Universidad de Buenos Aires
Facultades de Ciencias Económicas,

Cs. Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Tesis de Maestría

Título

Análisis de arquitectura y diseño de metodología de seguridad de confianza cero para los servicios en la nube

Autor/a:
Ing. Harold David Chaparro Zuñiga

Director/a del Tesis
Dr. Pedro Hecht

Año de Presentación 2023
Cohorte del Maestrando 2014

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual

Resumen

En el presente trabajo partiremos de un análisis de los riesgos actuales de la computación en nube, posteriormente realizaremos una recopilación de toda la documentación, estándares del mercado y documentos investigativos actuales asociados a confianza cero. Finalmente diseñaremos una metodología de fácil entendimiento y aplicación que ayude a las organizaciones a entender el valor generado en su adopción y los pasos para integrar estos principios, conceptos y prácticas a un modelo seguridad en ambientes de nube.

Palabras clave

Confianza cero, seguridad en la nube, Arquitectura de seguridad, ciberseguridad

INDICE GENERAL

1 Introducción

Las estrategias y arquitecturas actuales de seguridad no están diseñadas para las necesidades de las empresas modernas donde vemos un crecimiento exponencial en la adopción de tecnologías en nube [1] y la digitalización de los procesos de la organización [2]. Esta ruta que están adoptando las organizaciones las obliga a migrar a nuevos modelos de trabajo distribuido, a actualizar sus procesos y extenderlos a estas nuevas tecnologías. La movilidad es dominante en este mundo aumentado la superficie de exposición de las organizaciones y a su vez con la misma velocidad a crecido la capacidad de los cibercriminales para aprovechar estos cambios. Los ataques a las organizaciones se han vuelto más sofisticados y complejos donde vemos un aumento como objetivo a los usuarios posicionándose como el principal vector empleado por los cibercriminales [3].

Adaptarnos al cambio continuo y la evolución tecnológica debe ser uno de los objetivos estratégicos de una organización. Los peligros de no contar con una visión, un modelo y/o artefactos que ayuden a entender a la organización, de una forma ordenada, con un lenguaje fácil y estándar y alineados a las mejores prácticas y tendencias de la industria al momento de adoptar una estrategia y/o mover cargas de trabajo hacia la nube puede verse reflejado en la materialización de riesgos de seguridad e impactos asociados a perdidas de posicionamiento en el mercado, pérdidas económicas en su razón u objeto de negocio o derivadas de brechas de seguridad materializadas que su vez impacta en la imagen y reputación de la organización. Construir un modelo de seguridad basado en los principios de confianza cero que acompañe todos estos cambios que están sufriendo las organizaciones y que permita a las áreas del negocio y tecnología y a los procesos que identifican y habilitan soluciones, entender las necesidades del negocio frente a la seguridad es una necesidad imperativa que soluciona la problemática planteada.

2 Marcos de seguridad en nube

Los procesos que identifican y habilitan soluciones tecnológicas hacen parte de la columna vertebral de una organización, ya que tienen como objetivo generar valor al negocio identificando de manera sistemática, los requerimientos funcionales y no funcionales sobre las necesidades y/o oportunidades a cubrir y así poder llevar de manera armoniosa una solución a un ambiente productivo. Cuando nos enfrentamos a las preguntas sobre como deberíamos integrar la seguridad dentro estos procesos, en qué etapas y como se debían ser abordadas y priorizadas, comúnmente se presenta la falta de documentación y/o artefactos que brinden una gruía y forma clara de atacar este problema siendo una constate necesidad, sin embargo, diferentes entidades como el "*International Organization for Standardization*" en adelante ISO, el "*National Institute of Standards and Technology*" en adelante NIST, el "*Cybersecurity and Infrastructure Security Agency*" en adelante CISA y el "*The Cloud Security Alliance*" en adelante CSA, iniciaron la creación de un conjunto de marcos de trabajo con diferentes enfoques, pero con el único objetivo de reunir las mejores prácticas para poder resolver estas problemáticas

En la actualidad existen diferentes marcos de referencia de seguridad que nos brindan una guía de cómo debemos abordar los retos y riesgos del negocio y que son adaptables a las tecnologías/servicios en nube. Las organizaciones deben determinar si uno o más puede suplir las necesidades que tiene en cuento a su objeto de negocio y estrategia y estos pueden convivir si se adoptan de forma correcta. La elección del marco debe partir de los requerimientos normativos y regulatorios, la estrategia tecnológica, y las necesidades y objetivos de la organización ya que debe apoyar al éxito del plan estratégico de seguridad para soportar sus necedades actuales y futuras.

A continuación, nombramos algunos de los marcos de seguridad de referencia relevantes del mercado.

2.1 Guía de seguridad de áreas críticas para la computación en la nube propuesta por la CSA

La CSA es una organización con el objetivo de promover buenas prácticas de seguridad en entornos de nube, hoy por hoy es un referente en la comunidad gracias a las diferentes publicaciones orientadas a brindar una forma clara de entender las amenazas que se presentan al momento de adoptar servicios en nube y la forma de mitigarla por medio de controles técnicos y procedimentales listados en sus publicaciones. A continuación, se detalla el proceso propuesto por CSA a seguir para gestionar la seguridad en la nube:

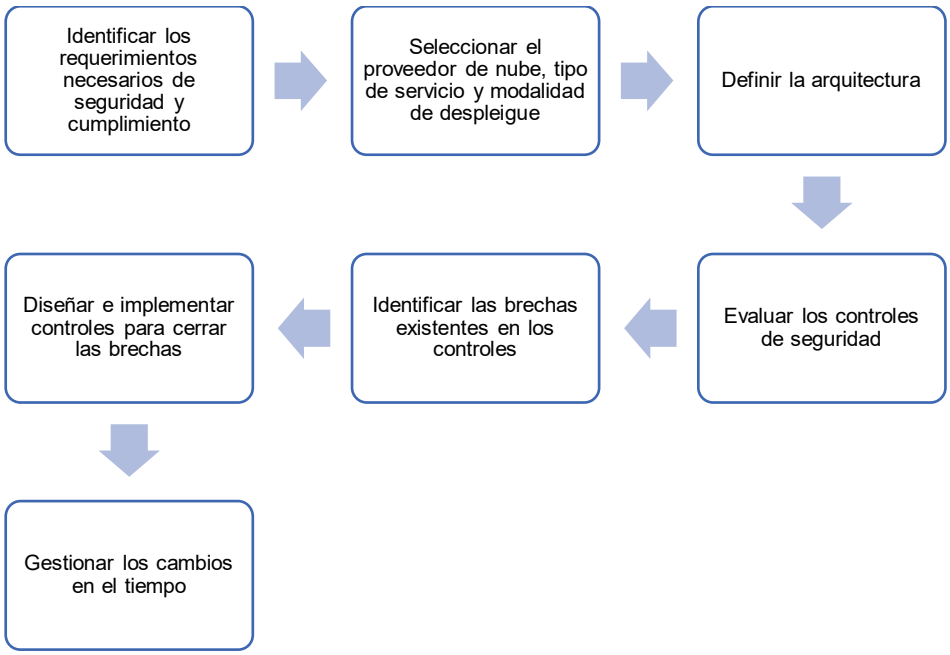

Ilustración 1: Gestión de seguridad en la nube, Guía de Seguridad de Áreas Críticas para la Computación en la Nube. Fuente: [4]

La “Guía de Seguridad de Áreas Críticas para la Computación en la Nube” [4] está construida a partir de las mejores prácticas actuales y nos ayuda a identificar las capacidades que debemos desarrollar para asegurar una buena postura de seguridad en la nube buscando aprovechar las herramientas nativas del proveedor de servicios para apoyar la estrategia de seguridad.

A continuación, se detallan las 13 categorías que define la CSA [4]:

- Gobierno y gestión de riesgos empresariales
- Cuestiones legales, contratos y descubrimiento electrónico
- Gestión de cumplimiento y auditoria
- Gobierno de la información
- Gestión y continuidad de negocio
- Seguridad en la infraestructura
- Virtualización y contenedores
- Respuesta, notificación y remediación de incidentes
- Seguridad en las aplicaciones
- Cifrado y seguridad de datos
- Gestión de identidad, derechos y accesos
- Seguridad como servicio
- Tecnologías relacionadas

2.2 Marco de trabajo de ciberseguridad de la NIST

El NIST, es una agencia estadounidense que promueve la evolución, innovación y el desarrollo de capacidades en ciencia y tecnología por medio de la publicación de estándares y directrices aplicables a organizaciones gubernamentales y diferentes sectores de la industria. En el ámbito de seguridad, apoya en la gestión de riesgos de cibernéticos por medio de la publicación de herramientas basadas en las mejores prácticas del mercado, que brindan una visión estratégica, ordenada, medible y adaptable de cómo debemos abordar estos riesgos de fácil entendimiento y adopción para el negocio. Los documentos se construyen con la participación de diferentes sectores por lo cual abarca las necesidades actuales de diferentes tipos de industria y las tendencias tecnológicas.

Impulsados por la necesidad del aseguramiento de infraestructuras críticas y a raíz del crecimiento de incidentes de seguridad, en el año 2013 se emite la orden ejecutiva 13636 por el gobierno de los estados unidos, la cual solicita el desarrollo y evolución continua de un marco de trabajo que permita

a las organizaciones adoptar un modelo de gestión de riesgos cibernéticos por medio de la definición un conjunto de etapas y prácticas de seguridad que se deben ejecutar de manera continua para reducir los riesgos en los ambientes tecnológicos en premisa y en nube.

El marco de trabajo de ciberseguridad [5] se conforma por 3 capítulos que se detallan a continuación:

- **Núcleo del marco de trabajo:** este capítulo detalla un conjunto de actividades, prácticas y controles tecnológicos definidos por diferentes marcos de seguridad, con el objetivo de apoyar su entendimiento e implementación apoyar el ciclo de vida de gestión del riesgo cibernético. Está compuesto por 5 funciones (identificar, detectar, proteger, responder y recuperar) que establecen las acciones a realizar por las diferente a áreas tecnológicas y de negocio. Estas funciones contienen 23 categorías y 108 subcategorías con los controles técnicos y procedimentales necesarios para soportar los resultados esperados definidos en las funciones.

- **Niveles de implementación:** este capítulo ayuda a la organización a identificar y establecer el nivel actual en cuanto a incorporación y ejecución de las actividades necesarias para la gestión del riesgo cibernético. La definición del nivel brinda una idea del nivel de madurez actual y apoya a la toma de decisiones frente a las actividades necesarias para apoyar y alinearse a la estrategia y objetivos de la organización. El marco define 4 niveles: nivel 1 - Parcial, nivel 2 - Riesgo informado, nivel 3 - Repetible y nivel 4 - Adoptado, siendo 1 el nivel más básico en cuanto a la formalización de un proceso de gestión de riesgos cibernéticos y su alineación con la organización y 4 el más avanzado demostrando una estrategia holista de gestión que apoya y habilita al logro de los objetivos de la organización.

- **Perfiles**: permite definir perfiles basados en las necesidades y objeto de negocio, es fundamental tener una visión clara del estado actual y estado deseado ya que sin poder medir nuestro estado actual y

avances no podemos definir una estrategia clara para su evolución y mejora. Adicionalmente, el perfil establece punto inicial para la integración y evolución de este marco de trabajo dentro de la estrategia de seguridad, permitiendo priorizar los esfuerzos e inversiones a realizar para alcanzar un nivel deseado a partir del desarrollo de nuevas capacidades y la evolución continua de las practica de seguridad definidas en este marco.

Por último, los proveedores de servicios de nube en busca de proveer de herramientas a los clientes para asegurar el entendimiento de la responsabilidad sobre los servicios y las practicas que se deben ejecutar para asegurar los entornos de nube que ofrecen, publican marcos de referencia arquitectónicos y de seguridad que determinan la mejor forma de emplear sus servicios de forma segura.

3 Amenazas de seguridad en entornos de nube

El desarrollo de los procesos y objetivos de negocio empleando tecnologías en nube y esquemas de trabajo distribuidos llevan a las organizaciones a plantear un nuevo objetivo de brindar acceso seguro de sus usuarios hacia aplicaciones y/o servicios en las modalidades de infraestructura como servicio en adelante “IaaS” por las siglas de (*Infrastructure as a Service*), plataforma como servicio en adelante “PaaS” por las siglas de (*Platform as a Service*), y software como servicio en adelante “SaaS” por las siglas de (*Software as a Service*), entre otros, con el reto de hacerlos accesibles desde cualquier ubicación y dispositivo no gestionado por la organización. Adoptar tecnologías en nube traen consigo nuevas amenazas que son desconocidas por la organización, es aquí cuando debemos identificarlas y entenderlas para así tener un claro panorama de cómo gestionarlas. Dicho esto, es imperativo entender los modelos de responsabilidad compartida que se establecen con los proveedores de servicios en nube, obteniendo así, un panorama claro de que debemos controlar y así determinar cuáles amenazas pueden afectar mi objetivo.

3.1 Modelo de responsabilidad compartida en la nube

La seguridad en la nube y de la nube son una responsabilidad compartida. Entender este concepto nos permite enfocarnos en las actividades y controles de seguridad que debemos implementar como clientes durante el proceso de migración y/o implementación de las soluciones tecnológicas que desplegamos en la nube, por lo cual es clave, entender los modelos de seguridad con el proveedor de servicios en nube y así tener una visión clara de los riesgos a los que enfrena y que debe gestionar. Estos modelos nos ayudan a determinar hasta qué punto es nuestra responsabilidad como cliente y cual es responsabilidad del proveedor. En los entornos en la premisa, la responsabilidad de cada capa de servicio debe estar a cargo de la organización, desde garantizar una correcta gestión de controles físicos de acceso, flujo de energía, ventilación, entre otros, hasta velar por la correcta

gestión y operación de la seguridad de sus activos tecnológicos. Sin embargo, uno de los beneficios de la nube, es que nos permite delegar la responsabilidad de algunas de estas actividades en nuestro proveedor, permitiendo así a la organización y sus equipos de trabajo, enfocarse en el desarrollo de su estrategia y objetivos de negocio. Esta definición la debemos tomar como base para la construcción de nuestros modelos de seguridad, ya que nos permite determinar los controles, la priorización de su implementación y el esfuerzo que tenemos como clientes para garantizar nuestra postura de seguridad en la nube.

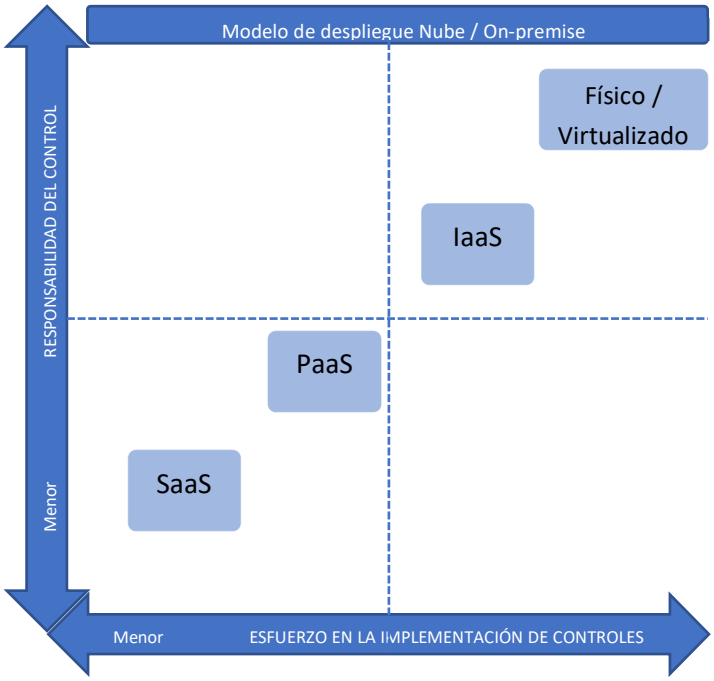

Ilustración 2: Responsabilidad y esfuerzo de implementación de controles en la nube. Fuente: Propia

La gestión y protección de la identidad y los datos siempre será responsabilidad del cliente en cualquier modelo de servicio lo cual expone cada vez más la relevancia de adoptar y/o migrar a modelos enfocados en mitigar las amenazas que puedan afectar a los usuarios y la información que almacenamos y procesamos en la nube.

Enfocar los esfuerzos en mayor medida sobre la gestión de seguridad de la modalidad IaaS debe ser prioridad para la organización. Otro factor que

podemos emplear es el nivel de exposición del recurso. Así, podremos generar una ruta priorizada de recursos a evaluar y asegurar en orden de su criticidad.

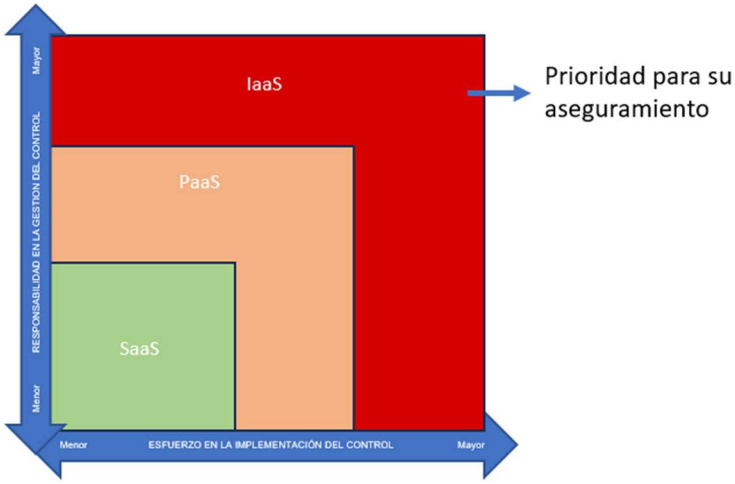

Ilustración 3: Priorización de modelos de servicio en nube. Fuente: Propia

Cabe resaltar que la organización puede evaluar la seguridad que brinda el proveedor de servicios de nube sobre los servicios ofrecidos, para esta actividad existen herramientas como la matriz de controles "*Cloud Controls Matrix and CAIQ*" de la CSA [6] o evidenciando sus capacidades por medio de autoevaluaciones y/o certificaciones tipo ISO, "*Security, Trust & Assurance Registry (STAR)*" de CSA o reportes de auditoría de externos tipo SOC (*System and Organization Controls*) 1,2,3 que den fiabilidad de los controles y practicas implementadas en cuanto a seguridad.

3.2 Amenazas en entornos de nube según *CSA*

La CSA nos brinda periódicamente un informe actualizado sobre los riesgos, amenazas y vulnerabilidades a media que evolucionan las capacidades de los ciberdelincuentes y que la tecnología avanza en el desarrollo de nuevos servicios y paradigmas de adopción. El último informe publicado en el año 2022 desarrolla una investigación sobre las amenazas de mayor importancia e impacto actual en ambientes de nube denominado "*Top Cloud Threats to Cloud Computing - Pandemic Eleven*" [7], el cual presenta

las principales 11 amenazas, el modelo de servicio en el cual se presentan y quien tiene la responsabilidad de realizar su correcta gestión:

Posición	Amenaza	Responsabilidad			Modelo de servicio		
		Compartida	Cliente	CSP	IaaS	PaaS	SaaS
1	Insuficiente identidad, credenciales, gestión de claves y accesos y usuarios privilegiados		X		X	X	X
2	Interfaces y APIs inseguras		X	X			
3	Configuraciones incorrectas e inadecuado control de cambios	X	X	X	X	X	X
4	Falta de arquitectura y estrategia de seguridad en la nube		X		X	X	X
5	Desarrollo de software inseguro	X	X	X	X	X	X
6	Recursos de terceros inseguros	X	X	X	X	X	X
7	Vulnerabilidades del sistema	X	X	X	X	X	X
8	Divulgación accidental de datos en la nube	X	X	X	X	X	X
9	Configuraciones incorrectas y explotación de cargas de trabajo tipo serverless y contenedores	X	X	X	X	X	
10	Crimen organizado/hackers/ amenazas persistentes avanzas (APT)	X	X	X	X	X	X
11	Exfiltración de datos almacenados en la nube	X	X	X	X	X	X

Tabla 1: Distribución de amenazas, responsabilidades y modelos de servicio. Fuente [7]

Con base al informe podemos concluir las organizaciones deben potenciar la constante investigación, evolución e innovación de sus modelos de seguridad para este mundo en constante cambio. Agentes fuera de nuestro control como la pandemia de 2020 fue un impulsador de la acelerada transformación digital que estamos viviendo actualmente, obligando a las organizaciones a adoptar escenarios de trabajo distribuido para los cuales no se encontraba preparado, aumentando su superficie de exposición y con ello las amenazas propias de cada escenario. Esto se ve reflejado en el aumento

de incidentes de seguridad por la masificación en el uso de internet y tecnologías en nube donde los elementos humanos son el principal factor de riesgo [3].

Falta de arquitectura y estrategia de seguridad en la nube y la débil gestión de la seguridad sobre sus usuarios posicionada en el top 1 y 4 de este reporte, impulsa a los responsables de seguridad dentro de las organizaciones a evaluar los modelos actuales de seguridad frente a estas amenazas y sirve como herramienta para concientizar al negocio sobre la importancia de integrarse y alinearse con la estrategia, asignación de recursos e interiorización por la alta dirección de la organización.

4 Modelo y arquitectura de confianza cero

4.1 Inicios de confianza cero

En el año 2010, conocimos el primer uso del término “confianza cero” gracias a las investigaciones de en su momento analista de seguridad de la empresa Forrester John Kindervag [8], quien es considerado el creador del concepto y el pionero en introducir su enfoque a los entornos empresariales como la ruta a seguir para hacer frente a las nuevas complejidades del mundo tecnológico y empresarial. El concepto de eliminar la confianza implícita que se tenía sobre el tráfico de red a partir de su ubicación u origen y diseñar los controles de seguridad basados en el perímetro, estableció los pilares para las estrategias y marcos de trabajo que adoptan las grandes organizaciones en la actualidad. Los primeros conceptos, principios y arquitecturas de referencia de un modelo de red de confianza cero fueron propuestos en su reporte “*Build Security Into Your Network’s*” [8] los cuales se enfocaban en diseñar una estrategia de seguridad ubicando a la red, datos y su acceso seguro como principal objetivo y la etapa inicial en el diseño de un modelo y arquitectura de confianza cero, teniendo claro esto y las necesidades de la organización, estas se agrupan en lo que denomino MCAP “*microcore and perimeter*” [8] por medio de la segmentación de redes y ubicando componentes de seguridad para centralizar el gobierno de accesos de cada MCAP y un registro y monitoreo continuo de este tráfico.

En los años siguientes, las tecnologías de nube se encontraban en auge y eran adoptadas cada vez más por grandes organizaciones llevando a expandir el enfoque inicial de John Kindervag para poder afrontar la evolución y transformación tecnológica que estaban efectuando las empresas en aquel momento como fue el caso de la empresa Google con su proyecto “*BeyondCorp*” [9] reinventando su estrategia de infraestructura y seguridad partiendo de un modelo de seguridad de confianza cero. Si bien en su primera entrega, John Kindervag se encontraba enfocado en soportar el modelo definido a parir de una estrategia segura sobre el diseño y control de seguridad en las redes de la organización, la nube y sus nuevos riesgos en cuanto al

acceso distribuido a la información y evolución del perímetro como los conocíamos, obligo a contemplar dentro del modelo, otros componentes claves a analizar y gobernar dentro de una organización. Este nuevo enfoque se contempló en la evolución que en el 2018, el investigador de seguridad de Forrester Chase Cunningham público en su el informe de investigación "*The Zero Trust eXtended (ZTX) Ecosystem*" [10], el cual propagó el enfoque del modelo de seguridad de confianza cero de manera holística hacia los componentes de un ecosistema de seguridad abarcando datos, redes, cargas de trabajo, personas, y dispositivos donde |cada uno de estos componentes debía tener un tratamiento y aseguramiento especifico además de desarrollar y/o potenciar de capacidades de análisis, monitoreo y automatización de procesos.

Por último, en 2019 el NIST, público el primer borrador del documento "*Special Publication 800-207 - Zero Trust Architecture*" [11], y en 2020 la versión final, en el cual plantea los conceptos de una arquitectura de confianza cero, sus objetivos, componentes, modelos de despliegue y una guía general de implementación entornos empresariales.

En noviembre de 2022 el departamento de defensa de los estados unidos publica el documento "*DoD Zero Trust Strategy*" [12] [13] definiendo 4 pilares enmarcados en un enfoque hacia las personas, buscando un cambio cultural y una capacitación en este nuevo modelo de confianza cero para que sea aplicado en el diseño, integración, desarrollo, despliegue y operación de la estrategia definida. El conjunto de áreas de trabajo sobre las cuales se enfoca la estrategia de seguridad como usuarios, dispositivos, cargas de trabajo, datos, redes, automatización y orquestación y visibilidad y analítica. Una ruta de capacidades tecnológicas y operativas que se deben integrar al ecosistema actual de seguridad. Por último, la restructuración y definición de nuevas políticas, procesos, procedimientos, lineamientos y prácticas para habilitar y gobernar la estrategia, acompañadas del plan de desarrollo y adquisiciones claves para su implementación.

En el desarrollo del documento utilizaremos como referencia los trabajos publicados por la NIST como marco principal y guía de construcción para el modelo a definir. Los documentos publicados por la empresa Forrester "*Build Security Into Your Network's DNA: The Zero Trust Network Architecture*" y "*The Zero Trust eXtended (ZTX)*", las publicaciones realizadas por la NIST sobre arquitecturas de confianza cero "*NIST Special Publication 800-207 - Zero Trust Architecture*" y del departamento de defensa de los estados unidos "*DoD Zero Trust Strategy*".

4.2 Fundamentos de la estrategia y arquitectura de confianza cero

Para iniciar el estudio del enfoque de confianza cero, debemos partir de los retos y riesgos que se presentan en las estrategias y arquitecturas actuales y/o tradicionales que hemos abordado a lo largo de este documento y que se presenta en el top 4 del reporte de amenazas del CSA [7]. Las nuevas tendencias en cuanto a las modalidades de trabajo, las nuevas capacidades de la nube y el uso masivo de dispositivos móviles gobernados y no gobernados por la organización, deben ser un impulsor para que las áreas de seguridad evalúen las capacidades actuales, identifiquen las necesidades y oportunidades que esto puede traer consigo para así evolucionar tanto en la definiciones de nuevos procesos, restructuración de las arquitecturas de seguridad y TI, la adquisición o implementación de nuevos servicios y tecnologías que le permitan habilitar y gestionar de forma segura estos cambios y no entorpecer los proceso de innovación de la organización.

No es común la evaluación de costo beneficio, la usabilidad juega un papel importante y la concientización de cómo llevar una solución tecnológica a producción, surtiendo todos los pasos que permitan sobre el brindar un servicio de forma segura nos puede llevar a confrontaciones con las áreas de negocio. Habilitar servicios en nube sin un respectivo control sobre su exposición que puede ser accedidos desde cualquier ubicación geográfica o dispositivo sin una previa validación del riesgo, el mal diseño de una red en cuanto a la falta de controles como listas de control de acceso, grupos de

seguridad, patrones de diseño de arquitectura, recursos de desarrollo, pruebas y producción en los mismos segmentos de red sin una segregación, y la confianza inherente que damos al tráfico de red, puede permitir conexiones no aprobadas y movimientos laterales luego de una intrusión exitosa a la red, creando así un escenario perfecto para la materialización de un incidente de seguridad.

Una débil estandarización de protocolos y modelos de acceso nos lleva a una no estandarización sobre como los usuarios de la organización, terceros y clientes acceden a nuestros recursos. la gestión de usuarios, permisos y protección de estas identidades sin un proceso y controles definidos puede abrir una brecha de seguridad, es común la asignación de permisos o grupos con políticas amplias, uso constante de usuarios privilegiados para tareas cotidianas y débil trazabilidad de las acciones que estos usuarios ejecutan luego de un acceso exitoso. Por ultimo las malas prácticas frente a la robustez y aseguramiento de credenciales, material criptográfico y/o secretos nos lleva a tener controles débiles frente a la autenticación a nuestra infraestructura y aplicaciones, a riesgos de fuga de información y suplantación de identidad.

La mayoría de las soluciones tecnológicas (infraestructura, aplicaciones, servicios) actualmente brindan un registro de eventos que se convierten en cargas operativas y costos en su almacenamiento. La ausencia de procesos fundamentales de la ciberseguridad como el monitoreo de seguridad, inteligencia de amenazas y cacería de amenazas limitan las estrategias de seguridad y no permite una vigilancia completa de nuestro entorno perdiendo así una valiosa herramienta para el monitoreo, análisis y toma de decisiones por los equipos de seguridad.

Por último, todos procesos de seguridad deben alimentarse unos a otros, ya que en muchos casos son la entrada o detonador de actividades de otros procesos.

Es importante entender los siguientes conceptos que trabajaremos a lo largo del documento. La identidad como “Un atributo o conjunto de atributos que describen de forma única un tema dentro de un contexto determinado” [14], la autenticación como “Verificar la identidad de un usuario, proceso o

dispositivo, a menudo como requisito previo para permitir el acceso a los recursos de un sistema de información" [15] y la autorización como "Privilegios de acceso otorgados a un usuario, programa o proceso o el acto de otorgar esos privilegios" [16].

A continuación, abordaremos los principios de confianza cero, componentes lógicos de la arquitectura y sus modalidades de implementación.

La NIST en su publicación NIST ZP 800-207 [11] nos define confianza cero y arquitectura de confianza cero como:

"Zero Trust proporciona una colección de conceptos e ideas diseñados para minimizar la incertidumbre al hacer cumplir decisiones de acceso precisas y de privilegio mínimo por solicitud en sistemas y servicios de información frente a una red que se considera comprometida. La arquitectura de confianza cero es el plan de ciberseguridad de una empresa que utiliza conceptos de confianza cero y abarca las relaciones de los componentes, la planificación del flujo de trabajo y las políticas de acceso. Por lo tanto, una empresa de confianza cero es la infraestructura de red (física y virtual) y las políticas operativas que existen para una empresa como producto de un plan de arquitectura de confianza cero." [11]

Adicionalmente, define 7 principios que permiten la adhesión a una estrategia de confianza cero los cuales se detallan a continuación:

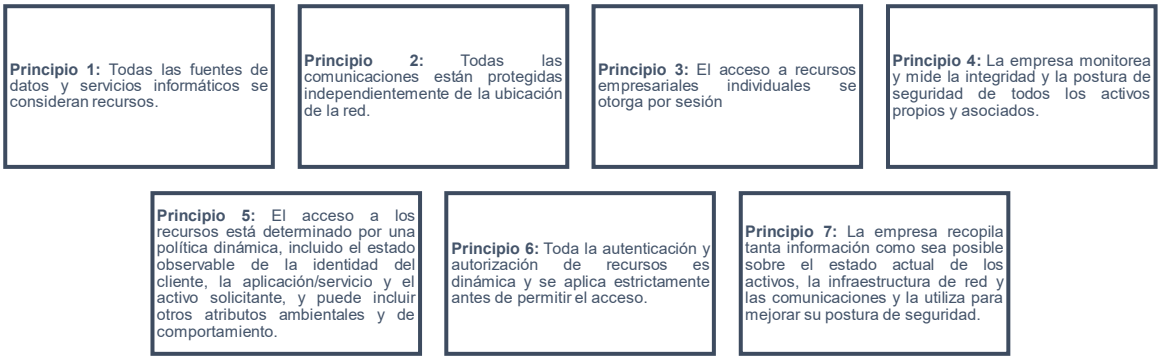

Ilustración 4: Principios confianza cero-NIST SP 800-207. Fuente: [11]

Microsoft aborda esta estrategia partiendo de un enfoque que denomina “asumir la brecha” [17] indicando que esto actualmente es inevitable debido a la complejidad actual de los entornos de tecnología, las arquitecturas de seguridad estáticas en el tiempo, la baja comprensión de la ciberseguridad por los usuarios y la constante evolución en las estrategias empleadas por los delincuentes para vulnerar la seguridad de una organización. Dicho esto, propone 3 principios a desarrollar dentro de la estrategia de confianza cero buscando minimizar el impacto al momento de que se materialice:

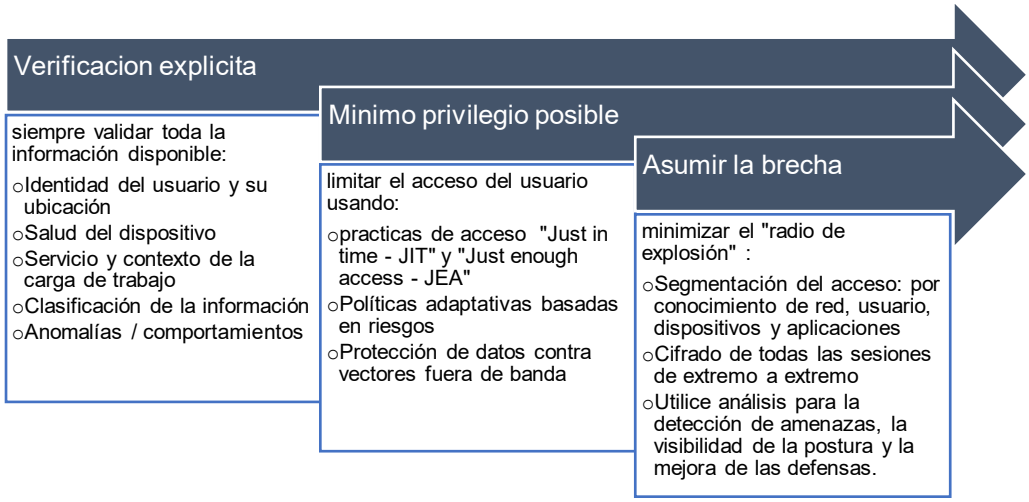

Ilustración 5: Principios confianza cero-Microsoft. Fuente: [17]

En conclusión, el foco principal de la estrategia de confianza es proveer una fuerte estandarización y gestión sobre los accesos que brindamos a los recursos de la organización, partiendo del mínimo privilegio posible, definiendo los accesos tan granular como sea posible, realizando un constante análisis y monitoreo del estado y tráfico de la red, comportamiento de los usuarios, infraestructura, aplicaciones y dispositivos y reducir las zonas de seguridad partiendo de que ninguna recurso es confiable independiente de su ubicación u origen.

4.2.1 Componentes logicos de una arquitectura de confianza cero

La adopcion de confianza cero como estrategia, parte de los principios anteriormente mencionados acoplados a un conjunto de componentes que permiten la materializacion de los mismos. Nos ayudaran a soportar los procesos, procedimientos y actividades que garanticen su correcta ejecucion. Para esta finalidad, la NIST nos propone un conjunto de componentes logicos que en un escenario completo e ideal, se deben implementar en una organización. Caba aclarar que como punto inicial una organización debe realizar una evaluacion sobre su nivel de cubrimiento actual e identificar una ruta de adquiscion e implementacion de estos componentes de aceurdo a su tamaño, necesidades actuales y a futuro y apetito de riesgo. Adicionalmente es claro que las organizaciones y su sector de negocio puede cambiar de acuerdo a las necesidades del ambiente o sector o bien de los objetivos propios por lo cual asi mismo se debe contemplar la evolucion de esta arquitectura.

A continuacion se detallan los componentes logicos propuestos por la NIST:

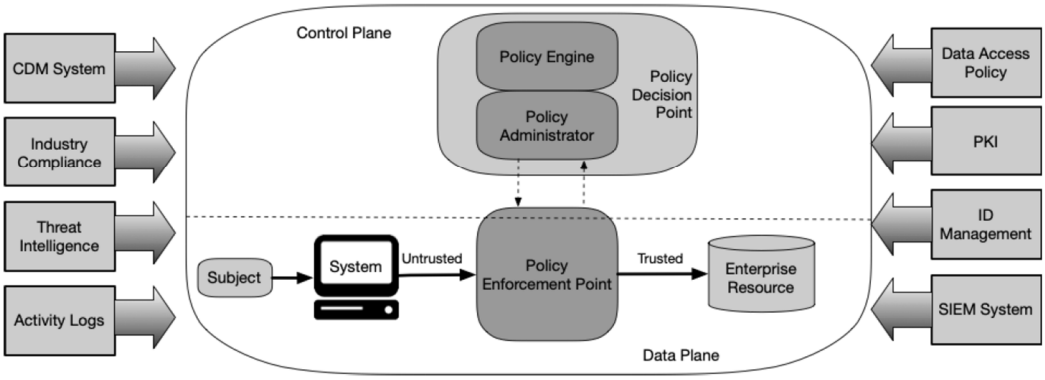

Ilustración 6: Componentes lógicos de la arquitectura de confianza cero - NIST SP 800-207. Fuente: [11]

En el diagrama de la ilustracion 6, encontramos el núcleo del modelo denominado PDP (*Policy Decision Point*), conformado por el PE **(***Policy*

*engine***)** el cual contiene la logica o como lo denomina NIST el "*algoritmo de confianza*"[11], encargado de la evaluacion y toma de decisión de aprobar o denegar la solicitud realizada esto evaluando la información de la solicitud de acceso y el contexto contra las políticas definidas por la organización. Para tomar esta decisión se pueden emplear dos enfoques:

- **Basado en nivel de riesgo:** la organización define umbrales o criterios que se deben cumplir y que son evaluados al momento de otorgar, retar, limitar o denegar el acceso solicitado. En este enfoque se busca recoletar toda la informacion disponible al momento de la solicitud para definir y alimentar un puntaje o nivel de confianza asociado al sujeto.

- **Basado en el contexto:** se evalua basado en el comportamiento, contexto y solicitudes recientes realizadas por le sujeto. Asi se identifican comportamientos anomalos o atipicos y patrones asociados a amenazas conocidas para determinar las acciones a tomar.

El PA (*Policy Administrator*) encargado de habilitar o denegar el consumo de un recurso de la organización.

El PEP (*Policy Enforcement Point*) es el componente encargado la generar o terminar el acceso a partir de las instrucciones dadas por el PA.

En conclusion, fuentes externas como procesos y/o herrramientas de inteligencia de amenazas, postura de seguridad, ubicación, contexto o bien fuentes internas como las políticas de seguridad de la organización, registro de eventos de seguridad, índice de confianza o nivel de riesgos del sujeto, permiten determinar y evaluar las amenazas presentes en la solicitud realizada y asi determinar la accion a ejecutar.

Ademas de los componentes claves, se definen unos componentes complementarios (herramientas, actividades y/o procesos) que permiten alimentar y apoyar la función del PDP brindando inteligencia accionable al momento de determinar la acción a tomar frente a la solicitud:

- **Sistena de diagnostico y mitigacion continua:** programa de identificacion y mitigacion continua de riesgos de seguridad.

- **Cumplimiento de estándares de industria:** la implementacion y evaluacion continua de cumplimiento normativo, regulatorio o de industria de acuerdo al objeto de negocio de la organización.

- **Inteligencia de amenazas:** actividades para identificar, modelar, analizar y gestionar amenazas que apoyen al PE para la toma de deciciones.

- **Eventos de actividad de red y sistemas:** registro de eventos de sistemas y trafico de red que permita detectar comportamiento anomalos o atipicos dentro de nuestra la actividad frente a la postura de seguridad definida.

- **Políticas de acceso a la información:** reglas y politicas para brindar el acceso a los recursos de la organización.

- **Infraestructura de clave publica (PKI):** conjunto de capacidades para la gestión (emisión, distribución, almacenamiento, renovación y revocación) de certificados digitales, empleados en la estrategia de autenticacion, cifrado y firmado de las comunicaciones de usuarios, dispositivos o servivios en el ambiente tecnologico de la organización. Estos pueden ser soportados por una autoridad certificadora publica o privada.

- **Sistema de administración de identidades:** componente para la gestion de cuentas de usuarios e identidades, roles y atibutos.

- **Gestion de eventos e informacion de seguridad:** recoleccion, correlacion y almacenamiento de todos los registros de seguridad para el analisis de comportamientos y amenazas.

Estos componentes pueden ser de tipo software o harware y soportar una o mas funcionaidalides de las descritas anteriormente.

4.2.2 Enfoques de implementación de la arquitectura de confianza cero

La arquitectura es la descompocion de una solucion en sus diferentes componentes y la forma en que interactuan entre si. La elecccion de una arquitectura parte de las necesidades de negocio, cumplimiento regulatorio y capacidades actuales en cuanto a la madurez de sus procesos y ecosistema de soluciones, no siendo un impedimiento este ultimo para diseñar arquitecturas objetivo o deseables que incorporen uno o todos los componentes propuestos por la NIST.

La identidad como defensa, la micro-segmentacion y la definicion de perimetros de confianza, son puntos de partida para diseñar nuestra estrategia y arquitectura de confianza cero, por lo cual NIST provee los siguientes 3 enfoques de referencia:

4.2.3 Arquitectura de confianza cero basada gobierno de identidad mejorada

El criterio principal de este enfoque tiene como pilar central el como definimos y ejecutamos las políticas de acceso a nuestros recursos empleando la identidad, sus atributos y el contexto como principal recurso. Una solicitud de acceso nos brinda información relevante para su evaluacion como el nivel de riesgo de la identidad y dispositivo empleado, si este ultimo es administrado o no por la organización, su nivel de cumplimiento de seguridad, la ubicación, fecha y hora de la solicitud, entre otros. Esta informacion la podemos convertir en inteligencia accionable para la toma de decisiones frente a otorgar o no este acceso. Este enfoque es comúnmente utilizado por organizacines con recursos en nube y modalidades de trabajo distribuido.

4.2.4 Arquitectura de confianza cero basada en microsegmentacion

Este enfoque nos propone la creación de pequeños segmentos de red de uno o más recursos agrupados, basados en su función o criticidad. Como indica John Kindervag [8], el objetivo es crear micro segmentos y el aseguramiento de su perímetro por medio de puertas de seguridad que funcionan como PEP. Este enfoque se puede aplicar tanto a la infraestructura de red como a nivel de punto final por medio de agentes que brinden acceso unicamente a los recursos permitidos. Es clave que estos permitan la gestión o sean gobernados por la organización, de esta manera podremos administrar las configuración y reglas que garanticen la postura en cuanto a las políticas de acceso definidas, la ejecución de las decisiones del PE y la gestión oportuna a cualquier amenaza que presente un riesgo para la organización.

4.2.5 Arquitectura de confianza cero basada infraestructura de red y perimedtros definidos por software

El perímetro definido por software estable una red superpuesta sobre internet comúnmente utilizada para brindar acceso a los servicios y recursos en nube. Permiten una comunicación segura (autenticada y cifrada) sobre una red insegura y no controlada brindando el acceso a los recursos de la organización y agregando capacidades de visibilidad y control sobre las actividades de los usuarios de la organización. Esta tecnología busca remplazar a las clásicas VPNs de cliente. La implementación se basa en el uso de agentes en los dispositivos finales y una puerta de entrada que abarca las funciones de un PEP bajos las instrucciones del PA.

4.3 Pilares de confianza cero según CISA

Finalmente, el CISA define 5 pilares en el contexto de confianza cero para la aplicación de los principios definidos por la NIST para elaborar un

modelo seguro de acceso a la información. A continuación, de detallan cada pilar desde el enfoque de aseguramiento propuesto por la CISA:

- **Identidad**: determinar que una entidad sea reconocida de manera inequívoca garantizando el acceso seguro, basado en el contexto y riesgos de la solicitud y únicamente los mínimos permisos necesarios a los recursos asignados para su operación durante un tiempo establecido.

- **Red**: su aseguramiento parte de la autenticación, cifrado y firma de las comunicaciones sin importar su origen y destino, realizar un monitoreo continuo del comportamiento de la red en busca de comportamientos anómalos o atípicos y eliminar los perímetros tradicionales empleando microsegmentación llevando los perímetros más cerca de los recursos, obteniendo una segmentación acorde sus necesidades de comunicación.

- **Dispositivos**: plantea la identificación, inventariado, monitoreo, evaluación y aplicación continua de estándares de seguridad sobre los recursos de la organización tenga acceso a la red, esto incluye los dispositivos móviles, estaciones de trabajo de escritorio y portátiles, servidores, equipos de red, IoT. En cuanto a los disipativos no gobernados, insta a determinar su correcta evaluación y controles a implementar para determinar su postura de seguridad frente a las solicitudes de acceso realizadas.

- **Aplicaciones**: promueve la integración de prácticas y herramientas seguridad durante el ciclo de vida del desarrollo, evaluaciones de seguridad periódicas en busca de posibles amenazas y/o vulnerabilidades, uso de estándares para la autenticación, autorización, publicación y consumo seguro de APIs y servicios y por último explorar la implementación de técnicas y/o herramientas que permitan reducir su superficie de exposición a los orígenes estrictamente necesarios para su consumo.

- **Datos**: la protección de los datos debe darse a nivel procedimental y técnico, desarrollando procesos que permitan el inventariado, evaluación, clasificación, y etiquetado y la implementación de herramientas tecnológicas que permitan proveer el nivel de confidencialidad, disponibilidad e integridad requerido por estos en cualquier estado del ciclo de vida de la información. Para finalizar, la organización debe implementar un descubrimiento de la ubicación de los datos y emplear técnica de detección y control de fuga de estos.

5 Metodología propuesta

Para establecer la estrategia como guía en la organización, es fundamental abordarla en diferentes fases que contribuirán al éxito de su implementación. Será un amplio trayecto con resultados claves en cada fase conectando equipos interdisciplinarios, abordando diferentes procesos y tecnologías y transformando el pensamiento de cómo debemos abordar la seguridad con este nuevo enfoque.

Partiremos de formalizar la estrategia con una definición de la dirección a seguir y los roles habilitadores desde los enfoques estratégicos, taticos y operativos dentro de la organización. Por otra parte, es necesario identificar las capacidades actuales con las cuales podremos abordar de manera parcial o completa la estrategia, para así iniciar una transformación de los procesos y tecnológicas de seguridad integrando los principios de confianza cero a su diseño y operación. Diseñar los artefactos que guíen en la adquisición, diseño e implementación de las soluciones que soportaran la estrategia será un objetivo clave para fortalecer su adaptabilidad frente las nuevas necesidades del negocio. Por último, identificar y gestionar de manera proactiva los desestabilizadores que podrían afectar el cumplimiento de la postura definida en la estrategia.

Ilustración 7: Fases de la metodología propuesta de confianza cero. Fuente: Propia

Como actividad inicial, debemos plantear cuáles serán los beneficios de la organización desde la perspectiva estrategia, táctica y operativa al momento de adoptar los principios de confianza. Identificar los grupos objetivos que habilitan la ejecución de la estrategia desde la dirección hasta la ejecución y el recurso humano encargado de apoyar y gestionar su desarrollo, con el fin de generar recursos, concientizar y promover este nuevo enfoque como la principal herramienta de seguridad para habilitar la evolución e innovación y transformación digital del negocio y enfrentar los nuevos retos de seguridad en los ambientes de trabajo distribuidos y en nube.

5.1 Formalizar postura de confianza cero

Lo primero es entender que el concepto de confianza cero no es únicamente el uso de tecnologías. Es una estrategia, un enfoque de arquitectura y un cambio en la forma de pensar alineada a la transformación de la organización en cuanto al uso y acceso de servicios de forma distribuida y el aumento en la contratación e implementación de soluciones tecnológicas en nube. En consecuencia, busca hacer frente a las amenazas en estos nuevos panoramas. Realizaremos las siguientes actividades como partida inicial:

Ilustración 8: Etapas de formalización de la metodología propuesta de confianza cero. Fuente: Propia

5.1.1 Entender las expectativas y necesidades del negocio

A nivel estratégico debemos dar respuesta a preguntas como ¿nuestro estado actual de capacidades de ciber-resiliencia cubre las amenazas actuales de la organización?, ¿qué impacto tienen los riesgos de seguridad en nuestra estrategia? o ¿actualmente cumplimos con los requerimientos de

regulatorios internos o definidos por lo entes de control?. Desde un punto de vista táctico, ¿cuáles son los planes para la gestión de riesgo de seguridad y cuál es su nivel de ejecución? o ¿cuáles son las capacidades actuales de la organización para la detección temprana y gestión de amenazas?. Finalmente, a nivel operativo, ¿se están ejecutando los procesos con el alcance y periodicidad definida?, ¿Cuál es la efectividad de los controles de seguridad implementados?. La formalización e implementación de la estrategia debe dar respuesta a estas preguntas y generar valor a cada nivel de la organización:

Nivel	Beneficios de la estrategia de confianza cero
Nivel estratégico	Llevar la organización a un nivel de riesgo aceptable gestionando de manera integral las amenazas emergentes que están presentes en los servicios en nube y las modalidades de trabajo distribuido.
	Apoya al cumplimiento regulatorio evitando impactos económicos o reputacionales gracias al robustecimiento de la postura de seguridad de la organización.
	Potencia la innovación y la transformación digital de la organización apoyando las diferentes iniciativas de forma segura adaptándose al cambio de oferta de servicios y modalidades de trabajo.
	Aumenta las capacidades de ciber-resiliencia reduciendo el radio de afectación por una brecha de seguridad.
Nivel táctico	Mejora los procesos de adquisición, diseño, desarrollo e implementación de soluciones tecnológicas desde la perspectiva de seguridad
	Aporta agilidad a la organización en la masiva adopción de servicios en nube.
	Impulsa la adopción de nuevas tecnologías que permiten mejorar la experiencia de los usuarios habilitando de forma segura el acceso distribuido a las herramientas y servicios empleados en su día a día.
Nivel operativo	Orienta a la organización en abordar la automatización y orquestación de los diferentes controles de seguridad.
	Insta a la organización a generar mayor visibilidad del estado de los recursos y el comportamiento de los mismo para una efectiva gestión de amenazas.
	Apoya al monitoreo de la postura de seguridad por medio de la evaluación continua del estado de seguridad de sus recursos.

Tabla 2: Beneficios en la adopción de confianza cero en la organización. Fuente: Propia

5.1.2 Identificar roles habilitadores

Una vez entendemos las expectativas y necesidades del negocio en los diferentes niveles organizacionales, debemos identificar los roles o cargos que son claves y/o habilitadores gracias al respaldo o liderazgo que pueden brindar para garantizar su ejecución:

Roles clave	Acciones habilitadoras de la estrategia de confianza cero
Junta directiva, presidente, vicepresidentes ejecutivos, vicepresidentes	Permitirá habilitar la estrategia desde el ámbito financiero, adquisición y/o asignación de recursos y aprobación de planes de transformación para soportar la estrategia.
Lideres de áreas de negocio	Apoyaran a la divulgación y fomentaran el cumplimiento de las prácticas de confianza cero en los procesos que soportan.
Lideres de TI y operaciones	Su principal rol será dar cumplimiento a los controles y directrices garantizando la correcta ejecución de la estrategia en la implementación y operación de los procesos y tecnologías extendiendo estas prácticas a los terceros o aliados estratégicos de la organización.
Recursos humanos	Encargados de comunicar las campañas de concienciación de usuarios y los planes de capacitación en seguridad que incluye la formación en capacidades de confianza cero para los colaboradores de la organización.
Gestión de la demanda y proyectos (Equipos PMO)	Responsables de conformar y orquestar los equipos cross-funcionales incluyendo a las áreas de seguridad TI y ciberseguridad en las fases de la identificación de un necesidad u oportunidad de negocio, durante el proceso de selección, adquisición e implementación de las soluciones y servicios de tecnología..
Gestión de riesgos	Encargados del monitoreo y evaluación continua de amenazas y riesgos en conjunto con las áreas de seguridad, asociados al desarrollo de nuevas iniciativas de negocio desde un punto de vista de riesgos operativos y de tecnología.
Áreas de control (auditoria, legal, cumplimiento)	Responsables de la evaluación de cumplimiento de la postura de seguridad a nivel interno (procesos de la organización) y a nivel externo por medio de la gestión de contratos y evaluación de proveedores y/o terceros.

Tabla 3: Acciones y áreas habilitadoras de la estrategia de confianza cero. Fuente: Propia

Es importante entender que espera cada grupo objetivo y que se espera de ellos para enfocar así los temas a tratar, definir responsabilidades, y acuerdos para el desarrollo armónico de la estrategia. En conclusión, conectar a las personas con la estrategia garantiza en gran medida el éxito de esta.

5.1.3 Comunicar la estrategia

Comunicar la estrategia será nuestra última actividad. Para ello, debemos enfatizar lo siguiente:

- Exhibir los beneficios de esta transformación en un lenguaje claro y sencillo será de gran ayuda para captar la atención y tomar un posicionamiento dentro de la organización.

- Presentar los planes y actividades que permitan la continuidad y estabilidad de la estrategia, un gobierno claro y definido demostrara el conocimiento y las capacidades para alcanzar los objetivos propuestos y el éxito de esta.

- Hay que destacar que la estrategia no será responsabilidad de un área específica. Al contrario, será un objetivo en común desarrollado por diferentes equipos donde apremia la proactividad, construcción y evolución colectiva de la estrategia.

5.2 Priorizar las capacidades de seguridad

Contar con una visión clara, transversal y una comprensión de las modalidades de servicio de nuestras aplicaciones y recursos, la criticidad de los procesos que habilita, su funcionamiento, flujos de datos, los diferentes usuarios y lugares de acceso, es una de las primeras actividades que debemos realizar.

Abordar los casos de uso prioritarios por medio de la intervención de las tecnologías y procesos actuales o bien iniciar la búsqueda de nuevas soluciones. La adopción de este enfoque no implica necesariamente la compra de tecnología o servicios adicionales. De manera inicial se deben identificar las tecnologías actuales o bien los servicios nativos en nube con el objetivo de potenciarlas e integrarlas a nuestro ecosistema de confianza para cubrir los principios de confianza cero. Sin embargo, existen capacidades básicas que se deben implementar por lo cual es factible buscar la adquisición de servicios o tecnologías, identificando y evaluando la mejor solución y/o servicio que supla la necesidad actual y garantice una postura de seguridad acorde al nivel requerido por la organización.

Conocer el nivel de madurez actual de las capacidades de seguridad permitirá identificar los procesos, capacidades tecnológicas y servicios actuales que requieren una priorización dentro de la estrategia con la meta de

mejorar su diseño, implementación u operación, de esta manera enfocar los esfuerzos y obtener victorias tempranas.

A continuación, detallamos un grupo de preguntas que nos permitirán identificar el estado actual de seguridad en la aplicación de los principios de confianza cero sobre los 5 pilares del CISA:

Pilar confianza cero	Autoevaluación de confianza cero
Identidad	¿Se tiene claros los flujos de acceso a los recursos de la organización?
	¿todas las identidades humanas y no humanas se tienen inventariadas? Incluyendo las externas /internas?
	Cuenta con proceso para la segregación de funciones
	Cuenta con lineamientos y/o procesos que garanticen una apropiada gestión del ciclo de vida de las identidades
	¿Realiza gestión de cuentas privilegiadas?
	¿Implementa un modelo de autenticación federado integrado con el proveedor de identidades autorizado?
	¿El gobierno del ciclo de vida de identidades es ejecutado por un gestor de identidades (IDM)?
	Se tiene políticas de sesión, basadas en contexto, ¿índice de confianza y riesgo de la identidad?
	¿Existe un modelo para la definición de roles y permisos basado en el mínimo privilegio?
	¿Implementa protocolos de autenticación y autorización seguros?
	¿Implementa múltiple factor de autenticación?
Dispositivos	¿Se tienen políticas para el uso de dispositivos personales?
	¿Cuenta con estándares de seguridad para los dispositivos de la organización?
	¿Cuenta con herramientas tipo MDM (Movile device management) / MAM (Movile application management) para dispositivos administrados y no administrados?
	¿El proceso de aseguramiento cubre la totalidad de dispositivos de la organización?
	¿Se evalúa la postura del dispositivo y nivel de riesgo sobre cada solicitud de acceso a un recurso?
	¿Cuenta con tecnologías para evaluar la postura de seguridad de su entorno de tecnología en nube y móvil?
	¿Cuenta con procesos de parches de seguridad?
	¿Todos los dispositivos generan logs y están siendo monitoreados?
	¿Todos los disipativos se encuentran inventariados?
Redes	Se tiene definidos lineamientos para el uso de protocolos y algoritmos seguros que permitan agregar controles de autenticación, cifrado y firma de las comunicaciones internas/externas?
	¿La red se encuentra segmentada por ambientes a nivel de red?
	¿Toda comunicación cuenta con su documentación de puertos necesarios para su funcionamiento?
	¿Cuenta con procesos y/o lineamientos para la creación y gestión segura de certificados digitales?
	¿Usa arquitecturas de referencia para el diseño de la comunicación entre ambientes, nubes y en la premisa?
Aplicación	¿Cuenta con procesos de desarrollo seguro?
	¿Integra el modelado de amenazas en los procesos de desarrollo?
	¿Se integran controles de seguridad automatizados en el ciclo de desarrollo seguro para análisis de código estático y dinámico?
	¿Implementa controles de seguridad para la exposición de aplicaciones de forma segura?
	¿Cuenta con tecnólogas para la exposición segura de APIs/servicios web?
	¿Las aplicaciones surten pruebas de seguridad periódicas y previo a su puesta en producción?
	¿Tiene definidos lineamientos para el aseguramiento de código, uso de librerías, dependencias y manejo de clave y secretos durante el ciclo de desarrollo?
	¿Realiza de manera periódica evaluaciones de seguridad sobre las aplicaciones?
	¿Cuenta con un modelo de acceso a las aplicaciones intranet, extranet y publicas?
	¿Todas las aplicaciones se encuentran inventariadas?
	¿Cuenta con herramientas para la gestión segura de llaves, claves y secretos?
	¿Cuenta con procesos de clasificación y etiquetado de información?
	La información de la organización se encuentra clasificada y etiquetada de acuerdo con su criticidad
	¿Se tiene un inventario de los flujos de la información?

Datos	¿La información se encuentra cifrada en procesamiento, tránsito y reposo?
	¿Define lineamientos para el cifrado de la información en tránsito, procesamiento y reposo?
	¿Define lineamientos para la gestión y robustes de material criptográfico?
	¿Cuenta con tecnologías para el descubrimiento automático de información?
	¿Implementa controles para la prevención de fuga de información?

Tabla 4: Autoevaluación de confianza cero. Fuente: Propia

5.3 Diseñar capacidades de seguridad

5.3.1 Procesos de confianza cero

Primero detallaremos los principales procesos habilitadores de la estrategia, describiendo su objetivo y el alcance deben abarcar para garantizar el éxito de la estrategia.

5.3.1.1 Clasificación de activos

Es claro que lo que no conocemos no lo podemos asegurar, por ello, nuestra primera actividad será intervenir los procesos que permitan inventariar de forma correcta los recursos de la organización y la forma en la cual se interrelacionan.

El inventario de activos debe contener como mínimo la siguiente información:

- Identificador único
- Nombre
- Etiqueta
- Estado
- Ambiente
- Fabricante
- Modelo
- Descripción
- Versión/ sistema operativo (según aplique)
- Unidad de negocio
- Accesibilidad

- Nivel de exposición
- Atributos de negocio del recurso (propietario/custodio/proveedor)
- Criticidad del recurso (valor dado por un ejercicio tipo BIA)
- Clasificación de la información que procesa, almacena o transmite

La clasificación de activos establece criterios como dueño y responsable del servicio, su criticidad frente a los procesos que soporta e información técnica relevante lo cual nos permitirá asignar los controles adecuados para salvaguardar la confidencialidad, integridad y disponibilidad de su información.

Los procesos tradicionales se enfocan principalmente en inventariar recursos de infraestructura, lo cual nos genera una vista parcial de la totalidad de recursos de la organización.

5.3.1.2 Clasificación de información

Determinar el valor de la información en términos de confidencialidad, integridad y disponibilidad será fundamental para realizar una gestión segura de la misma. En primera instancia podemos definir un valor de clasificación nominal que parte del tipo de información y las normativas aplicables como leyes y/o regulaciones, mejores prácticas del mercado o por su valor económico para la organización. Sin embargo, la clasificación debe establecer una tipología que permita establecer de manera clara su criticidad y debe darse con base al valor que genera para la organización a partir de ejercicios en acompañamiento con los dueños de los procesos que generan, procesan y/o usan la información. Los controles claves en estos procesos serán la clasificación, etiquetado y definición de propietarios de esta y la sensibilización sobre su valor, privacidad, aseguramiento y uso.

Una propuesta para la clasificación de la información con base a su criticidad es la siguiente:

- **Secreta**: el acceso se encuentra limitado a un grupo reducido, encargado de la estrategia, toma de decisiones a nivel de negocio, y procesos críticos de la organización.

- **Confidencial**: el acceso se encuentra limitado a los dueños y ejecutores de un proceso especifico.

- **Restringida**: el acceso se encuentra limitado a los colaboradores de la organización para uso interno.

- **Publica**: información de uso publico

Ahora bien, el impacto de la fuga, perdida o manipulación de la información puede acarrear impactos en los siguientes niveles:

- **Económico**: costos asociados a refactorización de productos y/o servicios, costos asociados a la interrupción, degradación o no desarrollo normal de la operación.

- **Reputacional**: pérdida de clientes, pérdida de confianza en los inversores y participación en el mercado.

- **Estratégico:** perdida de la ventaja competitiva, divulgación de estrategia en el mercado.

- **Regulatorio**: condenas judiciales, multas y sanciones por entes reguladores y/o demandas por clientes.

- **Operativo**: afectación a los procesos de negocio y tecnológicas afectando la disponibilidad de estos, perdida de oportunidad por la no ejecución de procesos y fraude.

5.3.1.3 Aplicación de configuración seguras

Definir y ejecutar las actividades necesarias para la construcción de estándares de seguridad, implementación, monitoreo de su aplicación y

gestión de las desviaciones, nos ayuda a mantener un ecosistema seguro, agregando una capa de seguridad al momento de presentar una intrusión o bien una exposición indebida de un recurso.

Este proceso debe tener dentro de su alcance todos recursos los cuales sea viable su definición y aplicación de un estándar de seguridad y no limitarse a la infraestructura desplegada y gestionada por la organización. Esto incluye la configuración propia de la nube y los servicios nativos de la misma. Como referencia, el CIS dispone de estándares de seguridad para los CSP más relevantes en la industria.

El proceso debe contar con una periodicidad definida para la evaluación de cumplimiento de los estándares definidos sin embargo debe encaminar sus esfuerzos a que esta actividad se realice de forma automática y en tiempo real, permitiendo la reacción y corrección oportuna a una deviación detectada, ya sea por una actualización del estándar o bien por una configuración incorrecta que pueda llevar al incumplimiento de una directriz de seguridad de la organización generando una amenazas en nuestro entorno de seguridad.

5.3.1.4 Monitoreo de eventos

La capacidad de detección y reacción frente a una amenaza dependerá en gran medida del alcance que se defina para la recolección y correlación de registros de seguridad de los recursos de la organización. Dicho esto, se debe adoptar un enfoque holístico en cuanto a la visibilidad que podamos obtener del estado de los recursos, eliminando el concepto de perímetros tradicionales y extendiendo su alcance a todos los componentes que permiten un flujo de datos desde o hacia la red de la organización.

Desde el enfoque de confianza cero debemos potenciar el monitoreo de seguridad abordando mas no limitándose a los siguientes eventos y comportamientos:

- **Identidad**: altas, bajas o modificaciones de usuarios y privilegios, comportamientos atípicos como el aumento o patrones de solicitudes de inicio de sesión exitosas y fallidas, solicitudes desde ubicaciones

atípicas, intentos de acceso a recursos no autorizados, evasión de controles o cambios en el estado de la información no esperados, accesos desde dispositivos no autorizados.

- **Aplicación**: eventos propios de la aplicación como actividad de los usuarios, modificaciones de servicios o configuraciones nativas, cambios en los flujos de datos y excepciones o incumplimientos a lineamientos de seguridad en el ciclo de desarrollo.

- **Red**: aumento en el tráfico, comunicaciones anómalas que se presenten como tráfico este-oeste, solicitudes a puertos críticos como de administración o no asociados a la operación normal del servicio.

- **Dispositivos**: salud del dispositivo, identificación de código malicioso, aumento de uso de recursos, instalaciones no autorizadas, cambios en la configuración de seguridad, uso de software no autorizado, comunicaciones atípicas.

- **Datos**: toda acción como creación, modificación y eliminación de información incluyendo la identidad que realizo la acción, lugar, fecha y hora.

La recolección de datos debe abarcar la totalidad de recursos desplegados por la organización, cada uno de los pilares detallados anteriormente deben estar en capacidad de generar registros y de enviarlos al componente de centralización para su correlación y almacenado sin importan su ubicación, esto incluye cualquier recurso en modalidades IaaS, PaaS, SaaS. Tradicionalmente se contemplan únicamente fuentes como máquinas virtuales y dispositivos perimetrales y de red limitando la visibilidad sobre las actividades que se originan en el entorno de tecnología de la organización. Adicionalmente, los SIEM (*Security information and event management*) soportan sus capacidades de correlación en firmas e índices de compromiso los cual nos lleva a adoptar enfoques reactivos, por esta razón se deben integrar herramientas de análisis de comportamiento tipo UEBA (*user and entity behavior analytics*) y/o inteligencia artificial para la detección

temprana basada en comportamientos. Para finalizar, el almacenamiento centralizado permitirá contar con la información disponible para el análisis a demanda y durante o después de un incidente, por esta razón, los tiempos de retención deben definirse y alinearse a las necesidades y regulaciones del proceso.

5.3.1.5 Inteligencia y gestión de amenazas

Proceso enfocado en el monitoreo, alertamiento y gestión de amenazas existentes o emergentes sobre la marca, productos, información y recursos en el ciberespacio, generando inteligencia accionable para su gestión proactiva. La información base de este proceso debe ser actualizada siempre que un nuevo recurso sea implementado o adquirido permitiendo que entren en el alance del proceso:

- **Monitoreo de marca:** detección del uso indebido de la marca y recursos asociados como campañas de phishing, ofertas de trabajo falsas, uso fraudulento de dominios primos, perfiles falsos en redes sociales, entre otros.

- **Monitoreo de información y descubrimiento de activos:** servicio de detección de información y descubrimiento de activos que se encuentren en publicados, almacenados y/o desplegados en ubicaciones no autorizadas por la organización.

- **Monitoreo de amenazas:** detección y alertamiento de amenazas que puedan afectar el desarrollo normal de las operaciones de la organización como código malicioso dirigido, amenazas persistentes avanzadas, vulnerabilidades, grupos criminales, entre otros.

Reducir la dependencia de tareas humanas integrando herramientas tipo SOAR (*security operation automation and response*) evolucionando del enfoque del uso de planes de respuesta a incidentes ejecutados manualmente a respuestas automatizada y en tiempo real para contención de una amenaza.

5.3.1.6 Gestión de identidad y accesos

Se debe definir una postura frente al uso de una identidad única para toda aplicación o servicio que se consuman dentro y fuera de nuestra infraestructura. Este gobierno debe extenderse a terceros que cuenten con algún tipo de acceso estándar o privilegiado hacia algún recurso de la organización evitando el uso de cuentas genéricas o no nombradas. El proceso debe tener alcance a las identidades humanas (usuarios internos, proveedores y terceros), identidades no humanas (usuarios de servicio).

El proceso debe contar con las vertientes necesarias para brindar un acceso seguro. Esto contempla los métodos de autenticación y autorización a partir del tipo de acceso solicitado (usuario estándar o privilegiado, interno o externo). Toda la información que genera en la solicitud debe ser recolectada y empleada constantemente como un factor de confiabilidad para la toma de decisiones de permitir o denegar el acceso basados en el contexto de la solicitud, índice de riesgo de la identidad, reputación de la dirección ip, recurso origen y destino, postura del dispositivo, ubicación, hora y cambios no esperados en la solicitud durante la fase de autenticación como cambio de la dirección ip.

La centralización del ciclo de vida de las identidades facilita la gestión de las altas, bajas y modificación que se requieran a lo largo de los recursos internos y externos, minimizando la probabilidad de que una amenaza sea materializada resultado de una débil o nula gestión de usuarios y/o proveedores desvinculados o deficiencias en la certificación de permisos.

Finalmente, la segregación de funciones debe ser parte integral del proceso y debe ejecutarse en las fases iniciales del diseño de una solución y periódicamente durante su operación, evitando la concentración o sumarización de privilegios en una única identidad.

5.3.1.7 Emisión de conceptos de arquitectura y seguridad

Por último, es necearía la construcción de artefactos de seguridad que le permitan a los equipos de negocio y tecnología que identifican y habilitan las soluciones de la organización, identificar de manera exacta, en un lenguaje de fácil entendimiento la postura de seguridad que debe dar cumplimiento y que será evaluada frente a la adquisición, implementación, modificación o evolución de tecnologías y/o servicios. Estos artefactos apoyaran la definición de conceptos de seguridad de acuerdo con el modelo de servicio e implementación, criticidad de del proceso de negocio y clasificación de la información que procesara. Algunas de las preguntas que debemos resolver para emitir el concepto de seguridad son:

- ¿Cuál es el contexto de la necesidad?
- ¿El proceso que soportara la solución es clasificado como crítico o de alcance regulatorio?
- ¿Qué tipo de información se va a procesar, transmitir o almacenar?
- ¿Es susceptible de cumplimiento normativo?
- ¿Qué recursos se ven impactados?
- ¿Cuáles son las expectativas y requisitos de las partes interesadas?
- ¿Se requiere una nueva definición o modificación del diseño debido a nuevas integraciones o comunicaciones internas o con terceros?
- ¿Se requiere modificar o generar excepciones a lineamientos actuales de arquitectura de seguridad?
- ¿Se requiere ampliar la exposición de una aplicación, recurso o servicio?
- ¿Cuál es el nivel de acceso requerido (interno/clientes/terceros) a la aplicación, recurso o servicio?
- ¿Se requiere una migración de datos?

Para la construcción de estos artefactos se puede emplear como guía los diferentes documentos de seguridad publicados por la NIST, CSA, CIS o bien las guías de referencia de cada fabricante.

En términos generales, toda implementación de una solución tecnológica debe ser previamente, evaluado, clasificado y registrado en nuestra herramienta de gestión de activos y debe dar cumplimiento a las directrices emitidas en el concepto de seguridad.

5.3.2 Controles de confianza cero

A continuación, se proponen los controles mínimos para la adopción de un enfoque de confianza cero en entornos de nube:

Pilar confianza cero	ID control	Control de seguridad	Descripción del control
Identidad	1	Acceso controlado por MFA	El acceso a las aplicaciones, estaciones de escritorio y portátiles se debe controlar con un múltiple factor de autenticación.
	2	Acceso condicional por geolocalización	Limitar el acceso a los recursos desde una zona geográfica correspondiente a la necesidad de la organización.
	3	Políticas de acceso basado en índice de confianza/riesgo	El acceso a un recurso será determinado empleando toda la información disponible al momento de la solicitud, se deben hacer uso de herramientas que permitan generar una puntuación o índice de riesgo basados en atributos como geolocalización, día, hora, recurso solicitado, intentos previamente fallidos, patrones de tiempo y comportamiento, dispositivo empleado. Este indicador debe ser constantemente actualizado basado en las características de riesgo manteniendo o decreciendo su puntuación.
	4	Control de sesiones	Toda sesión debe contar con tiempo de ejecución que permita evaluar los atributos de la solicitud periódicamente y esta debe ser única por identidad.
	5	Autenticación integrada con el proveedor de identidades de la organización	Establecer un proveedor de identidad para la autenticación y autorización empleando protocolos seguros como OIDC, Oauth, SAML en la su última versión.
	6	Integración con gestor de identidades (IDM)	El ciclo de vida de las identidades debe ser gobernado por una solución para este fin.
	7	Control de acceso privilegiado	Las soluciones tipo PAM (*Privileged Access Management*) permiten asegurar y monitorear la conexión a los recursos de la organización por medio del monitoreo y grabación de las actividades realizadas, control de sesión único y por periodos definidos y el aseguramiento de las credenciales de acceso por medio de bóvedas seguras. Por último, se deben definir los protocolos autorizados para el acceso administrativo a los recursos de la organización. No es recomendado emplear servidores tipo pivote para la operación administrativa de recursos.

	8	Mínimo acceso requerido	Los accesos se deben dar solo en momento requerido y durante el tiempo necesario para la actividad y empleando el mínimo privilegio posible para su funcionamiento usando un modelo estricto de acceso basado en roles y/o atributos.
	9	Segregación de funciones	Separar responsabilidades en los permisos otorgados a los usuarios
Dispositivos	**10**	Gestión de dispositivos móviles	Permitir el acceso a los recursos de la organización desde dispositivos móviles gobernados por medio de soluciones tipo MDM *(Movile deice management*) y los no gobernados por medio de funcionalidades tipo MAM (*Movile application management*) aplicando las configuraciones definidas por la organización.
	11	Monitoreo de postura de seguridad	Utilizar herramientas para evaluar y monitorear el estado de cumplimiento y desviaciones de acuerdo con el estándar de seguridad implementado para su fortalecimiento
	12	Fortalecimiento de configuraciones de seguridad	Configuración segura de los dispositivos empleando estándares de seguridad eliminando servicios o configuraciones por defecto o innecesarias para su funcionamiento
	13	Implementación de línea base de software de seguridad	Todo dispositivo debe ser desplegado garantizando la instalación de las aplicaciones de seguridad base para su aseguramiento, esto incluye agentes para la detección y contención de código malicioso, control de navegación, parchado e inventariado de software y análisis de vulnerabilidades. Estos serán instalados en mayor o menor medida de acuerdo con su condición (dispositivo gobernado o no por la organización).
	14	Actualización y parchado	Los procesos y herramientas parchado deben tener alcance a la totalidad de disipativos de la organización incluyendo los entornos de nube. En lo posible implementar soluciones de parchado virtual con el objetivo de mejorar los tiempos de respuesta para evitar la explotación y afectación a la organización
	15	Escaneo de vulnerabilidades	Los procesos y herramientas para la gestión de vulnerabilidades deben tener alcance a la totalidad de disipativos de la organización incluyendo los entornos de nube. Los escaneos de vulnerabilidades deben ejecutarse en preferencia de modo autenticado para lograr mayor visibilidad sobre el estado del dispositivo
Redes	**16**	Microsegmentación de red	Definir micro-perimetros de red a partir de la agrupación de recursos por su criticidad o funcionalidad y extendiéndola a cada recurso de la organización reduciendo así su exposición y permitiendo un mayor control de las comunicaciones por medio de políticas basadas en red.
	17	Comunicaciones empleando canales cifrados	La comunicación entre recursos internos/externos siempre debe realizarse de forma segura empleado protocolos y tecnologías para este fin. Implementar capacidades como VPNs *side to side* y TLS permiten el cifrado del tráfico sobre un canal inseguro como internet.
	18	Control de navegación a internet	Tecnologías como SWG (*secure web Gateway*) o proxys permiten agregar visibilidad y control sobre las comunicaciones que son requeridas por los recursos de la organización.

	19	Control de navegación interna	El diseño de una arquitectura de nube empleando centralizan las comunicaciones en componentes diseñados para esta función con la finalidad de controlar tráfico este-oeste y norte-sur.
	20	Prevención de ataques de denegación	Uso de soluciones anti-DDoS (*Distributed Denial-of-Service*). Estas pueden ser externas o nativas del proveedor de servicios de nube
	21	Comunicación mínima requerida	Utilización de componentes nativos de la nube como listas de controles de acceso y grupos de seguridad permitiendo únicamente la comunicación requerida para el funcionamiento de los recursos. Esta debe ser revisada periódicamente para la detección de desviaciones frente a su diseño
	22	Autenticación de las comunicaciones	Todo trafico de red debe ser autenticado independiente de su origen o destino, por lo cual se deben empelar protocolos que permitan el uso de autenticación de mensajes tipo MAC/HMAC.
	23	Inspección de trafico	Habilitar inspección de tráfico SSL
Aplicación	**24**	Acceso seguro a aplicaciones	Integrar soluciones tipo SDP (*software defined perimeter*) o ZTNA (*Zero trust network Access*) que permitan publicar aplicaciones y servicios de la organización de forma segura
	25	Mínima superficie de exposición	Los repositorios o componentes de almacenamiento no deberán estar expuestos a internet. Para los componentes que estrictamente deben estar expuestos a internet porque su funcionalidad lo requiere, se deben utilizar herramientas tipo WAF (*Web Application Firewall*), WAAP (*Web Application and API Protection*). Estas deben contemplar la detección y contención de ataques como mínimo los definidos en el owasp (*Open Web Application Security Project)* top 10 y control anti bots.
	26	Desarrollo seguro	Las aplicaciones deben ser desarrolladas siguiendo un ciclo de desarrollo seguro e integrando en el flujo herramientas que permitan automatizar la ejecución de los siguientes controles: análisis estático de código, análisis dinámico de código, análisis de dependencias y análisis de librerías.
	27	Aseguramiento de servicios web y APIs	Los servicios web y APIs deben ser desarrollados siguiendo un estándar de seguridad que defina los protocolos aprobados para la autenticación, autorización, cifrado, firma de mensajes y las cabeceras obligatorias para la comunicación. Se recomienda el uso de WS-security, oauth 2.0, JWT, JWE, JWS según aplique de acuerdo con el estándar empleado para los procesos de autenticacion, autorización, cifrado y firma los paquetes transmitidos desde y hacia el API o servicio web. Los servicios deben ser expuesto a través de una solución de gestión de APIs la cual puede ser nativa de la nube o externa y empleando TLS mutuo. Para este ultimo se recomienda emplear certificados generados por la PKI de la organización para agregar mayor control a la autenticación de solicitudes en el consumo de APIs y la robustez y ciclo de vida de los certificados.
	28	Escaneo de vulnerabilidades	Los procesos y herramientas para la gestión de vulnerabilidades deben tener alcance a la totalidad de aplicaciones de la organización incluyendo los entornos de nube. Se deben contemplar los boletines o notificación del fabricante para su correcta gestión bajo el proceso.

	29	Pruebas de seguridad	Establecer un calendario operativo para la ejecución periódica de pruebas de seguridad en sus modalidades caja negra, gris o blanca de acuerdo con la madures e historial de resultados. Tener en cuenta los acuerdos establecidos por terceros para la evaluación de aplicaciones o servicios en las modalidades tipo PaaS y SaaS dando cumplimiento a los requisitos para su ejecución.
	30	Configuraciones seguras	Ninguna aplicación o servicios debe ser implementado utilizando las configuraciones por defecto, se deben generar estándares de seguridad que reflejen la postura de seguridad definida por la organización.
	31	Gestión de postura de seguridad en nube	Las herramientas tipo CSPM (*Cloud Security Posture Management*) permiten la evaluación y remediación de divisiones frente a la postura de seguridad definida para el entorno en nube.
	32	Aseguramiento de infraestructura como código	La implementación de infraestructura o servicios de una aplicación debe ser desarrollada empleando infraestructura como código garantizando el uso de los módulos autorizados por la organización y controles de seguridad como escaneo de código, escaneo de imágenes, protección de máquinas virtuales, protección en tiempo de ejecución y aseguramiento del repositorio de imágenes. contemplar la implementación de herramientas tipo CWPP (*Cloud Workload Protection Platform*) para este fin.
	33	Alta disponibilidad de las capacidades de seguridad	Alta redundancia de los componentes críticos habilitadores de la estrategia como PE, PA y PEP empleando el concepto de seguridad por diseño.
	34	Uso de etiquetas para la identificación de los recursos	Los recursos deben contar con etiquetas indicando como mínimo el ambiente y la solución a la cual hacen parte para su identificación y gestión.
	35	Separación de ambientes	La aplicación ser desplegada empleando una separación de sus componentes de acuerdo con su función como de desarrollo, calidad y producción. Adicional se deben contemplar agrupamientos de capacidades transversales como las de seguridad.
Datos	**36**	Utilizar cifrado para los datos en procesamiento y reposo	Asegurar la confidencialidad e integridad de los datos por medio del cifrado de los mismos y delegado la gestión de las llaves en soluciones tipo KMS (*Key Management System*).
	37	Gestión segura de certificados	Definir lineamientos para la generación y revocación de certificados digitales que contemplen el almacenamiento seguro de llaves privadas, la robustez de los algoritmos a emplear y el tiempo de caducidad.
	38	Gestión segura de claves y secretos	Toda la administración de llaves, claves y/o secretos debe ser administrada y almacenada empleando herramientas nativas tipo KMS (*Key Management System*), dando cumplimiento al estándar FIPS 140-2. se debe definir controles para la renovación, versionado, acceso, monitoreo. No se debe emplear algoritmos obsoletos o vulnerados. por último, este componente debe ser centralizado y administrado por las áreas de seguridad.
	39	Prevención de fuga de información	Prevenir la fuga de información empleando tecnologías tipo DLP (*Data Lost Prevention*) o CASB (*Cloud Access Security Broker*) para el control del tránsito de información en línea y en reposo.

	40	Prevención de acceso a información no autorizados	Realizar descubrimientos, administración y aseguramiento del acceso a la información en la nube empleando tecnologías tipo IRM (*Information Right Management*).
Capacidades transversales			
Visibilidad inteligencia y gestión amenazas	**41**	Todo elemento que hace parte de la aplicación como administradores de identidad, APIs, servicios como KMS (*Key Management System*), balanceadores, bases de datos, servidores, contenedores, entre otros, deben ser configurados para la generación de registros de seguridad y enviados al componente SIEM (*Security Information and Event Management*) de la organización para su correlación y análisis en tiempo real de patrones o comportamiento anómalos.	
	42	Integrar capacidades de para realizar inteligencia de amenazas como servicio o nativas de los proveedores de servicio en nube.	
	43	Integrar capacidades de inteligencia artificial y analítica de comportamientos para detección de amenazas.	
	44	Implementación de herramientas tipo SOAR (*Security Orchestration, Automation and Response*) con el ecosistema de soluciones de seguridad para la automatización en la contención de amenazas de seguridad.	
Formación en ciberseguridad	**45**	Concientización de usuarios de la organización en conceptos, mejores prácticas, tendencias y amenazas en el ámbito ciberseguridad.	
	46	Evaluar el conocimiento de los empleados frente a las políticas, procesos y postura de seguridad de la organización.	
	47	Capacitación continua a los equipos de seguridad y tecnología en las capacidades requeridas para la implementación y operación de las capacidades de seguridad detalladas en la estrategia.	
Gobierno de seguridad	**48**	Políticas para el desarrollo, mantenimiento y actualización de capacidades de seguridad.	
	49	Definir un plan estratégico de seguridad que contemple la adquisición o actualización de las capacidades actuales de la organización con base a las necesidades propuestas en la estrategia.	
	50	Definir y ejecutar una metodología para la gestión integral de riesgos de seguridad.	
	51	Realizar una evaluación periódica de seguridad de contratos con proveedores y terceros.	

Tabla 5: Capacidades definidas de confianza cero propuestas por la metodología. Fuente: Propia

En resumen, la aplicación de los controles y capacidades anteriormente detalladas habilita una postura de seguridad robusta frente a los pilares de confianza cero de la siguiente forma:

- **Identidad**: La organización debe emplear políticas basadas en riesgos a partir del nivel asignado a una identidad y al flujo de la solicitud realizada, partiendo de los atributos e información recolectada durante este proceso, la cual es vital para la toma de decisiones para aprobar o denegar dicha solicitud. Es necesario adoptar un enfoque de evaluación individual, analizar no solo el entorno en general sino cada

solicitud que se realiza desde y hacia un recurso de la organización. Todo acceso debe basarse en el mínimo privilegio, de ninguna forma se asignarán más permisos de los requeridos para ejecutar la actividad solicitada y tienen que ser evaluados y otórganos de nuevo basado en los cambios asociados a la solicitud. Por último, todas las identidades deben ser gobernadas por un proceso de identidad y control de acceso para garantizar la correcta gestión de su ciclo de vida.

- **Seguridad en la red:** es imperativo reducir las áreas de confianza a nivel de red, basados en las características de los recursos que aloja. Esto se logra con la adopción de prácticas como segmentación de la red, minimizar la superficie de exposición, realizar un control granular de las comunicaciones y la separación de ambientes como parte fundamental en el diseño de una arquitectura, logrando así generar un control de las comunicaciones sobre el tráfico desde y hacia cualquier recurso y minimizando el impacto de una intrusión, conteniendo al intruso y evitando un movimiento lateral a segmentos con activos críticos para la organización. Adicionalmente, todo mensaje generado en las comunicaciones desde y hacia la organización deben estar autenticados y cifrados, por lo cual se deben emplear protocolos que permitan integrar este control al tráfico de red o bien agregar capas adicionales que incorporar este nivel de seguridad requerido. Ej: tls para protocolos http (https), ftp (ftps) o el remplazo de protocolos de acceso como telnet por ssh.

- **Seguridad en los dispositivos:** el reto actual de la evolución en el uso tradicional de estaciones de trabajo de escritorio a la necesidad de gestionar accesos desde dispositivos móviles, computadores portátiles ya sean personales o propiedad de la organización es una prioridad para la organización. Debido a esto, extender el perímetro y los controles de seguridad al punto final es una obligación para soportar los nuevos modelos de trabajo de forma segura. Continuar con proceso base como el monitoreo, evaluación y aplicación de estándares,

configuraciones de seguridad y cumplimiento de la línea base de software de seguridad definida para cada dispositivo reduciendo así configuraciones y servicios por defecto o innecesarios. Por último, ejecutar de manera periódica un monitoreo y gestión de actualizaciones, parches y vulnerabilidades.

- **Seguridad en las aplicaciones:** las APIs y servicios web actualmente se conocen como los diplomáticos en la nube. Son herramientas claves para la integración entre aplicaciones permitiendo el intercambio de información o gestión de las soluciones entre recursos internos o de terceros. Es necesario definir lineamientos de seguridad en cuanto a la publicación, protocolos de comunicación, autenticación, autorización para su consumo y cifrado y firma de los mensajes intercambiados para garantizar el aseguramiento de la información intercambiada. Los servicios web, APIs, aplicaciones e infraestructura deben ser gobernados por un proceso de desarrollo seguro que incluya un conjunto prácticas seguras en la codificación y automatice la ejecución de controles de seguridad durante todas las fases del ciclo previo a su liberación a un entorno productivo.

- **Seguridad en los datos:** asegurar los datos durante cada fase del ciclo de vida (creación, almacenamiento, uso, intercambio, archivado, y destrucción), empleando técnicas de cifrado, etiquetado, descubrimiento y controlar de acceso ayudara a salvaguardar la confidencialidad, integridad y disponibilidad requerida por la organización.

Finalmente, las arquitecturas cada día convergen a entornos de nube, por lo cual debemos incrementar la evaluación, monitoreo y aseguramiento de estos recursos y el acceso a su información. Emplear herramientas tipo CSPM permitirán obtener visibilidad y capacidades para remediar cualquier desviación a la postura de seguridad para la nube empleada.

5.4 Desestabilizadores de la estrategia

Denominamos desestabilizadores a las posibles circunstancias que puedan alterar o impactar en el desarrollo y cumplimiento de la estrategia. Conocerlos, comprender su origen y realizar una gestión oportuna e integral de estos, será el objetivo para desarrollar en esta fase.

5.4.1 Desviaciones en los procesos de seguridad

Lo que no podemos medir, no lo podemos gobernar y evolucionar, por lo cual cada proceso debe contar con su correspondiente indicador de medición que permita identificar el nivel de cumplimiento y generar planes de acción asociados a las deviaciones que se presenten. A continuación, se presenta una propuesta de indicadores mínimos que permitan evaluar la efectividad y eficacia los procesos de seguridad de la organización:

Indicador	Descripción	Formula de medición
Monitoreo y gestión de vulnerabilidades	cobertura del proceso de gestión de vulnerabilidades sobre la totalidad de recursos de la organización	Número total de recursos evaluados / Número total de recursos
Actualización tecnológica de la infraestructura	todos los recursos como servidores, bases de datos, equipos finales de cómputo, aplicaciones se deben encontrar actualizados a su última versión	Numero de recursos actualizados a su última versión / Número total de recursos
Control de cuentas privilegiadas	Las cuentas privilegiadas deben esta inventariadas, contar con un custodio asignado y ser gobernadas por una herramienta tipo PAM	Numero de cuentas privilegiadas gobernadas / Número total de cuentas privilegiadas
Cumplimiento de conceptos de arquitectura de seguridad y ciberseguridad	los conceptos emitidos para los proyectos deben cumplirse a la totalidad para puesta en producción de soluciones y/o servicios estables y seguros	Numero de conceptos en cumplimiento / Número total de conceptos emitidos
Gestión de eventos e incidentes de seguridad	los eventos e incidentes de seguridad deben ser gestionados en los tiempos acordados por la organización (ANS) Formula: Numero de eventos gestionados en cumplimiento de los ANS / Número total de eventos	Número de incidentes gestionados en cumplimiento de los ANS / Número total de incidentes
Endurecimiento de la infraestructura	recursos como servidores, bases de datos, equipos finales de cómputo, aplicaciones	Numero de recursos con estándar de seguridad aplicado / Número total de recursos

Tabla 5: Propuesta de indicadores de procesos de seguridad. Fuente: Propia

Al momento de evidenciar desviaciones el cumplimiento de los indicadores, estos deben ser reportados a las áreas de control para su análisis y así determinar las acciones a realizar o bien asumir la desviación frente al apetito de riesgo de la organización. Para cualquier caso, es imperativo que sea documentado y presentado al negocio para su conocimiento. La periodicidad de medición se definirá de acuerdo con la capacidad operativa, nivel de automatización y capacidad de generación de la información necesaria para su medición.

Si bien no definimos un indicador para medir la efectividad del programa de concientización, la organización debe poder identificar el nivel de adopción del programa buscando que los temas tratados en la campaña sean interiorizados y aplicados por todas las áreas dentro de sus roles y actividades diariamente. Así mismo debe medir el nivel de formación de los equipos en tecnologías o ámbitos específicos, en este caso en seguridad y ciberseguridad.

5.4.2 Shadow IT

Los beneficios de la computación en la nube como la agilidad para implementar soluciones, en algunos casos puede jugar en contra de las organizaciones ya que con la facilidad adquisición y uso de servicios de nube, es común que los usuarios finales o áreas de negocio puedan desplegar o hacer uso de aplicación y servicios sin pasar por las áreas y procesos encargados de evaluar, diseñar, desarrollar, implementar y certificar los proyectos que salen a producción para el uso de los usuarios, esto se denomina ShadowIT. Si bien existen varias herramientas para realizar el descubrimiento de estos servicios y/o aplicaciones, es imperativo definir un modelo a seguir que gobierne y define las acciones a realizar basado en los descubrimientos. A continuación, detallamos un modelo para identificar, gobernar y monitorear el uso de los “shadow IT.

Ilustración 9: Etapas de gestión de Shadow IT. Fuente: Propia

El objetivo es contar con visibilidad y evaluación continua del acceso a la nube y manejo de datos por parte de los usuarios.

- **Descubrir y registrar:** Obtener visibilidad para identificar los tipos de servicios empleados por los usuarios**.**
    - Clasificar por tipos de servicios como: almacenamiento, redes sociales, transferencia de datos, reuniones, descarga de software, correo, chat, entre otros.
    - Establecer una severidad de la situación actual basados en el número de aplicaciones/servicios descubiertos para llevar un registro de evolución

- **Analizar y evaluar:** Establecer un nivel de riesgo y analizar el caso de uso cubierto por el shadowIT determinando lo siguiente:
    - Determinar la ubicación de la información y el impacto de su uso.
    - Criticidad del shadowIT y nivel de riesgo, identificándola la calificación de la información y nivel de exposición de los datos de la organización.
    - Entender la necesidad de uso del shadowIT, área de negocio y grupo de usuarios y evaluar si esta puede ser cubierta por las aplicaciones y servicios autorizaos por la organización.

- **Gobernar y Monitorear:** Proporcionar una solución tecnológica que resuelva la necesidad.

- Ejecutar el proceso de evaluación y puesta en producción de una aplicación o servicio dentro de la organización. Durante este proceso se deben aplicar los controles de seguridad de acuerdo con el tipo de aplicación o servicio detallados en la estrategia.

- Capacitar a los usuarios en el riesgo del uso de aplicaciones y servicios no autorizados por la organización

5.4.3 Gestión de amenazas

Para Identificar, evaluar y gestionar las amenazas de la organización, debemos entender el entorno en el cual la organización desarrolla sus actividades. Con el objetivo de identificar los controles aplicables, debemos conocer y documentar las amenazas existentes y realizar actualizaciones periódicas con base a la evolución del negocio como al momento de adquirir y/o implementar nuevas soluciones o bien a medida que desarrollamos nuevas capacidades u objetivos dentro de nuestra estrategia de seguridad. Es imperativo que estas sean incorporadas y gestionadas dentro del proceso de gestión de riesgos de seguridad y ciberseguridad de la organización.

Es importante destacar que la arquitectura de confianza cero no está exenta de presentar amenazas en su implementación y operación. La organización debe contemplar no solo el despliegue de componentes tecnológicos, si estos no se configuran y operan bajo estándares y procesos que aseguren su correcto funcionamiento siguiendo los controles definidos en el mapa de amenazas. Si bien, las siguientes amenazas aplican para cualquier arquitectura de seguridad, es necesario detallar como puede afectar directamente a la estrategia de confianza cero definida:

Amenaza	Descripción	ID Control
Uso indebido o inadecuado de privilegios o atribuciones	La falta de control y monitoreo sobre las actividades que realizan los administradores de los componentes PE y PA permitiendo la modificación, eliminación o encubrimiento de las reglas configuradas resultado de un uso indebido y/o abuso de privilegios y ausencia o debilidades en los procesos de segregación de funciones.	Control 6
		Control 7
		Control 8
		Control 9
		Control 41
Denegación de servicio	Los componentes que ejecuten las funciones de PEP, PE o PA, o que se encuentren expuestos a internet pueden ser afectados por ataques de denegación de servicio limitando o anulando su capacidad brindar acceso a los recursos de la organización o la prestación de un servicio.	Control 20
		Control 33
Robo de credenciales, y/o suplantación de identidad	Usurpación de identidades para el acceso a recursos de la organización con la finalidad de ejecutar acciones mal intencionadas, robo de datos o degradación de la disponibilidad de los servicios debido al robo o uso indebido o falta de conocimiento en la gestión de credenciales por parte de los usuarios.	Control 1
		Control 3
		Control 4
		Control 8
		Control 9
		Control 41
		Control 45
Visibilidad deficiente de eventos de seguridad	Poca o nula generación, monitoreo y correlación de eventos de seguridad limitando la observabilidad y análisis de la actividad de los usuarios y componentes de seguridad y tecnología.	Control 41
		Control 42
		Control 43
Acceso no autorizado	Mecanismos de autenticación y algoritmos débiles, obsoletos o inseguros y débil gestión del ciclo de vidas de las identidades.	Control 5
		Control 6
		Control 27
		Control 41
		Control 43
Recursos con configuraciones predeterminaras	Obsolescencia en los estándares de seguridad definidos y deficiencia en los procesos de evaluación y aplicación de los estándares para los recursos de tipo software y hardware.	Control 11
		Control 12
		Control 30
		Control 31
		Control 32
Obsolescencia tecnológica de seguridad	Tecnologías que no permiten su integración con los nuevos esquemas de autenticación, monitoreo y cumplimiento definidos en la estrategia debido a una inadecuada gestión del ciclo de vida del software.	Control 48
		Control 49
		Control 50
		Control 51
Falta de capacitación y competencias	Poca o nula capacitación en tendencias y tecnologías asociadas a la estrategia de seguridad.	Control 47

Tabla 6: Amenazas y controles propuestos en la arquitectura de confianza cero. Fuente: propia

6 Conclusiones

A lo largo de documento abordamos la relevancia que ha tomado la computación en la nube, posicionándose como uno de los principales habilitadores de la estrategia de negocio de una organización. Cada día más áreas identifican una oportunidad o una necesidad que puede ser cubierta empleando estos servicios, lo cual lleva a la organización a una travesía con la responsabilidad suplir estas necesidades para ser competitivos en el mercado en el cual desempeñan su negocio, pero con una complejidad y un reto de habilitarlos de forma segura al mismo ritmo, impidiendo que la seguridad sea un bloqueante y evitando impactar la experiencia de los usuarios, ya que no adaptarse a las nuevas necesidades del negocio afecta en gran dimensión a la estrategia de innovación, generación de valor y la consecución de sus objetivos económicos. Por esta razón, a través del desarrollo del documento, abordamos las principales amenazas que están presentes en los entornos de nube en general. Esto se realizó con la finalidad de brindar un análisis desde el enfoque de seguridad a los desafíos que debemos conocer, evaluar y gestionar al momento de tomar decisiones sobre adoptar tecnologías en nube, sin embargo, la metodología propuesta, profundiza aún más en el estudio de las principales amenazas desde un enfoque específico sobre una estrategia de confianza cero, como el mal diseño y monitoreo de los procesos de seguridad, poca o nula visibilidad de nuestro entorno tecnológico y la ausencia de prácticas para la identificación, evaluación y gestión de amenazas de seguridad que podrían desestabilizar o impedir lograr el objetivo e implementación de la estrategia de acuerdo con la metodología planteada. Por último, a partir del desarrollo y entendimiento de los desestabilizadores de la estrategia, se realizó una definición de las prácticas y controles claves que deben ser implementados para su prevención y mitigación.

Como resultado de la investigación y análisis de los reportes de seguridad consultados, podemos concluir que, en la actualidad, el mayor porcentaje de brechas e incidentes de seguridad que afectan a las organizaciones, se deben a la materialización de amenazas presentes en los

procesos de gestión de identidades y controles de acceso. Por tal razón, la metodología propuesta resalta y prioriza la transformación de los procesos y controles tecnológicos que gobiernan y aseguran la gestión de identidades desde una perspectiva de confianza cero, promoviendo una evaluación estricta e individual sobre cada solicitud de acceso a un recurso, eliminando la confianza implícita independiente del dispositivo, usuario, ubicación, aplicaciones y datos vinculados en el flujo, obteniendo como resultado, una postura de seguridad rígida frente a estas amenazas y reduciendo el alcance e impacto generado debido a su materialización en la organización.

Uno de los principales objetivos del documento, es destacar que no existe una única tecnología que nos permite adoptar de manera holística una estrategia de confianza cero. Al contrario, el éxito de una correcta alineación a esta estrategia estará dado por un conjunto de actividades que deberán ejecutar los equipos de seguridad y las diferentes áreas de negocio que se verán impactadas o que se encargarán de habilitar desde sus funciones el desarrollo armónico y favorable de la estrategia. Por cual la metodología propuesta no solo explora la estrategia de confianza cero desde un enfoque netamente tecnológico dejando a un lago la estrategia y gobierno de esta. Al contrario, explora ambas necesidades brindando una guía clara de actividades para abordar la transformación a niveles estratégicos, tactitos y operativos de la organización y no solo desde una adquisición tecnológica, exponiendo una serie de necesidades presentes en cada nivel organizacional y proponiendo un guion para sustentar y exponer la necesidad de adoptar una estrategia de confianza cero como habilitador estratégico para la organización a partir de los resultados claves de su implementación. Adicionalmente propone un conjunto de actividades iniciales e imperativas, como alinear y dar dirección a los diferentes equipos cross-funcionales asociados a la estrategia, la concientización de la alta dirección, identificación de los impulsadores claves que tiene impacto sobre los objetivos del negocio, formalización de la postura de seguridad e inclusión y evaluación en los diseños de las soluciones para garantizar su cumplimiento.

Es importante destacar que si bien, la falta o nula gestión de seguridad en los procesos que diseñan, desarrollan e implementan una solución

tecnológica no es la principal amenaza que abruma a las organizaciones, subestimarla puede resultar en la generación de vectores que facilitan la materialización de las demás amenazas planteadas en el documento ya que partiendo de un diseño y/o arquitectura deficiente y vulnerable, directamente facilitamos el escenario para que se exploten dichas vulnerabilidades o ausencias de controles de seguridad resultando en un incidente de seguridad. Es aquí donde toma relevancia el definir, promover y velar por el cumplimiento del enfoque de confianza cero y las directrices de seguridad planteadas en el documento sobre cada uno de los pilares definidos.

Generar las condiciones necesarias para la implementación de soluciones seguras que habiliten las nuevas necesidades de las organizaciones, gestionar las amenazas presentes y contribuir en su diseño y operación partiendo de los principios de confianza cero es el aporte realizando con la construcción de la metodología descrita en este documento. Por consiguiente, detallamos los controles mínimos técnicos y procedimentales que se deben definir como directrices en el diseño e implementación de una solución tecnológica y las prácticas y tecnologías que se deben desarrollar o adquirir e integrar a la estrategia de seguridad para su aplicación en cada uno de los pilares detallados en la metodología dando cumplimiento a los principios de confianza cero y obteniendo como resultado, un postura segura y resiliente frente al entorno cambiante y hostil que se presenta en la actualidad.

En cuanto a la investigación y documentación desarrollada en el presente trabajo, cubriendo los orígenes, evolución, fundamentos, documentos de apoyo y estado del concepto de confianza cero en la actualidad, ayudara a las organizaciones que se encuentran en las fases iniciales de exploración y entendimiento de este nuevo enfoque de seguridad a entender su esencia, su objetivo principal, a identificar sus componentes y el valor que genera desarrollar sus estrategias de seguridad a partir de este enfoque o su integración a la ya existente.

Para finalizar, entendiendo la complejidad de gestionar servicios en nube, de las nuevas modalidades de trabajo distribuido y su necesidad

imperativa para hacer frente a las necesidades de una organización. Podemos concluir que la adopción del enfoque en confianza cero es en la actualidad el mejor aliado para hacer frente a estos desafíos, buscando cambiar la visión de ser 100% seguros a un enfoque que busque reducir la probabilidad de ocurrencia de una brecha de seguridad y minimizar el impacto debido a su materialización.

7 Glosario

API (Application Programming Interface): un punto de acceso al sistema o una función de biblioteca que tiene una sintaxis bien definida y es accesible desde programas de aplicación o código de usuario para proporcionar una funcionalidad bien definida. [18]

APT (Advanced Persistent Threat): un adversario con niveles sofisticados de experiencia y recursos significativos, que le permiten mediante el uso de múltiples vectores de ataque diferentes (por ejemplo, cibernético, físico y engaño), generar oportunidades para lograr sus objetivos, que generalmente son establecer y ampliar su presencia dentro del infraestructura de tecnología de la información de organizaciones con el fin de extraer continuamente información y/o socavar o impedir aspectos críticos de una misión, programa u organización, o colocarse en condiciones de hacerlo en el futuro; Además, la amenaza persistente avanzada persigue sus objetivos repetidamente durante un período prolongado, adaptándose a los esfuerzos de un defensor para resistirla y con determinación para mantener el nivel de interacción necesario para ejecutar sus objetivos. [19]

BeyondCorp: es la implementación de Google de un modelo de seguridad fiable de tipo confianza cero. Se basa en una década de experiencia en Google, en combinación con ideas y prácticas recomendadas de la comunidad. BeyondCorp pasa los controles de acceso del perímetro de red a usuarios concretos, por lo que permite trabajar de forma segura desde prácticamente cualquier ubicación sin necesidad de una VPN tradicional. [20]

BIA (Business Impact Analysis): un análisis de los requisitos, funciones e interdependencias de un sistema de información utilizado para caracterizar los requisitos y prioridades de contingencia del sistema en caso de una interrupción significativa. [21]

Bot: programa de software que realiza tareas automatizadas, repetitivas y predefinidas. Los bots suelen imitar o reemplazar el comportamiento de los usuarios humanos. Debido a que están automatizados, operan mucho más rápido que los usuarios humanos. Realizan funciones útiles, como la atención

al cliente o la indexación de motores de búsqueda, pero también pueden presentarse en forma de un código malicioso, utilizado para obtener el control total de un ordenador. [22]

CASB (Cloud Access Security Brokers): son puntos de aplicación de políticas de seguridad locales o basados en la nube, colocados entre los consumidores de servicios en la nube y los proveedores de servicios en la nube para combinar e interponer políticas de seguridad empresariales a medida que se accede a los recursos basados en la nube. Los CASB consolidan múltiples tipos de aplicación de políticas de seguridad. Los ejemplos de políticas de seguridad incluyen autenticación, inicio de sesión único, autorización, asignación de credenciales, creación de perfiles de dispositivos, cifrado, registro, alertas, detección/prevención de código malicioso, etc. [23]

CSPM (Cloud Security Posture Management): consta de ofertas que gestionan continuamente la postura de seguridad de IaaS y PaaS mediante la prevención, detección y respuesta a los riesgos de la infraestructura de la nube. El núcleo de CSPM aplica marcos comunes, requisitos regulatorios y políticas empresariales para descubrir y evaluar de manera proactiva y reactiva el riesgo/confianza de la configuración de los servicios en la nube y los ajustes de seguridad. Si se identifica un problema, se proporcionan opciones de solución (automatizadas o impulsadas por humanos). [24]

CWPP (Cloud Workload Protection Platform): son productos de seguridad centrados en cargas de trabajo que protegen las cargas de trabajo de servidores en entornos de centros de datos híbridos y multinube. Los CWPP brindan visibilidad y control consistentes para máquinas físicas, máquinas virtuales, contenedores y cargas de trabajo sin servidor, independientemente de su ubicación. Las ofertas de CWPP protegen las cargas de trabajo mediante una combinación de protección de la integridad del sistema, control de aplicaciones, monitoreo del comportamiento, prevención de intrusiones y protección antimalware opcional en tiempo de ejecución. Las ofertas de CWPP también deben incluir la exploración de riesgos de cargas de trabajo de forma proactiva en el proceso de desarrollo. [25]

DDoS (Distributed Denial of Service): una técnica de denegación de servicio que utiliza numerosos hosts para realizar el ataque. [26]

DLP (Data Loss Protection): describe un conjunto de tecnologías y técnicas de inspección utilizadas para clasificar el contenido de información dentro de un objeto, como un archivo, correo electrónico, paquete, aplicación o almacén de datos, mientras está en reposo (en almacenamiento), en uso (durante una operación) o en tránsito. (a través de una red). Las herramientas DLP también tienen la capacidad de aplicar dinámicamente una política (como registrar, informar, clasificar, reubicar, etiquetar y cifrar) y/o aplicar protecciones de gestión de derechos de datos empresariales. [27]

FIPS (Federal Information Processing Standard): este estándar especifica los requisitos de seguridad que cumplirá un módulo criptográfico utilizado dentro de un sistema de seguridad que protege información confidencial pero no clasificada (en adelante denominada información confidencial). El estándar proporciona cuatro niveles de seguridad cualitativos cada vez mayores: Nivel 1, Nivel 2, Nivel 3 y Nivel 4. Los requisitos de seguridad cubren áreas relacionadas con el diseño seguro y la implementación de un módulo criptográfico. Estas áreas incluyen la especificación del módulo criptográfico, los puertos y las interfaces del módulo criptográfico; roles, servicios y autenticación; modelo de estados finitos; seguridad física; entorno operativo; gestión de claves criptográficas; interferencia electromagnética/compatibilidad electromagnética (EMI/EMC); autopruebas; garantía de diseño; y mitigación de otros ataques. [28]

HMAC (Hash-based Message Authentication Code): es una técnica de autenticación criptográfica que utiliza una función hash y una clave secreta. Con HMAC, puede lograr la autenticación y verificar que los datos sean correctos y auténticos con secretos compartidos, a diferencia de los enfoques que utilizan firmas y criptografía asimétrica. [29]

IaaS (Infraestructure as a Service): la capacidad proporcionada al consumidor es procesamiento, almacenamiento, redes y otros recursos informáticos fundamentales donde el consumidor puede implementar y ejecutar software arbitrario, que puede incluir sistemas operativos y

aplicaciones. El consumidor no gestiona ni controla la infraestructura de la nube subyacente, pero tiene control sobre los sistemas operativos, el almacenamiento y las aplicaciones implementadas; y posiblemente control limitado de componentes de red seleccionados (por ejemplo, firewalls de host). [30]

IDM (Identity management): la gestión de identidades, también conocida como gestión de ID e IDM, es una solución de seguridad que se utiliza para verificar y asignar permisos a entidades digitales, que pueden ser personas, sistemas o dispositivos. La gestión de identidad incluye la creación, el mantenimiento y la verificación de estas identidades digitales y sus atributos y la asociación de derechos y restricciones de usuario con identidades establecidas. [31]

IoT (Internet of Things): dispositivos de usuario o industriales que estén conectados a internet. Los dispositivos IoT incluyen sensores, controladores y electrodomésticos. [32]

IRM (Information Rights Management): a gestión de derechos de información (IRM) es una forma de tecnología de seguridad de TI que se utiliza para proteger los documentos que contienen información confidencial del acceso no autorizado. A diferencia de la gestión de derechos digitales (DRM) tradicional que se aplica a medios producidos en masa, como canciones y películas, IRM se aplica a documentos, hojas de cálculo y presentaciones creadas por individuos. IRM protege los archivos contra copias, visualizaciones, impresiones, reenvíos, eliminaciones y ediciones no autorizadas. [33]

JEA (Just enough access): practica de gestionar permisos de IAM del tamaño adecuado para implementar privilegios mínimos para todas las identidades. [34]

JIT (Just In Time): el acceso JIT ayuda a las organizaciones a proporcionar acceso para que los usuarios solo tengan los derechos para acceder a cuentas y recursos con privilegios cuando lo necesiten, y no en cualquier otro momento. En lugar de conceder un acceso siempre activado (o permanente),

las organizaciones pueden utilizar el acceso JIT para limitar el acceso a un recurso específico durante un plazo de tiempo determinado. Este enfoque granular mitiga el riesgo de abuso de las cuentas con privilegios al reducir considerablemente la cantidad de tiempo que un ciberatacante o infiltrado malintencionado tiene para acceder a las cuentas con privilegios antes de moverse lateralmente a través de un sistema y obtener acceso no autorizado a datos confidenciales. [35]

JWE (JSON Web Encryption): representa contenido cifrado utilizando estructuras de datos basadas en JSON. Los mecanismos criptográficos JWE cifran y brindan protección de integridad para una secuencia arbitraria de octetos. [36]

JWS (JSON Web Signature): se utiliza para representar contenido protegido con firmas digitales o códigos de autenticación de mensajes basados en hash (HMAC) con la ayuda de estructuras de datos JSON. Protege criptográficamente un encabezado JWS y una carga útil JWS con una firma JWS. [37]

JWT (JSON Web Token): es un estándar abierto que define una forma compacta y autónoma de transmitir información de forma segura entre partes como un objeto JSON. Esta información se puede verificar y confiar porque está firmada digitalmente. Los JWT se pueden firmar mediante un secreto (con el algoritmo HMAC) o un par de claves pública/privada mediante RSA o ECDSA. [38]

KMS (Key Management System): es un sistema para la gestión de claves criptográficas y sus metadatos (por ejemplo, generación, distribución, almacenamiento, copia de seguridad, archivo, recuperación, uso, revocación y destrucción). Se puede utilizar un sistema automatizado de gestión de claves para supervisar, automatizar y proteger el proceso de gestión de claves. [39]

MAC (Message Authentication Code): se utiliza para autenticar el origen y la naturaleza de un mensaje. Los MAC utilizan criptografía de autenticación para verificar la legitimidad de los datos enviados a través de una red o

transferidos de una persona a otra. En otras palabras, MAC garantiza que el mensaje proviene del remitente correcto, no ha sido modificado y que los datos transferidos a través de una red o almacenados dentro o fuera de un sistema son legítimos y no contienen código dañino. [40]

MAM (Mobile Application Management): es una herramienta local o SaaS diseñada específicamente para la gestión de licencias, distribución, seguridad y gestión del ciclo de vida de aplicaciones para plataformas de dispositivos móviles. Brinda la capacidad de establecer políticas relacionadas con la seguridad, el uso y la gestión continua de aplicaciones o grupos de aplicaciones. [41]

MCAP (Microcore and Perimeter): en la red Zero Trust, cada una de las zonas de conmutación conectadas a una interfaz se denomina “microcore and perimeter”. Cada zona segmentada es su propio conmutador de micronúcleo y puede considerar cada zona como un microperímetro porque todos los recursos dentro de un micronúcleo específico comparten funcionalidades y atributos de política global similares. [8]

MDM (Mobile Device Management): capacidad para la administración de dispositivos móviles como teléfonos inteligentes, tabletas, computadoras, laptops y computadoras de escritorio. Generalmente se implementa a través de un producto de terceros que tiene funciones de administración para proveedores particulares de dispositivos móviles. [42]

MFA (Multi-Factor Authentication): authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). [43]

OAUTH (Open Authentication): es un estándar diseñado para permitir que un sitio web o una aplicación accedan a recursos alojados por otras aplicaciones web en nombre de un usuario. Sustituyó a OAuth 1.0 en 2012 y ahora es el estándar de facto de la industria para la autorización en línea. OAuth 2.0 proporciona acceso consentido y restringe las acciones que la

aplicación del cliente puede realizar en los recursos en nombre del usuario, sin compartir nunca las credenciales del usuario. [44]

OIDC (OpenID Connect): es un protocolo de autenticación e identidad federado a escala de Internet creado sobre el marco de autorización OAuth 2.0 y el sistema criptográfico JSON Object Signing and Encryption (JOSE). OpenID Connect se basa en el protocolo de autorización OAuth 2.0 para permitir que el suscriptor autorice a las partes a acceder a la identidad y la información de autenticación del suscriptor. [45]

OWASP (Open Web Application Security Project): proyecto abierto de seguridad de aplicaciones web, o OWASP, es una organización internacional sin ánimo de lucro dedicada a la seguridad de las aplicaciones web. Uno de los principios fundamentales del OWASP es que todos sus materiales están disponibles de forma gratuita y son fácilmente accesibles en su sitio web, lo cual posibilita que cualquiera pueda mejorar la seguridad de su propia aplicación web. Entre los materiales que ofrecen se incluyen documentación, herramientas, vídeos y foros. Quizá su proyecto más conocido sea el OWASP Top 10**.** [46]

PaaS (Platform as a service): la capacidad proporcionada al consumidor para implementar en la infraestructura de la nube aplicaciones creadas o adquiridas por el consumidor desarrolladas utilizando lenguajes de programación, bibliotecas, servicios y herramientas respaldados por el proveedor. El consumidor no administra ni controla la infraestructura de la nube subyacente, incluida la red, los servidores, los sistemas operativos o el almacenamiento, pero tiene control sobre las aplicaciones implementadas y posiblemente los ajustes de configuración para el entorno de alojamiento de aplicaciones. [47]

PAM (Privileged Access Management): las organizaciones implementan la gestión de acceso privilegiado para protegerse contra las amenazas que plantean el robo de credenciales y el uso indebido de privilegios. PAM se refiere a una estrategia integral de ciberseguridad (que comprende personas, procesos y tecnología) para controlar, monitorear, proteger y auditar todas las

identidades y actividades privilegiadas humanas y no humanas en un entorno de TI empresarial. [48]

PKI (Public Key Infrastructure): la arquitectura, organización, técnicas, prácticas y procedimientos que respaldan colectivamente la implementación y operación de un sistema criptográfico de clave pública basado en certificados. Marco establecido para emitir, mantener y revocar certificados de clave pública. [49]

SaaS (Software as a Service): la capacidad proporcionada al consumidor de utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura de nube. Se puede acceder a las aplicaciones desde varios dispositivos cliente a través de una interfaz de cliente ligero, como un navegador web (por ejemplo, correo electrónico basado en web), o una interfaz de programa. El consumidor no gestiona ni controla la infraestructura de la nube subyacente, incluida la red, los servidores, los sistemas operativos, el almacenamiento o incluso las capacidades de las aplicaciones individuales, con la posible excepción de ajustes limitados de configuración de aplicaciones específicas del usuario. [50]

SAML (Security Assertion Markup Language): El lenguaje de marcado de afirmación de seguridad, o SAML, es una forma estandarizada de indicar a aplicaciones y servicios externos que un usuario es quien dice ser. SAML hace posible la tecnología de inicio de sesión único (SSO) al proporcionar una forma de autenticar a un usuario una vez y luego comunicar esa autenticación a múltiples aplicaciones. La versión más actual de SAML es SAML 2.0. Piense en la autenticación SAML como si fuera una tarjeta de identificación: una forma breve y estandarizada de mostrar quién es alguien. En lugar de, digamos, realizar una serie de pruebas de ADN para confirmar la identidad de alguien, es posible simplemente echar un vistazo a su documento de identidad. [51]

SDP (Software Defined Perimeter): es una metodología de seguridad que distribuye el acceso a aplicaciones internas según la identidad de un usuario, con confianza que se adapta según el contexto. Mientras la seguridad tradicional está centralizada en el centro de datos, SDP está en todas partes,

se entrega a través de la nube. Utiliza la política comercial para determinar si autenticar a un usuario para que acceda a los recursos, lo que lo convierte en una parte importante de la seguridad de las organizaciones que priorizan la nube y los dispositivos móviles. [52]

Serverless: es un método para proporcionar servicios de backend según su uso. Un proveedor serverless permite a los usuarios escribir e implementar código sin la molestia de preocuparse por la infraestructura subyacente. Una empresa que obtiene servicios de backend de un proveedor sin servidor se le cobra en función de su cálculo y no tiene que reservar ni pagar una cantidad fija de ancho de banda o una cantidad de servidores, ya que el servicio se escala automáticamente. Tenga en cuenta que, a pesar del nombre sin servidor, todavía se utilizan servidores físicos, pero los desarrolladores no necesitan conocerlos. [53]

SIEM (Security Information and Event Management): aplicación que brinda la capacidad de recopilar datos de seguridad de los componentes del sistema de información y presentar esos datos como información procesable a través de una única interfaz. [54]

SOAR (Security Orchestration, Automation and Response): permite coordinar, ejecutar y automatizar tareas entre varias personas y herramientas, todo dentro de una única plataforma. Esto permite a las organizaciones no sólo responder rápidamente a los ataques de ciberseguridad, sino también observar, comprender y prevenir incidentes futuros, mejorando así su postura general de seguridad. [55]

SWG (Secure Web Gateway): una puerta de enlace web segura (SWG) es una solución que filtra software/malware no deseado del tráfico web/Internet iniciado por el usuario y exige el cumplimiento de las políticas corporativas y regulatorias. Estas puertas de enlace deben, como mínimo, incluir filtrado de URL, detección y filtrado de códigos maliciosos y controles de aplicaciones para aplicaciones web populares, como mensajería instantánea (IM) y Skype. También se incluye cada vez más la prevención de fuga de datos nativa o integrada. [56]

UEBA (User and Entity Behavior Analytics): es una solución de ciberseguridad que utiliza algoritmos y aprendizaje automático para detectar anomalías en el comportamiento no solo de los usuarios de una red corporativa, sino también de los enrutadores, servidores y puntos finales de esa red. [57]

VPN (Virtual Private Network): una red virtual construida sobre redes existentes que puede proporcionar un mecanismo de comunicación seguro para datos e información IP transmitida entre redes. [58]

WAF (Web Application Firewall): ayuda a proteger las aplicaciones web filtrando y monitoreando el tráfico HTTP entre una aplicación web e Internet. Por lo general, protege las aplicaciones web de ataques como falsificación entre sitios, secuencias de comandos entre sitios, inclusión de archivos e inyección SQL, entre otros. Un WAF es una defensa de protocolo de capa 7 (en el modelo OSI) y no está diseñado para defenderse contra todo tipo de ataques. Este método de mitigación de ataques suele ser parte de un conjunto de herramientas que juntas crean una defensa integral contra una variedad de vectores de ataque. [59]

WAAP (Web Application and API Protection): son la evolución de los servicios de firewall de aplicaciones web en la nube, y amplían el alcance y la profundidad de la seguridad. A diferencia de un firewall tradicional, un WAAP es una herramienta de seguridad altamente especializada diseñada específicamente para proteger aplicaciones web y API. En realidad, un WAAP reside en el borde exterior de una red frente al lado público de una aplicación web y analiza el tráfico entrante. Si bien esto es todo lo que hace, lo hace muy bien. Un WAAP se centra únicamente en la capa de aplicación (capa 7) del modelo OSI. [60]

WS security: describe mejoras en la mensajería SOAP para proporcionar calidad de protección a través de la integridad y la confidencialidad de los mensajes y la autenticación de un solo mensaje. WS-Security es un estándar a nivel de mensajes que se basa en la seguridad de los mensajes SOAP mediante firma digital XML, la confidencialidad mediante cifrado XML y la

propagación de credenciales mediante tokens de seguridad. La especificación de seguridad de servicios web define las facilidades para proteger la integridad y confidencialidad de un mensaje y proporciona mecanismos para asociar reclamos relacionados con la seguridad con el mensaje. [61]

ZTNA (Zero Trust Network Access): es un enfoque de seguridad de TI que proporciona un acceso remoto seguro a las aplicaciones, los datos y los servicios de una organización según una serie de políticas de control de acceso claramente definidas. El ZTNA se diferencia de las redes privadas virtuales (VPN) en que otorga acceso solo a servicios o aplicaciones específicos, mientras que las VPN conceden acceso a una red completa. Cada vez son más los usuarios que acceden a los recursos desde casa u otras ubicaciones, por lo que las soluciones ZTNA pueden ayudar a salvar las carencias de otras tecnologías y métodos de acceso remoto seguro. [62]

8 Bibliografía

[1]. International Data Corporation. (14 de 09 de 2021). IDC Forecasts Worldwide "Whole Cloud" Spending to Reach $1.3 Trillion by 2025. Recuperado el 30 de 11 de 2022, de https://www.idc.com/getdoc.jsp?containerId=prUS48208321

[2]. Mckinsey. (15 de 06 de 2022). Three new mandates for capturing a digital transformation’s full value. Recuperado el 30 de 11 de 2022, de https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/three-new-mandates-for-capturing-a-digital-transformations-full-value

[3]. Verizon. (2022). Data Breach Investigations Report. Recuperado el 30 de 11 de 2022, de https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[4]. Cloud Security Alliance. (27 de 06 de 2017). Recuperado el 20 de 03 de 2023, de Cloud Security Alliance: https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

[5]. National Institute of Standards and Technology. (05 de 02 de 2018). Recuperado el 20 de 03 de 2023, de https://www.nist.gov/: https://www.nist.gov/cyberframework/framework

[6]. Cloud Security Alliance. Cloud Controls Matrix (CCM). Recuperado el 20 de 07 de 2023, de https://cloudsecurityalliance.org/: https://cloudsecurityalliance.org/research/cloud-controls-matrix/

[7]. Cloud Security Alliance. (06 de 06 de 2022). Top Cloud Threats to Cloud Computing - Pandemic Eleven. Recuperado el 20 de 03 de 2023, de https://cloudsecurityalliance.org: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven/

[8]. Kindervag, J. (2010). Build Security Into Your Network’s DNA: The Zero Trust Network Architecture. Forrester. Recuperado el 30 de 11 de 2022

[9]. Google. (10 de 08 de 2022). Zero Trust and BeyondCorp Google Cloud. Recuperado el 30 de 11 de 2022, de https://cloud.google.com/blog/topics/developers-practitioners/zero-trust-and-beyondcorp-google-cloud

[10]. Cunningham, C. (2018). The Zero Trust eXtended (ZTX) Ecosystem. Forrester. Recuperado el 30 de 11 de 2022a

[11]. National Institute of Standards and Technology. (08 de 2020). NIST Special Publication 800-207 - Zero Trust Architecture. Recuperado el 30 de 11 de 2022, de https://csrc.nist.gov/publications/detail/sp/800-207/final

[12]. Department of Defense. (07 de 11 de 2022). DoD Zero Trust Strategy. Recuperado el 30 de 11 de 2022, de https://dodcio.defense.gov/Library/

[13]. Information Security RMF Resource center. (01 de 07 de 2021). Zero Trust Architecture in the DoD and Federal Civil Agencies. Recuperado el 30 de 11 de 2022, de https://rmf.org/2021/07/13/zero-trust-architecture-in-the-dod-and-federal-civil-agencies/

[14]. National Institute of Standards and Technology. (08 de 10 de 2023). Glosary. Recuperado el 20 de 08 de 2023, de csrc.nist.gov: https://csrc.nist.gov/glossary/term/identity

[15]. National Institute of Standards and Technology. (08 de 10 de 2023). Glosary. Recuperado el 20 de 08 de 2023, de csrc.nist.gov: https://csrc.nist.gov/glossary/term/authentication

[16]. National Institute of Standards and Technology. (08 de 10 de 2023). Glosary. Recuperado el 20 de 08 de 2023, de csrc.nist.gov: https://csrc.nist.gov/glossary/term/authorization

[17]. Microsoft. (29 de 03 de 2023). Secure networks with Zero Trust. Recuperado el 01 de 10 de 2023, de https://learn.microsoft.com/en-us/security/zero-trust/deploy/networks

[18]. National Institute of Standards and Technology. (01 de 06 de 2020). Computer Security Resource Center. Recuperado el 12 de 12 de 2023, de csrc.nist.gov: https://csrc.nist.gov/glossary/term/application_programming_interface

[19]. National Institute of Standards and Technology. (01 de 09 de 2012). Computer Security Resource Center. Recuperado el 13 de 12 de 2023, de csrc.nist.gov: https://csrc.nist.gov/glossary/term/APT

[20]. Google. (01 de 12 de 2014). BeyondCorp. Recuperado el 13 de 12 de 2023, de cloud.google.com: https://cloud.google.com/beyondcorp?hl=es

[21]. National Institute of Standards and Technology. (01 de 05 de 2010). Computer Security Resource Center. Recuperado el 13 de 12 de 2023, de nvlpubs.nist.gov: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

[22]. Kaspersky. (01 de 01 de 2023). What are bots? – Definition and Explanation. Recuperado el 13 de 12 de 2023, de kaspersky.com: https://www.kaspersky.com/resource-center/definitions/what-are-bots

[23]. Gartner. (13 de 12 de 2023). Gartner Glossary. Recuperado el 13 de 12 de 2023, de gartner.com: https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs

[24]. Gartner. (13 de 12 de 2023). Gartner Glossary. Recuperado el 13 de 12 de 2023, de gartner.com: https://www.gartner.com/en/information-technology/glossary/cloud-security-posture-management

[25]. medium. (17 de 11 de 2022). CWPP Gartner Definition. Recuperado el 13 de 12 de 2023, de medium.com: https://medium.com/@cloud_tips/cwpp-gartner-definition-91c2898a31d0

[26]. National Institute of Standards and Technology. (01 de 09 de 2011). Computer Security Resource Center. Recuperado el 13 de 12 de 2023, de csrc.nist.gov: https://csrc.nist.gov/glossary/term/ddos

[27]. Gartner. (13 de 12 de 2023). Gartner Glossary. Recuperado el 13 de 12 de 2023, de gartner.com: https://www.gartner.com/en/information-technology/glossary/data-loss-protection-dlp

[28]. National Institute of Standards and Technology. (21 de 05 de 2001). security requirements for cryptographic. Recuperado el 13 de 12 de 2023, de csrc.nist.gov: https://csrc.nist.gov/files/pubs/fips/140-2/upd2/final/docs/fips1402.pdf

[29]. Okta. (15 de 09 de 2023). HMAC (Hash-Based Message Authentication Codes) Definition. Recuperado el 15 de 12 de 2023, de okta.com: https://www.okta.com/identity-101/hmac/

[30]. National Institute of Standards and Technology. (01 de 09 de 2011). Computer Security Resource Center. Recuperado el 13 de 12 de 2023, de csrc.nist.gov: https://csrc.nist.gov/glossary/term/infrastructure_as_a_service

[31]. sailpoint. (16 de 03 de 2023). Identity management. Recuperado el 13 de 12 de 2023, de sailpoint.com: https://www.sailpoint.com/identity-library/identity-management/

[32]. National Institute of Standards and Technology. (01 de 06 de 2020). Computer Security Resource Center. Recuperado el 13 de 12 de 2023, de csrc.nist.gov: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-16.pdf

[33]. Trellix. (13 de 12 de 2023). What Is Information Rights Management. Recuperado el 13 de 12 de 2023, de trellix.com: https://www.trellix.com/security-awareness/cybersecurity/what-is-information-rights-management-irm/

[34]. Cyberark. (13 de 12 de 2023). Cloud Security. Recuperado el 13 de 12 de 2023, de cyberark.com: https://www.cyberark.com/products/cloud-security/

[35]. Cyberark. (13 de 12 de 2023). Acceso Just-In-Time. Recuperado el 13 de 12 de 2023, de cyberark.com: https://www.cyberark.com/es/what-is/just-in-time-access/

[36]. Internet Engineering Task Force (IETF). (01 de 05 de 2015). JSON Web Encryption (JWE). Recuperado el 2023, de rfc-editor.org: https://www.rfc-editor.org/rfc/rfc7516.txt

[37]. Loginradius. (13 de 12 de 2023). What are JWT, JWS, JWE, JWK, and JWA. Recuperado el 13 de 12 de 2023, de loginradius.com: https://www.loginradius.com/blog/engineering/guest-post/what-are-jwt-jws-jwe-jwk-jwa/

[38]. jwt. (13 de 12 de 2023). Introduction to JSON Web Tokens. Recuperado el 13 de 12 de 2023, de jwt.io: https://jwt.io/introduction

[39]. National Institute of Standards and Technology. (01 de 05 de 2020). Computer Security Resource Center. Recuperado el 13 de 12 de 2023, de csrc.nist.gov: https://csrc.nist.gov/glossary/term/key_management_system

[40]. Fortinet. (15 de 12 de 2023). What Is A Message Authentication Code? Recuperado el 15 de 12 de 2023, de fortinet.com: https://www.fortinet.com/resources/cyberglossary/message-authentication-code

[41]. Gartner. (13 de 12 de 2023). Mobile Application Management. Recuperado el 13 de 12 de 2023, de gartner.com: https://www.gartner.com/reviews/market/mobile-application-management

[42]. National Institute of Standards and Technology. (01 de 09 de 2020). Computer Security Resource Center. Recuperado el 13 de 12 de 2023, de csrc.nist.gov: https://csrc.nist.gov/glossary/term/mobile_device_management

[43]. National Institute of Standards and Technology. (15 de 06 de 2021). Computer Security Resource Center. Recuperado el 13 de 12 de 2023, de csrc.nist.gov: https://csrc.nist.gov/glossary/term/multi_factor_authentication

[44]. auth0. (13 de 12 de 2023). ¿Qué es OAuth 2.0? Recuperado el 13 de 12 de 2023, de auth0.com: https://auth0.com/es/intro-to-iam/what-is-oauth-2

[45]. National Institute of Standards and Technology. (01 de 06 de 2017). NIST Special Publication 800-63C -Digital Identity Guidelines. Recuperado el 13 de 12 de 2023, de pages.nist.gov: https://pages.nist.gov/800-63-3/sp800-63c.html

[46]. Cloudflare. (13 de 12 de 2023). ¿Qué es OWASP? ¿Qué es el OWASP Top 10? Recuperado el 13 de 12 de 2023, de cloudflare.com: https://www.cloudflare.com/es-es/learning/security/threats/owasp-top-10/

[47]. National Institute of Standards and Technology. (01 de 09 de 2011). Computer Security Resource Center. Recuperado el 13 de 12 de 2023, de csrc.nist.gov: https://csrc.nist.gov/glossary/term/platform_as_a_service

[48]. Cyberark. (13 de 12 de 2023). Privileged Access Management (PAM). Recuperado el 13 de 12 de 2023, de cyberark.com/: https://www.cyberark.com/what-is/privileged-access-management/

[49]. National Institute of Standards and Technology. (01 de 09 de 2011). Computer Security Resource Center. Recuperado el 15 de 12 de 2023, de csrc.nist.gov/: https://csrc.nist.gov/glossary/term/PKI

[50]. National Institute of Standards and Technology. (01 de 09 de 2011). Computer Security Resource Center. Recuperado el 13 de 12 de 2023, de csrc.nist.gov: https://csrc.nist.gov/glossary/term/software_as_a_service

[51]. Cloudflare. (15 de 12 de 2023). What is SAML? Recuperado el 15 de 12 de 2023, de cloudflare.com: https://www.cloudflare.com/learning/access-management/what-is-saml/

[52]. Zscaler. (13 de 12 de 2023). What Is a Software-Defined Perimeter? Recuperado el 13 de 12 de 2023, de zscaler.com: https://www.zscaler.com/resources/security-terms-glossary/what-is-software-defined-perimeter

[53]. Cloudflare. (13 de 12 de 2023). What is serverless computing? Serverless definition. Recuperado el 13 de 12 de 2023, de cloudflare.com: https://www.cloudflare.com/learning/serverless/what-is-serverless/

[54]. National Institute of Standards and Technology. (01 de 08 de 2011). Computer Security Resource Center. Recuperado el 13 de 12 de 2023, de csrc.nist.gov: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf

[55]. Paloaltonetworks. (13 de 12 de 2023). What Is SOAR? Recuperado el 13 de 12 de 2023, de paloaltonetworks.com: https://www.paloaltonetworks.com/cyberpedia/what-is-soar

[56]. Gartner. (13 de 12 de 2023). Gartner Glossary - Secure Web Gateway. Recuperado el 13 de 12 de 2023, de gartner.com: https://www.gartner.com/en/information-technology/glossary/secure-web-gateway

[57]. Fortinet. (13 de 12 de 2023). What Is UEBA? Recuperado el 13 de 12 de 2023, de fortinet.com: https://www.fortinet.com/resources/cyberglossary/what-is-ueba

[58]. National Institute of Standards and Technology. (01 de 09 de 2011). Computer security resource center. Recuperado el 12 de 12 de 2023, de csrc.nist.gov: https://csrc.nist.gov/glossary/term/VPN

[59]. Cloudflare. (13 de 12 de 2023). What is a WAF? | Web Application Firewall explained. Recuperado el 13 de 12 de 2023, de Cloudflare.com: https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

[60]. checkpoint. (13 de 12 de 2023). What is Web Application & API Protection (WAAP)? Recuperado el 13 de 12 de 2023, de checkpoint.com/: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-web-application-api-protection-waap/

[61]. IBM. (13 de 12 de 2023). WS-Security. Recuperado el 13 de 12 de 2023, de ibm.com: https://www.ibm.com/docs/en/app-connect/11.0.0?topic=security-ws

[62] Vmware. (13 de 12 de 2023). ¿Qué es el ZTNA? Recuperado el 13 de 12 de 2023, de vmware.com: https://www.vmware.com/es/topics/glossary/content/zero-trust-network-access-ztna.html