

Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

Diseño de un plan de seguridad basado en mejores prácticas y estándares para asegurar el acceso y operación de computación en la nube en Teradyne Inc

Javier Zamora Knudsen

Abril, 2021

Declaratoria de derechos de autor

Yo Javier Zamora Knudsen, autor de este documento de Tesis con título: “Diseño de un plan de seguridad basado en mejores prácticas y estándares para asegurar el acceso y operación de computación en la nube en Teradyne Inc” 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

Quiero agradecer a todas las personas que estuvieron a mi alrededor durante el proceso de la creación de este documento, por su paciencia, consejo y comprensión.

A Teradyne Inc. por permitirme desarrollar el trabajo final de graduación y a todas las personas involucradas en la recopilación de información.

Quiero dedicarle este trabajo a la familia Zamora Knudsen, en especial a mi mamá, por el apoyo incondicional.

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Zamora Knudsen Héctor Javier.**

MIGUEL PEREZ MONTERO (FIRMA)

M. Sc. Miguel Pérez Montero
Tutor

AARON DAVID AGUILAR ELIZONDO (FIRMA)
Digitally signed by AARON DAVID AGUILAR ELIZONDO (FIRMA)
Date: 2021.07.13 09:47:07 -06'00'

MPS. Aarón Aguilar Elizondo
Lector 1

IGNACIO TREJOS ZELAYA (FIRMA)
Firmado digitalmente por IGNACIO TREJOS ZELAYA (FIRMA)
Fecha: 2021.07.15 21:23:20 -06'00'

M. Sc. Ignacio Trejos Zelaya
Lector 2

San José, Costa Rica, 09 de julio de 2021

Tabla de contenido

Índice de tablas iii
Índice de ilustraciones iv
Abstract 1
Capítulo 1. Introducción 2
1.1 Generalidades 2
1.2 Antecedentes del problema 2
1.3 Definición y descripción del problema 3
1.4 Justificación 4
1.5 Viabilidad 5
1.5.1 Punto de vista técnico 5
1.5.2 Punto de vista operativo 6
1.5.3 Punto de vista económico 7
1.6 Objetivos 8
1.6.1 Objetivo general 8
1.6.2 Objetivos específicos 8
1.7 Alcances y limitaciones 9
1.7.1 Alcances 9
1.7.2 Limitaciones 9
1.8 Marco de referencia organizacional y socioeconómico 10
1.8.1 Historia 10
1.8.2 Tipo de negocio y mercado meta 11
1.8.3 Misión, visión y valores 11
1.8.4 Políticas institucionales 12
1.9 Estado de la cuestión 12
1.9.1 Planificación de la revisión 12
1.9.1.2 Selección de fuentes 16
1.9.1.2.1 Definición del criterio de selección de fuentes 16
1.9.1.2.2 Lenguaje de estudio 16
1.9.1.2.3 Identificación de fuentes 16
1.9.2 Ejecución de la revisión 18
1.9.2.1 Ejecución de la selección en la fuente IEEE Digital Library 19
1.9.2.1.1 Selección de estudios iniciales 19
Capítulo 2. Marco Conceptual 20
2.1 Conceptos sobre contenido 20
Capítulo 3. Marco metodológico 24

3.1 Tipo de investigación 24
3.2 Alcance investigativo 24
3.3 Enfoque 24
3.4 Diseño 24
3.5 Población y muestreo 25
3.6 Instrumentos de recolección de datos 25
3.7 Técnicas de análisis de información 25
3.8 Estrategia de desarrollo de la propuesta 25
Capítulo 4. Análisis del diagnóstico 27
Capítulo 5. Propuesta de solución 39
5.1 Desarrollo del estándar de seguridad 39
5.2 Desarrollo del manual de implementación 54
Capítulo 6. Conclusiones y recomendaciones 58
6.1 Conclusiones 58
Referencias 60
Apéndice A 62
A1.2 Evaluación de la calidad de los estudios. 62
A1.3 Revisión de la selección 63
A1.4 Extracción de información 63
A2 Ejecución de la selección en la fuente ACM Digital Library 64
A2.1 Selección de estudios iniciales 64
A2.4 Ejecución de la selección en la fuente Google Scholar 65
A2.4.1 Selección de estudios iniciales 65
A2.4.2 Evaluación de la calidad de los estudios 65
A2.4.4 Extracción de información 68
Apéndice B 74
Apéndice C 82

Índice de tablas

Tabla 1 Salario anual de profesiones relacionadas con el tema en el área de Boston, según el sitio Glassdoor.com 7

Tabla 2 *Estimado de costo en recurso humano basado en salario de tabla 1 y horas promedio de proyectos similares* 7

Tabla 3 *Listado de palabras* 13

Tabla 4 Resumen de varios servicios y sus ataques asociados 31

Tabla 5 Matriz de controles del Cloud Security Alliance 35

Tabla 6 *Resultados de búsqueda de IEEE Digital Library* 62

Tabla 7 *Detalle de resultados de búsqueda de IEEE Digital Library* 64

Tabla 8 *Resultados de búsqueda de Google Scholar* 66

Tabla 9 *Extracción fuente 1* 68

Tabla 10 *Extracción fuente 2* 69

Tabla 11 *Extracción fuente 3* 70

Tabla 12 *Extracción fuente 4* 71

Tabla 13 *Extracción fuente 5* 72

Índice de ilustraciones

Ilustración 1 *Nube de palabras con términos más utilizados*..... 20

Ilustración 2 *Diagrama de términos a definir. Confeccionado por el autor* 21

Ilustración 3 *Traducción de taxonomía de seguridad para servicios en la nube* (I Indu, 2018)... 28

Ilustración 4 *Diagrama de flujo para decisión de inclusión de dominios en propuesta de solución. Confeccionado por el autor.* 37

Ilustración 5 *Diagrama de dominios incluidos y excluidos en la propuesta de solución. Confeccionado por el autor.* 38

Ilustración 6 Modelo de responsabilidad compartida (AWS, 2021) 49

Ilustración 7 Modelo de responsabilidades compartidas para los diferentes servicios en la nube (Microsoft Azure, 2019)..... 50

Ilustración 8 *Valor SJR de la publicación según Scimago* 62

Ilustración 9 *Gráfico de citas en los primeros años de publicación* 63

Ilustración 10 *Captura de resultados de ACM Digital Library* 65

Ilustración 11 *Captura de resultados de Google Scholar* 65

Ilustración 12 *Gráfico de distribución de publicación por año* 65

Abstract

La necesidad de tener acceso a poder computacional en diferentes partes del mundo a corto plazo, y una reducción de costos de capital, ha causado una proliferación de compañías que adoptan Infraestructura como servicio (IaaS) dentro de su oferta para proveer soluciones de tecnologías de la información. Tal contexto causa que los diseños de infraestructura evolucionen y, con ellos, la manera en la cual se accede a los recursos. Por ende, la estrategia de seguridad de la información debe adaptarse e incluir métodos para asegurar estas nuevas plataformas y otras superficies de ataque. El objetivo de este trabajo es desarrollar un plan de seguridad para la compañía Teradyne Inc., capaz de satisfacer estos nuevos requisitos.

Palabras clave: computación en la nube, seguridad en la nube, Identity Access Management, aporte, innovación, viabilidad, alcances, limitaciones.

Capítulo 1. Introducción

1.1 Generalidades

Debido a que el presente trabajo expone fallas de seguridad y menciona funcionalidades nuevas en el mercado que pueden representar ventajas competitivas, el patrocinador ha pedido que el contenido de este trabajo se mantenga confidencial por 5 años. Este corresponde al tiempo suficiente para poder implementar las recomendaciones descritas y alcanzar un mayor nivel de madurez en cuanto a seguridad operacional en la nube.

El producto final está basado en métodos propuestos por organismos con reconocimiento en el campo de computación en la nube, entes como el Cloud Security Alliance y NIST.

1.2 Antecedentes del problema

Teradyne es una empresa dedicada a la creación de equipos para pruebas electrónicas automatizadas sobre circuitos digitales y memoria, con el fin de reducir el factor de errores en la producción de estos dispositivos. Cuenta con sistemas para soluciones de automatización industrial, que incluyen robots colaborativos y automatización de tareas para fabricantes de equipos y circuitos electrónicos.

Para cubrir su cartera de servicios, la empresa utiliza Infraestructura como Servicio (IaaS). Inicialmente la solución que se implementó con Microsoft Azure requería ser entregada lo más rápido posible, debido a limitaciones impuestas sobre importaciones de China por el gobierno de Estados Unidos. De este modo, se inició la cuenta con un usuario y una clave local de Azure. Conforme se incrementó la cantidad de personal de Tecnologías de Información con acceso a los servicios para

implementar servidores y otros activos, se hizo evidente la falta de autenticación individualizada y de separación de roles, además del registro de acciones por cada uno de los individuos.

Los servicios en *Amazon Web Services* (AWS, por sus siglas en inglés) iniciaron como una prueba de concepto pero rápidamente esta plataforma se convirtió en un servicio usado para hospedar múltiples servidores y servicios; sin embargo, esta también utiliza una sola cuenta de autenticación local. El personal tiene ideas para poder asegurar el acceso pero no tienen tiempo para implementarlas y no están seguros si serán las más adecuadas o si son suficientemente seguras. Lo anterior, principalmente, porque ninguno de ellos es profesional de la seguridad de información.

1.3 Definición y descripción del problema

La compañía no cuenta con un marco de referencia para definir estándares de seguridad a utilizar en servicios de infraestructura como servicio. Actualmente, se utiliza un solo usuario, lo cual dificulta la separación de tareas. Por ejemplo, un administrador de bases de datos cuya tarea es hacer un cambio, usa el mismo usuario que la persona encargada de administrar los recursos de los servidores. Por ende, cada persona tiene la capacidad de afectar, modificar o hasta eliminar otras partes de la infraestructura en la nube, bajo riesgo de afectar el resto de los servicios hospedados.

Por otro lado, no se tiene un control explícito sobre los gastos de los servicios consumidos y cual departamento de Tecnologías de Información está generándolos, para poder calcular costos en los proyectos de implementación y en el retorno de

inversión. Adicionalmente, no existe una manera de mantener trazabilidad sobre los cambios en la infraestructura ni de saber quién los realizó, como sí existe en los servidores en sitio. Tales servicios se pueden acceder exclusivamente desde la red interna, con acceso vía túnel de VPN en lugares estratégicos.

Otro aspecto importante por destacar es que, debido a la complejidad técnica de los productos que ofrece la compañía, se brinda entrenamiento para poder operarlos eficientemente. Tradicionalmente, esto se ha ofrecido de manera presencial en pocas oficinas alrededor del mundo. Las restricciones de viaje implementadas en respuesta a la pandemia de la COVID-19 evidenciaron la necesidad de proveer el servicio de forma remota, de manera que el cliente pueda conectarse a una clase virtual y tenga acceso a equipos de prueba para poder realizar ejercicios y laboratorios.

Lo anterior hace que se requiera tener acceso a recursos en la nube, por medio de Internet, por primera vez desde que se implementaron estas soluciones. Debido a esto se requiere un sistema de ingreso más robusto, para implementar un portal de acceso seguro a los recursos de IaaS, que pueden ingresar a la red interna. Dado que la intención es virtualizar los equipos en la nube de Azure, el acceso vía VPN corporativo es redundante porque, a pesar de que provee autenticación de factor múltiple, viene a degradar el tiempo de respuesta, ya que el tráfico viaja hasta uno de los portales de VPN, para luego ser ruteado hasta la nube de Microsoft.

1.4 Justificación

La investigación y creación de los documentos señalados en el alcance crean un marco de trabajo para poder proveer seguridad adecuada a los servicios de

infraestructura en la nube, tanto en servicios en uso, como en nuevas plataformas. Esto ayuda a tener una base inicial para asegurar los servicios y evitar exponer información confidencial, así cómo contener el acceso administrativo únicamente a los servicios requeridos por el personal de tecnologías de información. Así, se evita afectación de servicios e incrementos en facturación por errores humanos.

Habilitar el acceso externo para entrenamiento de clientes da la posibilidad de dar capacitación, cuando el servicio ha estado inactivo los últimos cinco meses debido a la pandemia y a la imposibilidad de viajar a los centros de entrenamiento. Lo anterior se debe hacer de manera que el departamento de entrenamiento pueda proveer los servicios de una manera remota sin exponer el resto de la arquitectura en ese servicio en la nube o en la red interna.

1.5 Viabilidad

El tema del trabajo final de graduación fue aprobado por el director de infraestructura de la empresa y el oficial en jefe de la seguridad de la información. A su vez, pusieron a disposición horas de recursos dentro de la compañía y la capacidad de hacer pruebas fuera de horas de operación.

1.5.1 Punto de vista técnico

Durante la carrera se han discutido temas relacionados a asegurar ambientes de nube, a través del estudio de estándares en el tema, como los propuestos por el Cloud Security Alliance, NIST e ISO. Se han utilizado servicios de infraestructura como servicio, como AWS y Azure, para llevar a cabo laboratorios sobre diferentes temas. Aunado a ello, se han estudiado en detalle

técnicas de autenticación y autorización, como acceso de menor privilegio, arquitectura de cero confianza y control de acceso basado en roles.

Asimismo, en el rol previo como ingeniero de seguridad de redes y certificado como Cisco Certified Security Professional (CCSP, por sus siglas en inglés), el autor ha tenido que diseñar e implementar, a menor escala y de manera local, equipos de red de una manera segura. Esto, en combinación con una investigación adecuada y trabajos de expertos en el campo, capacita al graduando a llevar a cabo la investigación y proveer una solución adecuada sobre este tema.

1.5.2 Punto de vista operativo

Al ser un tema de interés para la compañía, tanto el director de infraestructura como el oficial en jefe de la seguridad de la información autorizaron crear un proyecto interno, para poder asignar tiempo del personal que posee la información de funcionamiento actual y es capaz de dar opiniones adecuadas sobre las propuestas dentro del trabajo. También se autorizó al estudiante a ser parte de las reuniones y discusiones relacionadas con el tema de computación en la nube, con el objetivo de mantenerse al día y de proveer sugerencias relacionadas con la infraestructura y la seguridad de los servicios.

Los alcances del trabajo final de graduación se enfocaron en crear documentación y estándares, pero se consideró la posibilidad que la compañía quisiera implementar dichas medidas durante el proceso. Bajo esas condiciones, la mayoría de los cambios van a ser relacionados con el acceso del departamento de tecnología de información a los recursos para administración, no se espera impacto sobre los servicios.

En cualquier caso, se contó con un fin de semana por trimestre, donde el gerente de control de cambios de tecnología de información podía autorizar ventanas de mantenimiento que no afectaran el funcionamiento de los servicios hospedados en la nube; esto, en aquellos casos donde los departamentos en cuestión decidieron implementar sugerencias provenientes de este análisis.

1.5.3 Punto de vista económico

El sitio Glassdoor.com describe el salario promedio tanto de un ingeniero con experiencia en *cloud computing,* como de un ingeniero en Ciberseguridad para el área de Boston, donde se encuentra la compañía. A continuación se presentan los detalles en la tabla:

Tabla 1. *Salario anual de profesiones relacionadas con el tema en el área de Boston, según el sitio web Glassdoor.com*

	Salario Anual	Salario Mensual	Salario por Hora	Salario hora con cargas sociales
Cloud Engineer	$ 120,826.00	$ 10,068.83	$ 62.93	$ 91.25
Cybersecurity Engineer	$ 102,414.00	$ 8,534.50	$ 53.34	$ 77.34
Promedio	$ 111,620.00	$ 9,301.67	$ 58.14	$ 84.30

Al considerar el nivel de investigación, los documentos generados y la duración promedio del proyecto en la compañía, se estimaron 9 meses y 40 horas dedicadas al mes.

Tabla 2. *Estimado de costo en recurso humano basado en salario de tabla 1 y horas promedio de proyectos similares*

	Salario hora con cargas sociales	Horas al mes de proyecto	Meses requeridos para completar el proyecto	Total
Ingeniero de proyecto	$ 84.30	40	9	$ 30,346.69

El costo aproximado del proyecto en recurso humano ha sido de $30.346,69, mismo que absorbió el estudiante al hacer la investigación.

1.6 Objetivos

Se ha usado la taxonomía original de Bloom de 1956 para plantear los objetivos de esta investigación, debido a su robustez y a su uso como estándar de facto en el sistema educativo costarricense.

1.6.1 Objetivo general

Diseñar un plan de seguridad basado en las mejores prácticas y estándares para asegurar el acceso y operación de computación en la nube en Teradyne Inc.

1.6.2 Objetivos específicos

- Definir las medidas de seguridad aplicadas en instancias de computación en la nube, utilizadas en la compañía por medio de reconocimiento, para determinar la postura de seguridad en los servicios en la nube actuales.
- Replantear mejoras inmediatas a la seguridad aplicada en los diferentes proveedores en uso, basado en mejores prácticas, para proveer una línea base inicial de mejoras.
- Escoger estándares de seguridad en la nube aplicables a inquilinos mediante la utilización de infraestructura como un servicio (IaaS), para estandarizar técnicas de seguridad.
- Analizar las medidas de seguridad propuestas en los estándares versus las aplicadas actualmente en producción, así como definir cuáles son las medidas necesarias y pertinentes para recomendar su aplicación.

1.7 Alcances y limitaciones

1.7.1 Alcances

Se entrega un documento digital llamado “Manual para implementación de medidas de seguridad en infraestructura como servicio en Teradyne”, que detalla el estándar de seguridad por aplicar en servicios de computación en la nube e infraestructura como un servicio en la compañía.

Además, se provee de un documento digital llamado “Manual para implementación de medidas de seguridad en infraestructura como servicio en Teradyne”, con las mejoras por aplicar a los servicios actuales, divididas por proveedor. Parte del documento de mejoras incluye una sección sobre como implementar cajones de arena *(sand boxes)* en los servicios de IaaS; lo cuales pueden ser utilizados por clientes de Teradyne al realizar el entrenamiento sobre el uso de los diferentes productos disponibles; un servicio que actualmente es provisto solo de manera presencial.

1.7.2 Limitaciones

En este plan no se consideraron las compañías satélites cuya infraestructura y procesos de tecnología de información no estuvieran integrados con los de Teradyne. Este incluye empleados y contratistas de Teradyne, Eagle Test Systems y Nextest; no obstante, los documentos pueden ser usados como base para integrar servicios del resto de las compañías.

No se consideraron las instancias en uso de software como servicio (SaaS) utilizadas por la compañía, ya que actualmente utilizan *Single Sign-On* (SSO, por sus siglas en inglés) o se autentica directamente contra el usuario de dominio en el Active Directory de Teradyne.

Se consideraron mejoras a características de seguridad disponibles en las plataformas en cuestión y el uso de servicios externos como corredores de seguridad en la nube (CASB). Se contempló el acceso de clientes a servicios de computación en la nube con la finalidad de generar entrenamiento en los productos de Teradyne.

1.8 Marco de referencia organizacional y socioeconómico

1.8.1 Historia

Teradyne fue fundado en 1960 en Boston por Alex d'Arbeloff y Nick DeWolf, quienes fueron compañeros de clase en el Instituto Tecnológico de Massachusetts (MIT por sus siglas en inglés) a finales de los 40s. El nombre fue creado para representar una presencia enérgica, 1.000.000.000.000 dinas = 10 meganewtons.

En 1961 vendieron su primer producto: un probador puerta lógica de diodos a Raytheon. Desde ese momento, por medio de innovaciones internas y adquisiciones estratégicas, Teradyne ha expandido su portafolio para cumplir las expectativas de los avances tecnológicos y las necesidades de los clientes y fabricar tales avances. Actualmente, sus soluciones habilitan la posibilidad de correr pruebas sobre circuitos utilizados en diferentes dispositivos, como automóviles, teléfonos celulares, computadoras y equipo médico.

1.8.2 Tipo de negocio y mercado meta

El negocio principal de Teradyne es la creación de equipos que ejecutan pruebas electrónicas automatizadas sobre circuitos digitales varios y memoria, para reducir el factor de errores al producir equipos electrónicos. Además, tiene sistemas para soluciones de automatización industrial donde se incluyen robots colaborativos y automatización de tareas. El mercado meta está constituido por fabricantes de equipos y circuitos electrónicos, los cuales operan mayoritariamente en Estados Unidos, Asia y Europa.

1.8.3 Misión, visión y valores

Teradyne trae al mundo los productos más innovadores del mercado, a través de pruebas avanzadas y soluciones de automatización industrial. Esta compañía ayuda a otras de todos los tamaños y en diversos mercados para automatizar manufactura y entregar productos de alta calidad, de manera rápida y rentable. Sus clientes son líderes en sus mercados respectivos y, con ellos, estos ayudan al mundo a mejorar como se vive, trabaja e innova.

Entre los valores principales de la compañía de encuentran los siguientes:

> Una compañía sin puertas. Valoramos conversaciones cándidas y abiertas. La innovación es impulsada por la colaboración, nosotros empoderamos a nuestros empleados, para que usen su voz y compartan sus ideas.
>
> Honestidad e integridad. En Teradyne, somos transparentes en cuanto a nuestra estrategia corporativa y como llevamos a cabo los

> negocios. Creemos que la información es valiosa, cuando está disponible a todos y tiene la capacidad de ayudar a tomar las decisiones correctas.
>
> Los clientes cuentan con nosotros. Mantenemos un compromiso firme de inculcar confianza a nuestros clientes. Hacemos lo necesario para anticipar las necesidades, exceder expectativas y entregar soluciones y soporte superior. De esta manera aseguramos el éxito de nuestros clientes. (Teradyne. Inc, 2021)

1.8.4 Políticas institucionales

No existen políticas institucionales donde se aborde el tema. En el documento Teradyne Information Security Policy se detalla el funcionamiento básico de tipos de autenticación, políticas de claves, acceso a SaaS y servicios digitales externos. Todo desde un punto de vista de acceso interno o de *software* como servicio. La idea fue utilizar los mismos lineamientos para generar un estándar con más detalle técnico del acceso a servicios de computación en la nube, restricciones y permisos.

1.9 Estado de la cuestión

Para definir el estado actual, este estudio se basa en el formato propuesto en Systematic Review in Software Engineering (Jorge Biolchini et al, 2005).

1.9.1 Planificación de la revisión

Problema

Debido a las tensiones entre Estados Unidos y China, en los últimos años se han desarrollado una serie de restricciones tarifarias y arancelarias cuyo cambio se

da con mucha rapidez y requieren que las compañías cumplan con requisitos para evitar multas. Debido a esto, la implementación de servidores y servicios en la nube se ha acelerado, teniendo en mente solucionar problemas fronterizos y dejando de lado la implementación bajo estándares de seguridad adecuados para operar en este nuevo ambiente.

Pregunta de investigación

Basado en el problema descrito anteriormente, se formula la siguiente pregunta de investigación:

¿Qué trabajos se han llevado a cabo en el área de implementación de seguridad para Infraestructura como servicio (IaaS), basado en estándares aceptados en la industria, que puedan apoyar la seguridad de Teradyne en este campo?

Palabras clave y sinónimos

A continuación, se presenta un listado de palabras y términos a utilizar para crear las cadenas de búsqueda. Dado que la mayoría de desarrollo en este tema se encuentra en el idioma inglés, se utilizan términos de búsqueda en ese idioma.

Tabla 3. *Listado de palabras*

Palabra	**Termino en inglés**
Nube	Cloud
Seguridad	Security
Administración	Management
Tecnologías de información	IT
Infraestructura como servicio	IaaS

Manejo de acceso por identidad	IAM
Administración de identidad	IDM
Ente regulador de seguridad en la nube	CSA
Autenticación	Authentication

Fuente: Elaboración propia.

Intervención

Basado en los resultados, se extraen los documentos en los cuales se propone un método de autenticación y una autorización para ambientes de nube, ya sea en la solución propuesta o a través de una herramienta de terceros. Preferiblemente, mediante el uso de marcos de referencia de Cloud Security Alliance, NIST o ICS2.

Control

Al inicio de la investigación, se cuenta con conocimiento de los estándares más utilizados en la industria, pero no con conocimiento de implementaciones o de la creación de un estándar de seguridad basada en los mismos.

Efectos

Se esperaba encontrar documentos que sustentasen el uso de los estándares mencionados y la recurrencia a soluciones implementadas nativamente en los proveedores de nube, como *Identity Access Management* (IAM) para lograr un acceso basado en roles y un principio de mínimo privilegio.

Medida de salida

Se buscaron documentos de calidad y recientes, de sitios académicos especializados en ciberseguridad o seguridad de la información. Se hizo una revisión de los documentos resultantes.

Población

La población está compuesta por el departamento de tecnologías de información de la compañía que tiene acceso administrativo a los recursos de computación en la nube. Entre ellos se planea incluir al departamento de entrenamiento.

Aplicación

Esta investigación buscó beneficiar a personal en el área de tecnologías de la información, mediante la incursión en infraestructura como servicio de una manera segura, para hospedar múltiples servidores y sistemas de varios departamentos dentro del área de TI.

Diseño experimental

Durante el diseño experimental de este trabajo se hicieron análisis y la clasificación de muestras de resultados, para asegurar su calidad y su relevancia con el tema desarrollado.

1.9.1.2 Selección de fuentes

1.9.1.2.1 Definición del criterio de selección de fuentes

Se utilizó como criterio fuentes reconocidas, con documentos mencionados en otras investigaciones, con respaldo teórico y práctico de sus resultados. También se consideró aquellas con información suficiente para que los resultados pudieran ser replicables. Además, se tomaron en cuenta otras investigaciones hechas en universidades del país.

1.9.1.2.2 Lenguaje de estudio

Se concentraron las búsquedas en inglés, ya que la mayoría de información asociada al tema se encuentra en ese idioma. No obstante, se utilizan también las cadenas de búsqueda en español para cubrir la posible existencia de documentos relevantes en ese idioma.

1.9.1.2.3 Identificación de fuentes

Método de selección de fuentes

Se utilizaron motores de búsqueda tanto de repositorios académicos como motores generales, con un nivel más granular de detalle para encontrar resultados relevantes.

Cadena de búsqueda

Se utilizó la siguiente lista de cadenas para búsquedas preliminares con sintaxis de búsqueda avanzada ya como operadores AND, OR y intitle:

intitle:"cloud security" AND management AND IT AND authorization

intitle:cloud AND security AND management AND IT AND authorization AND iaas AND aaa

intitle:cloud AND security AND management AND IT AND authorization AND iaas AND csa

intitle:cloud AND security AND management AND IT AND authorization AND iaas AND iam AND idm

Lista de fuentes

Se consideraron como fuentes primarias sitios con alta reputación y trayectoria en temas de tecnología:

1. IEEE Digital Library
2. ACM Digital Library
3. Sistemas de Bibliotecas, Documentación e Información de la Universidad de Costa Rica
4. Resultados directos de Google académico, con una calificación aceptable en Scimago Journal & Country Rank

1.9.1.2.4 Selección de fuentes tras la evaluación

La selección de resultados dependió de que los documentos resultantes fuesen relevantes a la investigación, fuesen accesibles y con fuentes verificables.

1.9.1.2.5 Comprobación de las fuentes

En el momento de la escogencia, no se contaba con criterio experto para escoger las fuentes, por ende, se utilizaron herramientas como Scimago Journal & Country Rank para analizar las diferentes métricas de las fuentes; además de ello, se consideró la relevancia de la cuenta con el tema en cuestión.

1.9.1.3 Selección de los estudios

1.9.1.3.1 Definición del criterio de inclusión y exclusión de estudios

Se incluyeron los resultados de las cadenas de búsqueda propuestas en la sección 1.9.1.2.3. Se excluyeron los resultados en las siguientes condiciones: Se excluyó el tema de autenticación y autorización para *software* como servicio. No se utilizaron soluciones integrables con sistemas de autenticación actual, como Active Directory, LDAP, RBAC, TACACS y RADIUS.

1.9.1.3.2 Definición de tipos de estudio

Los estudios *in vivo* e *in silico* parecieron ser los más adecuados para una investigación con implicaciones en implementación, como esta.

1.9.1.3.3 Procedimiento para la selección de los estudios

Como procedimiento se procedió a revisar el *abstract* de cada documento en busca de información relevante para la investigación. En caso de tener información destacable, se procedió a analizar el documento completo, para confirmar su utilidad para la investigación en cuestión. En caso de que cumpliera con alguno de los criterios de exclusión, se descartó de los resultados relevantes.

1.9.2 Ejecución de la revisión

1.9.2.1 Ejecución de la selección en la fuente IEEE Digital Library

1.9.2.1.1 Selección de estudios iniciales

Detalles de la selección de estudios iniciales se detallan en el Apéndice A.

Capítulo 2. Marco Conceptual

Basado en el estado de la cuestión, se creó una nube de palabras con los términos más utilizados. Esta se presenta a continuación:



Ilustración 1. *Nube de palabras con términos más utilizados. Fuente: Elaboración propia.*

2.1 Conceptos sobre contenido

Basado en la información extraída de la nube de palabras, se pueden identificar algunas que pertenecen a términos utilizados en la investigación. Se procede a diagramar los términos necesarios:

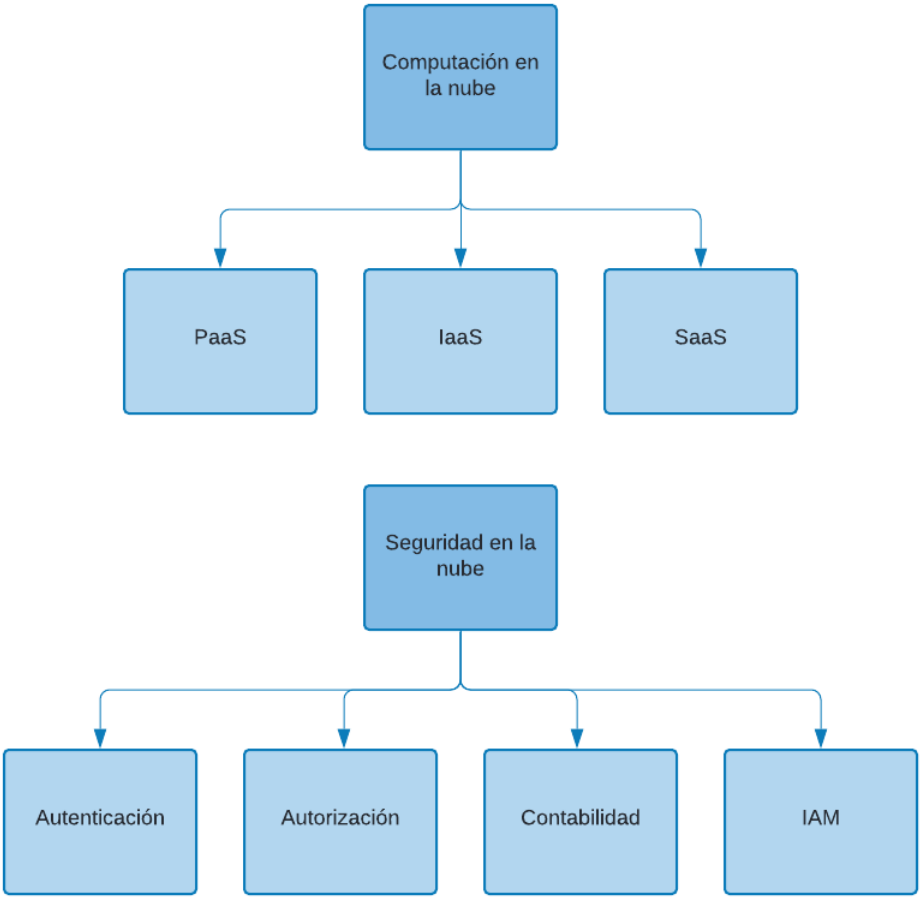


Ilustración 2. *Diagrama de términos a definir. Fuente: Elaboración propia.*

Estos son los términos contextualizados al tema:

- **Computación en la nube:** La definición de la nube puede parecer poco clara pero, básicamente, es el término utilizado para describir una red global de servidores donde cada uno posee una función única. No es una entidad física, sino una red enorme de servidores remotos de todo el mundo conectados para funcionar como un único ecosistema, los cuales están diseñados para almacenar y administrar datos, ejecutar aplicaciones o entregar contenido o servicios, como *streaming* de vídeos, correo web, *software* de ofimática o medios sociales. En lugar de acceder a archivos y datos en un equipo personal

o local, se accede a ellos en línea desde cualquier dispositivo conectado a Internet, es decir, la información está disponible en cualquier lugar y cuando se le necesite. (Microsoft, 2020)

- SaaS: Es una forma de hacer disponible *software* y soluciones de tecnología por medio de la internet, como un servicio. Con ese modelo, la empresa no necesita instalar, mantener y actualizar *hardware* y *software*. El acceso es fácil y simple: solo es necesario conexión con la internet. (Microsoft, 2020)
- PaaS: Entorno de desarrollo e implementación completo en la nube, con recursos que permiten entregar todo, desde aplicaciones sencillas basadas en la nube hasta aplicaciones empresariales sofisticadas habilitadas para la nube. (Microsoft, 2020)
- IaaS: Infraestructura informática inmediata que se aprovisiona y administra a través de Internet. Cada recurso se ofrece como un componente de servicio aparte, solo es necesario alquilar un recurso concreto durante el tiempo que sea necesario. (Microsoft, 2020)

- **Seguridad en la nube:** La seguridad en la nube abarca una amplia gama de controles, tecnologías, normas y procedimientos usados para proteger los datos, la infraestructura y las aplicaciones basadas en la nube.
  - IAM: Sus siglas son de Identity and Access Management o gestión de identidad y accesos. Se refiere a las políticas y herramientas usadas por los departamentos de tecnología de información para asegurarse que las personas y las entidades tengan el nivel de acceso apropiado a los recursos técnicos de la organización.

- Autenticación: Proceso mediante el cual un usuario es acreditado para operar en un sistema.
- Autorización: Corresponde al proceso que ocurre normalmente luego de la autenticación. En este se contempla el requerimiento de utilización de algún recurso por parte del usuario.
- Contabilidad: Proceso mediante el cual se registra cualquier actividad considerada importante sobre la utilización de recursos, pedidos de autenticación y autorización, estadísticas u otros.

Capítulo 3. Marco metodológico

3.1 Tipo de investigación

La investigación fue de tipo aplicada, ya que pretendió utilizar el conocimiento existente, análisis de investigaciones creadas previamente, recomendaciones de los proveedores de nube más prevalentes y estándares creados para generar una política de seguridad para Teradyne.

3.2 Alcance investigativo

Por el tipo de información que se buscaba analizar y generar, el alcance de esta investigación fue considerado como exploratorio. Aunque existe suficiente información, existen múltiples variables que se introducen al hablar de un escenario real. La premisa es explorar las opciones de seguridad y buscar crear un estándar de compañía aceptable y capaz de repeler los ataques principales.

3.3 Enfoque

Se propuso un abordaje cualitativo, ampliamente usado en la implementación de estándares y en el área de seguridad.

3.4 Diseño

El diseño que se decidió utilizar es el evaluativo, dado que el producto final corresponde a documentos con potencial de funcionar como estándares en un campo de la compañía.

3.5 Población y muestreo

El muestreo fue no probabilístico, ya que se trabajó con un grupo de personas que trabajan en diferentes áreas y tienen información relevante sobre los procesos actuales o las políticas relacionadas.

3.6 Instrumentos de recolección de datos

La recolección de datos utilizó dos métodos diferentes: Por un lado, el análisis documental, para poder analizar documentos internos de la compañía, investigaciones de organizaciones, artículos en revistas científicas reconocidas y trabajos académicos relacionados al tema. Por otro lado, la observación de campo no experimental, basado en las arquitecturas ya implementadas y documentos técnicos de cada proveedor de nube.

3.7 Técnicas de análisis de información

Se utilizaron múltiples técnicas para graficar y ayudar en el análisis de la información, a saber:

- Diagramas de flujo de datos
- Mapas conceptuales

3.8 Estrategia de desarrollo de la propuesta

Se desarrolla la propuesta basada en una combinación de políticas existentes en la compañía en ámbitos similares, así como en planes creados con fines académicos de empresas con características similares y recomendaciones de proveedores líderes en el mercado. También se consideran compañías de investigación y consultoría,

además de entidades de investigar y promover buenas prácticas en temas relacionados con la seguridad de la información, cuyas propuestas se consideran estándares *de facto* por la industria.

Capítulo 4. Análisis del diagnóstico

El caso de uso inicial de computación en la nube dentro de la compañía es de acceso interno, esto reduce la superficie de ataque, ya que solo usuarios con acceso a la red tienen posibilidad de acceder a la infraestructura. A pesar de esto, el no tener una política de seguridad y medidas consistentes a través de los diferentes proveedores, da lugar a riesgos explotables en ataques horizontales.

Las facilidades propias de este modelo de infraestructura han causado que el departamento de tecnologías de información considere el uso de recursos de computación en la nube para implementar nuevas soluciones y proyectos. Lo anterior incrementa la cantidad de servicios funcionando desde infraestructura en la nube. Esto, añadido a nuevos requerimientos, como el del servicio de entrenamiento de clientes (que requiere acceso público a la nube desde Internet), viene a incrementar la superficie de ataque y la necesidad de controles estandarizados en los diferentes proveedores. Tampoco se descarta el accionamiento de nuevos proveedores de nube, para lo cual se requiere un marco de referencia de controles necesarios de implementar.

I Indu, PMR Anand y V Bhaskar (2018) definen, en un diagrama, la taxonomía de seguridad para servicios en la nube. Este ayuda a entender los diferentes controles, protocolos y servicios por implementar:

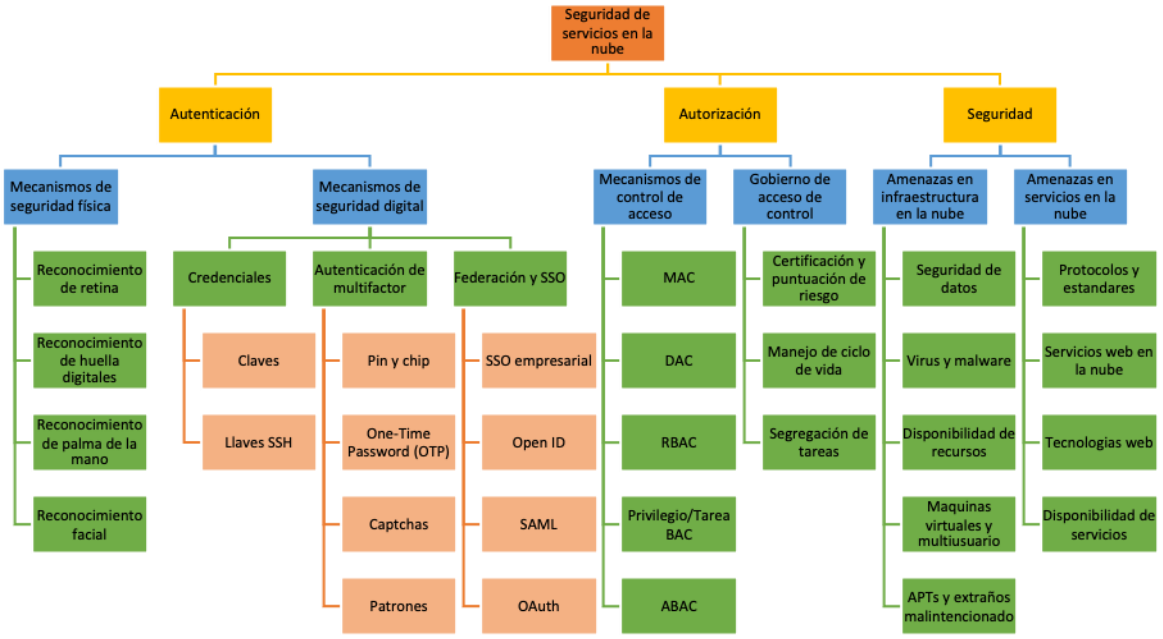


Ilustración 3. *Traducción de taxonomía de seguridad para servicios en la nube*. Fuente: I Indu, 2018.

Dentro de las primeras medidas que se consideran está el uso de algún tipo de credenciales para obtener acceso a los recursos. Fernandes, D.A.B., Soares, L.F.B., Gomes, J.V. et al (2014) definen credenciales como evidencia de autoridad, estatus, derechos de acceso y autorización. Esto evidencia que un usuario en particular está autorizado y tiene derecho a utilizar recursos o servicios. El uso de credenciales, como las contraseñas de un solo uso (OTP por sus iniciales en inglés), patrones y CAPTCHA[1] son maneras tradicionales para asegurar sistemas contra actividades maliciosas. Los mecanismos más comunes para gestionar credenciales de acceso para ambientes de nube son *Lightweight Directory Access Protocol* (LDAP) y tecnología *Microsoft Active Directory*. Ambos son gestionados por un proveedor

[1] CAPTCHA es una tecnología de desafío-respuesta que son utilizadas para determinar cuando el usuario es un humano o un programa automático. Siglas de Completely Automated Public Turing test to tell Computers and Humans Apart (prueba de Turing completamente automática y pública para diferenciar ordenadores de humanos).

externo o dentro de la infraestructura en la nube de la organización (Fernandes, 2014).

Ahora, al incrementar la cantidad de requerimientos para autenticación, se dificulta más un acceso no autorizado. Por tal motivo, la autenticación por múltiples factores ha pasado a tener una mayor tasa de adopción para acceso a Redes privadas virtuales (VPNs) corporativas y aplicaciones con información sensible o de índole financiera. I Indu, PMR Anand, V Bhaskar (2018) definen autenticación de múltiples factores como otro método para asegurar activos digitales y transacciones sobre Internet. Típicamente, OTPs, CAPTCHAs y patrones son usados como mecanismos secundarios de autenticación, junto con los credenciales.

La autenticación por múltiples factores provee capas adicionales de seguridad sobre la tradicional autenticación basada en credenciales. En transacciones financieras en línea, el servidor genera una contraseña de un solo uso, usando algoritmos específicos basados en su configuración. Posteriormente, la clave generada es enviada al usuario vía mensaje de texto al número de teléfono móvil registrado o por correo electrónico. Otro tipo de OTP es generado con la ayuda de generadores de *token* basados en hardware/software, estos son protegidos por un pin. Esta contraseña solo puede ser usada una vez y tiene un límite de tiempo para su uso (I Indu, 2018).

Una vez definidas las opciones de credenciales existentes y cuáles pueden ser utilizadas para las implementaciones actuales y futuras, lo siguiente es enfocarse en métodos de manejo de acceso, lo cual inicia por el procedimiento más común en *Microsoft Azure* y *Amazon AWS*: el IAM. La alianza de seguridad en la nube se refiere sobre al uso de IAM en ambientes de nube pública. El problema fundamental con la

computación en la nube es que la administración de identidad y manejo de accesos está a cargo de varias organizaciones, lo cual puede complicar el proceso. Por ejemplo, pueden presentarse situaciones donde se provisione el mismo usuario en docenas, o cientos de servicios en la nube diferentes. La herramienta principal a ser usada para resolver este problema es la federación, la cual se logra al construir relaciones de confianza entre organizaciones y reforzarlas a través de tecnologías estándar. (Alliance, 2020)

Además, las plataformas en la nube tienden a tener un soporte más amplio para el modelo de control de acceso basado en atributos (ABAC) para IAM, el cual ofrece más seguridad y flexibilidad con respecto al control de acceso basado en roles (RBAC). Este es el modelo tradicional para reforzar la autorización y depende normalmente en un solo atributo (o rol definido). ABAC permite decisiones más granulares y dependientes de contexto porque incorpora múltiples atributos, como el rol, la localización, el método de autenticación, entre otros.

La literatura consultada indica que ABAC es el modelo favorito para la administración de control de acceso basado en la nube (Alliance, 2020). Es necesario tener esto en consideración al definir una solución de estándar de seguridad. En el rubro de la seguridad, se deben tomar en cuenta las amenazas de la infraestructura en la nube y como mitigarlas. Entre las más explotadas en equipos finales se pueden mencionar: los virus, el malware y las vulnerabilidades.

F Chen et al (2016) definen virus y *malware* como *software* malicioso que es programado para interrumpir operaciones de computación, el cual es utilizado para recopilar información sensible o tener acceso a sistemas de computación aislados (F.

Chen, 2016). La intención de este es actuar en contra de los requerimientos del usuario, causando daño serio en sistemas basados en la nube.

Los cibercriminales comparten *malware* y buscar que los usuarios instalen este en sus computadoras o equipos móviles con promesas falsas. La meta final de tales criminales es lograr control sobre la computadora o el equipo móvil. Cuando el *malware* está instalado, los atacantes pueden (potencialmente) tomar control sobre el equipo; mientras el mismo accede a servicios en la nube, el *malware* intenta infectar las máquinas virtuales en el ambiente de nube, para luego infectar todo usuario que se conecte a recursos en esa nube. Eventos de malware o ataques de este tipo ocurren frecuentemente en organizaciones, donde se busca penetrar la infraestructura de seguridad de la organización (F. Zhang, 2016).

En la tabla 4 se puede observar como I Indu et al propone opciones para mitigar ataques. A pesar de estar enfocado en *web*, hay soluciones para mitigación con sentido en otras arenas, entre estos ataques se encuentran el *malware* y virus:

Tabla 4. Resumen de varios servicios y sus ataques asociados

SERVICIO	**PROBLEMAS/ATAQUES**	**MITIGACIONES**
Protocolos y estándares	Secuestro de sesiones, ataques basados en red, robo de *cookies*, ataques de TLS	Uso de sesiones seguras, *software* eficiente de antivirus y *antimalware*
Servicios Web	Ataque de *spoofing* y de cobertura de protocolos	implementación de políticas de seguridad estrictas tanto en el

		receptor como en el emisor
Tecnologías Web	Ataques de sesión, ataques de manipulación, descarga de *malware*, vulnerabilidades del navegador	Análisis de vulnerabilidades y acciones preventivas
Disponibilidad de servicios	Ataques de inundación, reflexión de DNS y ataques de amplificación	Regular la cantidad de servicios e implementar una gran cantidad de servidores

Fuente: I Indu, 2018.

Se pueden utilizar soluciones de análisis de vulnerabilidades que corren tanto en servidores en sitio, como en la nube y en máquinas de usuarios finales; de este modo se puede tener un sistema de detección granular. T Liggett (2018) menciona que los cibercriminales se encuentran constantemente evolucionando sus tácticas para infiltrar redes y mantenerse ocultos de herramientas de seguridad. El uso conjunto del *software* de protección de estaciones de trabajo y plataformas de detección con la respuesta de estaciones de trabajo (EDR, por sus iniciales en inglés) incrementa la efectividad de detectar amenazas conocidas y desconocidas (Liggett, 2018). Por lo tanto, el modelo de deteccion de virus, malware y analisis de vulnerabilidades que se aplica tanto en los equipos finales como en los servidores locales dentro del perimetro de la compañía; es replicable.

Lo anterior deja un punto más en el resumen de servicios que vale la pena analizar, la disponibilidad de los mismos. Existen varias soluciones que son implementadas en diseños en infraestructuras de centros de datos internas. I Indu et al (2018) proponen una gran cantidad de servidores como parte de la solución, pero hay maneras más eficientes; por ejemplo, el uso de balanceadores de carga tanto en *software* como en *hardware*, para que el servicio pueda ser provisto por varios servidores a la vez, mediante el uso de diferentes algoritmos de distribución de carga. Además, se pueden implementar *firewall* de aplicaciones web (WAF por sus iniciales en inglés), los cuales inspeccionan el tráfico en la capa siete del modelo OSI[2]. Dado lo anterior, se hace posible la inspección de los paquetes de manera profunda, encontrando ataques específicos de protocolos web que otros *firewalls* pueden no detectar, además, se suma el hecho de estos poseen acceso a los certificados de los servidores que protegen, lo cual le da opción de tener acceso a ver el flujo de tráfico desencriptado y da paso a una inspección más eficiente y profunda. Tales *firewall* se implementan en la nube de manera virtual, cada proveedor tiene una solución para proteger servicios web: Microsoft, por ejemplo, implementa un servicio llamado *Azure Web Application Firewall* (Azure, 2021) y otro llamado *Azure Load Balancer* (Azure, What is Azure Load Balancer?, 2021).

Otro punto a considerar es que la infraestructura de nube da la posibilidad de proveer soluciones a ataques más difíciles de mitigar de manera local, o con un costo de mitigación muy elevado; por ejemplo, el ataque de denegación de servicio distribuido (DDOS por sus iniciales en inglés). Los proveedores de servicios en la

[2] El modelo de arquitectura de redes OSI es un modelo de referencia para los protocolos de la red. Es un estándar que tiene por objetivo conseguir interconectar sistemas de procedencia distinta para que estos pudieran intercambiar información sin ningún tipo de impedimentos debido a los protocolos con los que estos operaban de forma propia según su fabricante.

nube tienen la capacidad de mitigar estos ataques de múltiples maneras, como redirección de DNS, además de redirección y sanitización de tráfico en plataformas intermedias. Un caso de esto ocurre con Microsoft, organización que lo implementa en varias categorías bajo *Azure DDOS Protection* (Microsoft Azure, 2021); por su parte, Akamai tiene soluciones completas, como la llamada *Kona Site Defender* (Akamai, 2021), creada para proteger aplicaciones web y APIs.

Parte de los conceptos base de la seguridad de redes es la segmentación, la cual enseña a crear diferentes secciones de la red donde se puedan aislar equipos basados en características similares: por funciones, por cumplimiento de legislación o hasta por protección, así para evitar que un atacante cuya capacidad le haya permitido acceder a una sección de la red, pueda hacer ataques de reconocimiento horizontales y tener acceso a otras secciones de la misma. En redes tradicionales, esto se logra con separación física, por medio de *firewalls;* o de manera virtual, por medio de redes virtuales (VLANs) o por dominios de enrutamiento separados llamados VRF. Esto permite crear filtros o controles para determinar cual tráfico puede deber ser permitido.

Tales conceptos se pueden lograr de diferentes maneras en el ambiente de infraestructura en la nube. Las VLANs se pueden traducir a su equivalente, las redes virtuales o VNETs, también existen grupos de recursos, en los cuales se pueden agrupar diferentes componentes en la nube, lo cual ayuda a mantener aquellos componentes de una misma solución asociados y aplican políticas de seguridad de manera uniforme, como autenticación o como respaldo.

Además, la comunicación entre un grupo de recursos y otro, requiere tareas específicas para crear un puente entre los espacios IP, lo cual genera la posibilidad

de implementar equipos de seguridad en medio, como un *firewall* que inspeccione todo el tráfico que cruza entre ellos. Existe otra herramienta más, el concepto de suscripción, donde este corresponde a la creación de contenedores completamente separados uno de otro, creados con el propósito de separar diferentes soluciones para diferentes centros de costo, pero que actúan como una manera más de separar las soluciones y crear barreras.

En cuanto a estándares para asegurar implementaciones de computación en la nube, hay dos versiones consideradas relevantes, una es creada específicamente para la nube y la otra para sistemas de información en general. El estándar implementado por el Cloud Security Alliance compila una matriz de controles para ambientes de nube (Cloud Security Alliance, 2021), el cual se encuentra en su version 4.0; en la anterior, cada control contenía referencias a cual es su equivalente en diferentes estandares de seguridad por diferentes organizaciones. El segundo estándar es relacionado con la publicación 800-53 del NIST llamada “Controles de privacidad y seguridad para sistemas de informacion y organizaciones” (NIST, 2021), este también posee una matriz de controles en las diferentes áreas de seguridad. La matriz de controles del Cloud Security Alliance divide los controles en diecisiete dominios diferentes, a saber:

Tabla 5. Matriz de controles del Cloud Security Alliance

Seguridad de interfaz y aplicaciones
Auditoría y seguridad
Administración de continuidad de negocios y resiliencia operacional
Administración de control de cambios y configuración
Criptografía, encriptación y gestión de llaves
Gestión de ciclo de vida de seguridad de datos y privacidad
Seguridad de centros de datos
Gobernanza, gestión de riesgos y cumplimiento
Recursos Humanos

Gestión de acceso e identidad
Seguridad de infraestructura y virtualización
Interoperabilidad y portabilidad
Registro de operaciones y monitoreo
Gestión de incidentes de seguridad, descubrimiento digital y recopilación de información forense en la nube
Gestión de cadena de suministro, transparencia y responsabilidad
Gestión de amenazas y vulnerabilidades
Gestión universal de estaciones finales

Fuente: Cloud Security Alliance, 2021.

Se utiliza un diagrama de flujo para definir si el dominio tiene aplicabilidad en la propuesta de la solución relacionada con el estándar de seguridad en la nube.

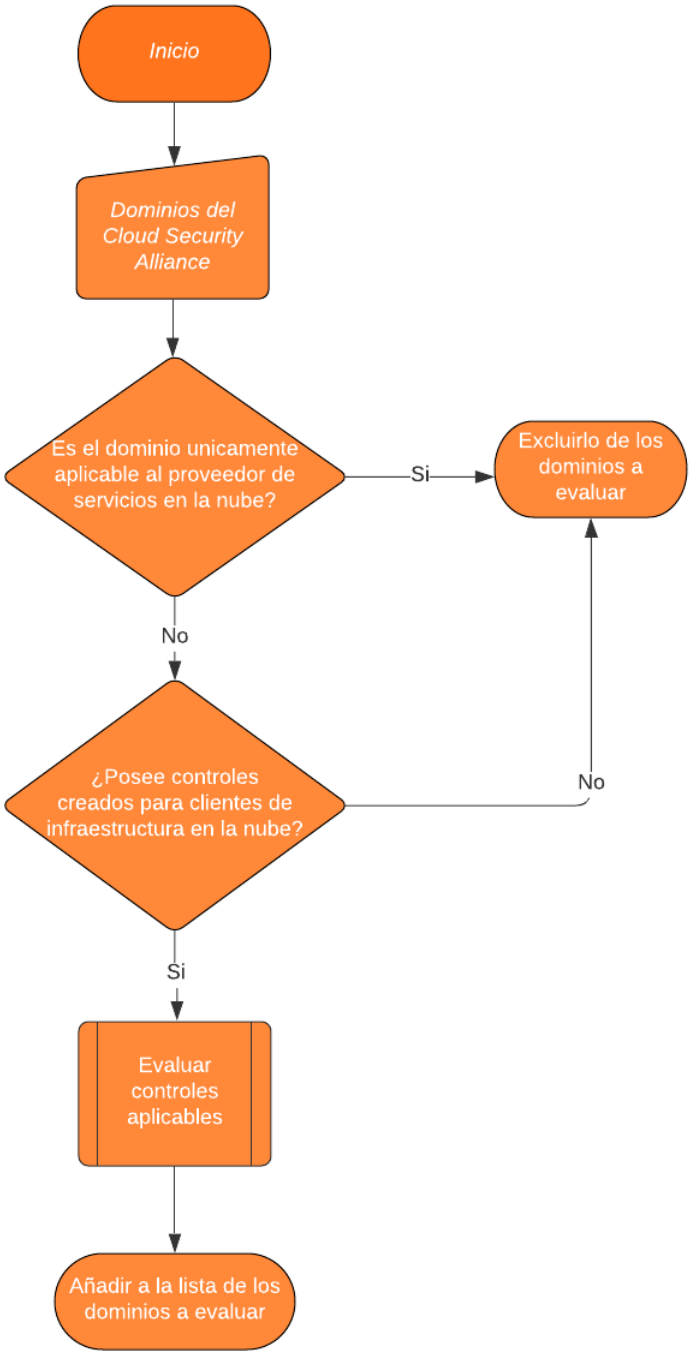


Ilustración 4. *Diagrama de flujo para decisión de inclusión de dominios en propuesta de solución. Fuente: Elaboración propia.*

Después de analizar los dominios utilizando el diagrama de flujo, se crea el siguiente diagrama:

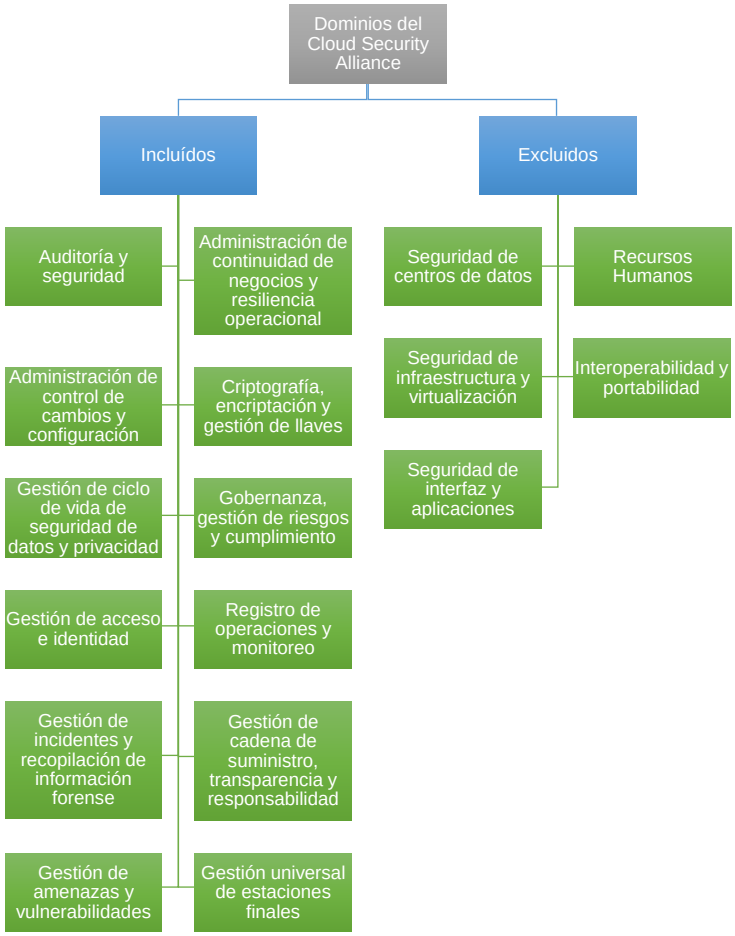


Ilustración 5. *Diagrama de dominios incluidos y excluidos en la propuesta de solución. Fuente: Elaboración propia.*

Capítulo 5. Propuesta de solución

La solución se enfoca en los dos documentos que corresponden a los entregables. Se considera la diferencia de profundidad técnica de cada uno y, además, se crea una sección para cada uno.

5.1 Desarrollo del estándar de seguridad

El estándar de seguridad es creado basado en los dominios aplicables de la guía de seguridad para áreas críticas de enfoque en computación en la nube por el Cloud Security Alliance (Alliance, 2020). De este modo, es más fácil enumerar los controles o requerimientos generales para cada área.

Se excluyen los dominios no relevantes a una solución en la nube desde un punto de vista de una compañía inquilina. Estos son interoperabilidad y portabilidad, recursos humanos, seguridad de centros de datos, seguridad de interfaz y aplicaciones, seguridad de infraestructura y virtualización. Estas áreas si se encuentran cubiertas para sistemas y soluciones físicamente alojadas en los centros de datos de la compañía, fuera del alcance de este documento.

Recientemente se implementó un proceso para revisión de seguridad sobre aplicaciones y servicios nuevos de TI, administrado y aprobado por el departamento de seguridad de la información. El mismo está compuesto por una serie de preguntas orientadas a documentar los siguientes elementos: el razonamiento de servicio, si el servicio es interno o accesible desde Internet, protocolo de control de acceso, métodos de almacenamiento y transferencia de datos. Lo anterior, con la intención de hacer una revisión comprensible del servicio y determinar si las medidas de seguridad son suficientes o si es necesario que sean reforzadas antes de la implementación.

Dado el aumento de soluciones en la nube, existe una categoría de preguntas y revisiones orientadas a servicios de este tipo y si los mismos se proveen de una manera segura. Esto viene a dar visibilidad al proceso de revisión de seguridad para nuevas aplicaciones y servicios; no obstante, se requiere una revisión sobre servicios actuales para diseñarlos de tal manera que puedan ser eficaces y seguros para la compañía.

Auditoría y seguridad

La compañía tiene procesos creados para auditorías internas y externas para servicios de tecnologías de información. Los equipos y servidores internos tienen procesos de auditoria mensual basados en análisis de vulnerabilidades y mejores prácticas. Actualmente, se utiliza el estándar del centro para seguridad de Internet (CIS por sus iniciales en inglés) para fortificar seguridad en configuraciones y en sistemas operativos.

La auditoría externa es llevaba a cabo una vez cada dos años y está basada en los estándares de seguridad propuestos por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST por sus iniciales inglés). La intención es auditar para lograr el nivel de madurez tres en seguridad de tecnologías de información de PRISMA[3].

Se recomienda que ambos procesos de auditoría sean extendidos a ambientes en la nube. A pesar de que los equipos de red de esta índole no proveen granularidad en cuanto a configuración (a diferencia de una solución local administrada por TI), es

[3] PRISMA es programa de revisión para asistencia en seguridad de la información de la NIST. Define cinco niveles de madurez al auditar la seguridad de la información en una compañía.

posible detectar riesgos aparentes en estas auditorias y mitigarlos de una manera preventiva. En el caso de CIS, existen documentos de referencia para los diferentes proveedores de la nube, en los cuales se documentan las recomendaciones a implementar para fortalecer la seguridad del ambiente.

Gobernanza, gestión de riesgos y cumplimiento

Tras una revisión inicial se confirma que la política de uso aceptable de tecnología y la política de seguridad de la información consideran ambiente en la nube. En el dominio de gestión universal de estaciones de trabajo se debe detallar los controles para el control de riesgos.

El departamento de seguridad de la información mantiene política y control sobre el cumplimiento según legislaciones locales en las múltiples áreas del mundo donde se opera. Tales directrices se alinean con el departamento legal que mantiene iniciativas de protección de datos y de propiedad intelectual, ya que la base del negocio requiere un manejo integral del cumplimiento de legislación. Existen procesos e iniciativas que cubren toda la compañía en este tema, el cual incluye definición de políticas y pruebas trimestrales. Las dos legislaciones con mayor impacto en la última década, Sarbanes-Oxley[4] (de los Estados Unidos) y GDPR[5] (para la Unión Europea) consideran ambientes de nube dentro su marco de acción, por ende, no hay mejoras aparentes en este campo.

Durante el proceso de selección de proveedores, se debe documentar y comparar cuales certificaciones poseen los diferentes proveedores de marcos de

[4] Legislación introducida en Estados Unidos en el 2002 para regular prácticas financieras y gobernanza corporativa.
[5] La regulación general de protección de datos es una regulación en la unión europea que regula la protección de datos y privacidad.

seguridad conocidos por la industria, como NIST-800, ISO-27001, SOC 1, SOC 2. El procedimiento de identificación y manejo de riesgos no está formalizado en la compañía, en procesos como en análisis de impacto de negocio y de recuperación de desastres se identifican riesgos y se mitigan, pero no hay documentación o seguimiento. Por lo tanto, se recomienda crear un proceso de gestión de riesgos alineado con estándares de industria, como ISO-31000.

Administración de continuidad de negocios y resiliencia operacional

Parte de las consideraciones con servicios en la nube es su continuidad y la resiliencia operacional, a pesar de que la responsabilidad de entidades físicas en servicios de este tipo recae sobre el proveedor de nube, es parte de la responsabilidad de los clientes definir su apetito de riesgo y planear servicios resilientes, según un análisis de riesgo y definición de RTO[6] y RPO[7].

La compañía cuenta con un sistema de recopilación y de análisis de documentos de recuperación de desastre, lo cual requiere una estrategia de alto nivel donde se incluya un documento con los pasos detallados para la recuperación y sus dependencias. Además, incluye un documento con el plan de pruebas y un evento anual, donde se realizan las pruebas de recuperación de desastre y se documentan los resultados. Todo esto se realiza con la intención de mejorar el proceso en la siguiente iteración.

---

[6] Son las iniciales en inglés para objetivo de tiempo de recuperación, es la cantidad de tiempo en la cual un proceso de negocio debe estar restaurado después de un desastre para evitar consecuencias desastrosas.

[7] Son las iniciales en inglés para objetivo de punto de recuperación, es el intervalo de tiempo que puede pasar durante una interrupción antes de la cantidad de datos perdidos exceda el nivel de tolerancia permitido por el plan de continuidad de negocio.

Además de este plan de la compañía, se recomienda desarrollar un plan de recuperación de desastre orientado a servicios de infraestructura en la nube. Por ende, se deben utilizar las plantillas definidas para crear la documentación necesaria, donde se registra si la solución está geográficamente distribuida en varios centros de datos del proveedor de nube, de tal manera que es capaz de soportar una falla localizada y si puede absorber la carga de trabajo completa, así como las capacidades del proveedor de nube de sobreponerse a fallas físicas. Además, se logra definir si los sistemas alojados en la nube cumplen criterios de criticidad para ser parte de procesos críticos que pueden afectar las operaciones en caso de una interrupción de servicio. Esto permite poder definir si se requiere una mayor resiliencia operacional y sopesarlo contra el costo financiero.

Administración de control de cambios y configuración

Al existir un proceso maduro de control de cambios dentro de la compañía, lo natural es extender ese proceso para que se aplique a cambios planeados y efectuados en el ambiente de computación en la nube, el cual establece una serie de aprobaciones, documentación del cambio, definición de impacto a operaciones y plan para reversar en caso de fallo. Además, este incluye la notificación a empleados y clientes si hay afectación de servicios por parte del cambio.

Lo anterior viene a reforzar el proceso de cambios en la nube y trae una lista de requerimientos más rigurosos a la hora de realizar cambios, ya que el gerente de gestión de cambios ha de estar satisfecho con la existencia una documentación del cambio suficientemente explícita; así como que esta contenga un razonamiento técnico del cambio y procesos documentados para revertirlos en caso de fallo.

Criptografía, encriptación y gestión de llaves

Los certificados con cara a Internet son manejados de manera centralizada, se utiliza un proceso de generación de requisito de certificado y este es procesado por el proveedor de certificados públicos. Esto evita que la llave privada sea exportada y tenga riesgo de ser comprometida.

Los certificados de utilización interna, creados por una herramienta de administración, son manejados de manera centralizada. Esta certificadora es configurada como una entidad confiable en las imágenes de sistema operativo de las estaciones de trabajo de la compañía. Este proceso lo maneja el escritorio de ayuda de tecnologías de información.

Los certificados mencionados son, en este momento, utilizados para autenticación de múltiples factores para el cliente de VPN de estaciones de trabajo y para autenticación a la red inalámbrica. Por ende, no existe un uso actual para equipos en la nube. De todas maneras, se recomienda que la clave del archivo de certificado sea generada de manera automatizada, para evitar la reutilización de claves y el poner en riesgo el acceso a un certificado con una clave conocida.

En cuando a llaves para servicios en la nube, estas son utilizadas para encriptación en los túneles de VPN hacia los proveedores de nube y son creadas al azar al momento de implementación y documentadas, en un repositorio seguro en la red. Se recomienda hacer una revisión anual de los algoritmos de encriptación utilizados para conexión a servicios en la nube y retirar los algoritmos que no se consideren seguros o que exista evidencia de su vencimiento. De esta manera se mantienen los más seguros e idóneos en operación.

Gestión de ciclo de vida de seguridad de datos y privacidad

Debido a que la compañía maneja información que puede variar entre información de identificación personal para personas alrededor del mundo, propiedad intelectual propia y de clientes y hasta información considerada secreta para ciertos países, se tiene un sistema maduro de clasificación de la información, para mantener control de la exportación de información entre países y entidades.

A pesar de que los ambientes actuales de nube no poseen información de carácter sensible, se recomienda aplicar las mismas políticas y sistemas para clasificar la información contenida y procesada en la nube. De esta manera, se reduce el riesgo en una eventual migración de servicios de carácter sensible a alguno de los proveedores. Esto incluye el control de copia de archivos y contenido a servicios en la nube no perteneciente a Teradyne para evitar una exfiltración intencional o accidental por parte de usuarios.

Gestión de acceso e identidad

El manejo de identidades y acceso para soluciones internas es adecuado y estandarizado. Existe una solución *de facto* en la compañía para empleados y contratistas, la cual integra las mejores prácticas de seguridad para el manejo de identidades. Por eso se recomienda el uso de la identidad de Active Directory para autenticar y autorizar usuarios para acceder y administrar recursos en la nube.

Este método implementa la política de uso de claves, mantiene registros para auditar accesos provistos y utiliza grupos para poder proveer y revocar acceso a sistemas. Por otra parte, en caso de un incidente de seguridad, se puede suspender el acceso a múltiples aplicaciones y servicios desde una sola plataforma.

En caso de acceso a sistemas en la nube, se recomienda habilitar autenticación de múltiples factores, utilizando una o múltiples opciones ya implementadas actualmente. Adicionalmente, se recomienda la creación de grupos para asignar los diferentes roles requeridos en cada solución en la nube, con la intención de poder mantener un control estricto de acceso a los recursos.

Para la administración y soporte de la infraestructura en la nube, se recomienda la misma identidad; sin embargo, la asignación de grupos puede ser llevada a cabo en el portal de administración de seguridad del proveedor en la nube, mediante el uso de roles definidos y de separación de tareas.

En caso de que se requiera acceso a usuarios fuera de Active Directory, se recomienda que el repositorio de usuarios se comunique de manera encriptada, con protocolos razonablemente seguros para autenticar y autorizar. También se deben almacenar las claves de manera encriptada y cumplir con los requisitos de clave establecidos por la compañía con autenticación de múltiples factores.

Las cuentas deben ser removidas cuando no sean necesarias y bloqueadas cuando exceda un número de intentos de acceso de manera no exitosa. Además, se debe soportar acceso basado en roles o en identidad, para poder restringir el ingreso basado en el usuario accediendo al recurso. Tales credenciales tendrán validez solo para la solución en cuestión. Finalmente, si requiere acceso a recursos en la red o aplicaciones que implementan *Single Sign On* (SSO), será necesario considerar el uso de Active Directory como método de autenticación y autorización.

En cuanto a claves de administrador local o de recuperación de desastre, estas deben ser administradas por la solución corporativa de claves de administración del

departamento de tecnologías de información, que almacena y gestiona el acceso de estas. Cada una de ellas requiere permisos específicos a la herramienta y una clave de único uso por medio de un generador de *token* en *software*. De ser necesario, el sistema ha de ser capaz de cambiar la clave local cada cierto tiempo, mediante la utilización de un generador de claves aleatorio. Así se dificulta la filtración de una clave con privilegios elevados y se obliga al administrador a acceder a la cuenta por medio de esta solución.

Registro de operaciones y monitoreo

Es necesario generar y almacenar registros de los diferentes componentes que posibilitan la operación de los recursos en la nube. Estos se pueden dividir en dos categorías principales: La primera comprende los registros generados por el sistema de gestión de recursos de la nube, tanto de auditoría como de seguridad. La segunda consta de los registros de sistema generados por los recursos; por ejemplo, los eventos de sistema que genera Linux al operar en una máquina virtual o los producidos con un equipo de infraestructura, como un router o un *firewall*.

Se recomienda el almacenamiento en un repositorio centralizado, con capacidad de retención adecuada y con la posibilidad de búsqueda. Como requerimientos básicos se recomienda utilizar una fuente de tiempo confiable para sincronizar los equipos. Esto permite poder correlacionar registros a través de diferentes equipos en caso de un evento de seguridad.

Se debe restringir el acceso al repositorio, de tal manera que solo el personal autorizado pueda acceder y el borrado debe ser restrictivo y auditable. Además, los sistemas administrables deben ser monitoreados en uno centralizado, tanto en lo

asociado a su disponibilidad como en el estado de los recursos. Para poder detectar un fallo o un decremento dramático en recursos disponibles. Debe contar con un proceso para la notificación y la apertura de incidente en caso de sobrepasar los límites establecidos de operación normal.

Gestión de incidentes de seguridad, descubrimiento digital y recopilación de información forense en la nube

Este dominio se concentra en el manejo de incidentes de seguridad, recopilación de información forense pertinente y, finalmente, el proceso de notificación en caso de una violación de seguridad, según lo requiera la política interna y las leyes o regulaciones aplicables.

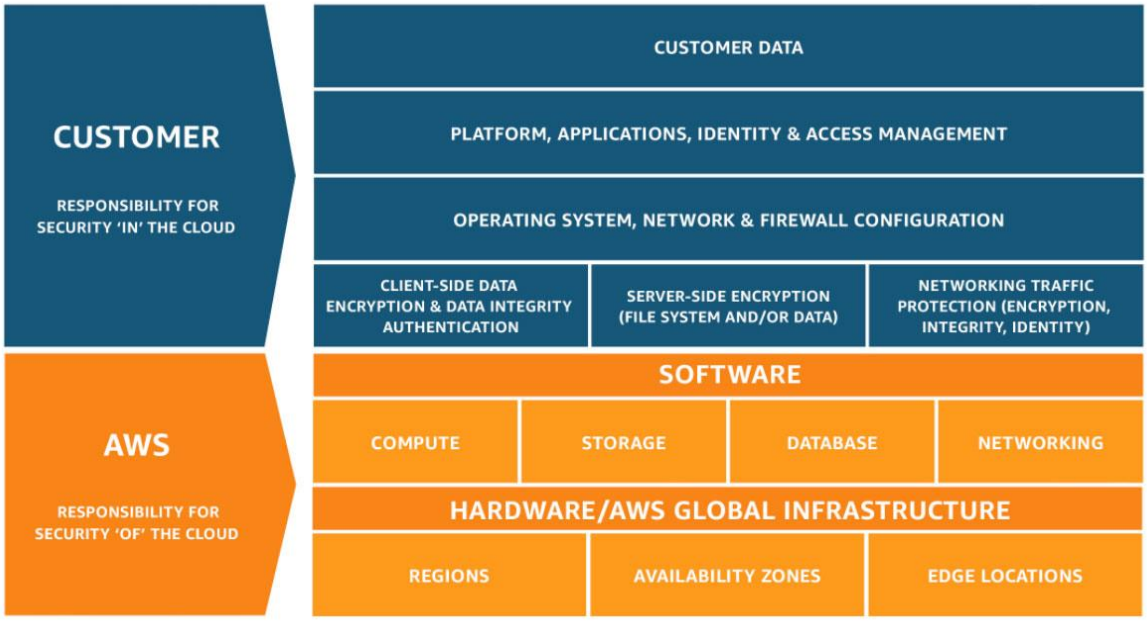
Los eventos de sistema deben ser monitoreados con el fin de detectar incidentes de seguridad. Se recomienda que el proceso de monitoreo incluya acciones para eventos de sistema de nivel alto y crítico; de este modo, se investiga a la mayor brevedad y se descarta una brecha de seguridad o un evento que pueda demostrar una interrupción de servicio.

Tras la revisión de la política de respuesta a incidentes de seguridad de la compañía, se confirma que es suficientemente comprensiva para incluir eventos en ambiente de nube. También la política considera la recopilación de evidencia, la información forense necesaria y la notificación a las entidades pertinentes, según lo requiera la legislación.

Gestión de cadena de suministro, transparencia y responsabilidad

El foco principal de este dominio es definir responsabilidades en ambientes de nube. El mismo corresponde al insumo principal: el modelo de responsabilidad compartida de seguridad, esto es, dibujar la línea entre las responsabilidades que recaen sobre el alcance del proveedor de nube y las del cliente. Por ejemplo, Amazon AWS define en su modelo que este “es responsable de proteger la infraestructura que ejecuta todos los servicios provistos en la nube de AWS” (AWS, 2021). En la ilustración 6, se dibuja las responsabilidades principales del proveedor de nube y del cliente.

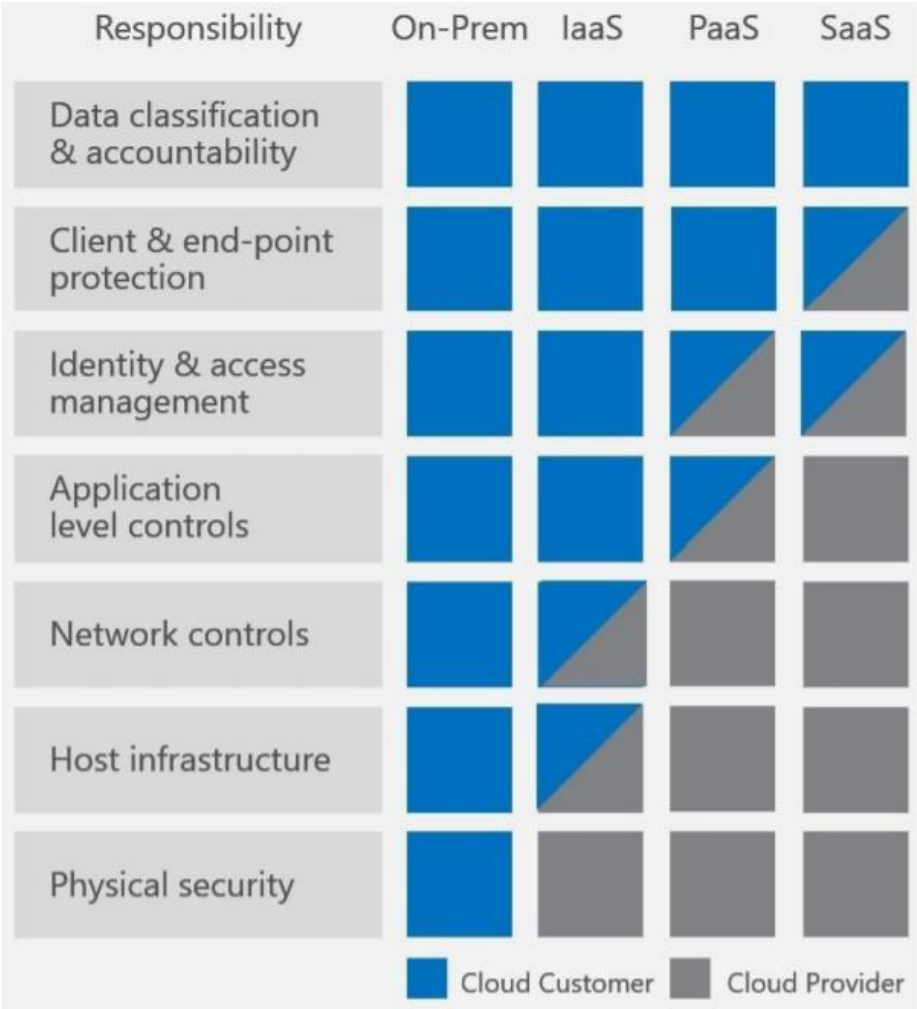
Ilustración 6. Modelo de responsabilidad compartida (AWS, 2021)



Fuente: AWS, 2021.

Además, este asevera que las responsabilidades cambian dependiendo del tipo de servicios en la nube usados en el momento. En este caso, Microsoft Azure logra diagramarlo de una manera más comprensible en la ilustración 7.

Ilustración 7. Modelo de responsabilidades compartidas para los diferentes servicios en la nube (Microsoft Azure, 2019)



Fuente: Microsoft Azure, 2019.

Para infraestructura como servicio, los elementos como edificios, servidores, equipos de red y el hipervisor deberían ser manejados por el proveedor de servicios en la nube. El cliente es responsable o tiene una responsabilidad compartida en

asegurar y administrar el sistema operativo, configuración de red, aplicaciones, identidad, clientes y datos.

Las soluciones de plataforma como servicio se construyen sobre implementaciones de IaaS, en donde el proveedor de servicios en la nube es responsable, adicionalmente, de administrar y asegurar los controles de red. El cliente todavía es responsable o tiene responsabilidad compartida para asegurar y administrar aplicaciones, identidad, clientes y datos.

> La importancia de comprender esta responsabilidad compartida es esencial para clientes que están migrando a la nube. Proveedores de servicios en la nube ofrecen ventajas considerables en seguridad y cumplimiento de legislación, pero estas ventajas no absuelven al cliente de proteger sus usuarios, aplicaciones y servicios. (Microsoft Azure, 2019)

Se recomienda solicitar el modelo de responsabilidad compartida de seguridad por proveedor de nube, así se pueden ajustar los procedimientos de soporte y eventos de seguridad a la responsabilidad en cada caso.

Gestión universal de estaciones finales

Las estaciones de trabajo implementadas en ambientes de nube deben cumplir los mismos requisitos que las estaciones de trabajo físicas en la compañía. Esto incluye medidas como bloqueo de sesión y habilitación de salvapantallas por inactividad, aplicadas por medio de políticas de grupo; por lo cual, también es recomendable que estas máquinas virtuales sean parte del dominio.

Además, el control de aplicaciones aprobadas por el departamento de tecnologías de información se logra creando las estaciones mediante el uso de imágenes de sistema estandarizadas, es decir, el mismo proceso usado para configurar las estaciones de trabajo físicas. La restricción de instalación de *software* no aprobado se obtienen mediante la utilización de políticas de perfiles de usuario con derechos administrativos restringidos e inventario de *software*.

Parte de las consideraciones para proteger las estaciones de trabajo es tener el sistema operativo y las diferentes aplicaciones instaladas al día con parches de seguridad y actualizaciones necesarias, se recomienda usar el sistema corporativo de control de parches y actualizaciones. Así se gestionan de una manera integral y centralizada. Las estaciones de trabajo también deben contar con una solución de antivirus y *antimalware* manejada centralmente, esto con la intención de poder detectar, reportar y contener tanto infecciones como ataques.

En cuanto a encriptación en reposo, se recomienda que el almacenamiento sea encriptado. A su vez, la solución corporativa para realizar esta labor en los discos de estaciones de trabajo no es aplicable, ya que utiliza la herramienta del fabricante instalada en las PCs por defecto, y las llaves para desencriptar son almacenadas de manera centralizada por el departamento de tecnologías de información. Por el contrario, para este caso se recomienda que se habilite encriptación de almacenamiento mediante la solución provista por el proveedor de nube, tomando en cuenta la necesidad de un adecuado manejo de llaves de encriptación con acceso solo a administradores de estaciones de trabajo.

El hecho de que el almacenamiento en nube no depende de un solo disco duro físico, hace los eventos de pérdida de datos más escasos. De todas maneras, se

recomienda que la información y los documentos sean almacenados en medios compartidos los cuales poseen medidas de prevención de perdida de datos, como carpetas compartidas en servidores y soluciones de almacenamiento en nube aprobados por la compañía.

Gestión de amenazas y vulnerabilidades

Las medidas de gestión de amenazas y de vulnerabilidades tienen una relación estrecha con la gestión universal de estaciones de trabajo. Están principalmente asociadas con el control de parches y de actualizaciones para aplicaciones y sistemas operativos, así como con la implementación de la solución centralizada utilizada en estaciones finales, con las cuales se logra programar la instalación de parches y actualizaciones instaladas; además, se puede tener un inventario de parches instalados en las diferentes estaciones. Así se puede obtener una sola política de parcheo y actualizaciones, recurriendo a la local y expandiendo su alcance a las estaciones de trabajo en la nube.

En cuanto a la detección de *malware* y antivirus, como se menciona en la sección anterior, se recomienda utilizar la solución actual para estaciones de trabajo locales pues permite tener las mismas políticas de protección en todas las estaciones, más allá de su ubicación. Debido a esto, estas estaciones están incluidas en los reportes semanales y mensuales de infecciones y ataques, para poder detectar, contener y prevenir amenazas. Estos reportes son parte del procedimiento de gestión de estaciones de trabajo. El documento 'Manual para implementación de medidas de seguridad en infraestructura como servicio en Teradyne' se adjunta en apéndice B.

5.2 Desarrollo del manual de implementación

Para cumplir los requerimientos del laboratorio de entrenamiento se propone la utilización de una combinación de soluciones. La principal consta de un producto de Azure llamado *Azure Lab Services*, el cual permite crear máquinas virtuales desechables bajo demanda. Estas son creadas según una imagen de sistema, así que en cada clase se pueden crear cuantas máquinas sean necesarias, sin necesidad de instalar el *software* requerido para el entrenamiento. Es una solución diseñada para proveer clases con elementos de computación de manera remota, esto se adapta perfectamente a los requerimientos precisados.

La manera en la cual los estudiantes accederán a esta solución será por medio de un portal web residido en Azure. El administrador del laboratorio, en este caso, el entrenador, enviará el enlace al portal de la clase y los usuarios utilizarán las credenciales de Office 365 propias de la cuenta corporativa de su compañía para registrarse. El portal estará habilitado para autenticar múltiples dominios de Microsoft Azure con una conexión de negocio a negocio (B2B) con Teradyne.

Una vez registrado, a cada usuario se le asignará una máquina virtual por una cantidad de tiempo determinada. Al acceder el portal con las credenciales, el estudiante tiene la posibilidad de iniciar la máquina virtual en caso de que esté apagada, de ahí tiene acceso al archivo RDP (*Remote Desktop Protocol*), el cual posee una IP pública asignada dinámicamente y utiliza un puerto TCP de un rango (49152 a 65535) no relacionado con el protocolo de escritorio remoto, para conectarse. Esta solución es de plataforma como servicio, es decir, el proveedor incluye los detalles de cada máquina, almacenamiento, redes, enrutamiento y de proteger por medio de un *firewall*, para permitir únicamente los puertos requeridos.

Esta solución requiere que los usuarios de la compañía a la cual pertenecen los clientes tengan implementación de Office 365 y acceso a Internet en un rango de puertos muy amplio en TCP. Esto no siempre es posible en un ambiente corporativo con *firewalls* y políticas de acceso, por lo tanto, se desarrolla una segunda solución con diferentes productos. Esta es directamente generada por Microsoft Azure y utiliza rutinas de automatización para crear las máquinas virtuales y una serie de usuarios temporales para los estudiantes, en un grupo de recursos previamente establecido y preparado con los elementos de infraestructura necesarios para soportar el entrenamiento.

Las credenciales creadas en la rutina de automatización, junto con la clave temporal, son enviadas a cada estudiante manualmente y a través de correo. Además, se hace uso de un servicio de gestión de conexiones de acceso remoto en Azure llamado *Bastion*, el cual permite que las máquinas virtuales previamente creadas sean accesibles para cada estudiante por medio de un portal web. Al autenticarse exitosamente en dicho portal, el servicio provee acceso al equipo por medio de *Remote Desktop Protocol* a través del navegador web, lo cual se logra encapsulando el protocolo dentro de HTTPS. Esta solución, al utilizar un puerto estándar para HTTPS y no requerir cuenta corporativa de Office 365, es más accesible para ambientes corporativos sin la utilización de Microsoft para correo y provee una doble capa de encriptación. Ha de notarse que, a pesar de que es una solución alojada en Azure, los recursos de infraestructura, las rutinas de automatización y las máquinas virtuales son creadas y administradas por el departamento de tecnologías de información de Teradyne.

En cuanto a medidas a implementar en el manual, la autenticación se divide en dos frentes: la autenticación para administración y la que usa el portal de acceso para los usuarios al laboratorio. La primera se va a beneficiar de la implementación reciente de Outlook 365 como solución corporativa de correo, esto requiere que Azure tenga acceso al *Active Directory* de la compañía para poder autenticar de manera centralizada, determinar usuarios, correos y pertenencia a grupos.

Para la autenticación del portal de administración, se propone implementar IAM para ligar el correo corporativo, y el usuario de *Active Directory* a un perfil de *Azure portal*. Lo anterior permite asignar acceso a las diferentes implementaciones dentro de la plataforma, ante lo cual se recomienda crear perfiles para los diferentes niveles de acceso requerido, como la administración de recursos de infraestructura y de computación y personal de monitoreo.

En este caso, se recomienda crear un contenedor de recursos para cada solución y una suscripción para agrupar los recursos relacionados con el laboratorio. Por lo tanto, se asigna el acceso administrativo para la suscripción a todo el personal de TI que requiera soportar la solución por medio de los perfiles descritos previamente, esto por medio de la cuenta de *Active Directory*.

Para las credenciales de usuario de los estudiantes, la implementación utilizada en *Azure Lab Services* es suficientemente segura y la carga de autenticación recae sobre la instancia de Office 365 de la compañía del cliente. De este modo, se evita el compartir credenciales y crear usuarios temporales, además de tener la confirmación de que el usuario accediendo el recurso es el adecuado.

En cuanto a la segunda solución, compartir el usuario y la clave por medio de correo no se considera seguro, a pesar de que la clave es temporal y debe ser cambiada durante el primer acceso. Se recomienda habilitar autenticación por múltiples factores durante el proceso de registro; así, el estudiante requiere el usuario, la clave y un código de único uso generado por medio de OTP. Además, se recomienda que las credenciales de la cuenta local de la máquina virtual sean compartidas durante la sesión de entrenamiento por medio de voz o de chat individual. Estas deben ser cambiadas tras cada clase, para evitar la reutilización.

Ambas soluciones propuestas requieren acceso a la red interna de Teradyne y el uso de recursos internos, desde aplicaciones hasta equipo físico. Esto se logrará con un túnel de VPN que conecta Azure al proveedor de SD-WAN[8] llamado Aryaka el cual, a su vez, se conecta a cada oficina de la compañía y, más importante, a los *datacenters* que albergan los recursos internos requeridos por los estudiantes y el instructor. Por lo tanto, se recomienda que la red virtual conectada al túnel de VPN tenga un *firewall* de última generación en línea; esto, para restringir el acceso a la red interna e inspeccionar el tráfico en tiempo real, para detectar virus, *malware* y riesgos similares.

El documento 'Manual para implementación de medidas de seguridad en infraestructura como servicio en Teradyne', se adjunta en apéndice C.

[8] SD-WAN es la WAN definida por software, es un enfoque para diseñar e implementar una red de área amplia empresarial que utiliza redes definidas por software para determinar la forma más eficaz de enrutar el tráfico a ubicaciones remotas.

Capítulo 6. Conclusiones y recomendaciones

6.1 Conclusiones

Se logró establecer una línea base de los controles de seguridad aplicados en los diferentes ambientes de nube implementados en la compañía, lo cual ayudó a identificar la postura actual de la infraestructura. De este modo se evidenciaron brechas en la seguridad a ser atendidas con mayor urgencia.

Se plantearon mejoras inmediatas y específicas al ambiente de infraestructura en la nube, con la intención de robustecer la seguridad a corto plazo y mitigar faltas de seguridad presentes desde la implementación.

Se escogió como estándar de seguridad una combinación de la norma de NIST *800-53 controles de seguridad y privacidad para sistemas de información y organizaciones* y la del *Cloud Security Alliance* llamada *Garantía confiable de seguridad y riesgo*. Lo anterior, con la intención de utilizar una combinación de los controles aplicables de cada estándar y de crear un plan de seguridad eficaz y adaptable a Teradyne.

Mediante el análisis de las medidas y los controles aplicables en contraste con el estado actual y las diferentes políticas de la compañía, en relación con seguridad de la información, se definieron aquellos factores a ser propuestos para consideración y eventual implementación.

Se diseñó el plan de seguridad para acceso y operación de computación en la nube, fundado en los controles aplicables según los estándares y las buenas prácticas. De esta manera, este puede ser implementado en ambientes de nube

actualmente en operación y ser utilizados para el diseño e implementación de nuevas soluciones.

Al momento de analizar y definir un plan de seguridad basado en estándares para una compañía, se evidencia que una implementación completa de un estándar requiere un nivel de madurez alto en relación con procesos de seguridad de la información. El desarrollar un híbrido de varios estándares y mejores prácticas basado en la situación actual de la compañía, provee la posibilidad de proponer controles y políticas ajustables a la realidad de Teradyne.

Debido al constante cambio de tecnologías y la oferta de servicios de infraestructura en la nube, es recomendable realizar ejercicios de investigación y análisis similares a este con una frecuencia regularizada. Por lo tanto, se pretende que, en una futura iteración, se beneficie de las mejoras propuestas en el trabajo actual, para así ahondar en controles más específicos y apuntar a un mayor de nivel de madurez de los procesos.

Referencias

Akamai. (21 de febrero, 2021). *Akamai*. Obtenido de Kona Site Defender: https://www.akamai.com/us/en/products/security/kona-site-defender.jsp

Alliance, C. S. (3 de junio, 2020). *The Security Guidance for Critical Areas of Focus in Cloud Computing v4.0.* Obtenido de Cloud Security Alliance: https://cloudsecurityalliance.org/download/securityguidance-v4/

AWS. (24 de marzo, 2021). *Shared Responsibility Model*. Obtenido de AWS: https://aws.amazon.com/compliance/shared-responsibility-model/

Azure, M. (21 de febrero, 2021). *What is Azure Load Balancer?* Obtenido de Microsoft Azure: https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

Azure, M. (21 de febrero, 2021). *What is Azure Web Application Firewall on Azure Application Gateway?* Obtenido de Microsoft Azure: https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview

Cloud Security Alliance. (06 de marzo, 2021). *Cloud Controls Matrix v4.* Obtenido de Cloud Security Alliance: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/

F. Chen, T. X. (2016). Secure cloud storage meets with secure network coding. *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications* (págs. 1936-1948). Toronto: IEEE.

F. Zhang, K. H. (2016). Skyline Discovery and Composition of Multi-Cloud Mashup Services. *IEEE Transactions on Services Computing (Volume: 9, Issue: 1, Jan.-Feb. 1 2016)*, 72-83.

Fernandes, D. S. (2014). Security issues in cloud environments: a survey. *International Journal of Information Security*, 113–170.

I Indu, P. A. (2018). Identity and access management in cloud environment: Mechanisms and challenges. *Engineering Science and Technology, an International Journal*, 574-588.

Johnson, F. M. (2020). Robust identity and access management for cloud systems. *Faculty of Graduate Studies, Concordia University of Edmonton*.

Jorge Biolchini, P. G. (2005). *TECHNICAL REPORT – ES 679 / 05 Systematic Review in Software Engineering.* Rio de Janeiro: COPPE / UFRJ .

Liggett, T. (2018). *Evolution of Endpoint Detection and Response Platforms .* Utica: Utica College.

Microsoft. (20 de octubre, 2020). *¿Qué es IaaS?* Obtenido de Microsoft Azure: https://azure.microsoft.com/es-es/overview/what-is-iaas/

Microsoft. (20 de octubre, 2020). *¿Qué es la nube?* Obtenido de Microsoft Azure: https://azure.microsoft.com/es-es/overview/what-is-the-cloud/#:~:text=La%20definici%C3%B3n%20de%20la%20nube,uno%20con%20una%20funci%C3%B3n%20%C3%BAnica.&text=Las%20empresas%20utilizan%20cuatro%20m%C3%A9todos%20diferentes%20para%20implementar%20recursos%20

Microsoft. (20 de octubre, 2020). *¿Qué es PaaS?* Obtenido de Microsoft Azure: https://azure.microsoft.com/es-es/overview/what-is-paas/

Microsoft. (20 de octubre, 2020). *¿Qué es SaaS?* Obtenido de Microsoft Azure: https://azure.microsoft.com/es-es/overview/what-is-saas/

Microsoft Azure. (25 de octubre, 2019). *Shared Responsibility for Cloud Computing.* Obtenido de Azure: https://azure.microsoft.com/mediahandler/files/resourcefiles/shared-responsibility-for-cloud-computing/Shared%20Responsibility%20for%20Cloud%20Computing-2019-10-25.pdf

Microsoft Azure. (21 de enero, 2021). *Azure DDoS Protection Standard overview*. Obtenido de Microsoft Azure: https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview

N. Mimura Gonzalez, M. T. (2013). A framework for authentication and authorization credentials in cloud computing. *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications.* Melbourne: IEEE.

NIST. (21 de enero, 2021). *Security and Privacy Controls for Information Systems and Organizations.* Obtenido de National Institute of Standards and Technology: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Teradyne. Inc. (25 de enero, 2021). *About Us*. Obtenido de Teradyne: https://www.teradyne.com/company/about-us/

Apéndice A

Se realiza la búsqueda con las cadenas provistas previamente, este devuelve solo dos resultados, como se ejemplifica en la tabla:

Tabla 6. *Resultados de búsqueda de IEEE Digital Library*

#	Titulo	Autores	Año	Link
1	Cloud computing security management	Sameera Abdulrahman Almulla, Chan Yeob Yeun	2010	https://ieeexplore.ieee.org/document/5542654/
2	Cloud Security and Data Protection	LLC Cloud Strategy Partners	2014	https://ieeexplore.ieee.org/courses/details/EDP406

Fuente: Elaboración propia.

A1.2 Evaluación de la calidad de los estudios.

Se analizan los dos resultados encontrados, el primero llamado S. Abdulrahman, C. Yeob (2010) Cloud Computing Security Management por 2nd International Conference on Engineering System Management and Applications, ICESMA 2010, se analiza con Scimago y este el indicador:



Ilustración 8 *Valor SJR de la publicación según Scimago*

La cantidad de citas por año incrementa de manera saludable

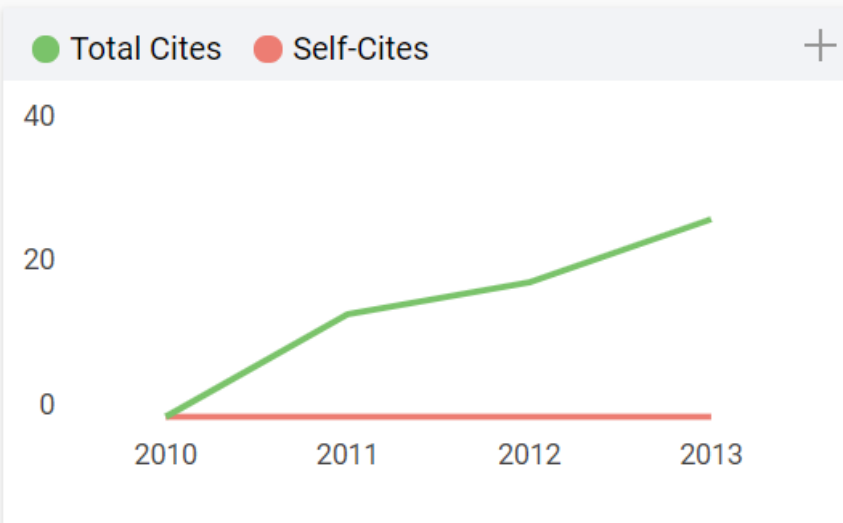


Ilustración 9. *Gráfico de citas en los primeros años de publicación*

El segundo resultado es un curso de IEEE, no relevante para la búsqueda en cuestión, se descarta.

A1.3 Revisión de la selección

La publicación se concentra en administración de acceso por identidad (IAM por sus siglas en inglés), su implementación y vista de ciclo de vida en el año de su publicación. Discute sobre posibilidades de OAuth, SAML.

A1.4 Extracción de información

Para la extracción de información relevante sobre los estudios primarios, se consideran los siguientes elementos:

- Autenticación de acceso a servicios en la nube
- Gestión de Identidad y Acceso
- Evaluaciones de riesgos centradas en los datos
- Acceso de herramientas de auditoría
- Autorización de acceso de usuarios
- Seguridad de la red

Tabla 7. *Detalle de resultados de búsqueda de IEEE Digital Library*

Repositorio	**IEEE Digital Library**
Titulo	Cloud computing security management
Publicación	2010 Second International Conference on Engineering System Management and Applications
Autores	Sameera Abdulrahman Almulla, Chan Yeob Yeun
Referencia	S. A. Almulla and Chan Yeob Yeun, "Cloud computing security management," 2010 Second International Conference on Engineering System Management and Applications, Sharjah, 2010, pp. 1-7.
Descripción	
Área	Administración de seguridad en computación en la nube
Resumen	Computación en la nube es un nuevo paradigma computacional que ofrece un modelo de negocio innovativo para organizaciones que quieren adoptar tecnologías de información sin inversión inicial. A pesar de las ventajas potenciales logradas con computación en la nube, el modelo de seguridad es todavía cuestionable, lo cual causa un impacto en la adopción de este modelo. La complejidad de manejo de seguridad incrementa en un modelo de nube, hay que considerar arquitectura a gran escala, elasticidad, múltiples inquilinos en el mismo espacio y capas de dependencia. En este documento, se presenta un análisis sobre el problema de seguridad en la nube. Investigamos el problema desde la arquitectura de la nube, desde la perspectiva de las características ofrecidas por la nube, los desde la perspectiva de las partes interesadas y desde el punto de vista de los modelos de servicio. Basado en este análisis se deriva una especificación detallada de los problemas de seguridad que presenta la nube y las características que debe cubrir cualquier solución propuesta.
Aspectos Por Destacar	
	El documento hace propuestas iniciales para seguridad en la nube, en una época donde las soluciones de seguridad eran limitadas

A2 Ejecución de la selección en la fuente ACM Digital Library

A2.1 Selección de estudios iniciales

Utilizando las cadenas de búsqueda definidas previamente, no se encuentran resultados en el repositorio.

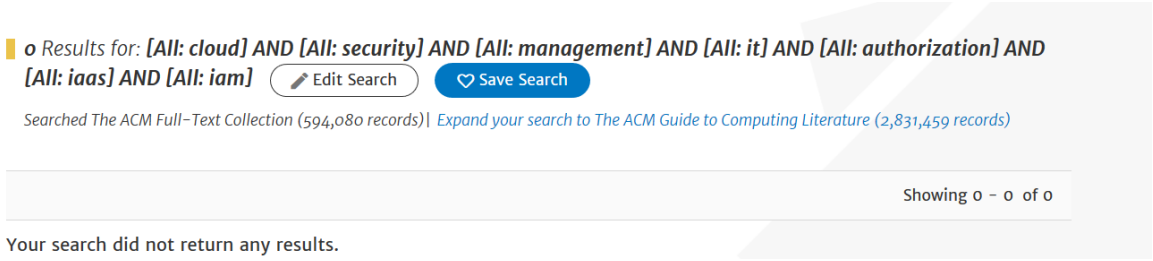


Ilustración 10. *Captura de resultados de ACM Digital Library*

A2.4 Ejecución de la selección en la fuente Google Scholar

A2.4.1 Selección de estudios iniciales

Utilizando la cadena de búsquedas recibimos 3700 resultados.

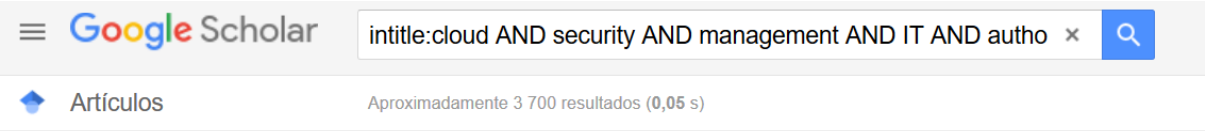


Ilustración 11. *Captura de resultados de Google Scholar*

A2.4.2 Evaluación de la calidad de los estudios

Se utilizan los primeros mil resultados para ser analizados en diferentes propiedades. Primero revisamos la distribución de resultados por año publicado.

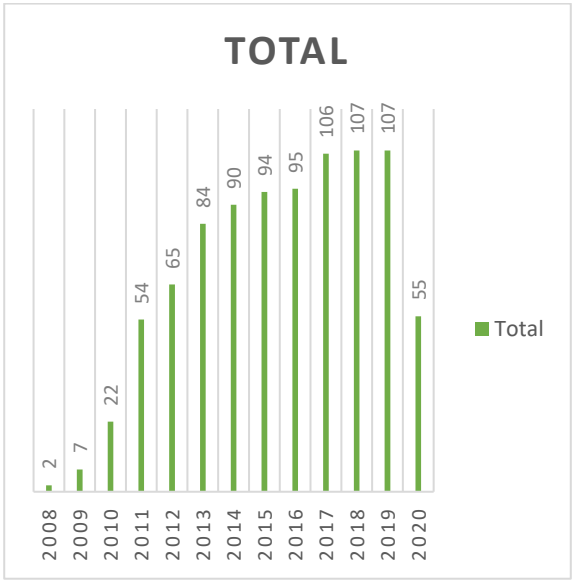


Ilustración 12. *Gráfico de distribución de publicación por año*

Ademas, se toman en consideración las publicaciones con más citas y los años de publicación de las mismas. Se observa que la mayor cantidad de citas son de investigaciones con mas de 5 años

A2.4.3 Revisión de la selección

Se toman los primeros 15 resultados con más citas generadas:

Tabla 8. *Resultados de búsqueda de Google Scholar*

#	Titulo	Autores	Año	Link
1	An Identity and Access Management Architecture in Cloud	Yan Yang, Xingyuan Chen, Guangxia Wang, Lifeng Cao	2014	https://ieeexplore.ieee.org/abstract/document/7081970/
2	An Analysis of Open Standard Identity Protocols in Cloud Computing Security Paradigm	Nitin Naik, Paul Jenkins	2016	https://ieeexplore.ieee.org/abstract/document/7588881/
3	Cloud Identity And Access Management – A Model Proposal	Dragoş Marian	2012	https://www.researchgate.net/profile/Laura_Brad/publication/260083273_AN_ADJUSTMENT_MODEL_FOR_EVA_COMPUTATION_IN_FINANCIAL_INSTITUTIONS_AND_NON-FINANCIAL_COMPANIES/links/02e7e5340019978b89000000/AN-ADJUSTMENT-MODEL-FOR-EVA-COMPUTATION-IN-FINANCIAL-INSTITUTIONS-AND-NON-FINANCIAL-COMPANIES.pdf#page=1014
4	A framework for authentication and authorization credentials in cloud computing	N. Mimura Gonzalez, M. Torrez Rojas, M. Maciel da Silva, F. Redígolo, T. Melo de Brito Carvalho,	2013	https://ieeexplore.ieee.org/abstract/document/6680881/

		C. Miers, M. Näslund and A. Shohel Ahmed		
5	Authorization Federation in IaaS Multi Cloud	Navid Pustchi, Ram Krishnan, Ravi Sandhu	2015	https://dl.acm.org/doi/abs/10.1145/2732516.2732523
6	Cloud computing security: protecting cloud-based smart city applications	Alkiviadis Giannakoulias	2016	https://www.udspub.com/ajj/public/index.php/jsc/article/view/67
7	Cloud security and privacy: an enterprise perspective on risks and compliance	T Mather, S Kumaraswamy, S Latif	2009	https://books.google.com/books?hl=es&lr=&id=BHazecOuDLYC&oi=fnd&pg=PR7&dq=Cloud+security+and+privacy:+an+enterprise+perspective+on+risks+and+compliance&ots=FA8cI7kSBb&sig=0FPhd6eT-T3a5IVyU-Lt5uJdJXk
8	An analysis of the cloud computing security problem	M Almorsy, J Grundy, I Müller	2016	https://arxiv.org/abs/1609.01107
9	Cloud computing: implementation, management, and security	JW Rittinghouse, JF Ransome	2016	https://books.google.com/books?hl=es&lr=&id=YRIeASgVUJoC&oi=fnd&pg=PP1&dq=Cloud+computing:+implementation,+management,+and+security&ots=z7EOrajmUI&sig=QxnwUAXVNqwWXRl0_zTKmg1-fBU
10	Towards secure mobile cloud computing: A survey	AN Khan, MLM Kiah, SU Khan, SA Madani	2013	https://www.sciencedirect.com/science/article/pii/S0167739X12001598
11	Security and privacy in cloud computing: a survey	S Srinivasamurthy, DQ Liu, AV Vasilakos…	2013	https://core.ac.uk/download/pdf/47229243.pdf
12	Cloud computing: theory and practice	DC Marinescu	2017	https://books.google.com/books?hl=es&lr=&id=O9smDwAAQBAJ&oi=fnd&pg=PP1&dq=Cloud+computing:+theory+and+practice&ots=NOpWIBoZEO&sig=lO-YiQ7tX_Yu0zLHDd8JXe3-h3g

13	Making use of cloud computing for healthcare provision: Opportunities and challenges	N Sultan	2014	https://www.sciencedirect.com/science/article/pii/S0268401213001680
14	Identity and access management in cloud environment: Mechanisms and challenges	I Indu, PMR Anand, V Bhaskar	2018	https://www.sciencedirect.com/science/article/pii/S2215098617316750
15	Robust identity and access management for cloud systems	FMPD Johnson	2020	https://era.library.ualberta.ca/items/e0cb46ef-903d-4aaa-b0ee-97c0a9102dd1

A2.4.4 Extracción de información

Para la extracción de información relevante sobre los estudios primarios, se consideran los siguientes elementos:

- Autenticación de acceso a servicios en la nube
- Gestión de Identidad y Acceso
- Evaluaciones de riesgos centradas en los datos
- Acceso de herramientas de auditoría
- Autorización de acceso de usuarios
- Seguridad de la red

Tabla 9. *Extracción fuente 1*

Repositorio	**Google Scholar**
Titulo	An Identity and Access Management Architecture in Cloud
Publicación	2014 Seventh International Symposium on Computational Intelligence and Design
Autores	Yan Yang, Xingyuan Chen, Guangxia Wang, Lifeng Cao
Referencia	Y. Yang, X. Chen, G. Wang and L. Cao, "An Identity and Access Management Architecture in Cloud," 2014 Seventh International Symposium on Computational Intelligence and Design, Hangzhou, 2014, pp. 200-203, doi: 10.1109/ISCID.2014.221.

Descripción	
Área	Gestión de Identidad y Acceso
Resumen	Gestión de identidad y acceso es esencial para asegurar servicios en la nube. Este documento presenta una arquitectura de gestión de identidad y acceso para resolver una serie de problemas que el modelo de computación en la nube ha traído en este espacio. La arquitectura que se considera para gestión de identidad y acceso provee a los usuarios acceso a los recursos en la nube para resolver algunos de las limitaciones en la arquitectura existente. La arquitectura usa seguridad como servicio para poder lograr una solución escalable y estandarizada, además propone una solución específica a ser implementada.
Aspectos Por Destacar	
	El documento propone implementaciones de Identity Access Management, dado que en ese momento no estaban desarrolladas las soluciones internas de cada proveedor de nube

Tabla 10. *Extracción fuente 2*

Repositorio	**Google Scholar**
Titulo	An Analysis of Open Standard Identity Protocols in Cloud Computing Security Paradigm
Publicación	2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress
Autores	Nitin Naik, Paul Jenkins
Referencia	N. Naik and P. Jenkins, "An Analysis of Open Standard Identity Protocols in Cloud Computing Security Paradigm," 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), Auckland, 2016, pp. 428-431, doi: 10.1109/DASC-PICom-DataCom-CyberSciTec.2016.85.
Descripción	
Área	Protocolos de identidad de estándar abierto

Resumen	Computación en la nube habilita a negocios la posibilidad de usar recursos computacionales bajo demanda, desde cualquier lugar del mundo sin tener que construir y mantener infraestructuras computacionales locales. Este modelo implica diferentes partes ejecutando diversas operaciones a través de Internet, por múltiples organizaciones. Los empleados y clientes pueden acceder a recursos y servicios desde sus propias organizaciones. A pesar del éxito de la computación en la nube, el paradigma de seguridad tiene un gran desafío: como determinar la identidad y los derechos de acceso para los usuarios a través de todas las organizaciones. Las credenciales de usuario e información sensitiva son almacenadas y mantenidas por la organización primaria, pero, otras organizaciones requieren verificar la identidad del usuario y derechos de acceso para permitirle acceder a los servicios y recursos de esa organización. La dificultad más grande es comunicar la identidad del usuario a las demás organizaciones, sin enviar información sensitiva. Numerosos protocolos de estándar abierto para identidad han sido introducidos en las últimas dos décadas. Entre ellos, tres protocolos conocidos, el Lenguaje de Marcado para Confirmaciones de Seguridad, conocido como SAML, autenticación abierta, conocido como OAuth y OpenIdConnect (OIDC) son los más establecidos en la industria. Por ende, este documento presenta un prototipo y análisis crítico de SAM, Oauth y OIDC. También explora los criterios de evaluación que son utilizados para propósitos de análisis. Finalmente, discute las fortalezas y las limitaciones, determina el estándar más adecuado para todo tipo de modelos de computación en la nube.
Aspectos Para Destacar	
	El documento se centra en protocolos estándar, para uno en desarrollos complejos con muchas organizaciones diferentes involucradas. El escenario de este trabajo es más homogéneo y con repositorios de autenticación creados entre las compañías involucradas.

Tabla 11. *Extracción fuente 3*

Repositorio	**Google Scholar**
Titulo	Cloud Identity And Access Management – A Model Proposal
Publicación	7th International Conference Accounting and Management Information Systems AMIS 2012
Autores	Dragoş Marian
Referencia	Dragos Marian MANGIUC, 2012. "Cloud Identity and Access Management – A Model Proposal," Journal of Accounting and Management Information Systems, Faculty of Accounting and Management Information Systems, The Bucharest University of Economic Studies, vol. 11(3), pages 484-500, September.
Descripción	
Área	Gestión de Identidad y Acceso

Resumen	Aun en una organización típica, en la cual las aplicaciones son implementadas dentro del perímetro de la organización, el perímetro de confianza es mayoritariamente estático es monitoreado y controlado por el departamento de TI; con la adopción de servicios en la nube, el perímetro de confianza de la organización se va a volver dinámico y moverse fuera del control de TI. Con computación en la nube, la red, sistemas y perímetro de aplicaciones se extiende dentro del proveedor de servicios. Esta pérdida de control continúa retando el modelo establecido de control y gobernanza, y si no es manejado adecuadamente, va a obstruir la adopción de servicios en la nube. Basado en Revisión de literatura e investigación, este documento a una síntesis de los resultados de una Revisión detallada de las opiniones e intentos de estudios realizados durante los últimos anos entre compañías rumanas y extranjeras, para encontrar y formular un modelo consistente para gestión de identidad y acceso integrada, y de ser posible, una extensión del modelo para la nube. Este documento es parte de una investigación más grande realizada por el autor en el campo de computación en la nube y tecnologías aledañas.
Aspectos Para Destacar	
	Discute gestión de identidad y acceso utilizando herramientas internas como LDAP y Active director, además habla sobre autorización y la implementación de RBAC

Tabla 12. *Extracción fuente 4*

Repositorio	**Google Scholar**
Titulo	A framework for authentication and authorization credentials in cloud computing
Publicación	2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications
Autores	N. Mimura Gonzalez, M. Torrez Rojas, M. Maciel da Silva, F. Redígolo, T. Melo de Brito Carvalho, C. Miers, M. Näslund and A. Shohel Ahmed
Referencia	N. M. Gonzalez et al., "A Framework for Authentication and Authorization Credentials in Cloud Computing," 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Melbourne, VIC, 2013, pp. 509-516, doi: 10.1109/TrustCom.2013.63.
Descripción	
Área	Gestión de Identidad y Acceso

Resumen	Una de las preocupaciones principal es cuando se adopta tecnologías en la nube es la seguridad. Las soluciones en la nube no solo incluyen problemas heredados de tecnologías relacionadas, como virtualización y computación distribuida, pero también trae preocupaciones nuevas asociadas a la complejidad del ecosistema en la nube, compuestos por entidades de nube y sus interacciones. Una de las preocupaciones es relacionada con la autenticación y la autorización en la nube, su capacidad para proveer mecanismos robustos para identificar y establecer sus permisos y roles en la nube, como controlan el uso de recursos, promueve aislamiento y contabilidad de acciones. Este documento identifica el estado de la cuestión en manejo de credenciales enfocándose en ecosistemas de nube. Propone una clasificación de credenciales y un marco de trabajo para estudiar y desarrollar soluciones en este contexto, unificando conceptos relacionadas con modelos de implementación en la nube, tipos de servicios, entidades y controles de ciclo de vida.
Aspectos Para Destacar	
	Se basa en NIST y propone un marco de trabajo de manera holística

Tabla 13. *Extracción fuente 5*

Repositorio	**Google Scholar**
Titulo	Robust identity and access management for cloud systems
Publicación	Faculty of Graduate Studies, Concordia University of Edmonton
Autores	Florence Mary Paul David Johnson
Referencia	David, M. P., J. (2020). Robust identity and access management for cloud systems (Unpublished master's thesis). Faculty of Graduate Studies, Concordia University of Edmonton. Retrieved July 1, 2020, from https://era.library.ualberta.ca/items/e0cb46ef-903d-4aaa-b0ee-97c0a9102dd1
Descripción	
Área	Gestión de Identidad y Acceso
Resumen	Con el incremento en ataques que generan pérdidas financieras y brechas que causan exposición de datos en ambientes basados en nube, las organizaciones deben considerar de manera urgente en invertir en soluciones de gestión de identidad y acceso, que sean útiles y cumplan con los requerimientos para proteger identidades en la nube. Un sistema robusto de IAM actúa como una frontera de seguridad, que controla la autenticación, autorización y control de acceso para ambos identidades y equipos dentro y fuera de la organización. Este documento detalla los requerimientos de un sistema de gestión de identidad y acceso, además de varios ataques debido a controles débiles. El análisis comparativo de las tecnologías y requerimientos dota un marco de trabajo de IAM dirigido a un acercamiento más integrado para asegurar identidades y los sistemas de gestión de identidad y acceso. El marco de trabajo es logrado creando un algoritmo robusto, para mejorar el nivel de confianza en la verificación de identidad, y monitoreo continuo de las identidades y actividades en la nube.

Aspectos Para Destacar	
	Crea un marco de trabajo para una gestión de identidad y acceso robusto, basado en CSA y NIST, parte de lo que espero crear con este trabajo

Apéndice B

Plan de seguridad para infraestructura y plataforma como servicio en Teradyne

Objetivo del plan

Este documento provee una guía para asegurar infraestructura de servicios en la nube, para ser usado por empleados, contratistas y consultores de tecnologías de información en servicios actuales o durante la implementación de nuevos servicios.

Toda implementación de computación en la nube sea en modelo de plataforma como servicio o infraestructura como servicio en Teradyne y las unidades de negocio, deben cumplir con los requisitos de seguridad planteados a continuación.

Auditoría y seguridad

Todo servicio en la nube debe someterse al proceso de revisión de seguridad del departamento de información de seguridad. El responsable técnico del servicio debe llenar el documento llamado “Teradyne BPIT Cloud Security Checklist”. Este contiene una lista de verificación de controles de seguridad que debe cumplir antes de poder ser activado.

Los servidores y dispositivos que provean el servicio deben someterse a un escaneo de vulnerabilidades mediante la utilización de la solución corporativa, los hallazgos clasificados como críticos y altos deben ser resueltos antes de poder dar de alta al servicio. Además, se debe calendarizar el escaneo de vulnerabilidades de manera mensual, de tal manera, se puede mantener al día con nuevas amenazas.

Gobernanza, gestión de riesgos y cumplimiento

Todo servicio en la nube debe apegarse a lo definido en la política de uso aceptable de tecnología y la política de seguridad de la información.

Se debe documentar en la lista de verificación de controles de seguridad los estándares de seguridad que aplica el proveedor de nube, si posee certificaciones y los controles que posee para cumplir con las diferentes legislaciones sobre protección de datos en las diferentes regiones en las que opera.

Administración de continuidad de negocios y resiliencia operacional

Se debe identificar los riesgos más grandes que posee el servicio y cuantificar las posibilidades de materializarse. Además, es necesario documentar si existen controles que lo mitiguen.

Se debe crear la documentación adecuada para evidenciar las capacidades de recuperación de desastre y su procedimiento. Iniciando por el documento “High level recovery strategy” que como dice su nombre debe demostrar la estrategia de alto nivel para la recuperación de este servicio. Seguido por una descripción paso a paso del proceso de recuperación y la reversión al estado original en el documento “Detailed disaster recovery procedure”.

El proceso de recuperación se debe justificar con una lista de pruebas para confirmar operación. Esto debe estar plasmado en el documento “Test Plan and results for disaster recovery”. Se debe probar este procedimiento una vez al año y los resultados grabados en el mismo documento.

Esto debe ser almacenado en la aplicación de base de datos de recuperación de desastre y aprobado por el departamento de seguridad de la información y el cumplimiento legal.

Administración de control de cambios y configuración

Los cambios para ambientes en la nube deben seguir los lineamientos definidos en el proceso de control de cambios definido para el departamento de tecnologías de información. Los detalles y el flujo de la descripción funcional se pueden encontrar en la publicación “Change Control Database”.

Esto incluye cambios realizados por el proveedor de servicios en la nube, a pesar de que no son ejecutados por un empleado de la compañía, se debe considerar el posible impacto a la disponibilidad de ese servicio.

Criptografía, encriptación y gestión de llaves

Se debe utilizar la solución corporativa para generar certificados con uso de cara a Internet. Esto ha de ocurrir si el servicio requiere el uso de certificados para encriptar el tráfico y el acceso se provee por medio de uno de los dominios públicos de Teradyne o sus unidades de negocio.

Si el certificado es de uso interno y es de cara a usuarios finales, debe utilizar la solución corporativa interna para certificados privados. La persona técnica responsable del servicio en ambos casos debe almacenar la llave privada en un repositorio privado, con acceso restringido y auditable.

El almacenamiento de las estaciones de trabajo y los servidores debe estar encriptada en reposo. Las llaves de autenticación para los túneles que conectan a los servicios en la nube deben ser almacenadas en un servicio centralizado para tener acceso limitado y auditado.

En caso de que las estaciones de trabajo en la nube requieran certificados de usuario final, se debe utilizar el certificado generado para el cliente de VPN VT3. De

manera que sea centralizada la gestión y pueda ser fácilmente revocable en caso de ser necesario.

Si es un ambiente de desarrollo, pruebas o de acceso exclusivo para BPIT[9], es aceptable el uso de certificados autofirmados.

Gestión de ciclo de vida de seguridad de datos y privacidad

Si el servicio usa datos restringidos o información de identificación personal para personas se debe cumplir con las auditorias y controles propuestos por el comité de protección de la información. Además, ha de tenerse en consideración las leyes de exportación de datos en los países donde residen los ambientes de nube y de donde se operan.

Toda estación de trabajo debe tener los sistemas de protección y sistema de etiquetado de datos y prevención de exfiltración de datos. Debe incluirse esta instalación en el proceso de creación de máquinas virtuales.

Gestión de acceso e identidad

El acceso al portal administrativo de la solución de nube debe ser integrado con un recurso interno de administración de usuarios, de preferencia Active Directory y con autenticación de múltiple factor habilitado. Debe autorizarse el acceso basado en roles, de tal manera que el personal tenga acceso a modificar los elementos relacionados con su posición. Lo mismo aplica para la asignación de grupos de recursos, se dará acceso a modificar solo los grupos que sean relevantes para

[9] El departamento llamando Business Processes and Information Technology que contiene el departamento tecnologías de información.

mantenimiento y administración. Se puede proveer acceso de lectura a los otros grupos de la solución, para dar contexto al diseño macro.

El acceso de usuarios a la plataforma debe ser integrado con Active Directory para centralizar accesos y claves por medio de la gestión de acceso e identidad. Además, debe controlarse el acceso por medio de grupos de seguridad, estos deben estar asignados a roles que provean el mínimo acceso requerido basado en la teoría de acceso basado en roles y el acceso de menor privilegio.

En caso de tener que usar otra solución para gestión de acceso, se debe apegar a la política de claves definida por la compañía, habilitar, de ser posible, autenticación de múltiples factores, capacidad de auditoria, mantenimiento de registros y tener un proceso creado para la suspensión o eliminación de cuentas de manera expedita para terminación de usuarios y eventos de seguridad.

Estos usuarios deben ser asignados a una sola persona. Al no estar integrados con un repositorio, debe contener detalles suficientes para poder identificar el dueño de la cuenta, debe contar con autenticación de múltiple factor. La cuenta debe ser creada con una clave inicial, generada automáticamente y forzar al usuario a cambiarla durante el primer acceso. Esta clave no debe ser compartida por medios no encriptados.

Si el usuario requiere gestión de claves, se utiliza la solución corporativa y se refiere a la política “Password Manager Tools”

Las claves de usuarios locales y claves de acceso administrativo deben ser almacenadas y accedidas desde el repositorio de claves centralizado.

Registro de operaciones y monitoreo

Los sistemas deben utilizar una fuente de tiempo confiable y tener la configuración de registros de sistema habilitada y estandarizada.

Se debe generar y almacenar registros de sistema, para los dispositivos en la nube en un repositorio centralizado con acceso restringido, capacidad de auditoria, separación por equipo y ambiente, búsqueda y filtración.

Los sistemas administrables deben ser monitoreados en un sistema centralizado, tanto la disponibilidad como estado de los recursos, debe contar con un proceso para notificación y apertura de incidente en caso de sobrepasar los límites establecidos de operación normal.

Gestión de incidentes de seguridad, descubrimiento digital y recopilación de información forense en la nube

Los eventos de sistema deben ser monitoreados para detectar incidentes de seguridad, se recomienda que el proceso de monitoreo incluya acciones para eventos de sistema de nivel alto y crítico, el cual debe tener notificación por correo y creación de un incidente para investigación.

Al comprobar un incidente de seguridad, se debe trabajar en la resolución, considerando conservar evidencia forense para poder realizar un análisis post mortem del incidente. Hacer un respaldo de la imagen, el estado del equipo y la configuración actual.

Gestión de cadena de suministro, transparencia y responsabilidad

Para cada modelo de servicio diferente en un proveedor de nube, se debe definir un modelo de responsabilidad compartida de seguridad. Con esta información, se pueden definir las responsabilidades del departamento de tecnología de

información, el proceso de reporte de incidentes y escalación en caso de una interrupción de servicio. Este proceso debe tener una revisión anual, de tal manera que se pueda implementar mejoras.

Gestión de amenazas y vulnerabilidades

Las estaciones de trabajo en la nube deben contar con el control de parches y actualizaciones para aplicaciones y sistemas operativos utilizado en el resto de las estaciones de trabajo, para asegurar uniformidad en versiones de software y parches de seguridad.

En cuanto a la detección de malware y antivirus, se debe utilizar la solución actual para estaciones de trabajo locales, esto permite tener las mismas políticas de protección en todas las estaciones, sin importar su ubicación.

Las estaciones están incluidas en los reportes calendarizados de infecciones y ataques, para poder detectar, contener y prevenir amenazas.

También debe contar con la solución de protección de amenazas a estaciones finales definida en el documento “Crowdstrike Falcon Endpoint Protection”

Gestión universal de estaciones finales

Las estaciones de trabajo en la nube deben cumplir los mismos requerimientos que las físicas en sitio. Deben pertenecer a uno de los dominios y tener las políticas de grupo aplicadas, para forzar políticas como las definidas en “Screensaver Password Protection”

Los perfiles de usuario deben tener el rol de usuario y no utilizar permisos de administrador, cualquier modificación al sistema debe ser aprobada y ejecutada por el personal tecnologías de información.

El *software* instalado debe apegarse al estándar “Teradyne Desktop Software Standards”, en caso de requerir software no estándar seguir el proceso “Order Non-Standard IT Hardware and software”

El almacenamiento de las estaciones de trabajo en la nube debe poseer encriptación en reposo y la clave debe ser administrada de manera centralizada.

La información clasificada como secreto, confidencial y propiedad intelectual debe ser almacenada en repositorios seguros y no localmente en las estaciones.

Recomendaciones para infosec

Se recomienda que el departamento de información de seguridad considere las siguientes mejoras en procesos:

- Se debe incluir los servicios provistos desde la nube en el proceso para alcanzar el tercer nivel de madurez definido por la NIST.
- Se recomienda crear un proceso de gestión de riesgos alineado con estándares de industria, como ISO-31000.
- Se recomienda desarrollar una política que detalle los algoritmos de encriptación aceptables en la compañía con revisión anual.
- Integrar claves de encriptación para túneles de IPSec en el repositorio de claves.
- Generar un proceso para recolección de evidencia forense en caso de un incidente de seguridad.
- Recopilación de procesos de escalación y SLAs en caso de incidentes en los diferentes proveedores de nube.
- Definir política de gestión de claves de encriptación para estaciones de trabajo en la nube.

Apéndice C

Se adjunta documento ‘Manual para implementación de medidas de seguridad en infraestructura como servicio en Teradyne’

Manual para implementación de medidas de seguridad en infraestructura como servicio en Teradyne

Primero se debe confirmar que el módulo Azure AD Connect[10] se encuentre instalado en un controlador de dominio local y esté configurado correctamente para obtener información desde Azure. El desglose paso a paso se puede encontrar en https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install

Se debe conectar el Access Control (IAM) de la suscripción para utilizar las credenciales de Active Directory y utilizar Single Sign-On (SSO)[11]. Se pueden utilizar los roles creados por defecto en Azure para designar niveles de acceso, estos deben ser asignados a grupos de usuarios manejados desde AD, de tal manera que exista un solo repositorio para mantener el privilegio sobre las actividades en la nube.

Se deben crear roles separados para los administradores de la clase y los estudiantes, para que tengan acceso solo a los recursos relevantes. Se recomienda que el rol de administrador de clase sea un grupo de Active Directory para asignar los permisos específicos para el rol.

En cuanto a la administración de Azure Bastion, la solución actual en la que se comparte el usuario y la clave por medio de correo no se considera seguro, a pesar de que la clave es temporal y debe ser cambiada durante el primer acceso. Se

[10] Herramienta para conectar una implementación de Active Directory local a la nube de Microsoft Azure

[11] El inicio de sesión único es un procedimiento de autenticación que habilita un usuario acceder varios sistemas con una sola instancia de identificación.

recomienda habilitar autenticación por múltiples factores durante el proceso de registro, así el estudiante requiere el usuario, la clave y un código de único uso generado por medio de OTP.

En cuanto a la segunda solución, compartir el usuario y la clave por medio de correo no se considera seguro, a pesar de que la clave es temporal y debe ser cambiada durante el primer acceso. Se recomienda habilitar autenticación por múltiples factores durante el proceso de registro, así el estudiante requiere el usuario, la clave y un código de único uso generado por medio de OTP. Además, se recomienda que las credenciales de la cuenta local de la máquina virtual sean compartidas durante la sesión de entrenamiento por medio de voz o chat individual. Estas claves deben ser cambiadas después de cada clase, para evitar la reutilización.

El usuario con privilegios de super administrador debe ser una cuenta separada de la cuenta de Active Directory del usuario, para reducir la posibilidad de escalación de privilegios por parte de un atacante. Además, se debe habilitar autenticación de múltiples factores para Microsoft Azure Management. El desglose paso a paso se puede encontrar en https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa

La red virtual (VNET) donde se conecta a Aryaka SD-WAN debe implementar un firewall para filtrar e inspeccionar el tráfico de entrada y salida del ambiente, para poder limitar el acceso en caso de un evento de seguridad.

Las estaciones de trabajo deben contar con Kace Agent para administración de parches y actualizaciones. También debe contar con Crowdstrike Falcon Endpoint Protection para protección de estaciones y el cliente de Forcepoint para el filtrado de URLs y control de acceso web. Estos deben incluirse en la imagen de la máquina virtual.

En caso de servidores, deben contar con el agente de Rapid7 Insight para manejo de vulnerabilidades. Si no puede instalarse un agente, se debe manejar vulnerabilidades de manera remota con Rapid7 Nexpose Scanner y se debe calendarizar escaneos semanales.