Los Angeles, CA, USA	Hong Kong, China	Amsterdam, Netherlands
Miami, FL, USA	Shanghai, China	Dubai, United Arab Emirates
Ashburn, VA, USA		Johannesburg, South Africa
Seattle, WA, USA	Delhi, India	
Toronto, ON, CA	Bangalore, India	
	Chennai, India	
Sao Palo, Brazil	Mumbai, India	
	Taipei, Taiwan	
	Tokyo, Japan	
	Singapore, Republic of Singapore	
	Seoul, Korea	

Figura 6. Aryaka POPs por zona geográfica. (Aryaka Pop Locations, s.f.)

En 2018 algunos esfuerzos individuales de grupos de Ingeniería en Teradyne comienzan a incursionar en los servicios de Amazon Web Services, inicialmente para hostear máquinas con el fin de hacer pruebas de software, utilizando Amazon EC2.

Más recientemente en 2019 debido a cambios de legislación en Estados Unidos y en China como resultado de una llamada “guerra comercial”, el gobierno de Estados Unidos comienza a poner impedimentos a negocios con empresas las cuales tengan operaciones en China. Al punto, por ejemplo, de prohibir a empresas estadounidenses hacer negocios

con el fabricante chino Huawei. Como parte de las restricciones se incluye: las empresas estadounidenses no pueden vender o proporcionar tecnología a empresas chinas, se adoptan medidas para lograr que la operación de Teradyne en el Continente Asiático opere de una forma autónoma, sin tener dependencia directa de la Operación en Estados Unidos.

Es necesario entonces, como primera acción utilizar el servicio de Amazon S3 (Simple Storage) con el propósito de almacenar la información necesaria para procesos de fabricación, diseño de software y pruebas en una ubicación externa, en este caso en Singapur y se considera en esta propuesta tener una réplica de algunos de los servicios para accederse localmente en lugar de accederlos en Estados Unidos.

Al hacer una búsqueda sobre empresas e instituciones las cuales implementan los servicios de AWS se puede observar casos de éxito en diferentes focos de negocio, van desde empresas financieras, educativas, de gobierno, tecnológicas, de comunicación, deportivas, entre otras.

Algunos nombres que pueden resultar familiares: Departamento de Estado de EE. UU, Netflix, Shazam, National Instruments, Mercado Libre, Cinépolis, Tecno Lite, La compañía de Seguros Mapfre, Futbol Club Barcelona. La página de compras en línea Amazon.com de hecho en 2011, pasa de utilizar el backup en cinta a usar Amazon S3, para realizar copias de seguridad de la mayoría de sus bases de datos de Oracle. Mediante el uso de AWS, Amazon.com logra eliminar el software de backup y alcanza una mejora de desempeño 12 veces mayor, reduce el tiempo de restablecimiento de 15 a 2,5 horas aproximadamente. (Todas las historias de éxito de los clientes, s.f.)

El periódico en línea El Mundo en su edición del 14 de noviembre de 2014, habla de “Un Millón de empresas en la nube de Amazon”, dentro de ellas destaca: empresas como Dropbox, Spotify, Pinterest y Netflix a pesar de ser de empresas muy distintas, todas comparten igual infraestructura. A pesar de ser Amazon conocida por su plataforma de compras en línea, o por sus dispositivos Kindle, desde 2006 es líder de servicios infraestructura en la nube. (Un millón de empresas en la nube de Amazon, s.f.)

Forbes hace una revisión de los resultados financieros de AWS en su edición del 29 de diciembre de 2016, exalta los buenos resultados (Trefis Team, Great Speculations group, 2016)

Si se va al Cuadrante Mágico de Gartner se observa: AWS está entre los líderes tanto en 2017 como 2018, además se encuentra en el sitio de AWS en un blog del año 2017 de quien aparece como chief Evangelist for AWS, Jeff Barr, el título "*AWS Named as a Leader in Gartner's Infrastructure as a Service (IaaS) Magic Quadrant for 7th Consecutive Year*", lo cual evidencia se mantiene en esa posición por varios años.



Figura 7. Cuadrante Mágico de Gartner IasS 2017. (Barr, 2017)



Figura 8 Cuadrante Mágico de Gartner IasS 2018. (Gartner Magic Quadrant IaaS Providers 2018, s.f.)

Capítulo 2. Marco Conceptual

2.1 ¿Qué es la nube?

Es una práctica común cuando se recibe lecciones donde se aborda temas referentes a redes y conectividad, ejemplificar internet en un diagrama donde se usa una representación de una nube. Al parecer se utiliza mucho antes también en esquemas de telefonía y como representación para equipos de la ARPANET, predecesora de la Internet que hoy se conoce. Consiste en una red creada por encargo del Departamento de Defensa de los Estados Unidos entre las diferentes instituciones académicas y del estado.

En cualquiera de los casos, por simplicidad, el símbolo de nube busca representar múltiples equipos, servidores y otros. Todos interconectados entre sí, proveen servicios. Con el tiempo el término "la Nube" se convierte en la forma para describir una red enorme de servidores remotos en todo el mundo, conectados para funcionar como un único ecosistema. Se diseñan para almacenar y administrar datos, ejecutar aplicaciones, entregar contenido o servicios, como streaming de vídeos, correo web, software de ofimática o medios sociales. En lugar de acceder a archivos y datos desde un equipo personal o local, accede a ellos en línea desde cualquier dispositivo conectado a Internet, la información está disponible siempre que la necesite, mientras se tenga acceso a internet. (Origen del termino la nube, s.f.)

Existen diferentes tipos de nube, como la nube pública, comparte recursos y ofrece servicios al público a través de Internet. La nube privada, por lo general es accesible solo a través de una red interna privada, normalmente hospedada en el entorno local; la nube híbrida, comparte servicios entre nubes públicas y privadas, según su finalidad; y la nube comunitaria, comparte recursos solo entre organizaciones asociadas de alguna forma. (Que es la nube, s.f.)

2.2 Computación en la nube, ¿qué es?

Amazon Web Services en su página de documentación lo define como "*la entrega bajo demanda de capacidad informática, almacenamiento de bases de datos, aplicaciones y otros recursos de TI a través de una plataforma de servicios mediante Internet con un sistema de precios basado en el consumo."* (¿Qué es la informática en la nube?, s.f.)

En 2011, y tras un estudio del MIT elaborado por Antonio Regalado, se llega a la conclusión de que el término computación en la nube, como se conoce hoy, se utiliza por primera vez en 1996 en un documento interno de la extinta compañía COMPAQ.

Una de las primeras empresas en ofrecer sus servicios a través de un sitio web es Salesforce.com en 1999, posteriormente, en 2002, Amazon moderniza su centro de datos. Da así comienzo al desarrollo de un nuevo servicio para ofrecer computación en la nube a clientes externos. Así nace Amazon Web Services (AWS).

En 2006, Google lanza Google Docs., con elementos de la nube alcanza los usuarios medios. Ese año Amazon introduce en el mercado lo que llama Elastic Compute Cloud (EC2). Con este servicio, pequeñas empresas y personas pueden alquilar equipos virtuales donde ejecutar las aplicaciones de su propio ordenador.

La carrera por lanzar productos y servicios, tales como servicios en la nube, crece exponencialmente desde entonces. Entre ellas, Microsoft con Microsoft Azure y Office 365; IBM y su SmartCloud u Oracle Cloud. (Origen del termino la nube, s.f.)

2.3 ¿Cuáles son los tipos de informática en la nube?

Hay tres tipos de informática en la nube. Comúnmente se denominan infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y software como servicio (SaaS). Es importante seleccionar el tipo adecuado según las necesidades para alcanzar el equilibrio conveniente entre control, reducción de tareas manuales y costos de mantener, ya sea la infraestructura, plataformas o servicios por cuenta propia.



Figura 9. IaaS, PaaS, SaaS. (¿Qué es PaaS?, s.f.)

2.4 Ventajas

- Cambio de los gastos de capital por gastos variables

En lugar de tener que realizar una inversión grande en centros de datos y servidores y demás equipos, puede utilizar la informática en la nube y pagar únicamente cuando consuma recursos informáticos, y solamente en función del consumo realizado.

- Beneficios de la economía de gran escala

Mediante el uso de la informática en la nube, podrá tener costos variables más bajos de los que tendría con sus propios recursos. En la nube se suman los consumos realizados por cientos de miles de usuarios en todo el mundo. De esta forma, los proveedores, como Amazon Web Services, pueden aplicar mayores economías de escala que se traducen en precios más bajos por el consumo realizado para los usuarios.

- Facilidad para hacer variaciones de capacidad

Al tomar una decisión respecto a la capacidad requerida antes de implementar una aplicación, a menudo se acaba por acumular recursos caros y ociosos o por el contrario se descubre que se tiene una capacidad limitada. Con la informática en la nube, estos problemas desaparecen ya que podrá obtener acceso a los recursos que necesite y hacer ajustes sobre la marcha para aumentar o reducir la capacidad.

- Aumento de la velocidad y la agilidad

Siguiendo la línea del punto anterior en un entorno de la informática en la nube, la disponibilidad de nuevos recursos está en todo momento a unos cuantos clics del mouse. Esto significa que puede reducir el tiempo que dichos recursos tardan en estar disponibles desde el momento que se detecta el requerimiento hasta que se proveen de semanas a cuestión de minutos. El resultado es un aumento de la agilidad en la organización, ya que se reduce notablemente el tiempo y los costos necesarios para proveer recursos informáticos y ponerlos en producción.

- Reducción de gastos de la ejecución y el mantenimiento de los centros de datos

La informática en la nube le permite enfocarse en tareas de ejecución más que en tareas de instalación servidores en racks, proporcionarles electricidad, conectividad, mantener las condiciones adecuadas de temperatura y humedad, herramientas de monitoreo, control de incendios, seguridad, etc. Dicho de otra forma, convertimos gastos operativos (OPEX[4]) a gastos en capital (CAPEX[5])

- Pague solo lo que necesita

En un esquema de infraestructura en la nube se utiliza la figura de pagar solamente lo que se consume, no existen pagos por adelantado, contratos por periodos de tiempo o cargos por dejar de consumir un servicio o recurso. Los recursos son escalables en cualquier momento por lo que sobredimensionarlos previendo crecimiento se convierte en un gasto innecesario ya que de hecho se puede automatizar el crecimiento o disminución de recursos basado en condiciones preestablecidas. Existen además herramientas adicionales como por ejemplo una calculadora que le permite estimar el gasto o tener un desglose de cuanto ha consumido hasta el momento y analizadores de gastos que proveen sugerencias para la reducción de costos

[4] Operative Expenditure, Gastos operativos. (Descubra las diferencias entre CAPEX y OPEX, 2017)
[5] Capital Expenditure, es el gasto que se realiza en bienes y que genera beneficios para una compañía. (Descubra las diferencias entre CAPEX y OPEX, 2017)

- Implementación a nivel mundial en minutos

Las aplicaciones pueden ser implementadas de forma sencilla en múltiples regiones alrededor del mundo con solo unos clics. De esta forma, puede ofrecer una menor latencia y una mejor experiencia a sus clientes de forma sencilla y con un costo mínimo.

2.5 Desventajas

- Percepción de pérdida de privacidad de datos sensibles.

A pesar de que se firman acuerdos de confidencialidad y se utilizan otros mecanismos para asegurar la información, siempre existe la percepción de que queda expuesta ante el tercero que proporciona el servicio.

- Dependencia de la infraestructura y plataformas de terceros para operar.

Se genera una dependencia de los recursos proporcionados por el tercero ya que toda la infraestructura, aplicaciones y servicios se diseñan y se adaptan con base en esos recursos. Realizar cambios a otro proveedor o hacia algo propio se vuelve más complicado.

- Fuerte dependencia de Internet para el acceso a la información.

Evidentemente el acceso a internet se convierte en un recurso imprescindible para el acceso a la información, aplicaciones o infraestructura en la nube. Este recurso a su vez es provisto por un tercero sobre el cual no tenemos control. Es necesario entonces utilizar mecanismos de contingencia para garantizar la continuidad de este servicio.

- Arquitectura Multitenancy[6].

Una de las principales preocupaciones de implementar infraestructura y servicios en la nube es el hecho de que al final la infraestructura del proveedor es compartida entre todos sus clientes. A pesar de que se ofrece una segmentación lógica entre cliente y cliente se deben tomar medidas para evitar fuga de datos si hubiera fallos en esa segmentación.

[6] Multitenacy. Multi propietario. (Arquitecturas Multi-Tenant, s.f.)

2.6 Servicios de Amazon Web Services



Figura 10. Áreas de Servicios AWS. (Productos de la nube, s.f.)

Amazon web Services ofrece diversos productos dentro de una gran gama de áreas de servicios que sirven para cubrir desde necesidades básicas, hasta las más específicas. Para esta investigación el enfoque es sobre todo en soluciones para:

2.6.1 Computación

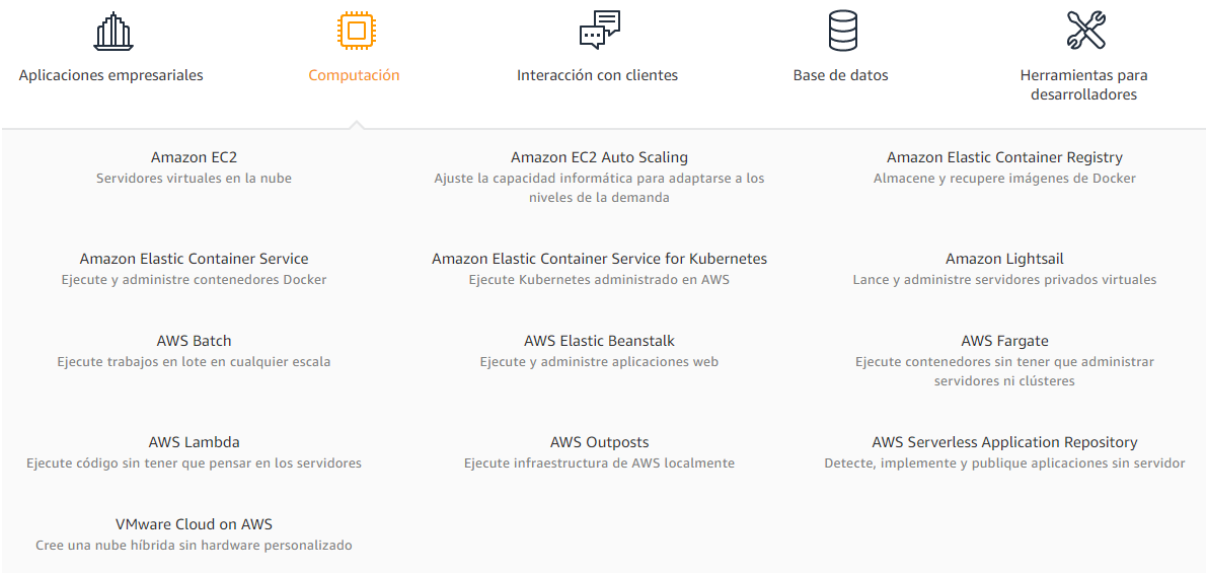


Figura 11. Servicios Computación AWS. (Productos de la nube, s.f.)

2.6.2 Redes

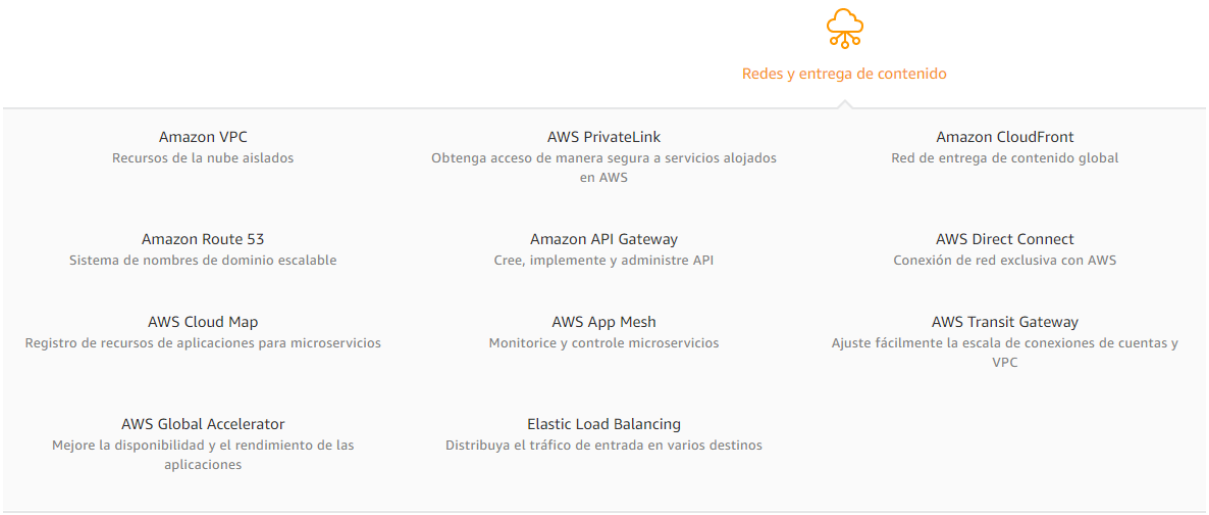


Figura 12. Servicios Redes AWS. (Productos de la nube, s.f.)

2.6.3 Almacenamiento

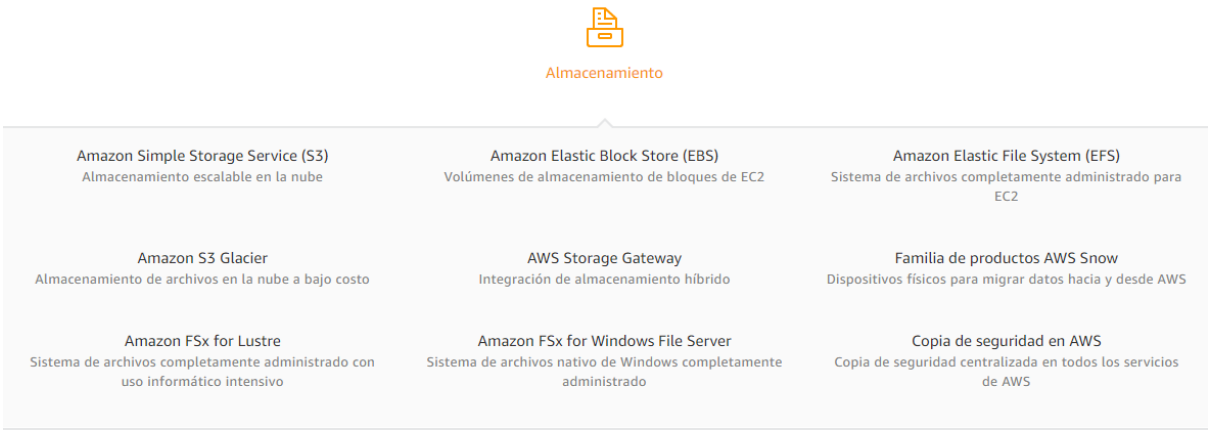


Figura 13. Servicios Almacenamiento AWS. (Productos de la nube, s.f.)

2.6.4 Bases de Datos

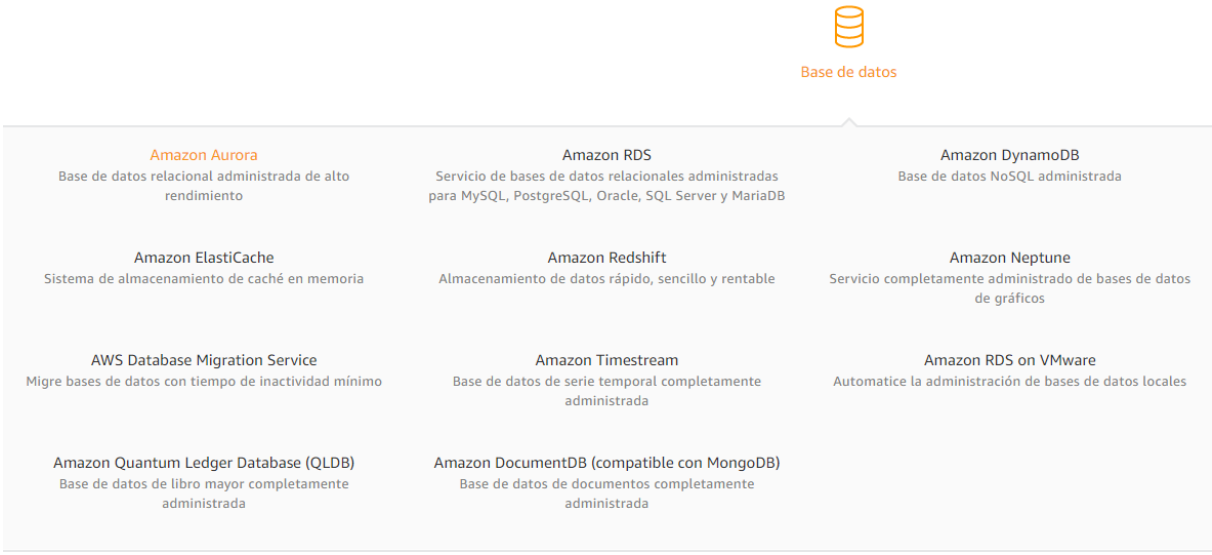


Figura 14. Servicios Bases de Datos AWS. (Productos de la nube, s.f.)

.

2.6.5 Seguridad

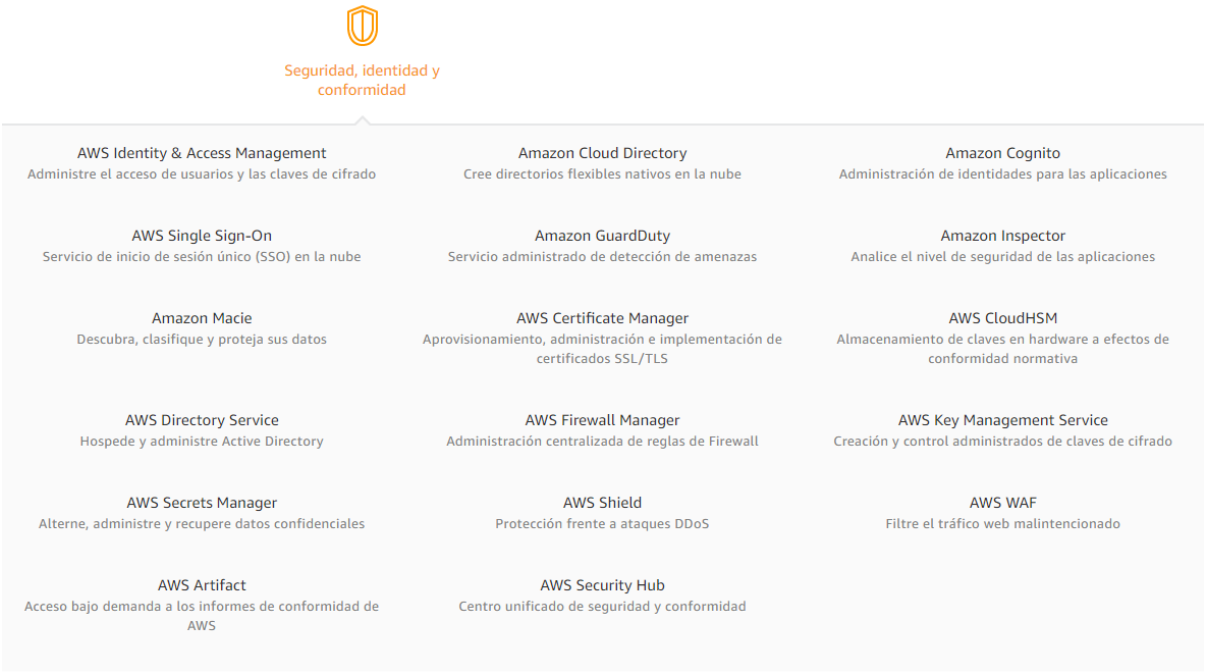


Figura 15. Servicios Seguridad AWS. (Productos de la nube, s.f.)

2.6.6 Herramientas de Administración

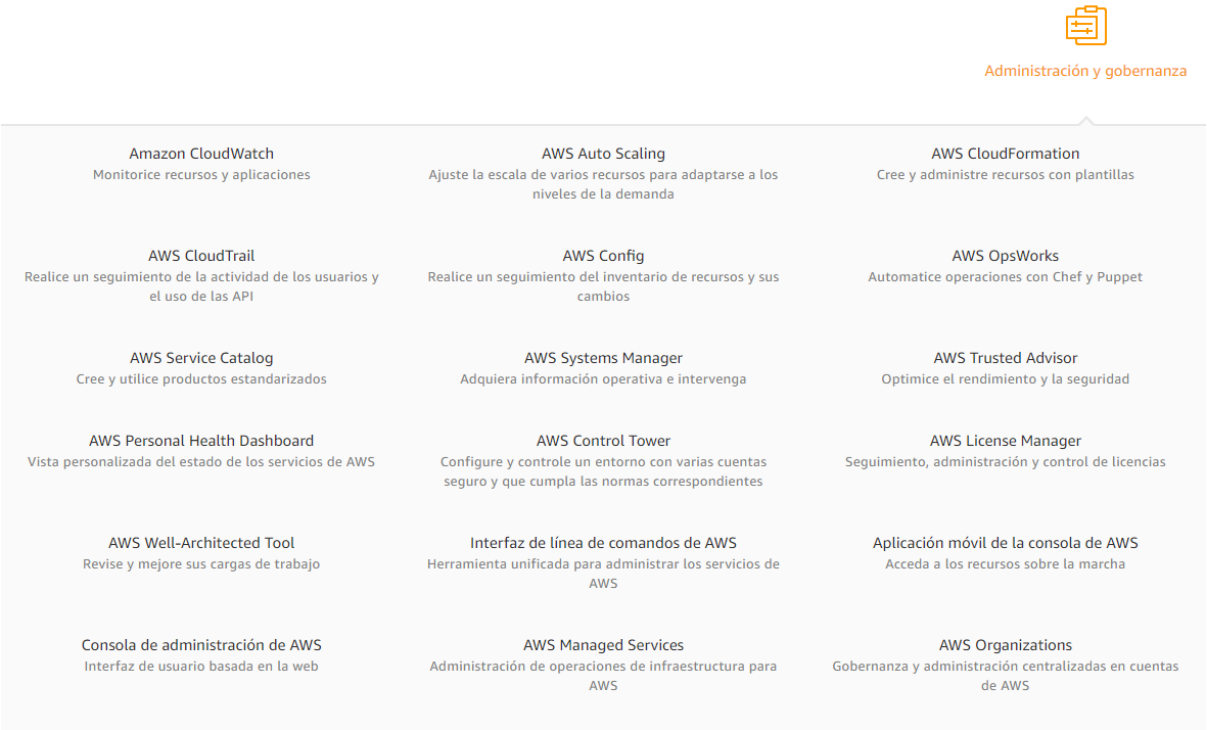


Figura 16. Herramientas de Administración AWS. (Productos de la nube, s.f.)

2.7 Zonas de Disponibilidad y Regiones de AWS

Amazon ofrece lo que se conoce como Regiones y Zonas de Disponibilidad desde las cuales se ofrecen sus servicios. Cada región es una zona geográfica en el mundo diseñada de tal forma que está completamente aislada de las demás, con la finalidad de mejorar la estabilidad y tolerancia a fallas. Dentro de cada región existen 2 o más zonas de disponibilidad, que son básicamente ubicaciones dentro de la misma zona geográfica conectadas entre sí por enlaces de baja latencia.

Al diseñar una instancia de Amazon Elastic Cloud se escoge la región donde se desea ejecutar esa instancia y es posible configurar que los servicios ejecutados se distribuyan entre las diferentes zonas de disponibilidad de forma automática en caso de algún fallo en alguna de las zonas.

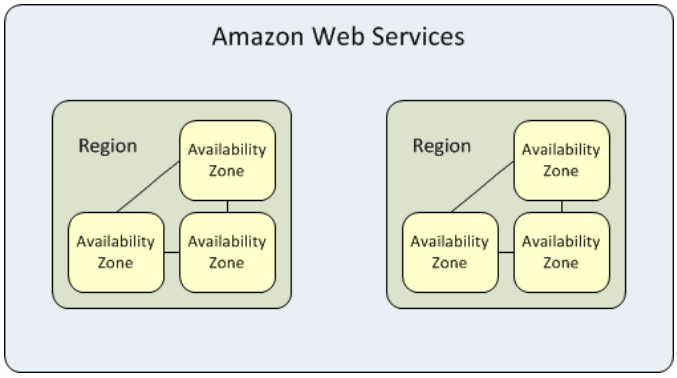


Figura 17. Descripción Regiones y Zonas de Disponibilidad. (Regiones y zonas de disponibilidad, s.f.)



Figura 18. Regiones AWS. (Productos de la nube, s.f.)

Capítulo 3. Requerimientos

3.1 Requerimientos Generales

Se considera en la propuesta que no existe ni infraestructura ni aplicaciones actualmente en la nube de AWS por lo que se desea hacer la propuesta desde el diseño. Se consultó a los diferentes equipos involucrados en el diseño y soporte de la infraestructura actual para que plantearan sus requerimientos para poder dar soporte a la infraestructura en la nube de la misma forma que lo hacen para la infraestructura física.

A pesar de que los Centros de datos están en Estados Unidos, y se cuenta con algunos miembros de forma local, la mayoría de integrantes de los grupos de soporte de infraestructura y aplicaciones se encuentran distribuidos en Costa Rica y Filipinas por lo que el soporte remoto ya es una realidad en la actualidad.

3.2 Requisitos Infraestructura

3.2.1 Network

- Failover automático de túneles
- Incorporar en el modelo de conectividad la SD WAN de Aryaka
- Incorporar modelo DMVPN
- Optimización y/o caching entre la nube y los puntos de entrada a la red local de Teradyne
- Dual homing de servidores
- Estructuras redundantes (múltiples paths para llegar de una parte a otra en caso de que estén en diferentes clouds, zonas o centros)
- Layer 2 Security (Vlans, PVlans, VRFs o métodos para separar de los demás inquilinos)
- Mutiles puntos de acceso a la nube basado en cercanía geográfica, como lo que hablamos de Asia, Europa y América.
- Capacidad de reporteo en tráfico, tipo Netflow
- Dashboard de alarmas y tiquetes relacionados con la infraestructura

- Acceso a administrar subnets, y tablas de enrutamiento.

3.2.2 Windows

- Al menos un Servidor de Active Directory en AWS configurado como Catalogo Global
- Al menos un servidor DNS para resolución interna
- Posibilidad de conectar mediante Remote Desktop integrado con CyberArk
- Posibilidad de crear, iniciar, reiniciar, apagar, terminar instancias
- Poder Monitorear recursos como memoria, disco duro, CPU de los servidores y tener alertas cuando excedan los valores recomendados
- Poder agregar el servidor al dominio
- Poder aplicar Políticas de grupo a esos servidores
- Flexibilidad, que tan rápido se pueden hacer cambios
- Que exista un control, log de cambios hechos y quien los hizo

3.2.3 Unix

- Posibilidad de conectar mediante ssh integrado con CyberArk
- Posibilidad de crear, iniciar, reiniciar, apagar, terminar instancias
- Poder monitorear recursos de los servidores e integrarlos con las herramientas de monitoreo actuales
- Posibilidad de configurar IP primaria y secundaria
- Acceso a repositorios de RedHat para descargas de actualizaciones durante las ventanas de mantenimiento
- Posibilidad de crear snapshots de las instancias

3.2.4 Storage

- Integración con AD de TER para poder realizar administración y acceso con grupos y demás heredados del dominio, así como logs de auditoria donde se puedan identificar los usuarios.
- Proveer acceso a los datos almacenados como NFS, SMB y FTP como mínimo.
- Permite la creación de snapshots para realizar copias de seguridad.

- Replicación interna (provista por la solución) como Disaster recovery.
- La solución debe incluir un servicio de scan de archivos en busca de virus.
- Debe permitir incrementos de espacio disponible en caliente.

3.2.5 Backup

- Posibilidad de habilitar encriptación en el almacenamiento donde se guarden los backups
- Poder escoger el tipo de almacenamiento
- Posibilidad de exportarlos a otra ubicación geográfica
- Poder definir reglas de retención
- Poder integrar el almacenamiento en la nube con las herramientas de Backup actuales
- Posibilidad de realizar Backup de recursos bajo demanda o mediante tareas programadas

3.2.6 Security

- Acceso a la consola de administración de la infraestructura basado en roles.
- Cuentas de administradores globales deben almacenarse en CyberArk
- Poder controlar y aplicar reglas al tráfico que ingresa y egresa a la nube de AWS
- Delimitar una zona de servicios accesibles desde internet la cual tenga acceso limitado a el resto de la infraestructura (simulando lo que sería una DMZ)
- Cifrado de la información en tránsito, así como de los datos almacenados.
- La posibilidad de escanear regularmente los servidores en busca de vulnerabilidades.
- Segregación de servidores de diferentes servicios.
- Herramientas de Monitoreo.
- La posibilidad de realizar pruebas de recuperación ante desastres al menos una vez por año.
- Evaluar la posibilidad de integrar a la infraestructura de Firewalls existente.

3.3 Requerimientos del Negocio

El negocio delega a su división de Tecnologías de Información el análisis de las propuestas de proveedores de tecnología, para la adquisición de bienes o servicios. Sin embargo, como parte del proceso interno es necesaria la discusión y aprobación de miembros de la gerencia cuando la carga al presupuesto sea considerable. Además, como parte del proceso interno para la adquisición de servicios es necesario una revisión de seguridad por parte de un comité, el cual fundamenta la revisión en un checklist que se adjunta en el anexo 1, con una sección adicional por tratarse de un servicio en la nube. Con base en base en las respuestas de ese checklist el comité analiza y determina si se aprueba la adquisición del servicio o si es necesario solventar algún requerimiento adicional.

Después de que se dé el visto bueno en esta revisión es necesario que la parte legal revise el contrato antes de que se firme y como parte de la negociación debe haber un acuerdo de confidencialidad. Este acuerdo es revisado por Teradyne Inc. y de acatamiento obligatorio por parte del proveedor. En el mismo se establecen sanciones legales y monetarias en caso de incumplimiento.

3.4 Requerimientos Generales Aplicaciones

Las aplicaciones y los grupos de soporte de las mismas tienen como requerimiento general para aplicaciones donde se haga algún nivel de desarrollo, tener un ambiente de pruebas, así como uno de producción. Ya que como parte del proceso de control de cambios utilizado por Teradyne es necesario garantizar que antes de ejecutar cambios en el ambiente de producción (el que utiliza el usuario final) haya sido probado antes en un ambiente controlado (ambiente de desarrollo). Parte del proceso incluye un UAT (User Aceptance Testing) que básicamente es cuando uno o más usuarios prueban los cambios realizados en el ambiente de pruebas y dan el visto bueno para que sean movidos a producción.

Las aplicaciones que van a ser migradas a la nube de AWS son en su mayoría aplicaciones de uso general en cualquier empresa, tal es el caso del correo electrónico, pagina web, servidores de archivos entre otros. A pesar de ser de uso común en algunos casos tienen ciertas modificaciones que las hacen muy particulares. Estas modificaciones

pueden ir desde la necesidad de versiones específicas de alguno de sus componentes, de sistema operativo o inclusive de ser ejecutados en hardware especializado. Por lo tanto, en la siguiente sección se listarán los requerimientos específicos de las aplicaciones contempladas en esta propuesta para analizar de qué forma pueden ser solventadas en AWS.

3.5 Requerimientos Específicos aplicaciones Enterprise:

3.5.1 Active Directory

No tiene requerimientos particulares

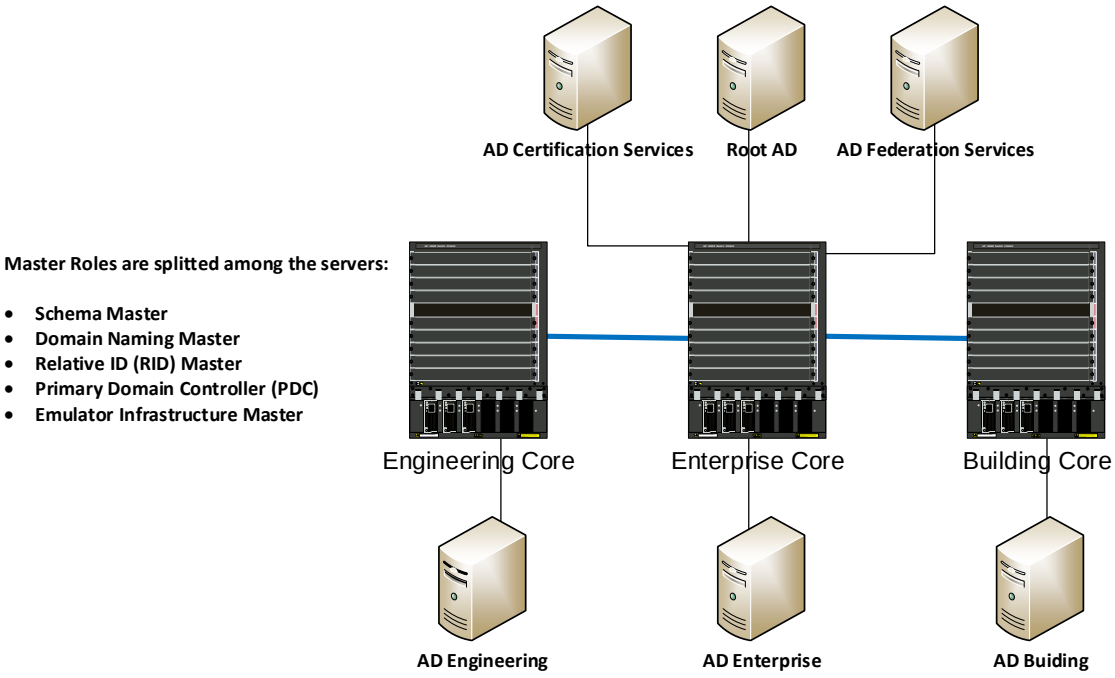


Figura 19. Diagrama Lógico Active Directory. Basado en Documentación Interna

Tabla 1. Inventario de Equipos Active Directory

Nombre	Físico/VM	SO	RAM	Procesador	Almacenamiento	Conexiones de red
gogo	Físico	Windows Server2008 R2 Enterprise	128 GB	2 x Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz (6 cores)	320 GB	2 Activa/Pasiva
goldfish	VM	Windows Server2008 R2 Standard	32 GB	1 x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (2 cores)	120 GB	1 Activa / Redundancia Implícita en ESX

taken	VM	Windows Server2008 R2 Standard	24 GB	4 x Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz (2 cores)	120 GB	1 Activa / Redundancia Implícita en ESX
tricks	Físico	Windows Server2008 R2 Standard	24 GB	2x Intel(R) Xeon(R) CPU E5504 @ 2.00GHz (4 cores)	120 GB	2 Activa/Pasiva
zylo	Físico	Windows Server2008 R2 Standard	24 GB	2x Intel(R) Xeon(R) CPU E5504 @ 2.00GHz (4 cores)	120 GB	2 Activa/Pasiva
armour	Físico	Windows Server2008 R2 Standard	24 GB	2x Intel(R) Xeon(R) CPU E5504 @ 2.00GHz (4 cores)	120 GB	2 Activa/Pasiva

3.5.2 DNS interno

Deben migrarse las diferentes zonas de DNS ya que existen varias. Los valores de DNS son entregados por el DHCP en casa oficina y por lo general son servidores locales por lo que para AWS básicamente se ocupará para resolución interna de los servicios que se implementen ahí. Para el usuario final el DNS seguirá estando local en el sitio donde se encuentre con la excepción de cuando esté trabajando remoto conectado al VPN de AWS

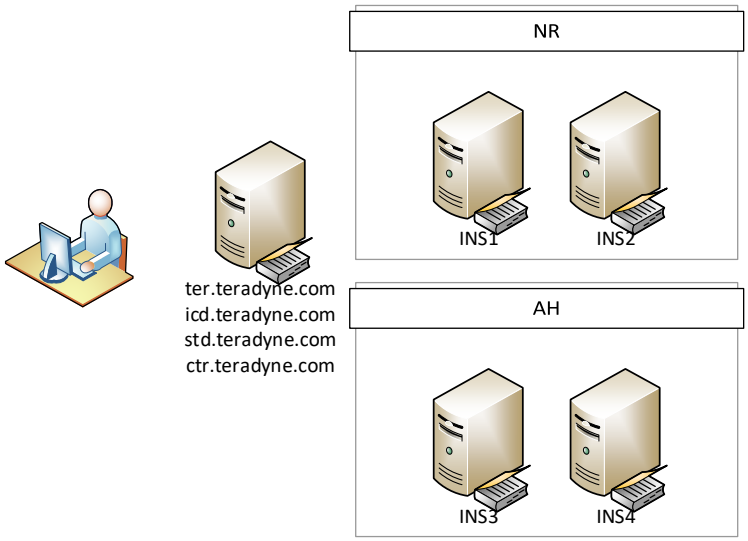


Figura 20. Diagrama Lógico DNS Interno. Basado en Documentación Interna

Tabla 2. Inventario de Equipo DNS Interno

Nombre	Físico/VM	SO	RAM	Procesador	Almacenamiento	Conexiones de red

INS1	Físico	Windows Server2008 R2 Enterprise	64 GB	1 x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (2 cores)	320 GB	2 Activa/Pasiva
INS2	VM	Windows Server2008 R2 Standard	24 GB	2x Intel(R) Xeon(R) CPU E5504 @ 2.00GHz (4 cores)	120 GB	1 Activa / Redundancia Implícita en ESX
INS3	Físico	Windows Server2008 R2 Standard	64 GB	1 x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (2 cores)	320 GB	2 Activa/Pasiva
INS4	VM	Windows Server2008 R2 Standard	24 GB	2x Intel(R) Xeon(R) CPU E5504 @ 2.00GHz (4 cores)	120 GB	1 Activa / Redundancia Implícita en ESX

3.5.3 DNS Externo

Esto implica un cambio en los DNS registrados en el dominio teradyne.com el cual esta hosteado en Network Solutions, LLC. Actualmente en el dominio están registrados 4 servidores de DNS los cuales están físicamente 2 en North Reading y dos en Agoura Hills. Antes de hacer el cambio debe haber una copia de cada registro DNS en AWS Route53

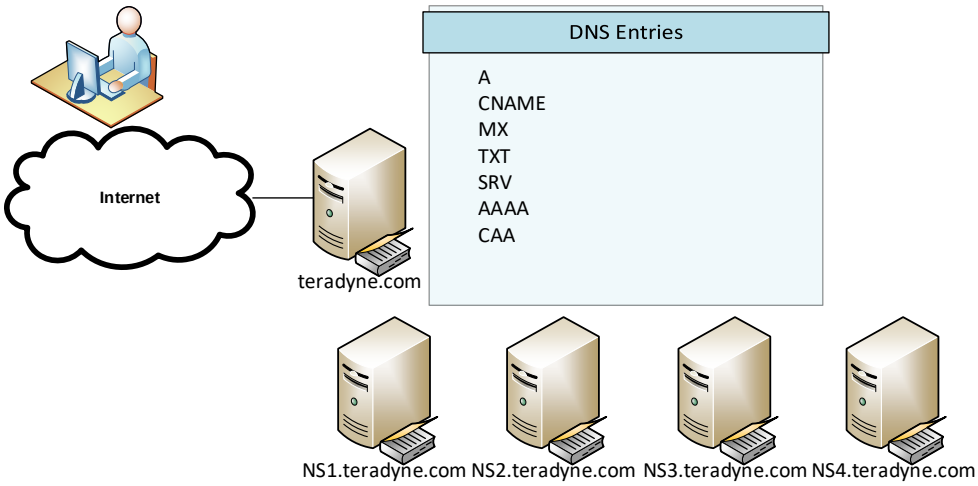


Figura 21. Diagrama Lógico DNS Externo. Basado en Documentación Interna

Tabla 3. Inventario de Equipos DNS Externo

Nombre	Físico/VM	SO	RAM	Procesador	Almacenamiento	Conexiones de red
NS1	Físico	Windows Server2008 R2 Enterprise	24 GB	2x Intel(R) Xeon(R) CPU E5504 @ 2.00GHz (4 cores)	320 GB	2 Activa/Pasiva

NS2	Físico	Windows Server2008 R2 Standard	24 GB	2x Intel(R) Xeon(R) CPU E5504 @ 2.00GHz (4 cores)	320 GB	2 Activa/Pasiva
NS3	Físico	Windows Server2008 R2 Standard	24 GB	2x Intel(R) Xeon(R) CPU E5504 @ 2.00GHz (4 cores)	320 GB	2 Activa/Pasiva
NS4	Físico	Windows Server2008 R2 Standard	24 GB	2x Intel(R) Xeon(R) CPU E5504 @ 2.00GHz (4 cores)	320 GB	2 Activa/Pasiva

3.5.4 SharePoint

Requiere ambiente de desarrollo, como se está en el proceso de actualización a 2019 en AWS se deberá implementar la versión actualizada

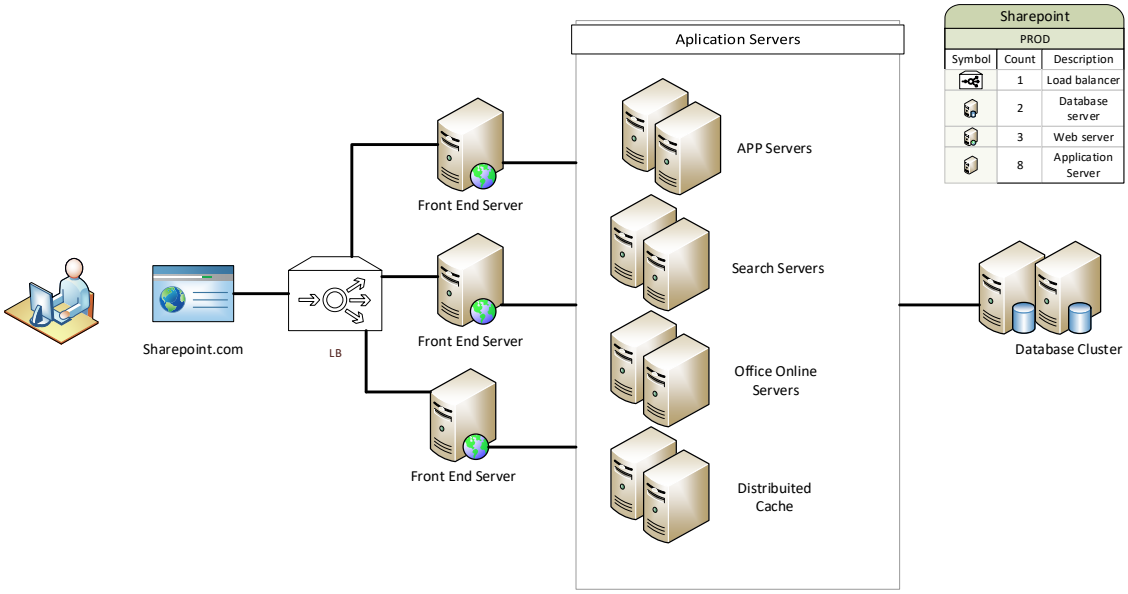


Figura 22. Diagrama Lógico SharePoint. Basado en Documentación Interna

Tabla 4. Inventario Equipos SharePoint

Nombre	Físico/VM	SO	RAM	Procesador	Almacenamiento	Conexiones de red
KIRKWOOD	Físico	Microsoft Windows Server 2016 Standard	32 GB	2x Intel(R) Xeon(R) CPU E5-2665 0 @ 2.40GHz (8 cores)	2 TB	2 Activa/Pasiva
DEERVALLEY	Físico	Microsoft Windows Server 2016 Standard	32 GB	2x Intel(R) Xeon(R) CPU E5-2665 0 @	2 TB	2 Activa/Pasiva

				2.40GHz (8 cores)		
SQUAW	Físico	Microsoft Windows Server 2016 Standard	32 GB	2x Intel(R) Xeon(R) CPU E5-2665 0 @ 2.40GHz (8 cores)	2 TB	2 Activa/Pasiva
HOOD	VM	Microsoft Windows Server 2016 Standard	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	550 GB	1 Activa / Redundancia Implícita en ESX
MANSELL	VM	Microsoft Windows Server 2016 Standard	32 GB	2 x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	550 GB	1 Activa / Redundancia Implícita en ESX
VAIL	Físico	Microsoft Windows Server 2016 Standard	128 GB	2x Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz (6 cores)	2.5 TB	2 Activa/Pasiva
PARKMAN	Físico	Microsoft Windows Server 2016 Standard	128 GB	2x Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz (6 cores)	2.5 TB	2 Activa/Pasiva
TARGHEE	Físico	Microsoft Windows Server 2016 Standard	32 GB	2x Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz (6 cores)	2.5 TB	2 Activa/Pasiva
JACKSON	Físico	Microsoft Windows Server 2016 Standard	32 GB	2x Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz (6 cores)	2.5 TB	2 Activa/Pasiva
PARKCITY	Físico	Microsoft Windows Server 2016 Standard	24 GB	2x Intel(R) Xeon(R) CPU E5620 @ 2.40GHz (4 cores)	1.8 TB	2 Activa/Pasiva
ALTA	Físico	Microsoft Windows Server 2016 Standard	24 GB	2x Intel(R) Xeon(R) CPU E5620 @ 2.40GHz (4 cores)	1.8 TB	2 Activa/Pasiva
WILDCAT	Físico	Microsoft Windows Server 2016 Standard	128 GB	2x Intel(R) Xeon(R) CPU E5-2623 v4 @ 2.60GHz (4 cores)	4 TB	2 Activa/Pasiva
HEAVENLY	Físico	Microsoft Windows	128 GB	2x Intel(R) Xeon(R) CPU	4 TB	2 Activa/Pasiva

		Server 2016 Standard		E5-2623 v4 @ 2.60GHz (4 cores)		

3.5.5 Portal de Clientes internos y externos (Eknowledge)

Requiere ambiente de desarrollo, QAT y la capacidad implementar en el IBM Aspera Download server para descargas a alta velocidad y bases de Datos DB2. También el acceso externo debe permitir tanto clientes internos del Active Directory, como clientes registrados con un correo electrónico

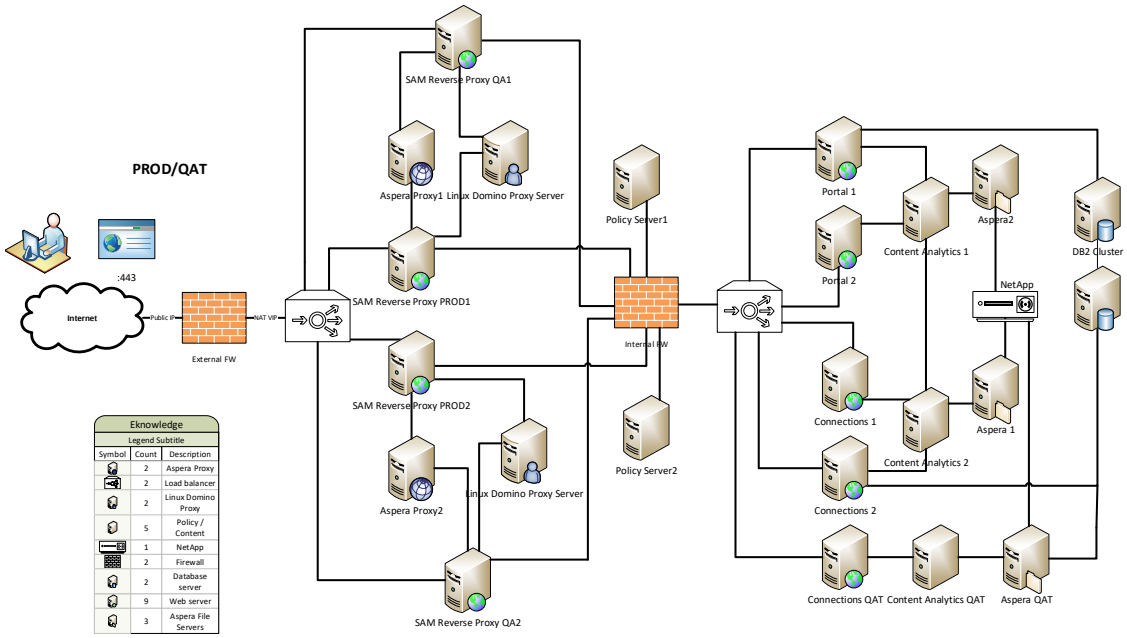


Figura 23. Diagrama Lógico Eknowledge PROD / QAT. Basado en Documentación Interna

Tabla 5. Inventario Equipos Eknowledge PROD/ QAT

Nombre	Físico/VM	SO	RAM	Procesador	Almacenamiento	Conexiones de red
goldeagle	VM	IBM Custom Unix based	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	100 GB	1 Activa / Redundancia Implícita en ESX
sanmiguel	VM	IBM Custom Unix based	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	100 GB	1 Activa / Redundancia Implícita en ESX

libertas	VM	Redhat RHEL 6.6	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	50 GB	1 Activa / Redundancia Implícita en ESX
redhose	VM	Redhat RHEL 6.6	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	50 GB	1 Activa / Redundancia Implícita en ESX
redhorse	VM	IBM Custom Unix based	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	80 GB	1 Activa / Redundancia Implícita en ESX
superdry	VM	IBM Custom Unix based	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	80 GB	1 Activa / Redundancia Implícita en ESX
strongice	VM	IBM Custom Unix based	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	100 GB	1 Activa / Redundancia Implícita en ESX
escalante	VM	IBM Custom Unix based	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	100 GB	1 Activa / Redundancia Implícita en ESX
habs	VM	Redhat RHEL 6.6	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	100 GB	1 Activa / Redundancia Implícita en ESX
hurricane	VM	Redhat RHEL 6.6	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	100 GB	1 Activa / Redundancia Implícita en ESX
senator	VM	IBM Custom Unix based	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	100 GB	1 Activa / Redundancia Implícita en ESX
expos	VM	IBM Custom Unix based	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	100 GB	1 Activa / Redundancia Implícita en ESX
expos2	VM	IBM Custom Unix based	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	100 GB	1 Activa / Redundancia Implícita en ESX
everton	VM	Redhat RHEL 6.6	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	80 GB	1 Activa / Redundancia Implícita en ESX
everton2	VM	Redhat RHEL 6.6	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	80 GB	1 Activa / Redundancia Implícita en ESX

avalanche	VM	Redhat RHEL 6.6	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	80 GB	1 Activa / Redundancia Implícita en ESX
lakings	VM	Redhat RHEL 6.6	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	80 GB	1 Activa / Redundancia Implícita en ESX
detroitredwings	VM	Redhat RHEL 6.6	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	80 GB	1 Activa / Redundancia Implícita en ESX
chicagoblackhawks	VM	Redhat RHEL 6.6	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	4 TB	1 Activa / Redundancia Implícita en ESX
bostonbruins	VM	Redhat RHEL 6.6	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	4 TB	1 Activa / Redundancia Implícita en ESX
buffalosabores	VM	Redhat RHEL 6.6	32 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	4 TB	1 Activa / Redundancia Implícita en ESX
nyrangers	VM	Redhat RHEL 6.6	64 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	2 TB	1 Activa / Redundancia Implícita en ESX
flyer	VM	Redhat RHEL 6.6	64 GB	2x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (4 cores)	2 TB	1 Activa / Redundancia Implícita en ESX
tima	Físico	NetApp Custom	16 GB	No especificado	20 TB	4 Activas

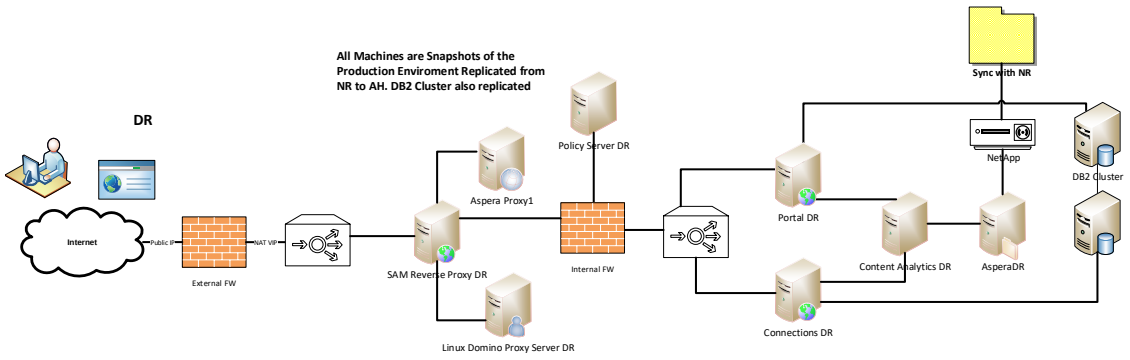


Figura 24. Diagrama Lógico Eknowledge DR. Basado en Documentación Interna

3.5.6 Página Web (www.teradyne.com)

Requiere ambiente de desarrollo el cual es accesible solo internamente.

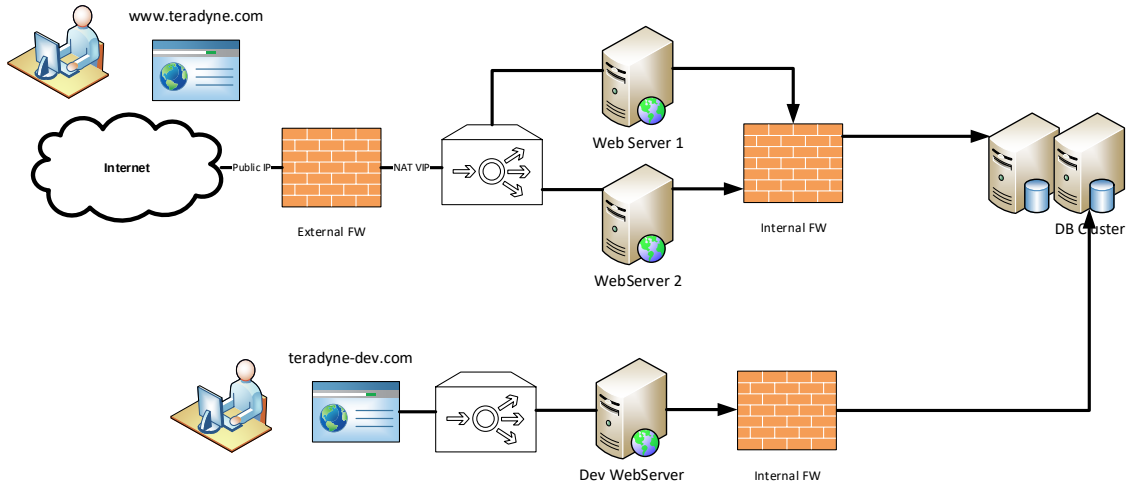


Figura 25. Diagrama Lógico Pagina Web PROD/ DEV. Basado en Documentación Interna

Tabla 6. Inventario Equipos Pagina Web PROD / DEV

Nombre	Físico/VM	SO	RAM	Procesador	Almacenamiento	Conexiones de red
wise	Físico	Windows Server2008 R2 Standard	32 GB	1 x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (2 cores)	320 GB	2 Activa/Pasiva
wise2	VM	Windows Server2008 R2 Standard	32 GB	2x Intel(R) Xeon(R) CPU E5504 @ 2.00GHz (4 cores)	320 GB	1 Activa / Redundancia Implícita en ESX
wise-dev	VM	Windows Server2008 R2 Standard	32 GB	2 x Intel(R) Xeon(R) Gold 6146 CPU @ 3.20GHz (2 cores)	320 GB	1 Activa / Redundancia Implícita en ESX
pilsen	Físico	Windows Server2008 R2 Standard	64 GB	2x Intel(R) Xeon(R) CPU E5504 @ 2.00GHz (4 cores)	2 TB	2 Activa/Pasiva
imperial	Físico	Windows Server2008 R2 Standard	64 GB	2x Intel(R) Xeon(R) CPU E5504 @ 2.00GHz (4 cores)	2 TB	2 Activa/Pasiva

3.5.7 Carpetas Compartidas dentro del esquema DFS-R

Requerimientos de almacenamiento sobre todo y la adición de al menos un servidor de DFS dentro del esquema existente

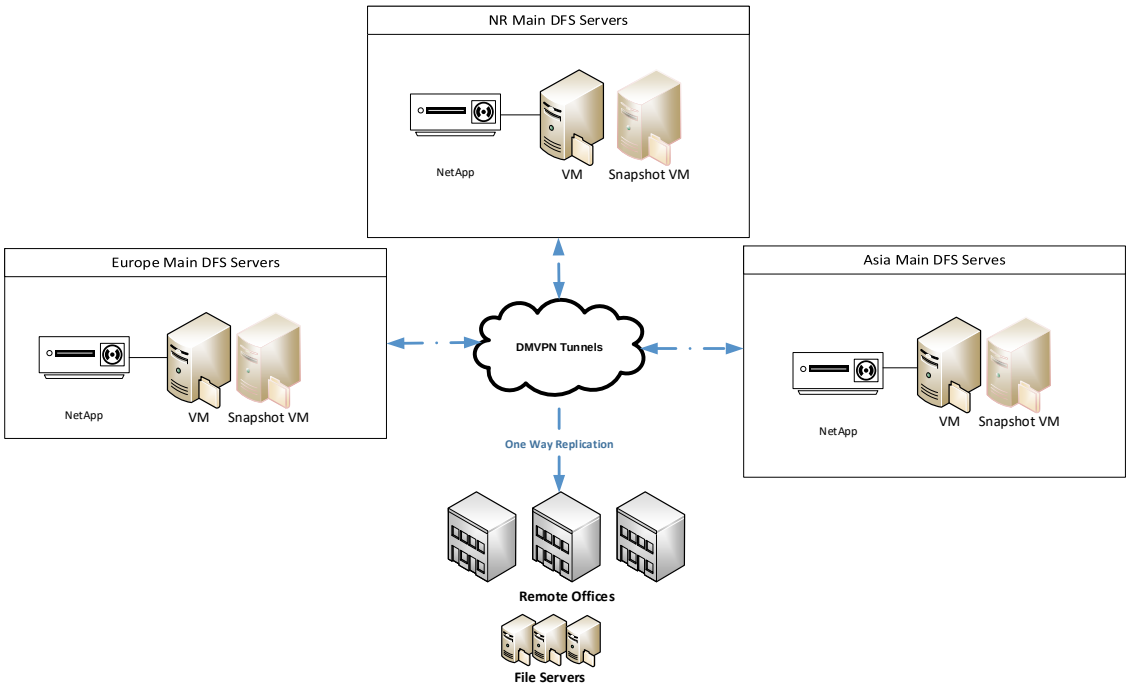


Figura 26. Diagrama Lógico Esquema DFS. Basado en Documentación Interna

Tabla 7. Inventario Equipos Principales Esquema de DFS

Nombre	Físico/VM	SO	RAM	Procesador	Almacenamiento	Conexiones de red
nradmin	Físico	Windows Server2008 R2 Standard	32 GB	2x Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz (6 cores)	2 TB	2 Activa/Pasiva
munich01	Físico	Windows Server2008 R2 Standard	32 GB	2x Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz (6 cores)	2 TB	2 Activa/Pasiva
monkey2	Físico	Windows Server2008 R2 Standard	32 GB	2x Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz (6 cores)	2 TB	2 Activa/Pasiva
tima	Físico	NetApp Custom	16 GB	No especificado	20 TB	4 Activas
etima	Físico	NetApp Custom	16 GB	No especificado	20 TB	4 Activas
atima	Físico	NetApp Custom	16 GB	No especificado	20 TB	4 Activas

3.5.8 LSF

De todas las aplicaciones a migrar LSF, es la que representa el mayor reto por sus características y requerimientos. Actualmente existen 2 grandes granjas, una ubicada en North Reading, conformada por 50 Servidores y una secundaria en Agoura Hills

conformada por 30 Servidores. Se tomó la decisión de mantener las granjas actuales y adicionalmente empezar por construir una granja adicional conformado por 10 equipos en AWS con el fin de poder hacer una comparación de rendimiento. Esto porque para poder ejecutar LSF se requiere hardware especializado, procesadores con características particulares y una versión certificada de Ret Hat para este fin, por lo que actualmente todos estos equipos son servidores físicos con características exactamente iguales y con una imagen de sistema operativo probada y certificada por nuestros ingenieros. Además, porque esto garantiza hasta cierto punto que la misma tarea ejecutada en cualquier equipo debería durar lo mismo y esto permite medir rendimientos.

LSF Load Sharing Farm es una tecnología que utiliza High Performance Computing (HPC) y computación distribuida para realizar tareas que requieren muchos recursos distribuyéndolas en tareas más pequeñas ejecutadas en múltiples servidores al mismo tiempo. Todo esto depende que el ambiente este sincronizado y el aprovechamiento al máximo del paralelismo y el uso de múltiples hilos (threads) de ejecución.

En Teradyne se utiliza IBM Spectrum LSF como resultado de un benchmark entre varias soluciones. Una de las razones es porque al ser una infraestructura crítica se ocupa tener respaldo en caso de que surja algún problema.

En conjunto con esta plataforma se utiliza otro componente también de IBM llamado Clearcase que es un administrador de ambientes y versiones de software que es la que genera las tareas a ser ejecutadas.

Cuando un grupo de desarrollo de software genera una versión nueva de código Clearcase genera un ambiente nuevo sobre el cual se va a compilar y ejecutar ese código, y lanza la tarea a un servidor master de LSF. Este calcula los recursos que le necesita para ejecutar esa tarea y la distribuye entre un grupo de servidores. El Servidor Master se encarga de asignar y coordinar el estatus de las tareas, control de recursos, sincronización de todos los elementos y al final de la recopilación de resultados de todas las tareas.

A pesar de que AWS ofrece dentro de sus servicios una sección denominada AWS HPC. (Informática de alto rendimiento, s.f.) existe cierto recelo por parte de Ingeniería sobre el posible rendimiento y aunque resultara ser más barato, la decisión está basada prácticamente en rendimiento.

Como referencia Herbert Hoeger del Centro Nacional de Cálculo Científico de La Universidad de Los Andes en Venezuela describe "*La eficiencia de un computador depende directamente del tiempo requerido para ejecutar una instrucción básica y del número de instrucciones básicas que pueden ser ejecutadas concurrentemente… estos tiempos están decreciendo lentamente y parece que están alcanzando límites físicos como la velocidad de la luz. Por lo tanto, no podemos depender de procesadores más rápidos para obtener más eficiencia"* de ahí la importancia de la computación distribuida, sin embargo, esta también tiene limitaciones. La ley de Amdahl explica de existe un punto en el que la implementación de más recursos como lo serían más procesadores, hilos no representa una mejor eficiencia. Interpretado para nuestro caso particular la adición de esos recursos alcanza un límite en donde el código a ejecutar ya no se puede subdividir en tareas más pequeñas paralelizables. (Ley de Amdahl, s.f.)

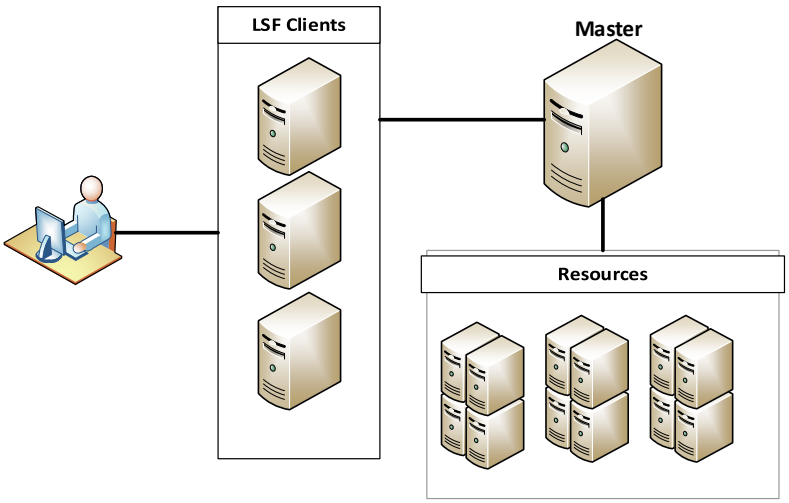


Figura 27. Diagrama lógico IBM LSF. Basado en Documentación Interna

3.5.9 Enterprise Backup

Requerimiento de espacio y un ancho de banda considerable para subir los datos. Las oficinas remotas exportan sus backup al Enterprise Server según su región y este a su vez exporta hacia NR donde se recolectan todos.

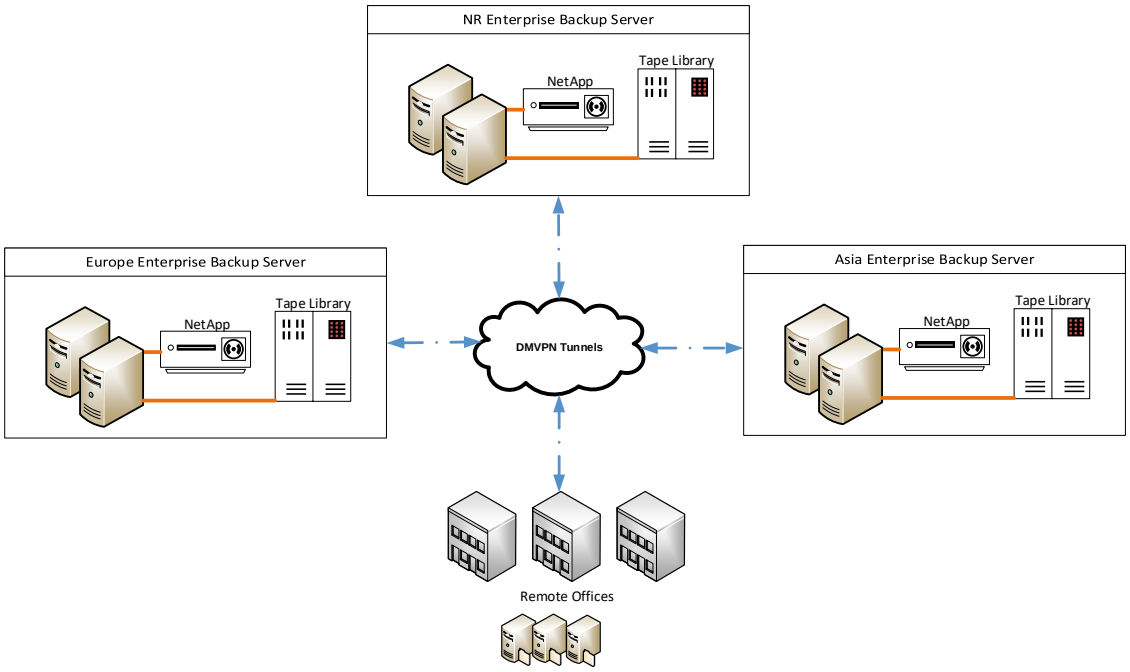


Figura 28. Diagrama Lógico de Enterprise Backup. Basado en Documentación Interna

Tabla 8. Inventario equipos principales Enterprise Backup.

Nombre	Físico/VM	SO	RAM	Procesador	Almacenamiento	Conexiones de red
onset	Físico	Redhat 6.9	32 GB	2x Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz (6 cores)	2 TB	2 Activa/Pasiva
onset2	Físico	Redhat 6.9	32 GB	2x Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz (6 cores)	2 TB	2 Activa/Pasiva
onset-tl	Físico	Other	na	Other	na	na
bravo	Físico	NetApp Custom	16 GB	No especificado	20 TB	4 Activas
samurai	Físico	Redhat 6.9	32 GB	2x Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz (6 cores)	2 TB	2 Activa/Pasiva
samurai2	Físico	Redhat 6.9	32 GB	2x Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz (6 cores)	2 TB	2 Activa/Pasiva
samurai-tl	Físico	Other	na	Other	na	na
tropus	Físico	NetApp Custom	16 GB	No especificado	20 TB	4 Activas
Jodiak	Físico	Redhat 6.9	32 GB	2x Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz (6 cores)	2 TB	2 Activa/Pasiva

jodiak2	Físico	Redhat 6.9	32 GB	2x Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz (6 cores)	2 TB	2 Activa/Pasiva
jodiak-tl	Físico	Other	na	Other	na	na
sunset	Físico	NetApp Custom	16 GB	No especificado	20 TB	4 Activas

3.5.10 Team Center PLM

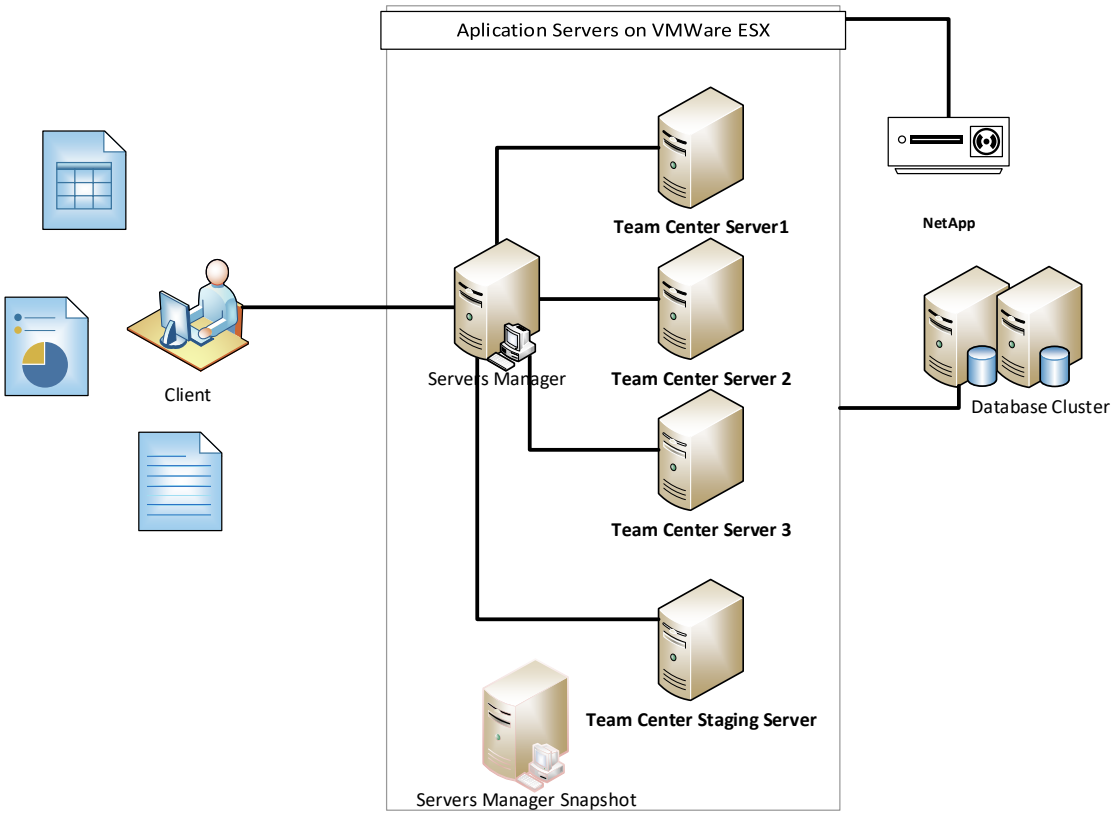


Figura 29. Diagrama Lógico Team Center PLM. Basado en Documentación Interna

Tabla 9. Inventario Equipos Team Center PLM.

Nombre	Físico/VM	SO	RAM	Procesador	Almacenamiento	Conexiones de red
PDM-MS	Físico	Windows Server2008 R2 Standard	32 GB	2x Intel(R) Xeon(R) CPU E5620 @ 2.40GHz (4 cores)	1 TB	2 Activa/Pasiva
TC1	Físico	Windows Server2008 R2 Standard	32 GB	2x Intel(R) Xeon(R) CPU E5620 @ 2.40GHz (4 cores)	3 TB	2 Activa/Pasiva
TC2	Físico	Windows Server2008 R2 Standard	32 GB	2x Intel(R) Xeon(R) CPU E5620 @ 2.40GHz (4 cores)	3 TB	2 Activa/Pasiva

TC3	Físico	Windows Server2008 R2 Standard	32 GB	2x Intel(R) Xeon(R) CPU E5620 @ 2.40GHz (4 cores)	3 TB	2 Activa/Pasiva
TC-ST	Físico	Windows Server2008 R2 Standard	32 GB	2x Intel(R) Xeon(R) CPU E5620 @ 2.40GHz (4 cores)	3 TB	2 Activa/Pasiva
ghost	Físico	Windows Server2008 R2 Standard	64 GB	2x Intel(R) Xeon(R) CPU E5620 @ 2.40GHz (4 cores)	4 TB	2 Activa/Pasiva
vault	Físico	Windows Server2008 R2 Standard	64 GB	2x Intel(R) Xeon(R) CPU E5620 @ 2.40GHz (4 cores)	4 TB	2 Activa/Pasiva
tima	Físico	NetApp Custom	16 GB	No especificado	20 TB	4 Activas

3.5.11 Servidor de administración de Antivirus

No tiene ningún requerimiento particular pero que las maquinas descarguen actualizaciones de servidor de administración desde NR o AWS representa para el Site una descarga a través de los túneles IPsec por lo que de igual forma el ancho de banda se consume. Por esta razón solo se requiere mover la consola de administración y las descargas seguirán haciéndose desde los servidores de actualización de Symantec.

Las maquinas se comunican con el Management server usando el puerto TCP/8014 por lo que el puerto debe estar permitido.

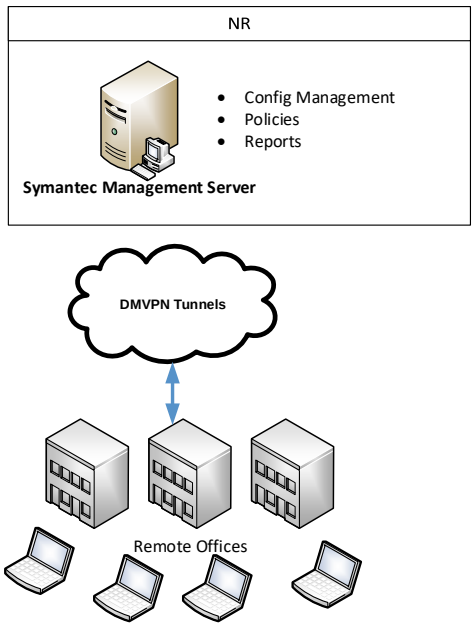


Figura 30. Diagrama Lógico Servidor de administración Antivirus. Basado en Documentación Interna

Tabla 10. Inventario Equipos Administración Antivirus

Nombre	Físico/VM	SO	RAM	Procesador	Almacenamiento	Conexiones de red
nations	Físico	Microsoft Windows Server 2016 Standard	32 GB	2x Intel(R) Xeon(R) CPU E5-2665 0 @ 2.40GHz (8 cores)	1 TB	2 Activa/Pasiva

1.7 3.6 Modelo de Conectividad Actual

Teradyne cuenta en la actualidad en sus centros de datos Principal y secundario un modelo de red divido en 4 grandes segmentos compuestos cada uno por múltiples subnets y Vlans. Un segmento Enterprise donde se hospedan los servicios dentro de esa categoría, algunos de ellos contemplados en esta propuesta para ser migrados. Un segmento de Ingeniería que su propósito es que pueda funcionar independientemente ya que cuenta con todos los recursos para que los trabajos relacionados al área de ingeniería puedan darse sin tener que usar recursos de los otros segmentos. Un segmento de DMZ donde se encuentra todo lo relacionado a conectividad externa y uno adicional que sirve para la interconexión de edificios y conectividad de usuarios en áreas de trabajo como cubículos, salas de reuniones etc. Se utiliza la figura de Core switches y switches de acceso. Los Core Switches son modulares, con redundancia tanto de alimentación como de conectividad. Se utiliza una configuración de stack (conocida como IRF en la marca HP) formado por 2 switches iguales para que cada elemento conectado a él tenga un puerto activo en uno de los Core y uno pasivo en el segundo, o activo-activo si así se requiere. Tienen capacidades de manejo de tráfico mucho más amplia, así como conectividad a 10Gbps para dispositivos finales, o la posibilidad de unir varios puertos para lograr anchos de banda superiores en casos particulares.

Los switches de acceso están ubicados en gabinetes distribuidos en los 3 edificios, se configuran en stack y cada stack está conectado al Building Core Switch como punto central.

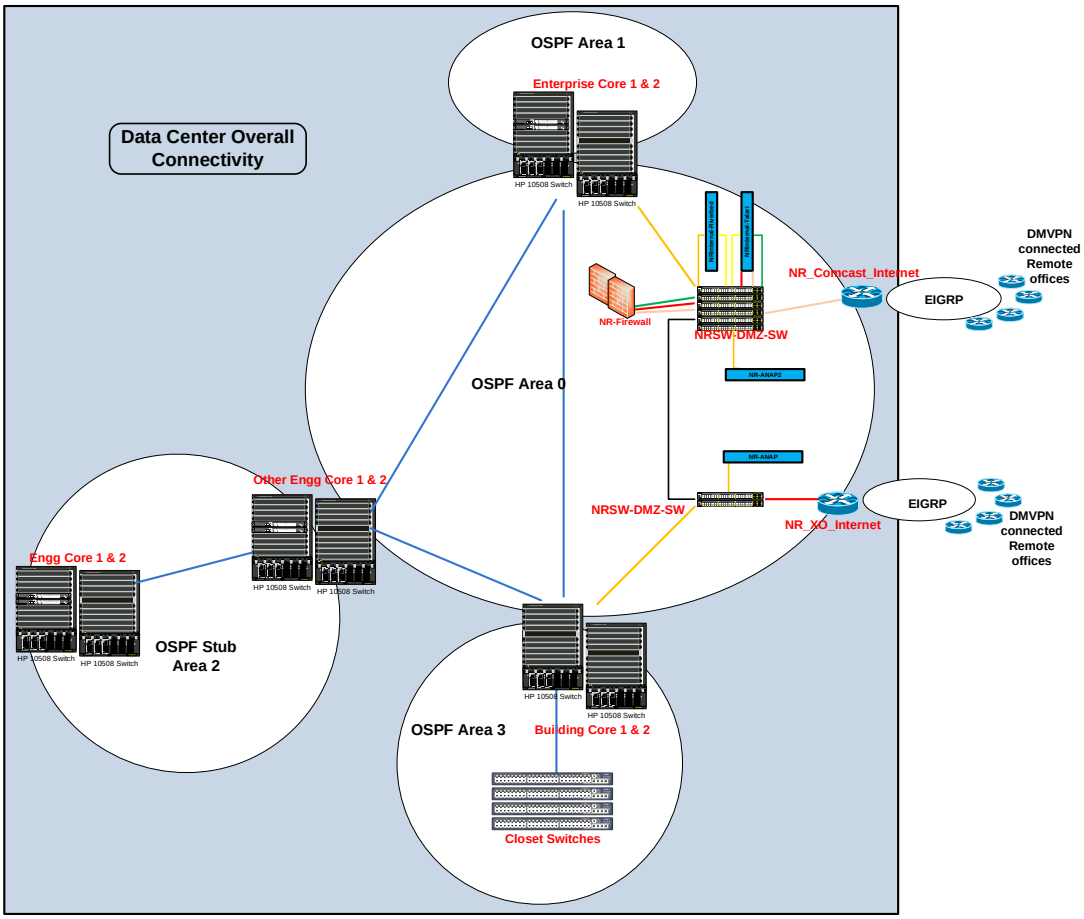


Figura 31. Diagrama Lógico de conectividad en Data Center. Basado en Documentación Interna

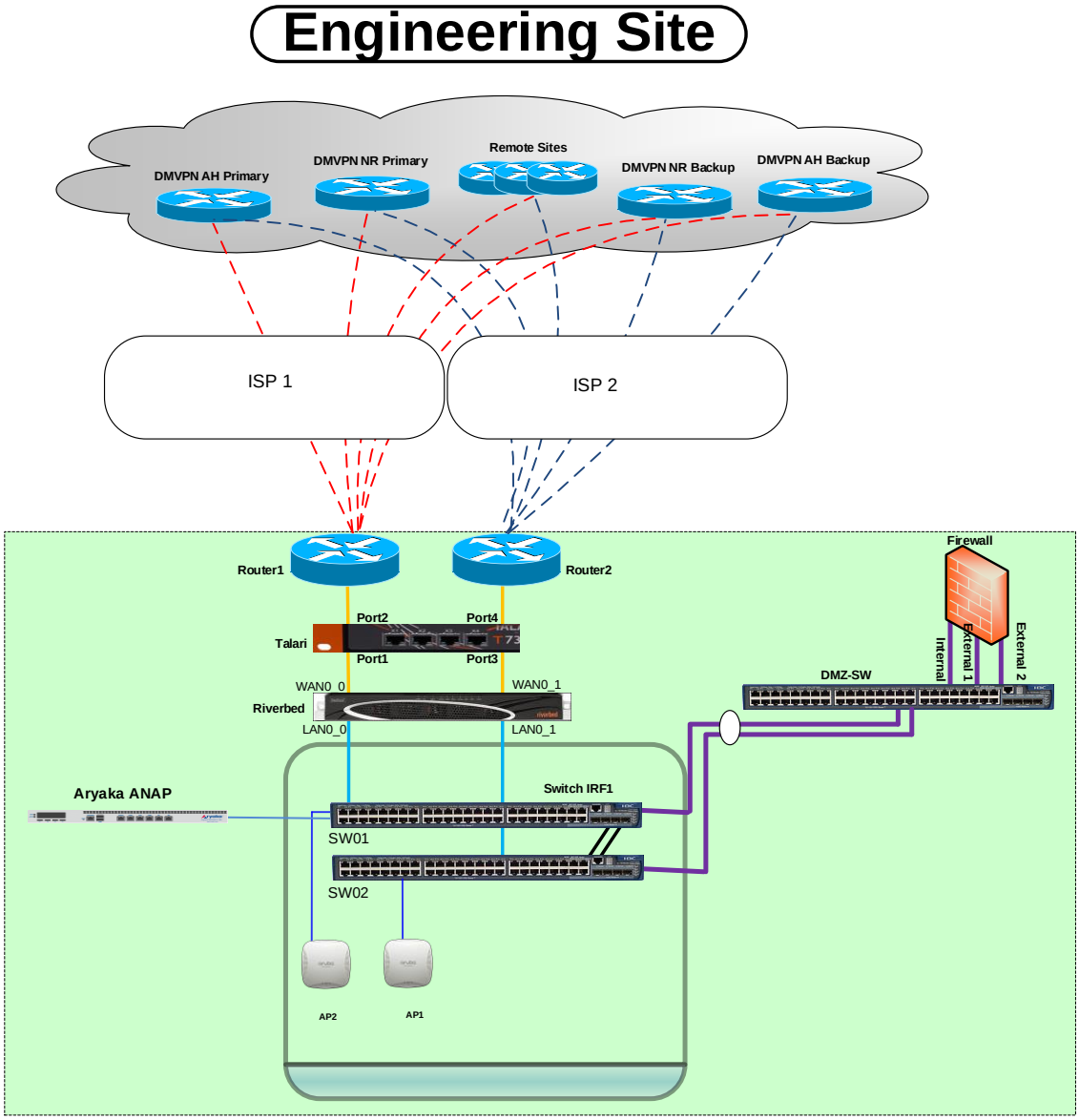


Figura 32. Diagrama Lógico de Conectividad Sitio Ingeniería. Basado en Documentación Interna

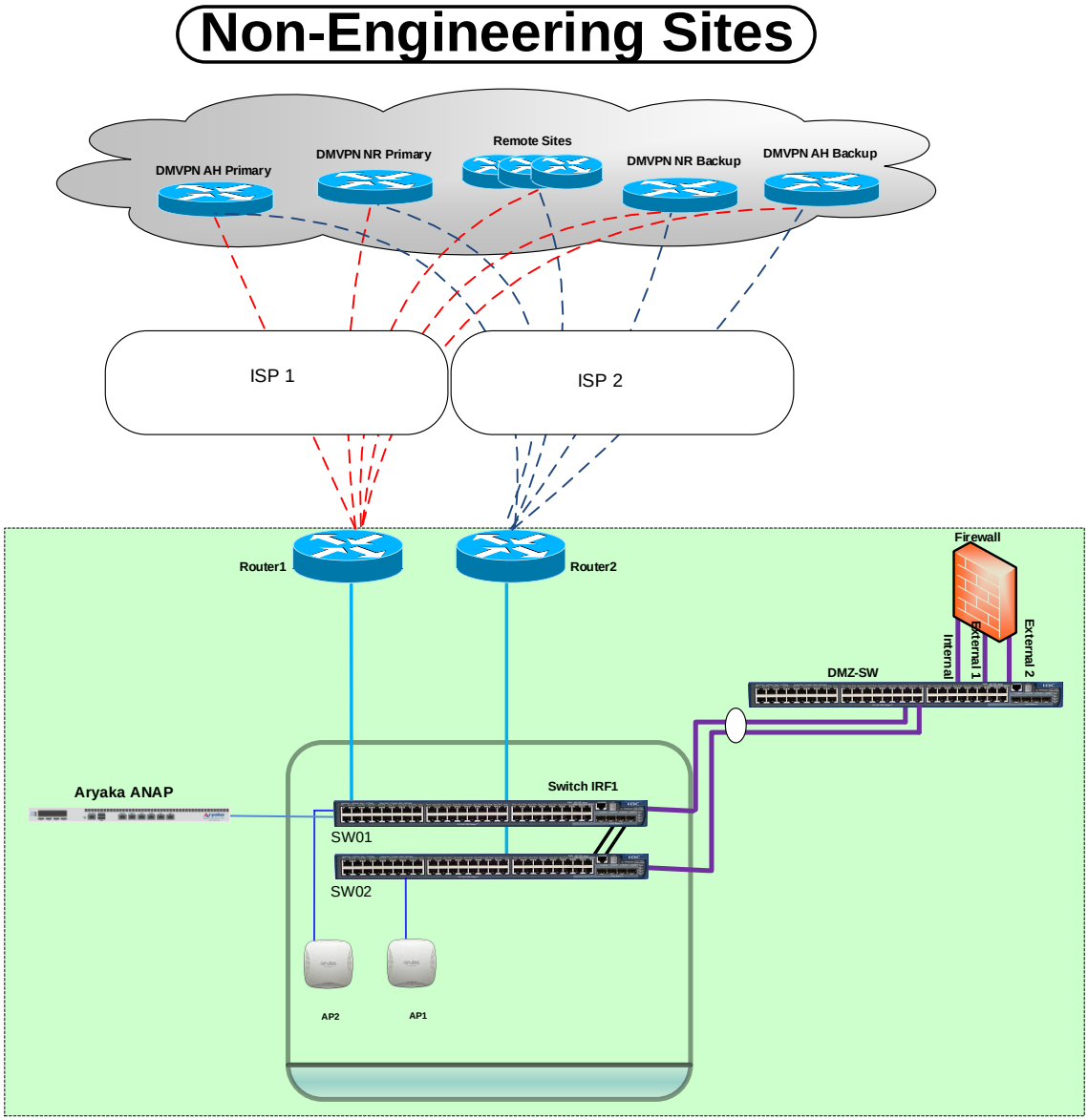


Figura 33. Diagrama Lógico de conectividad sitios estándar. Basado en Documentación Interna

A nivel general todos los sitios de Teradyne alrededor del mundo tienen varias tecnologías de conectividad implementadas. Como método principal, siempre y cuando ambos sitios que traten de comunicarse entre sí cuenten con un dispositivo de Aryaka conocido como ANAP utilizaran la red SD-WAN de Aryaka para esta comunicación. De lo contrario utilizaran los túneles IPSec dinámicos construidos entre los router de ambos sitios mediante el uso de DMVPN. Entre sitios de Ingeniería como opción secundaria por encima del uso de DMVPN, se utilizan túneles construidos entre los dispositivos Talari los cuales utilizan una tecnología conocida como WAN Aggregation para crear un túnel con el ancho de banda de la sumatoria de los enlaces, además de poder hacer duplicación de paquetes para trafico UDP prioritario como de telefonía, QoS entre otras cosas.

Capítulo 4. Propuesta

4.1 Modelo de Infraestructura propuesto

4.1.1 Regiones

Tabla 11. Regiones AWS.

Code	Nombre
us-east-1	US East (N. Virginia)
us-east-2	EE.UU. Este (Ohio)
us-west-1	EE.UU. Oeste (Norte de California)
us-west-2	EE.UU. Oeste (Oregón)
ca-central-1	Canadá (Central)
eu-central-1	UE (Fráncfort)
eu-west-1	UE (Irlanda)
eu-west-2	UE (Londres)
eu-west-3	UE (París)
eu-north-1	UE Estocolmo
ap-east-1	Asia Pacífico (Hong Kong)
ap-northeast-1	Asia Pacífico (Tokio)
ap-northeast-2	Asia Pacífico (Seúl)
ap-northeast-3	Asia Pacífico (Osaka-local)
ap-southeast-1	Asia Pacífico (Singapur)
ap-southeast-2	Asia Pacífico (Sídney)
ap-south-1	Asia Pacífico (Mumbai)
sa-east-1	América del Sur (São Paulo)

(Regiones y zonas de disponibilidad, s.f.)

Se toman en cuenta para la propuesta 3 Regiones, marcadas en verde en la tabla anterior donde us-east-1 se considera como sitio principal ya que geográficamente es la región más cercana al Data Center actual en las oficinas centrales de Teradyne Inc. De igual forma manteniendo la zona geográfica del sitio alterno para recuperación ante desastres actual en Agoura Hills California, se utilizará us-west-1 y se escoge una región adicional en Asia Pacífico ap-southeast-1 para colocar algunos de los servicios y que puedan ser accedidos por los sites de Europa y Asia con un mejor tiempo de respuesta y rendimiento. No se escoge una región dentro de China ya que a pesar de que AWS en un servicio privado, el gobierno chino mantiene un fuerte control sobre las comunicaciones que entran y salen del país y la experiencia de los años nos ha demostrado que existen muchos problemas de congestionamiento con las salidas internacionales sobre todo hacia Europa

y Estados Unidos, ya que todo tiene que pasar por lo que se conoce como “El gran Firewall de China” que no es más que una alusión a La gran Muralla China pero en este caso para referenciar a lo que oficialmente se llamó Proyecto Escudo Dorado, que pretende mediante el uso de tecnología, equipos y legislación, vigilar y censurar el acceso a internet y otros medios de comunicación por parte del Ministerio de Seguridad Publica.

En el pasado hemos recibido notificaciones de que túneles IPSec de sitios dentro de China estableciendo conexiones a sitios fuera de China a los que no tengan acceso a analizar el trafico debido al cifrado podrán ser interrumpidos sin previo aviso por lo que usualmente son bastante inestables.

4.1.2 Zonas de Disponibilidad

Las zonas de disponibilidad tienen nombres iguales al nombre de la región con un consecutivo, lo cual no describe la ubicación geográfica exacta dentro de la región seleccionada por razones de seguridad. Para las regiones seleccionadas existen al menos 5 zonas de disponibilidad; se especifica para las instancias a crear la primera zona disponible para que la ubicación sea consistente en todas ya que de no seleccionar ninguna serán seleccionadas al azar.

4.1.3 Direccionamiento

Teradyne es dueña del segmento de red 131.101.0.0/16 y 132.223.0.0/16 que a pesar de ser un segmento de direcciones IP clase B considerados como de IPs públicas se usa internamente para direccionamiento dentro de la LAN en segmentos más pequeños /24 asignados a los diferentes sitios alrededor del mundo. También se usan otros segmentos como lo son 10.180.0.0/16 y 192.168.0.0/16, este último para conectividad con sites de terceros, o servicios en la zona DMZ.

Para el caso particular de Amazon Web Services se han definido algunas subnets y se han reservado otras para crecimiento a futuro. Siguiendo la práctica actual se crean subnets independientes para servicios publicados, servidores de aplicaciones, servidores de base de datos, almacenamiento y backup. Al no existir la figura de VLAN en la nube

de AWS la segmentación se hará solamente con subnets, pero además se implementan Access Lists y Security Groups.

De esta forma, para la implementación en AWS se utiliza:

Tabla 12. Definición de Subnets a utilizar.

Subnet	Pública / Privada	Región	Uso
192.168.90.0/24	Pública	EE.UU. Este (Norte de Virginia)	Servidores con acceso externo
192.168.91.0/24	Privada	EE.UU. Este (Norte de Virginia)	Capa Aplicaciones
192.168.92.0/24	Privada	EE.UU. Este (Norte de Virginia)	Reservada
192.168.93.0/24	Privada	EE.UU. Este (Norte de Virginia)	Capa Base de Datos
192.168.94.0/24	Privada	EE.UU. Este (Norte de Virginia)	Capa Backup
192.168.100.0/24	Pública	EE.UU. Oeste (Norte de California)	Servidores con acceso externo
192.168.101.0/24	Privada	EE.UU. Oeste (Norte de California)	Capa Aplicaciones
192.168.102.0/24	Privada	EE.UU. Oeste (Norte de California)	Reservada
192.168.103.0/24	Privada	EE.UU. Oeste (Norte de California)	Capa Base de Datos
192.168.104.0/24	Privada	EE.UU. Oeste (Norte de California)	Capa Backup
192.168.110.0/24	Pública	Asia Pacífico (Singapur)	Reservada
192.168.111.0/24	Privada	Asia Pacífico (Singapur)	Capa Aplicaciones
192.168.112.0/24	Privada	Asia Pacífico (Singapur)	Reservada
192.168.113.0/24	Privada	Asia Pacífico (Singapur)	Reservada
192.168.114.0/24	Privada	Asia Pacífico (Singapur)	Capa Backup

4.1.4 Selección de Servidores y Sistema Operativo

Tomando en cuenta que el inventario actual contiene una cantidad considerable de equipos ejecutando Windows Server 2008 R2, el cual según Microsoft dejará de tener soporte el 14 de enero de 2020 (Windows 2008 R2 End of support, s.f.). Se utilizará como opción en AWS Windows server 2016 cuando se vaya a montar un servidor con sistema operativo Windows. Según los requerimientos de los servicios a migrar existe compatibilidad con esta versión de sistema operativo. Para el caso de Linux, las versiones utilizadas se encuentran todavía vigentes y con soporte dentro del ciclo de vida de Red Hat Enterprise por lo que se mantendrá la versión actual. (Red Hat Enterprise Linux Life Cycle, s.f.)

En el caso de configuraciones de Memoria, disco duro y procesadores es una práctica común que cuando se estiman para los requerimientos de una aplicación se contemple un nivel de crecimiento por lo que los valores actuales de uso real muestran que están

subutilizados. Una de las ventajas de la computación en la nube descrita en este documento es la capacidad de hacer ajustes de capacidad y que se pueden hacer sobre la marcha, por lo que inicialmente se utilizaran los valores de memoria, cantidad de procesadores y espacio de almacenamiento descritos en el inventario como punto de partida y utilizando la herramienta CloudWatch se puede monitorear el uso real de estos componentes, establecer parámetros para generar alertas cuando el uso incremente o disminuya por sobre un valor establecido y utilizando herramientas de Auto Scaling se puede automatizar el aumento o disminución de recursos en función del uso real. Recordemos que en computación en la nube se paga por lo que se usa solamente por lo que tener recursos ociosos representa un gasto innecesario.

4.1.5 Almacenamiento

En AWS existen diferentes tipos de almacenamiento para diferentes propósitos según sea el caso particular.

La mayoría de las instancias de EC2 utilizan almacenamiento de Amazon Elastic Block Store (EBS) el cual es un servicio de almacenamiento escalable para el que existen diferentes niveles de rendimiento. Según la documentación de AWS "*En Amazon EBS se implementa una amplia gama de cargas de trabajo, como bases de datos relacionales y no relacionales, aplicaciones empresariales, aplicaciones en contenedores, motores de análisis de big data, sistemas de archivos y flujos de trabajo de medios*". (Amazon Elastic Block Store, s.f.). Por esta razón este será el almacenamiento utilizado en las instancias implementadas ya que cubre los casos de uso incluidos en esta propuesta. En Instancias muy grandes de la categoría xlarge se ofrecen volúmenes con discos SSD de memoria rápida no volátil (NVMe) como alternativa.

Una instancia puede tener múltiples volúmenes de EBS sin embargo también existen otro servicio de almacenamiento utilizando Amazon S3 el cual provee múltiples niveles de rendimiento y funcionalidades adicionales. Para esta propuesta particular se propone el uso de S3 Intelligent-Tiering como almacenamiento adicional para los servicios de Sharepoint, Eknowledge y el esquema de carpetas compartidas DFS-R ya que son servicios que almacenan una gran cantidad de archivos. Este almacenamiento trabaja almacenando en dos capas, una optimizada para acceso frecuente, y otra para acceso poco frecuente, esto permite optimizar costos. Existe un cargo de monitoreo y automatización

para que los archivos que no son accedidos en un periodo de 30 días, se muevan a la capa más barata y los que son accesados frecuentemente se mantengan en la capa optimizada. Todo esto sin afectar las aplicaciones o servicios que lo utilicen. Además, es posible agregar este tipo de almacenamiento detrás de un Load Balancer como un mecanismo de contingencia adicional.

Entre otras cosas Amazon S3 se utiliza para: para almacenar imágenes de máquina de Amazon (AMI), para almacenar instantáneas (copias de seguridad) de los volúmenes de datos. (Tipos de almacenamiento de Amazon S3, s.f.)

Para el servicio de Enterprise Backups se utilizará el servicio Amazon S3 Glacier que es un almacenamiento de bajo costo ($0.004 por Giga al mes) que es útil para almacenar datos como backups o información que no es accedida regularmente.

En caso de que la información se requiera accesar se cobra un adicional por datos recuperados de la bóveda, este adicional depende de la tasa de recuperación que se requiera, es decir a menor tiempo de recuperación mayor es el costo.

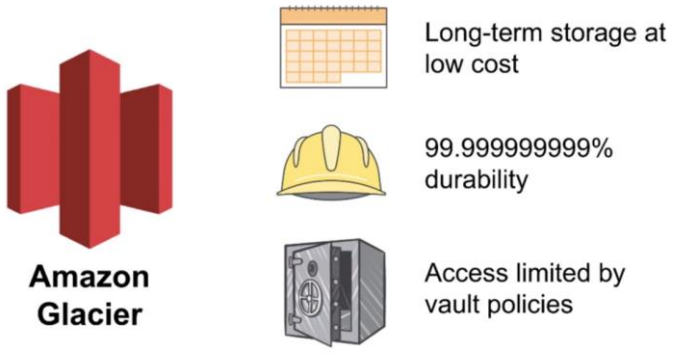


Figura 34. Amazon S3 Glacier. (AWS Cloud Practitioner Training, s.f.)

4.1.6 Distribución de Aplicaciones y servicios

Tabla 13. Distribución de Aplicaciones en Regiones

Aplicación	Región EE.UU. Este (Norte de Virginia)	EE.UU. Oeste (Norte de California)	Asia Pacífico (Singapur)
Active Directory	Sí	Sí	Sí
DNS interno	Sí	Sí	Sí
DNS Externo	Sí	No	No
SharePoint (Intranet)	Sí	DR	No
Portal de Clientes internos y externos (Eknowledge)	Sí	DR	Implementar CloudFront
Página Web (www.teradyne.com)	Sí	DR	Implementar CloudFront
Carpetas Compartidas dentro del esquema DFS-R	Sí	Sí	Sí
LSF	Sí	No	No
Enterprise Backup	NR exportará a AWS	Sí	Sí
Team Center (PLM)	Sí	DR	No
Servidor de administración de Antivirus	Sí	No	No

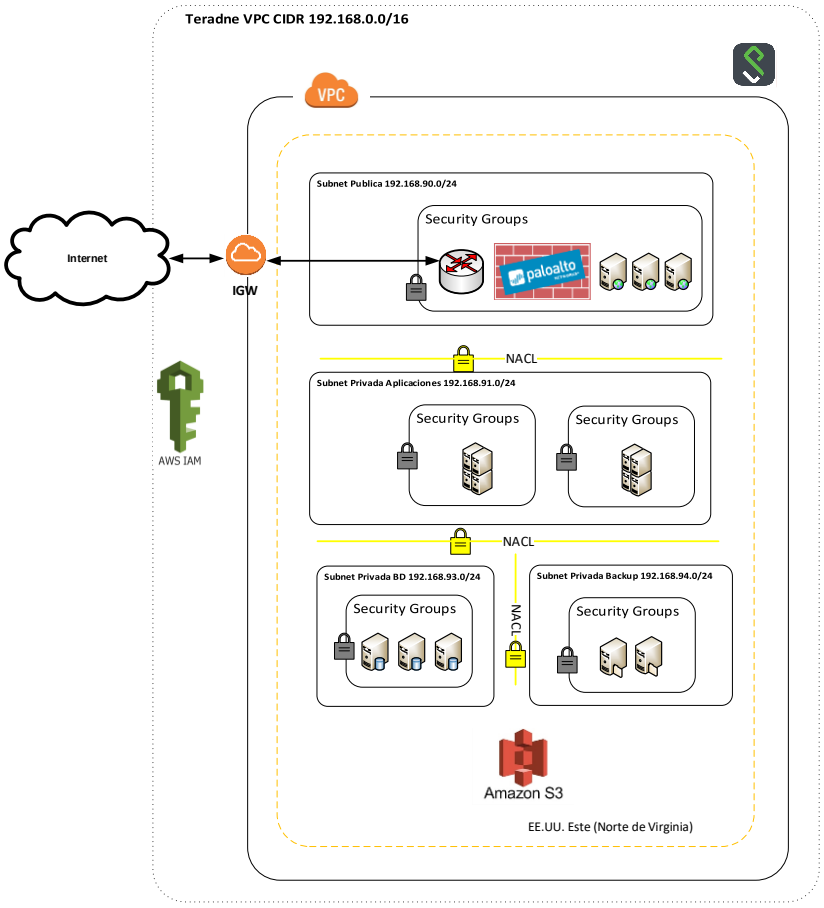


Figura 35. Diagrama Lógico VPC Propuesta. Región EE.UU (Norte de Virginia)

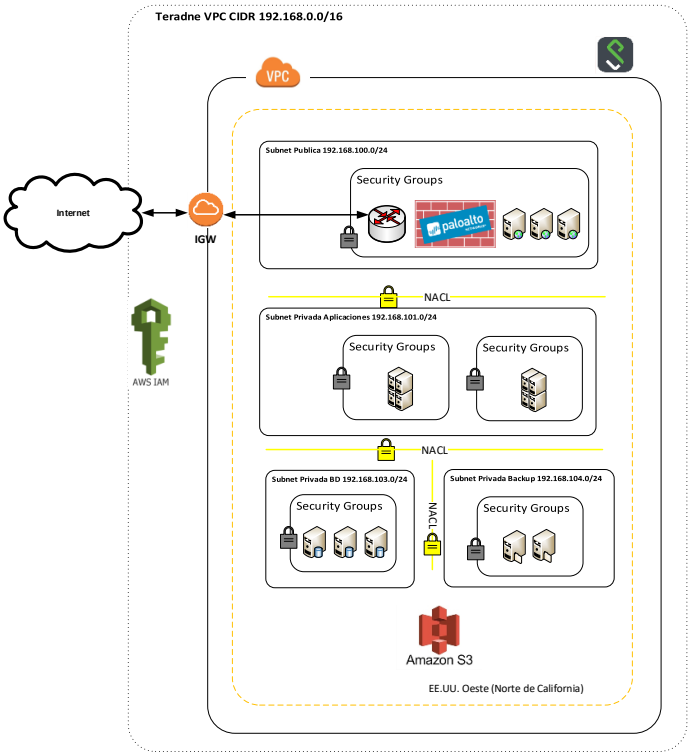


Figura 36. Diagrama Lógico VPC Propuesta. Región EE.UU. Oeste (Norte de California)

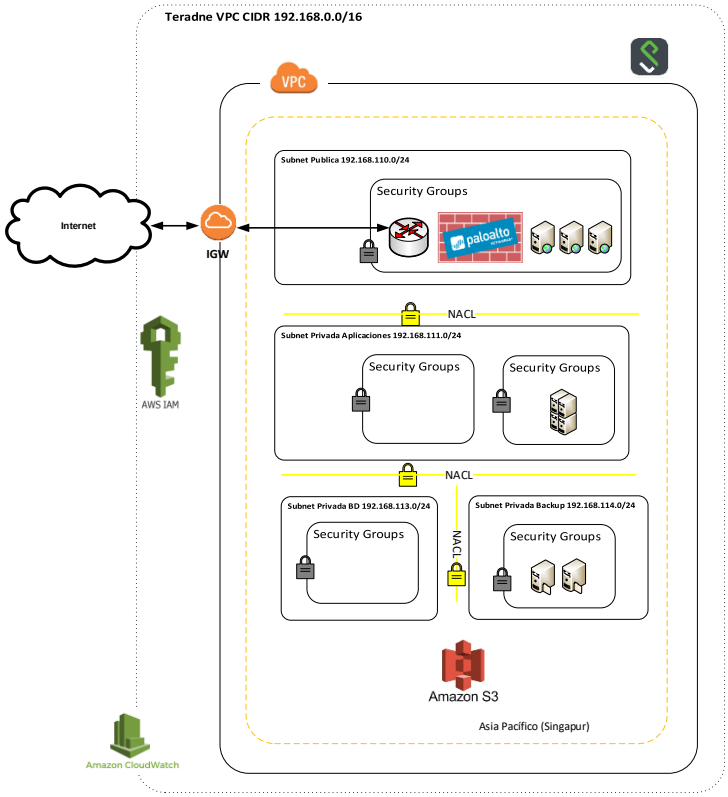


Figura 37. Diagrama Lógico VPC Propuesta. Región Asia Pacífico (Singapur)

4.2 Modelo de Conectividad Propuesto

La Infraestructura en la nube de AWS se considera para efectos prácticos como una oficina nueva, por lo tanto, al seguir los estándares existentes se utiliza iguales mecanismos y tecnologías de conectividad. Básicamente hay dos escenarios posibles: el primero, los tres servicios que requieren accesarse desde internet como son el DNS Externo para el dominio Teradyne.com, la página web y el portal de clientes internos y externos. El segundo, conectividad entre oficinas, es decir, cualquier oficina de Teradyne pueda acceder a la infraestructura de AWS.

En el primer escenario, a pesar de existir mecanismos para publicar los servicios en AWS directamente, mediante el uso de un Internet Gateway asociado a la instancia por publicar, en este caso específico y con el fin de agregar una capa adicional de seguridad se hará a través del Firewall, el cual se configurará en la subnet pública del VPC. (Palo Alto en AWS, s.f.)

Para el segundo de los escenarios se propone dos mecanismos, según se menciona son los utilizados actualmente para la conectividad entre oficinas.

El primer método de conectividad es a través del partner de SD-WAN Aryaka. Por medio de de los dispositivos ANAP, los cuales se tiene en prácticamente todas las oficinas, se configura túneles IPSec hacia la red de Aryaka, donde las subnets configuradas en las diferentes regiones se conocen mediante el protocolo de enrutamiento RIP. Aryaka se encarga de llevar el tráfico de la oficina de Teradyne a través de su red, hacia la Región de AWS y se le aplica calidad de servicio y optimización.

Entre Aryaka y AWS se habilita dos túneles IPSec para cada región configurada. Entre cada oficinas de Teradyne y Aryaka, a la vez existen dos túneles IPsec en modo Activo/Pasivo.

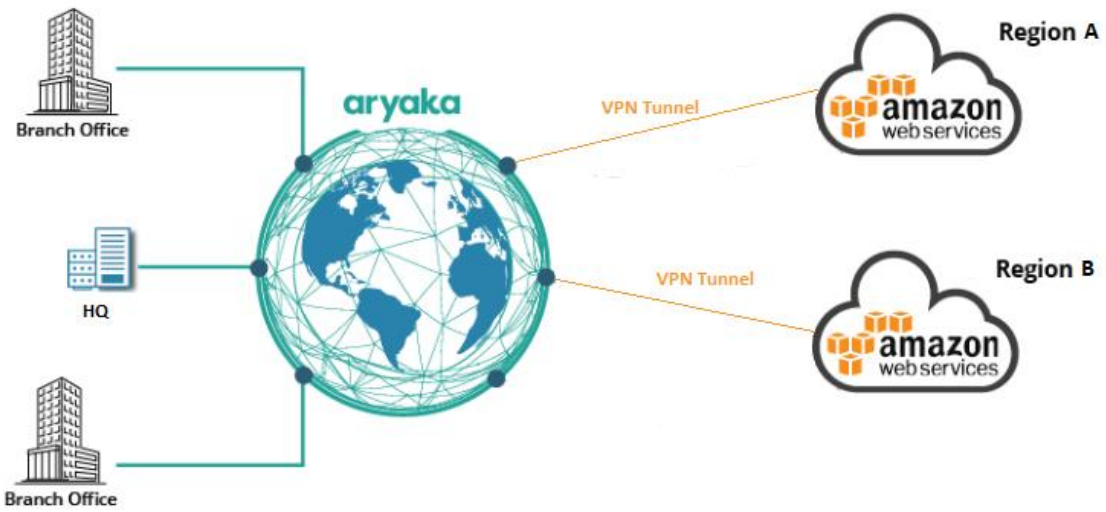


Figura 38. Diagrama Lógico de Conectividad mediante Aryaka. (SD-WAN FOR AMAZON WEB SERVICES, s.f.)

El segundo método de conectividad es mediante túneles IPsec entre los router de cada oficina mediante el uso de DMVPN (Dynamic Multipoint VPN). Para lograr esto, AWS es necesaria la implementación de routers Cisco Cloud Services Router (CSR) 1000V. Este Router virtual está disponible en el market place (Cisco Cloud Services Router on AWS Market, s.f.) bajo la modalidad BYOL (Bring your own License[7]). El dispositivo se implementa en la Subnet Pública del VPC, se le asigna un Internet Gateway con una

[7] Bring your Own License (BYOL) Permite a las empresas usar licencias adquiridas y utilizarlas en infraestructura en la nube. (Bring Your Own License, s.f.)

IP pública NATteada a la IP a la cual se le haya asignado dentro de la subnet y las interfaces adicionales pueden asignarse a las redes privadas. En el presente caso, como se menciona, adicionalmente se coloca un FW Palo alto bajo igual modalidad, para poder adjuntar a sus características de FW, funciones agregadas de seguridad, por ejemplo, habilitar la función de Data Loss Prevention. (Data Filtering Support for Data Loss Prevention (DLP) Solutions, s.f.)

Un Túnel DMVP es un túnel dinámico, se construye entre un sitio remoto conocido como spoke y un sitio principal, conocido como hub. Cada hub provee la información de todas las subredes disponibles en cada sitio y cómo generar túneles entre sitios remotos (spoke to spoke), de esta forma cualquier sitio el cual necesite llegar a una subred en AWS le consultará al Hub principal la información necesaria (IPs, llaves, parámetros y otros) e iniciará un túnel dinámico directo con AWS. Este se construye en menos de un segundo y se mantendrá activo mientras exista tráfico a través de él; si no se detecta tráfico después de un periodo, se deshabilita automáticamente. Esto también aplica para generar túneles entre dos regiones de AWS. (Cisco, 2008)

4.2.1 Enrutamiento

A nivel de enrutamiento, entonces se tendrá para el escenario de conectividad mediante Aryaka, el protocolo RIP versión 2 y para DMVPN el EIGRP. Ambos protocolos de enrutamiento dinámico pueden coexistir, pues se le asigna una prioridad más baja a las rutas que se aprenden mediante RIP y de esta forma en una eventualidad donde Aryaka presente algún incidente dentro de su red y tenga una caída en el servicio, automáticamente se instalará las rutas de DMVPN para prever un failover automático.

También al ser Aryaka un servicio el cual se paga por ancho de banda suscrito, es posible enrutar tráfico masivo a través de DMVPN y consumir menos ancho de banda dentro de la red de Aryaka.

4.3 Aseguramiento de la infraestructura

Amazon en su documentación de entrenamiento comenta: el usuario final retiene el control completo de los datos, en qué región los almacena, cómo quiere manejar el cifrado y cómo almacena la clave de cifrado. La tecnología que se utiliza a nivel de centro

de datos cumple con los más avanzados sistemas de vigilancia electrónica y control de acceso multifactorial, guardias de seguridad capacitados y el acceso está estrictamente regulado. De hecho, la ubicación física de las zonas de disponibilidad no se revela a los clientes por seguridad.

Cuentan además con sistemas ambientales diseñados para minimizar el impacto de las interrupciones en las operaciones. Las regiones y las zonas de disponibilidad permiten a AWS mantenerse resiliente en caso de desastres naturales o fallas del sistema.

Además, tiene por defecto servicios en sus centros de datos, entre ellos la mitigación de ataques de denegación de servicio distribuidos (DDoS), conexiones dedicadas, encriptación de datos en tránsito y la implementación de firewalls, esto implícitamente se traslada al cliente.

Pero todo ello es insuficiente si el usuario final no toma las previsiones de seguridad adecuadas.

4.3.1 Modelo de Responsabilidad Compartida AWS

El modelo consiste en un esquema donde tanto el cliente como el proveedor tienen a cargo elementos de seguridad y de ellos depende su adecuada gestión.

Amazon no tiene visibilidad en las capas superiores, pues son responsabilidad del cliente.

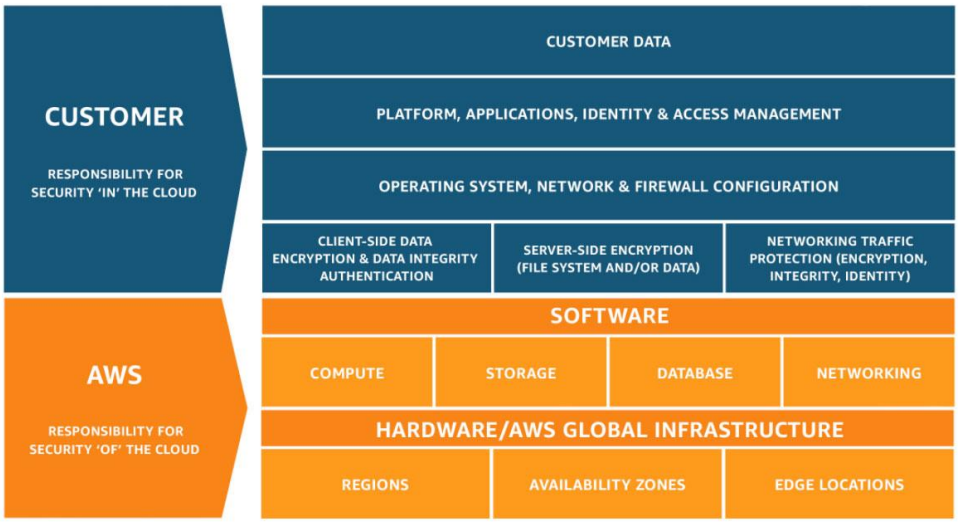


Figura 39. Modelo de Responsabilidad Compartida de AWS. (Modelo de responsabilidad compartida, s.f.)

4.3.3 Security Groups y Network ACLs

Existe en AWS dos elementos básicos, ambos juegan un papel importante en el aseguramiento de la infraestructura. Básicamente se puede ver el Security Group como el firewall de las instancias EC2, mientras las NACL son el firewall de las subredes.

Cada instancia se vincula a un Security Group, por tanto, le aplican las reglas ahí estipuladas, de igual forma como a cada subred le aplican las reglas que se defina en la NACL asignada. Esto en lo particular es útil, por ejemplo, si se desea segmentar equipos dentro de una subred, pues al compartir igual rango de IPs para hablar una con otra no requieren pasar por la NACL.

Un dato importante es que los Security Groups aplican las reglas para el tráfico en ambos sentidos, es decir cualquier cambio aplicado a una regla entrante se aplicará automáticamente a la regla saliente. Las NACL en cambio pueden tener reglas diferentes de entrada y salida. (AWS Cloud Practitioner Training, s.f.)

Para la presente implementación solo se permite que las subnet privadas sean accesibles desde las subnet de las oficinas de Teradyne a través de los túneles IPSec. Para el caso del servidor web, solo puede accederse desde internet por puerto 443 y él a su vez solo puede conectar con su servidor de su base de datos y solamente por un puerto específico.

4.3.4 Seguridad en Sistema Operativo

Como se controla los servidores de la organización y se es responsable del mantenimiento y seguridad del sistema operativo, se aplica las medidas implementadas a nivel general para todos los servidores de Teradyne.

Por lo tanto, se utiliza el sistema Kace para la administración de parches en servidores Windows, los cuales se instalan después de haberse verificado en ambientes de prueba y solamente en las ventanas de mantenimiento establecidas. En servidores Unix el proceso involucra un trabajo manual, de igual forma se instala las actualizaciones solamente en las ventanas de mantenimiento establecidas.

Se utiliza la versión para server de Symantec junto con el agente de CrowdStrike en servidores Windows y el agente de CrowdStrike para servidores Unix.

También se instala un agente de un analizador de vulnerabilidades, el cual escanea en tiempo real los servidores y brinda un reporte del estado del servidor en un Dashboard de administración y alertas en el caso de descubrir una nueva vulnerabilidad.

El método de acceso a los servidores es por Remote Desktop en el caso de Windows y por SSH en el caso de Unix, pero no se hace directamente, sino a través de una herramienta de Privileged Access Management (PAM) llamada CyberArk, se accede a una interfaz utilizando autenticación multifactor con las credenciales del administrador de Windows o Unix, los cuales no tienen privilegios sobre los servidores y desde ahí se ejecuta la conexión remota automáticamente hacia los servidores, para ello se utiliza la cuenta privilegiada. Entre las ventajas que provee esta herramienta se encuentra la facilidad de auditar las conexiones, grabación de las sesiones y el hecho de que los password de cuentas privilegiadas no es necesario conocerlos.

4.3.5 Encriptación de Datos

La decisión de encriptar los datos, tanto almacenados como en tránsito, está en el cliente, según la política de responsabilidad compartida de AWS se tiene el control total sobre cuáles algoritmos usar, las llaves y cómo almacenarlas. En el presente caso todos los túneles, bases de datos, almacenamiento y backups estarán encriptados.

Se mantendrá los algoritmos utilizados actualmente para cada caso particular.

Túneles IPsec: esp-aes 256

Bases de Datos: TDE en SQL y Native Encryption en DB2

Datos almacenados en EBS, S3 Buckets o Amazon Glacier: AES-256

Las llaves actualmente se almacenan en CyberArk, por tanto, se mantendrá esta práctica.

4.3.6 IAM (Identity and access management)

El acceso a la consola de administración de AWS requiere un control muy granular, pues Teradyne cuenta con diferentes grupos de infraestructura, los cuales requieren de un cierto nivel de acceso para administrar los componentes correspondientes.

Existe una cuenta maestra almacenada en CyberArk con Autenticación multifactorial habilitada, pero se crea un proveedor de autenticación dentro del IAM, es el Active Directory, de esta forma la asignación de usuarios se hace al utilizar grupos definidos en el Active Directory de la manera en la cual se hace actualmente.

Si se parte del principio de mínimo privilegio, se configura roles específicos para cada grupo de infraestructura, con acceso solamente a los elementos de la consola de administración necesarios para sus labores, un rol adicional con solo acceso a herramientas de monitoreo y uno para ver datos de facturación para algunos Managers.

Los grupos de aplicaciones no requieren acceso a la consola de AWS, pues ellos administran las aplicaciones a través de consolas, o ingresan a los servidores a través de CyberArk.

Actualmente no existe requerimiento de desarrolladores que requieran acceso a recursos de AWS, por lo tanto, tampoco se contempla un nivel de acceso para ellos.

4.3.7 AWS Shield

AWS Shield es un servicio de protección contra ataques de denegación de servicio distribuidos. Existen dos versiones: standard, por defecto implícita y sin cargo adicional para todos los clientes. La versión advanced ofrece un nivel adicional de protección. (AWS Cloud Practitioner Training, s.f.) Como la propuesta incluye la publicación de varios servicios, se contempla la versión advanced particularmente como mecanismo de protección del servicio de DNS Externo, para eso se usa Router 53.

La versión avanzada permite visibilidad de ataques en tiempo real y ofrece un equipo de respuesta en caso de enfrentar un ataque de DDoS (DDoS Response Team)

4.4 Monitoreo

Una parte importante al administrar cualquier infraestructura es la capacidad de monitorearla, pues no se puede estar 100% del tiempo revisando su estado o logs. Para

facilitar esa tarea AWS ofrece varias herramientas de monitoreo. En esta propuesta se contempla Cloudtrail y CloudWatch.

Cloudtrail es básicamente un syslog de cualquier acción realizada en AWS y CloudWatch, mediante cuatro componentes los cuales comprenden: recolección de métricas, recolección de eventos y logs de monitoreo, un componente para generar alarmas con base en los datos obtenidos de los anteriores, y un componente capaz de reaccionar ante las alarmas para enviar, por ejemplo, notificaciones por email, ejecutar una secuencia de Auto Scaling para agregar o remover recursos automáticamente, o reiniciar una instancia de EC2.

También existe en la consola un Dashboard configurable donde se puede tener una visión general de los elementos de CloudWatch. (AWS Cloud Practitioner Training, s.f.)

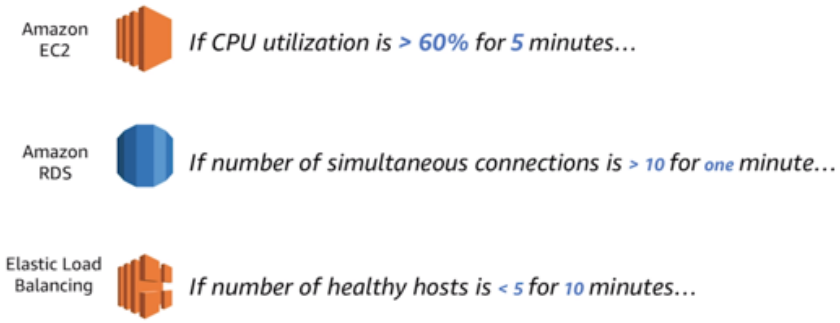


Figura 40. Ejemplos de configuración de alarmas. (AWS Cloud Practitioner Training, s.f.)

Uno de los requerimientos del grupo de Network incluye la implementación de Netflow, protocolo para recolectar información estadística del tráfico que atraviesa por interfaces de dispositivos de red con el fin de hacer análisis posterior del tráfico. Para este caso particular se puede habilitar Netflow en las interfaces del router y Firewall y configurarlos para exportar los datos al colector que se encuentra en North Reading.

4.5 Otras consideraciones

AWS ofrece servicios los cuales permiten homologar prácticamente cualquier componente de infraestructura, inclusive ofrecer funcionalidades adicionales. Estas

pueden resultar en un diseño más eficiente. Algunos servicios evaluados en la presente propuesta, vale la pena describirlos un poco más en detalle. Se presentan a continuación

4.5.1 Amazon Elastic Load Balancing

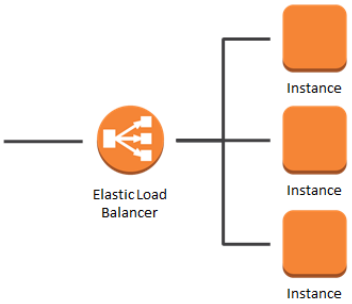


Figura 41. Diagrama Lógico Elastic Load Balancer. (AWS Cloud Practitioner Training, s.f.)

Como varios de los servicios utilizan en la actulidad Balanceadores de carga, la forma de replicar ese dispositivo en AWS es mediante el uso de Elastic Load Balancer. Este dispositivo puede utilizarse además como un mecanismo de failover automático y detrás de él los servidores o servicios pueden ubicarse en diferentes zonas de disponibilidad, lo cual agrega una capa adicional de redundancia.

4.5.2 Amazon Route 53

Para el servicio de DNS externo se utiliza en esta propuesta Route 53. Algunas de sus características incluyen resolución con base en geolocalización, lo cual permite para un servicio distribuido en varias regiones, resolver apuntando al servidor más cercano, failover automático, algoritmos de balanceo de solicitudes entre servidores DNS y resolución con base en la menor latencia.

Al registrar una zona de dominio en Route 53 se provee al menos servidores DNS para registrar en el dominio. (AWS Cloud Practitioner Training, s.f.)

4.5.3 Amazon RDS

Los servicios que necesiten base de datos en esta propuesta se presentan de la forma en la cual se encuentran actualmente con servidores de base de datos exclusivos para cada servicio. Sin embargo, esto implica que parte de la administración de ellos involucra

temas de sistema operativo, mantenimiento, configuraciones de redundancia, backups entre otros.

AWS ofrece la posibilidad para algunos de los motores de base de datos comunes, de solo administrar la base de datos como tal, olvidándose de las capas inferiores y componentes descritos. Esta opción representa una disminución en las labores administrativas y un incremento durante el periodo en que el servicio se encuentra disponible, pues no habrá tiempos de mantenimiento.

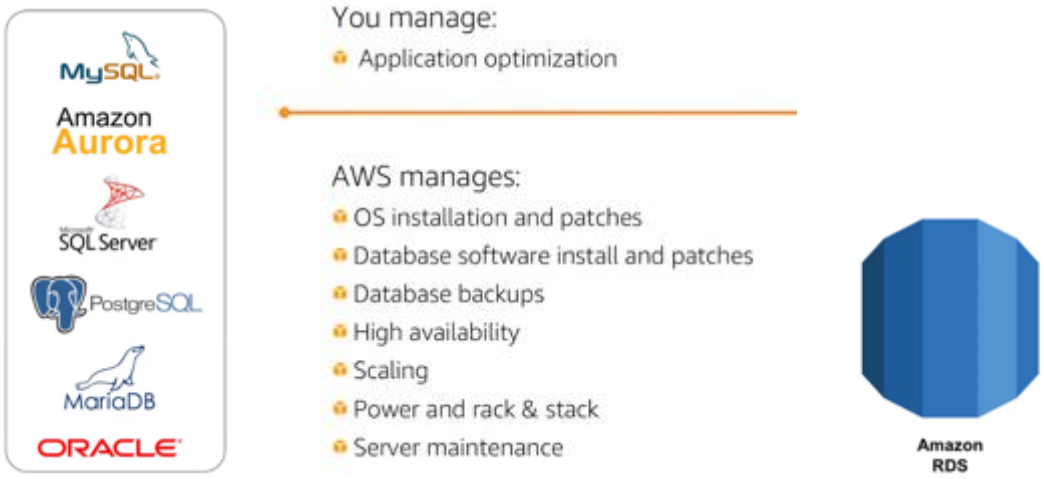


Figura 42. Motores Soportados y Distribución de responsabilidades Amazon RDS. (AWS Cloud Practitioner Training, s.f.)

Una característica adicional es poder configurar réplicas de solo lectura, pueden estar hosteadas en una región diferente a la master y se puede usar para redirigir solicitudes a la réplica según la ubicación geográfica, así se reduce la latencia y en caso de un desastre esta réplica puede convertirse en master. (AWS Cloud Practitioner Training, s.f.)

Los servicios incluidos en esta propuesta, los cuales usan bases de Datos DB2, pueden seguir con el modelo actual donde se administra tanto el server como el motor.

4.5.4 Amazon CloudFront

Es una red, sirve para publicar contenido en ubicaciones más cercanas a los usuarios finales con el fin de reducir tiempos de respuesta. Estas ubicaciones incluyen puntos estratégicos inclusive fuera de las regiones de AWS. (Características clave de Amazon CloudFront, s.f.)

Por ejemplo, si se tiene una aplicación en North Reading y algunos usuarios en Asia CloudFront junto con Router 53, puede direccionar la solicitud del usuario a una réplica en Asia. Y no necesariamente el servicio original debe estar hosteado en AWS. Prácticamente puede usar CloudFront para publicar cualquier aplicación accesible desde internet.

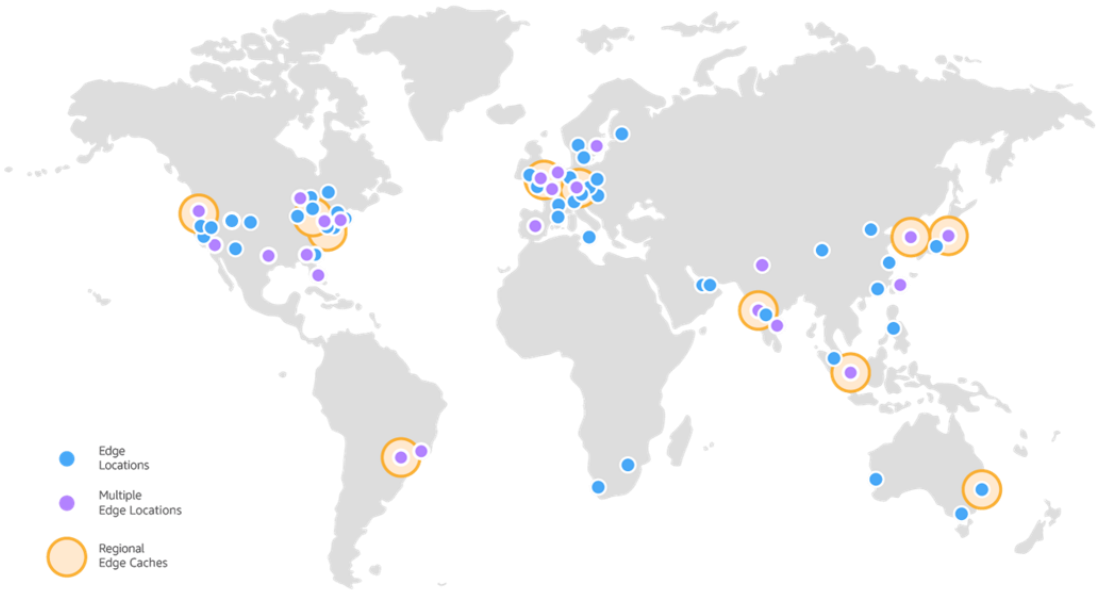


Figura 43. Edge Locations AWS CloudFront. (Características clave de Amazon CloudFront, s.f.)

4.5.5 Auto Scaling

Auto Scaling es un servicio, permite de forma dinámica y automatizada agregar o reducir recursos como subnets, Load Balancers, instancias, almacenamiento con base en reglas predefinidas o alertas



Figura 44. Descripción Amazon Glacier. (AWS Cloud Practitioner Training, s.f.)

4.5.6 Certificaciones AWS

AWS cuenta con las siguientes acreditaciones y certificaciones



Figura 45. Certificaciones y Acreditaciones AWS. (AWS Cloud Practitioner Training, s.f.)

4.5.8 Implementación de requisitos en AWS

Tabla 14. Implementación de Requisitos Network

Network	Requerimiento Implementado en AWS
Failover automático de túneles.	Aryaka y DMVPN utilizan protocolos de enrutamiento dinámicos que redirigen el trafico al túnel backup en caso de fallo del primario.
Incorporar en el modelo de conectividad la SD WAN de Aryaka.	Aryaka ofrece el servicio mediante Direct Connect o túneles IPSEc.
Incorporar modelo DMVPN	Se utiliza un VDI csr1000v, se puede obtener en el AWS MarketPlace
Optimización y/o caching entre la nube y los puntos de entrada a la red local de Teradyne.	Aryaka optimiza el tráfico que atraviese su red, también existen servicios como CloudFront, este permite publicar una versión "Cached" de un servicio publicado.
Dual homing de servidores.	La figura de dual homing en este caso se usa conectando un servidor a dos switches diferentes en modo activo/pasivo, más que todo por un tema de fallo del switch, o de la tarjeta de red del equipo. En AWS no existe la figura de switches y la conectividad es

	virtualizada. Además de garantizarse por ellos, en consecuencia, la figura de dual home no se considera necesaria.
Estructuras redundantes (múltiples paths para llegar de una parte a otra en caso de que estén en diferentes clouds, zonas o centros)	Al menos existirán 2 túneles entre Teradyne-Aryaka-AWS o a través de DMVPN, todos con enrutamiento dinámico.
Layer 2 security (Vlans, PVlans, VRFs o métodos para separar de los demás inquilinos)	Se hace a través de Security Groups y NACL. La figura de VLAN no existe en AWS.
Múltiples puntos de acceso a la nube con base en cercanía geográfica, como lo que se habla de Asia, Europa y América.	Aryaka cubre esa parte, garantiza la mejor ruta desde el origen al destino, servicios publicados en diferentes regiones podrían redireccionarse por el DNS a la región más cercana con base en geolocalización.
Capacidad de reporteo en tráfico, tipo Netflow.	Si se usa un router virtual, se puede habilitar Netflow en sus interfaces y utilizar las herramientas de monitoreo actuales. Además de CloudCatch y Cloudtrail.
Dashboard de alarmas y tiquetes relacionados con la infraestructura.	A través de CloudWatch.
Acceso a administrar subnets, y tablas de enrutamiento.	Se proveerá acceso con IAM a estas funciones específicas.

Tabla 15. Implementación de Requisitos Windows

Windows	**Requerimiento Implementado en AWS**
Al menos un Servidor de Active Directory en AWS configurado como Catálogo Global.	En las tres regiones propuestas habrá dos.
Al menos un servidor DNS para resolución interna.	En las tres regiones propuestas habrá dos
Posibilidad de conectar mediante Remote Desktop integrado con CyberArk.	Se permitirá el puerto de Remote desktop solamente desde los servidores de CyberArk.
Posibilidad de crear, iniciar, reiniciar, apagar, terminar instancias.	Se proveerá acceso con IAM a estas funciones específicas.
Poder Monitorear recursos como memoria, disco duro, CPU de los servidores y tener alertas cuando excedan los valores recomendados.	A través de CloudWatch.
Poder agregar el servidor al dominio.	Una vez establecida la conectividad los servidores pueden agregarse. Se crea una estructura de replicación en el ambiente de Active Directory para los servidores nuevos.

Poder aplicar Políticas de grupo a esos servidores.	Una vez establecida la conectividad y agregar los servidores al dominio, se puede aplicar GPOs.
Flexibilidad, qué tan rápido se pueden hacer cambios.	La mayoría de cambios se pueden hacer en caliente. Internamente se seguirá el proceso de Control de Cambios para cualquier modificación.
Que exista un control, log de cambios hechos y quién los hace.	Cloudtrail prove esta funcionalidad.

Tabla 16. Implementación de Requisitos Unix

Unix	Requerimiento Implementado en AWS
Posibilidad de conectar mediante ssh integrado con CyberArk.	Se permitirá el puerto de ssh solamente desde los servidores de CyberArk.
Posibilidad de crear, iniciar, reiniciar, apagar, terminar instancias.	Se proveerá acceso con IAM a estas funciones específicas.
Poder monitorear recursos de los servidores e integrarlos con las herramientas de monitoreo actuales.	A través de CloudWatch y siguiendo el proceso de commisioning de servidores normal, se agregará a las herramientas de monitoreo actuales.
Posibilidad de configurar IP primaria y secundaria.	La opción está disponible para todas las instancias de EC2.
Acceso a repositorios de RedHat para descargas de actualizaciones durante las ventanas de mantenimiento.	Se configura una regla para la URL particular.
Posibilidad de crear snapshots de las instancias.	Dentro del menú de cada instancia existe la opción de generar snapshots para los volúmenes que se escoja. También se puede generar una AMI (Amazon Machine Image) a partir de una instancia creada para utilizarla como base para una nueva.

Tabla 17. Implementación de Requisitos Storage

Storage	Requerimiento Implementado en AWS
Integración con AD de TER para poder realizar administración y acceso con grupos y demás heredados del dominio, así como logs de auditoría donde se pueda identificar los usuarios.	En las VPC habrá dos servidores de Active Directory que pueden ser proveedores de autenticación y los almacenamientos se adjuntan a servidores y en ellos se puede definir permisos, también está la opción de hacerlo a través de un rol del IAM si el

	almacenamiento se usa sin estar adjunto a un servidor.
Proveer acceso a los datos almacenados como NFS, SMB y FTP como mínimo.	Esto se puede configurar desde el Sistema operativo donde esté conectado el almacenamiento.
Permite la creación de snapshots para realizar copias de seguridad.	La opción está disponible en la consola de administración de S3. Se puede hacer manuales o automáticos
Replicación interna (provista por la solución) como Disaster Recovery.	Se puede colocar almacenamientos que estén en zonas diferentes detrás de un Load Balancer para un failover automático. La replicación se puede hacer a través de los túneles entre Región y Región o internamente de una zona de disponibilidad a otra dentro de la Región.
La solución debe incluir un servicio de scan de archivos en busca de virus.	Existen Servicios de terceros que permiten hacerlo directamente. Pero siguiendo la práctica actual se hará a través del antivirus del servidor donde se adjunte el almacenamiento.
Debe permitir incrementos de espacio disponible en caliente.	La herramienta permite hacer estos cambios en caliente.

Tabla 18. Implementación de Requisitos Backup

Backup	**Requerimiento Implementado en AWS**
Posibilidad de habilitar encriptación en el almacenamiento donde se guarden los backups.	Habilitar encriptación y escoger el algoritmo son opciones dentro de la configuración del almacenamiento.
Poder escoger el tipo de almacenamiento.	Hay múltiples opciones disponibles a diferentes precios.
Posibilidad de exportarlos a otra ubicación geográfica.	Esto se puede hacer mediante replicación entre Zonas de AWS configuradas por Teradyne.
Poder definir reglas de retención.	Se puede definir reglas dentro de un plan de copias de seguridad, por ejemplo tiempo de retención
Poder integrar el almacenamiento en la nube con las herramientas de Backup actuales	Las herramientas de backup como Veritas Backup Exex se puede instalar en instancias en AWS y permite agregar fuentes de información para ser respaldada y destinos sin importar la ubicación. Solo deben estar disponibles en la red. Inclusive existe una versión para AWS disponible en el AWS Marketplace.
Posibilidad de realizar Backup de recursos bajo demanda o mediante tareas programadas.	Se puede programar tareas para realizar backups utilizando AWS Lambda o las herramientas en Veritas Backup Exec

Tabla 19. Implementación de Requisitos Security

Security	Requerimiento Implementado en AWS
Acceso a la consola de administración de la infraestructura con base en roles.	Mediante IAM + Active Directory Federado
Cuentas de administradores globales deben almacenarse en CyberArk.	Una vez configurado el IAM con acceso basado en Roles, las cuentas de administración globales no serán necesarias. Se almacenan según el procedimiento actual en CyberArk.
Poder controlar y aplicar reglas al tráfico que ingresa y egresa a la nube de AWS.	Mediante Reglas en el FW, Security Groups, NACLs.
Delimitar una zona de servicios accesibles desde internet la cual tenga acceso limitado a el resto de la infraestructura (simulando lo que sería una DMZ)	La subnet pública en el VPC solo tendrá acceso a los recursos internos estrictamente necesarios para su operación. Esto controlado con Security Groups, NACLs y reglas en el FW.
Cifrado de la información en tránsito, así como de los datos almacenados.	Ambos estarán cifrados mediante algoritmos definidos por la organización. Las llaves se almacenarán en CyberArk.
La posibilidad de escanear regularmente los servidores en busca de vulnerabilidades.	Mediante la herramienta actual Rapid7. Se instalará el agente en las instancias dentro del VPC.
Segregación de servidores de diferentes servicios.	Mediante varias subnets privadas, cada una con su respectiva NACL.
Herramientas de Monitoreo.	Se usará las actuales, además de CloudWatch y Cloudtrail
La posibilidad de realizar pruebas de recuperación ante desastres al menos una vez por año.	Esto se controla por la organización de la forma en la cual se hace en las pruebas anuales de los centros de datos propios.
Evaluar la posibilidad de integrar a la infraestructura de Firewalls existente.	Diferentes marcas de Firewall están disponibles en el AWS MarketPlace, permiten usar instancias en AWS

4.6 Propuesta de migración

Antes de realizar cualquier migración de servicios, se necesita una serie de tareas de preparación, las cuales se consideran la primera etapa. Estas incluyen, por ejemplo: creación de la cuenta maestra, aceptación del contrato, agregar métodos de pago y la creación de infraestructura base y asegurarla. Tareas como la aceptación del contrato y la inclusión de métodos de pago no se deben tomar a la ligera, pues involucra

internamente una serie de aprobaciones y revisiones inclusive por la parte legal. Internamente estas tareas se coordinarán por el Manager de Infraestructura.

Una vez subsanada esta parte es necesario configurar todo lo relacionado al Identity and Access Management (IAM) donde se incluirá un proveedor de autenticación, se agregará los grupos de usuarios y se configura los roles y permisos de cada grupo. Antes de completar esta tarea es necesario una auditoría interna para verificar se cumple con el principio de mínimo privilegio, por lo tanto, cada rol se probará individualmente para garantizar que solo tiene acceso a las secciones de la consola de administración correspondientes a las tareas de cada grupo de infraestructura. Lo anterior está a cargo del comité de Ciberseguridad.

Una vez conseguido esto, se procede con la infraestructura base. Comprende las regiones, zonas de disponibilidad, subnets, NACLs y las instancias de router y firewall ubicadas en la subnet pública de cada VPC, con sus respectivos Security Groups, para poder construir los túneles IPsec con las oficinas de Teradyne, configurar el enrutamiento e implementar las reglas de FW necesarias para permitir solamente el tráfico estrictamente necesario. Estas tareas están a cargo de los líderes de los grupos de Network y de Seguridad.

Para concluir la primera etapa se someterá la infraestructura configurada a una serie de pruebas para verificar la correcta comunicación entre las partes y además se agregará los dispositivos a los sistemas de monitoreo correspondientes.

Como segunda etapa se iniciará la implementación de los servicios de Active Directory y DNS Interno, pues sus componentes se utilizan por la mayoría de aplicaciones por migrar.

La Etapa tres comprende la migración del DNS Externo utilizando Route 53, el cual tiene un mínimo impacto para la infraestructura actual, pues se puede generar todos los registros del DNS actuales y una vez completada esta tarea simplemente se actualiza los valores de DNS del Dominio Teradyne.com, con las IPs de los servidores de Route 53 y automáticamente las solicitudes comenzarán a direccionarse a los nuevos servidores. Actualmente el DNS externo se administra por el grupo de UNIX, por lo cual esta tarea estará a cargo de ellos.

Como parte de esta etapa, también el servicio de administración de Antivirus y la página web migrarán, por cuanto requieren una cantidad mínima de servidores, pero servirán para probar componentes como los Elastic Load Balancer, Motores de base de datos de Amazon RDS, los Security Groups y NACLs, la configuración de servicios publicados y el servicio CloudFront.

En la etapa cuatro se procede con la migración del resto de servicios. Esto implica una cantidad grande de equipos, recursos y tiempo de múltiples equipos por ello se espera sea la que tome más tiempo. Se les dará prioridad a los servicios como la página web y Team Center, porque la infraestructura actual tiene sus servidores en Windows Server 2008, el cual dejará de tener soporte en enero de 2020.

Cada implementación seguirá el procedimiento establecido para la implementación de los servidores, revisiones de seguridad, y procesos de puesta en producción actuales. Se estima esta etapa se extienda durante todo el 2020.

Una vez concluida la migración de todas las aplicaciones contempladas en la presente propuesta, se considera tener la suficiente criterio y experiencia adquirida para contemplar la migración de servicios adicionales, estos están fuera del alcance de este documento.

Al concluir la cuarta etapa también se propone implementar un servicio de VPN, así los usuarios remotos se pueden conectar directamente a las VPCs de una forma segura. Esto se logra mediante la implementación de un dispositivo VPN Gateway de Pulse Secure (es la marca utilizada actualmente para estos fines), el cual se implementará en la subnet pública mediante una IP NATeada del FW. Actualmente el VPN utiliza dos factores de autenticación, el primero es un usuario y contraseña del Active Directory, y el segundo, un Certificado Digital, este se genera para cada empleado, se instala en su máquina de trabajo. (Pulse Secure LLC, s.f.)

Capítulo 5. Conclusiones

La propuesta contemplada en este documento y los servicios incluidos en la misma son el resultado de un consenso entre los grupos de infraestructura, aplicaciones y en conjunto con la administración, que obedece a la necesidad de proveer para estos servicios un ambiente resiliente ante eventualidades. A pesar de que la infraestructura actual ha sido un punto alto para proveer los servicios y garantizar la continuidad del negocio, eventos aislados que sucedieron simultáneamente en 2018 pusieron en evidencia que existe varios puntos de mejora. Garantizar la continuidad de los servicios a migrar es una prioridad y un compromiso de todos los grupos de Infraestructura y aplicaciones para con el Negocio y los usuarios finales.

Estamos conscientes que existen muchos otros servicios a nivel de ingeniería y de grupos particulares que podrían beneficiarse a futuro de la infraestructura implementada por lo que no se descartan futuros esfuerzos en esa dirección.

Cada uno de los requerimientos planteados por los diferentes grupos consultados fue evaluado e investigado para comprobar que sí existe un servicio, componente o configuración que permita homologar el requerimiento. Algunos por supuesto representan un cambio de paradigma entre lo que se puede hacer con dispositivos físicos en un ambiente local y lo que se puede hacer en un ambiente de nube. A manera de ejemplo, el hecho de definir las subnets y enrutamiento en un ambiente diferente a un router o Switch, el hecho de no tener necesidad de ver por medios de conexión y el hecho de que no existe la figura de VLAN como mecanismo de segmentación, entre otros. Parte del compromiso del investigador es precisamente volver a los diferentes grupos y mostrar para cada uno de los requerimientos cuál sería la forma de cumplirlo.

Al Teradyne estar iniciando este proceso de migración hacia la nube, quiere mantener un mayor control sobre la infraestructura y sus componentes lo más cercano a como se hace hoy en sus equipos dentro de sus centros de datos, por eso, para efectos prácticos cada VPC en AWS es considerada como una oficina nueva. La infraestructura propuesta y la conectividad mantiene el estándar utilizado en el resto de oficinas con la finalidad de que para el usuario final sea transparente.

El modelo de responsabilidad compartida representa un compromiso de que AWS garantizará la seguridad física y lógica de las instalaciones, la disponibilidad de la plataforma y los equipos que se utilizan para brindar los servicios que nos ofrecen a nosotros como clientes, pero a su vez, deja en claro que el cliente tiene en sus manos la responsabilidad sobre el diseño, la configuración y los mecanismos que implemente para asegurar los servicios que utilice y sobre todo de la información que cargue, descargue o almacene en ellos. El investigador comprende la importancia de la disponibilidad, confidencialidad e integridad como pilares de la seguridad por lo que esta propuesta contempla la implementación de medidas para garantizar cada uno de estos puntos. Algunas de estas medidas son utilizadas en la actualidad en los centros de datos de Teradyne, pero algunas otras propias de AWS, serán implementadas por primera vez. Se le ha dado suma importancia en esta propuesta al principio de mínimo privilegio y la separación de roles para los accesos a la consola de administración, así como la práctica de boquear todo y solo permitir lo estrictamente necesario, en lo que a tráfico entre equipos y subnets se refiere. Los datos tanto almacenados como en tránsito serán cifrados y para cada servicio o aplicación a migrar se configurará al menos el mismo nivel de redundancia que se tenía en los centros de datos de Teradyne.

La propuesta para la migración en etapas está pensada para que inicialmente se realice la implementación de la infraestructura base y se implementen los principales mecanismos de seguridad con el fin de que en el momento que se muevan los primeros servicios, se tenga la certeza de que el diseño se ajusta a los requerimientos. Se sabe que la lista de servicios y aplicaciones a migrar es pequeña, pero también que esto es solo el comienzo y que conforme se vaya adquiriendo experiencia y confianza en la implementación de servicios en AWS, la posibilidad de que a corto plazo la lista aumente.

La planeación para la migración de las aplicaciones comprendidas en la cuarta etapa obedece a una serie de estrategias de las diferentes partes involucradas. Algunas tienen una necesidad por un tema de soporte del sistema operativo en el que están instalados. Algunas otras porque se quiere hacer una actualización a una versión más reciente, como es el caso de SharePoint, el cual se pretende migrar a la versión 2019. Otras por un tema de obsolescencia del hardware, cambios de regulaciones con proveedores o clientes que requieren hacer cambios a algunos procesos internos, entre otros. Por eso se menciona que se espera que se trabaje en esta etapa durante todo el 2020.

Referencias

¿Qué es la informática en la nube? (s.f.). Recuperado el 20 de Febrero de 2019, de https://aws.amazon.com/es/what-is-cloud-computing/

¿Qué es PaaS? (s.f.). Recuperado el 20 de Febreo de 2019, de https://azure.microsoft.com/es-es/overview/what-is-paas/

Arquitecturas Multi-Tenant. (s.f.). Recuperado el 02 de 08 de 2019, de https://gravitar.biz/tecnologia-negocios/arquitecturas-multi-tenant/

Aryaka Pop Locations. (s.f.). Recuperado el Enero de 2019, de https://www.aryaka.com/global-pop-locations/

AWS Cloud Practitioner Training. (s.f.). Recuperado el Noviembre de 2018, de https://www.aws.training/

AWS Marketplace. (s.f.). Recuperado el 23 de Marzo de 2019, de Cisco Cloud Services Router: https://aws.amazon.com/marketplace/pp/Cisco-Systems-Inc-Cisco-Cloud-Services-Router-CSR-/B07DM9MG9L

Barr, J. (16 de Junio de 2017). *AWS Named as a Leader in Gartner's Infrastructure as a Service (IaaS) Magic Quadrant for 7th Consecutive Year*. Recuperado el 17 de Febrero de 2019, de https://aws.amazon.com/es/blogs/aws/aws-named-as-a-leader-in-gartners-infrastructure-as-a-service-iaas-magic-quadrant-for-7th-consecutive-year/

Bring Your Own License. (s.f.). Recuperado el 14 de Julio de 2019, de https://netlicensing.io/blog/2016/04/25/bring-your-own-license/

Características clave de Amazon CloudFront. (s.f.). Recuperado el 25 de Julio de 2019, de https://aws.amazon.com/es/cloudfront/features/

Cisco. (Febrero de 2008). Cisco IOS DMVPN Overview. Recuperado el 20 de Marzo de 2019, de Cisco IOS DMVPN

Como funciona un Steelhead Wan Accelerator. (s.f.). Recuperado el 13 de Enero de 2019, de https://www.youtube.com/watch?v=e1U346GPC3Q)

Configuring Amazon Web Services for LSF resource connector. (s.f.). Recuperado el 30 de Junio de 2019, de IBM Knowledge Center: https://www.ibm.com/support/knowledgecenter/en/SSWRJV_10.1.0/lsf_resource_connector/lsf_rc_aws_config.html

Descubra las diferencias entre CAPEX y OPEX. (23 de Octubre de 2017). Recuperado el 26 de 05 de 2019, de https://www.myabcm.com/es/blog-post/descubra-las-diferencias-entre-capex-y-opex/

Distribucion de Empleados Teradyne. (s.f.). Recuperado el 13 de Enero de 2019, de https://www.teradyne.com/aboutus/locations

DMVPN on AWS. (s.f.). Recuperado el 18 de Junio de 2019, de https://www.thinkahead.com/TheLAB/aws-vpn-cloudhub-cisco-dmvpn-consider-evaluating-vpn-solutions/

DMVPN on AWS cvd-csr1000v-aws.pdf. (Agosto de 2014). Recuperado el 31 de 07 de 2019

Gartner Magic Quadrant IaaS Providers 2018. (s.f.). Recuperado el 17 de Febrero de 2019, de https://www.gartner.com/doc/reprints?id=1-50WJ5DV&ct=180525&st=sb

Historia de Teradyne. (s.f.). Recuperado el Enero de 2019, de https://www.teradyne.com/about-teradyne/teradyne-history

Informática de alto rendimiento. (s.f.). Recuperado el 25 de Julio de 2019, de https://aws.amazon.com/es/hpc/

Modelo de responsabilidad compartida. (s.f.). Recuperado el 9 de Junio de 2019, de https://aws.amazon.com/es/compliance/shared-responsibility-model/

Origen del termino la nube. (s.f.). Recuperado el 12 de Enero de 2019, de https://ozein.es/origen-de-la-nube/

Palo Alto en AWS. (s.f.). Obtenido de AWS Marketplace: https://aws.amazon.com/marketplace/seller-profile?id=0ed48363-5064-4d47-b41b-a53f7c937314

Productos de la nube. (s.f.). Recuperado el 17 de Febrero de 2019, de https://aws.amazon.com/es/products/?hp=tile&so-exp=below

Programas del ROTC. (s.f.). Recuperado el 22 de Enero de 2019, de https://www.todaysmilitary.com/es/education-training/rotc-programs

Que es la nube. (s.f.). Obtenido de https://azure.microsoft.com/es-es/overview/what-is-the-cloud/

Red Hat Enterprise Linux Life Cycle. (s.f.). Recuperado el 6 de Julio de 2019, de https://access.redhat.com/support/policy/updates/errata

Regiones y zonas de disponibilidad. (s.f.). Recuperado el 19 de Febrero de 2019, de https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

Reporte de Inventario, Sistema Platinum. (30 de 06 de 2019).

Salazar, G. (30 de Setiembre de 2016). *Introducción a DMVPN - Dynamic Multipoint VPN*. Recuperado el 16 de Enero de 2019, de https://community.cisco.com/t5/blogs-routing-y-switching/introducci%C3%B3n-a-dmvpn-dynamic-multipoint-vpn-fase-1-y-fase-2/ba-p/3103707

SD WAN as a Service (Aryaka). (s.f.). Recuperado el 13 de Enero de 2019, de https://www.aryaka.com/services/sd-wan-as-a-service/

SD-WAN FOR AMAZON WEB SERVICES. (s.f.). Recuperado el 14 de Julio de 2019, de https://www.aryaka.com/sd-wan-amazon-web-services/

Set Up the VM-Series Firewall on AWS. (s.f.). Recuperado el 20 de Julio de 2019, de https://docs.paloaltonetworks.com/vm-series/8-0/vm-series-deployment/set-up-the-vm-series-firewall-on-aws.html

Store, Protect, and Collaborate on Enterprise Files with Nasuni on AWS. (15 de Junio de 2018). Recuperado el 15 de 06 de 2019, de https://www.nasuni.com/partner/amazon-aws/

Talari WAN Aggregation. (s.f.). Recuperado el 13 de Enero de 2019, de https://www.talari.com/glossary_faq/wan-aggregation/

Teamcenter on AWS Cloud. (s.f.). Recuperado el 7 de Julio de 2019, de https://community.plm.automation.siemens.com/t5/Teamcenter-Blog/Teamcenter-on-AWS-Cloud-In-Step-with-the-Latest-Cloud-Solutions/ba-p/492366

TERADYNE A500 - Analog VLSI Test System. (s.f.). Recuperado el 12 de Enero de 2019, de http://www.lsi.usp.br/~rnc/instituicoes/cpqd-telebras/equipamentos/a500.html

Teradyne D133. (s.f.). Recuperado el Enero de 2019, de https://www.computerhistory.org/collections/catalog/102713116

Todas las historias de éxito de los clientes. (s.f.). Recuperado el 16 de Enero de 2019, de https://aws.amazon.com/es/solutions/case-studies/all/

Top 9 Biggest AWS Security Mistakes to avoid. (s.f.). Recuperado el 18 de Junio de 2019, de https://www.crn.com/slide-shows/security/top-9-biggest-aws-security-mistakes-to-avoid/1

Trefis Team, Great Speculations group. (29 de Diciembre de 2016). *Amazon Web Services: 2016 In Review*. Obtenido de https://www.forbes.com/sites/greatspeculations/2016/12/29/amazon-web-services-2016-in-review/#6044277d2c28

Un millón de empresas en la nube de Amazon. (s.f.). Recuperado el 16 de Enero de 2019, de https://www.elmundo.es/tecnologia/2014/11/14/54656ac6268e3ed9408b456d.html

Unidades de Negocio. (2019). Recuperado el 12 de Enero de 2019, de https://www.teradyne.com/

Windows 2008 R2 End of support. (s.f.). Recuperado el 6 de Julio de 2019, de https://www.microsoft.com/en-us/cloud-platform/windows-server-2008

Anexos

Anexo 1

Teradyne BPIT Security checklist

Complete this checklist early in the project lifecycle (design phase) for any new project that goes through the PMO or the WorkCentre process. Completing this checklist does not mean a further review is not needed; this decision lies solely with the BPIT Security and Risk and Compliance team.

All Security Reviews should be reviewed and approved by a member of the BPIT Security, Risk and Compliance Team;

- Aarón Aguilar
- Graham Banks
- Anne-Marie Zuchowski
- Pankaj Desai

Selection Criteria

A Security Review is required if you answer "Yes" to any of the below;

1. Is this a new solution? (Never implemented before at Teradyne)?
2. Is this a significant change to an existing solution? (adding a new module, moving from on-prem to cloud, etc.)?
3. Does the solution house sensitive data (e.g. private, personal, customer confidential, Teradyne confidential, export controlled/ITAR)?
4. Is the solution subject to SOX controls (part of our in scope SOX list)?
5. Is the solution accessed by non-Teradyne owned equipment (smartphone, home PC, contractor PC, etc.)?
6. Is the solution accessed by any non-Teradyne personnel (customers, contractors, suppliers, etc.)?

Checklist

SOLUTION INFORMATION	
Solution Name	
BPIT Contact/Owner	
Business Contact/Owner	
Solution Description	
Solution Purpose	
Cloud or On-Premise	
Architecture Diagram	

CHECKLIST – If you do not know the answer to a question and cannot find it out, select No.		
Response	**Control Question**	**Comment**
☐ Yes ☐ No	Will the solution be Public Facing?	Is the solution accessible from outside of the Teradyne Network?
☐ Yes ☐ No	Is this a Cloud SaaS solution?	Complete Cloud Security Checklist at the end of this document in addition to these questions
☐ Yes ☐ No	Has a Rapid 7 Vulnerability scan been run? N/A for cloud solutions	Assume no scan has been run and one needs to be done. All Critical vulnerabilities must be remediated and the VA Scan agent

		installed on all devices where supported.
☐ Yes ☐ No	Is data encrypted during transit?	Describe how the data is encrypted and to what level?
☐ Yes ☐ No	Is data encrypted at rest?	Describe how the data is encrypted and to what level?
☐ Yes ☐ No	Does the password policy meet the Teradyne BPIT Standard?	Provide proof of this for all types of accounts
☐ Yes ☐ No	Are accounts removed/disabled when no longer required?	Describe process and provide proof
☐ Yes ☐ No	Are the administrator accounts stored in CyberArk?	All Administrator accounts should be stored in CyberArk, please provide a Business Justification if this should not be the case.
☐ Yes ☐ No	Will the solution house sensitive data?	(e.g. private, personal, customer confidential, Teradyne confidential, export controlled/ITAR)?
☐ Yes ☐ No	Does the solution support SSO and SAML authentication?	We use Active Directory and IBM SDS for SSO and SAML authentication. Does it support one or both of these?

☐ Yes ☐ No	Has this solution gone through a commissioning checklist and all items completed?	All items on the new server commissioning checklist must be met.
☐ Yes ☐ No	Is this solution used by Teradyne employees only?	Describe how employees and non-employees will use this tool
☐ Yes ☐ No	Is this solution used by Teradyne standard endpoints or accessible by other devices, i.e. smartphones, non-Teradyne machines?	

BPIT Cloud Security Checklist

CHECKLIST – To be completed if you said Yes to is this a Cloud SaaS solution.		
Response	**Control Question**	**Comment**
☐ Yes ☐ No	Is the vendor certified against a well-known security framework?	NIST-800, ISO-27001, SOC 1 SOC 2. Describe which one and provide certificate where applicable
☐ Yes ☐ No	Does the vendor conduct, at minimum, a yearly penetration test?	Request summary of results and remediation work from the vendor and attach here
☐ Yes ☐ No	Does the vendor have and maintain a Security & Incident Response process (SIRT)?	Does the vendor inform the customer if there is a Security

CHECKLIST – To be completed if you said Yes to is this a Cloud SaaS solution.		
Response	**Control Question**	**Comment**
		incident that impacts the customer instance.
☐ Yes ☐ No	Will the cloud solution house sensitive or Personal data?	(e.g. private, personal, customer confidential, Teradyne confidential, export controlled/ITAR)?
☐ Yes ☐ No	Is the vendor listed on the Gartner Magic Quadrant?	Describe position (top leader, niche, visionary, etc)
☐ Yes ☐ No	Does the vendor execute yearly disaster recovery exercises?	