Universidad de Buenos Aires

Facultades de Ciencias Económicas,
Ciencias Exactas y Naturales e Ingeniería

Carrera de Maestría en Seguridad Informática

TESIS DE MAESTRIA

Tema:

Zero Trust

"En busca de la Confianza Cero"

Autor: Esp. Lic. Carlos Quiroga

Tutor: Dr. Pedro Hecht

Diciembre 2023 - Cohorte 2020

Declaración Jurada

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.

FIRMADO

Carlos Alberto Quiroga Juncos
DNI 18.317.942

Resumen

El término “Confianza Cero” (*ZT - Zero Trust*), acuñado por la industria informática hace ya más de un decenio, resuena en el 2023 en todos los ámbitos de la Seguridad de la Información cada vez con mayor intensidad.

Abundan los recursos que se refieren al mismo provenientes de la academia, los informes y recomendaciones de las consultoras de renombre, las conferencias y los organismos tanto privados como públicos a nivel internacional, a tal punto que pareciera ser casi obligatorio el incorporar esta nueva idea al enfoque de trabajo de los profesionales del ramo.

Esta explosión de popularidad se debe a distintos factores, tales como el surgimiento de los servicios en la nube y la creciente migración de las organizaciones hacia ese modelo operativo, la pandemia mundial que lo ha potenciado y exigido, y en particular una Orden Ejecutiva del Gobierno de los EE. UU. de mayo de 2021 instando a las agencias gubernamentales de ese país a adoptar *ZT*.

Aún con todo el entusiasmo que genera este ya no tan nuevo término, es difícil establecer con exactitud su definición. Qué es, para qué sirve y cómo se aplica esta “Confianza Cero”, y si no se trata solamente de una expresión de moda (*buzzword*).

Palabras Clave:

Zero Trust, Confianza Cero, Seguridad de Redes, Ciberseguridad, Arquitectura.

Índice de Contenidos

Agradecimientos

A mi querida Madre, la Dra. Antonia Juncos Brizuela.

Introducción

Al comienzo del año 2023, el concepto de “Confianza Cero” se enfrenta a una extraña dicotomía. Por un extremo, pareciera ser el enfoque indiscutido para la ciberseguridad hacia el futuro, y por el otro, un ardid más de la disciplina del *marketing*.

Sin embargo, tan solo por su creciente resonancia, las predicciones de las consultoras de renombre tales como Gartner y Forrester, la implacable tenacidad de los fabricantes y proveedores de soluciones, las recomendaciones gubernamentales y su ya frondosa línea de tiempo repleta de eventos relevantes, *Zero Trust* es sin duda un tema que debe ser tomado en cuenta por el profesional de la Seguridad de la Información, y más aún, por aquellos que deben tomar decisiones estratégicas.

El problema que se desea abordar en este trabajo es, en primer lugar, el de encontrar una definición única para Confianza Cero si es que existe, y a partir de ella evaluar su verdadera relevancia.

En segundo lugar, intentar establecer para qué sirve exactamente este nuevo concepto y si realmente se trata de la inserción de un cambio disruptivo en una disciplina que lleva tantos años de desarrollo y sobre la que se trabaja con tamaña intensidad como frecuencia.

Por último, si todo lo que promete *ZT* es verdadero, constatar si existe una metodología bien definida para aplicar sus principios, lineamientos o prescripciones.

En la carrera de Maestría en Seguridad Informática se ha hecho hincapié en nuestra formación como tomadores de decisiones a nivel de miembros de un directorio, considerando nuestro posible rol como *CISO* de una organización.

Es por ello por lo que este trabajo está orientado a investigar qué es *ZT* desde una perspectiva estratégica.

Objetivo y Alcance

El objetivo de este trabajo es elaborar una guía clara y actualizada sobre Confianza Cero, que pueda ser de utilidad como referencia para un profesional de la Seguridad de la Información que ocupe un cargo ejecutivo en una organización.

De este objetivo principal, se desprenden los siguientes:

- **Determinar qué es Confianza Cero.**
- **Definir cuál es su utilidad.**
- **Encontrar su modo de aplicación.**

El alcance comprende una exploración de su línea de tiempo y los eventos de mayor relevancia que han forjado su evolución, intentando resolver las preguntas arriba enunciadas a partir de cada uno de esos aportes.

El enfoque de este trabajo es principalmente teórico, y no orientado a describir ni abordar soluciones propietarias, o implementaciones específicas.

Las fuentes de información consultadas serán primordialmente de libre acceso a través de la red Internet, en concordancia con la propia perspectiva agnóstica de quienes impulsan a *Zero Trust*.

La iniciativa supone un particular desafío, dado que el concepto se encuentra en constante desarrollo y replanteo. *ZT* puede abarcar tanto a un conjunto de principios, como a un marco de trabajo, una estrategia, e incluir una arquitectura, un modelo de madurez, y es posible que estas definiciones y propuestas evolucionen, incluso durante el tiempo que dure este análisis.

Estos cambios que suceden de manera constante pueden afectar a las formas en que se conciben la arquitectura de redes, la práctica de la Seguridad Informática y los controles que conforman su ámbito de cumplimiento.

1. Antecedentes

La historia del término *Zero Trust* comienza en el año 1994 a partir de una tesis de doctorado en filosofía, titulada “Formalizando a la Confianza como un Concepto Matemático” [1] cuyo autor es Stephen Paul Marsh.

En este trabajo, Marsh menciona al término solo tres veces, y dos en un mismo párrafo. Y en él propone como su nombre lo indica, un enfoque formal para discutir con claridad qué significa el concepto de confianza en el ámbito humano.

Dicha normalización podría resultar en la implementación del concepto de confianza entre dos agentes no humanos operando en el dominio de la inteligencia artificial distribuida.

El autor no estaba preocupado a la fecha de su publicación por cuestiones de seguridad informática, sino por lograr una definición precisa para la confianza en general.

Es por ello por lo que, en su formalización matemática, propone a la variable T_x como representativa de esa confianza asignándole valor cero cuando la misma es nula, y justificando los casos en que surge tal situación.

Si bien el destacado trabajo de Marsh queda como una interesante anécdota, la línea de tiempo de la Confianza Cero comienza sin duda unos diez años más tarde, cuando se forma el “Foro Jericó” (*Jericho Forum*).

Esta organización internacional basada en el Reino Unido e iniciada por David Lacey [2] se formó y tuvo como principal objetivo el definir y promover la eliminación del perímetro tradicional de las redes (*de-perimeterisation*).

De hecho, su nombre hacía alusión a la historia bíblica sobre la caída de las murallas de esta afamada ciudad palestina. Y tuvo como miembros a los *CISO* de importantes corporaciones globales tales como *Boeing*, *British Telecom* y *British Petroleum* entre otras.

El foro Jericó funcionó entre el año 2004 de su inauguración y el 2013 cuando declaró su éxito, y su trabajo fue continuado desde entonces por la organización *The Open Group* [3], la *Global Identity Foundation* [4] en lo referido a las identidades, y por la *Cloud Security Alliance* [5] en lo que atañe a los estándares para los servicios en la nube.

El aporte de este foro ha sido fundamental en el posterior desarrollo del tema que nos ocupa, la Confianza Cero, a través de numerosas publicaciones clave y de posicionamiento (*positioning papers*).

El primero y más importante de sus objetos de análisis fue sin duda la eliminación del perímetro, a partir del cual se originó su formación. Sus miembros fundadores consideraban que este tema no estaba siendo discutido adecuadamente en ese momento.

En el año 2005 publicaron su informe de visión estratégica (*Visioning White Paper*) titulado “Qué es el Foro Jericó” [6]. En él se describen su visión, misión, la estructura organizacional, una hoja de ruta y en particular, lo que ellos llaman la transición hacia el nuevo mundo sin un perímetro bien definido.

Se invita al lector interesado a revisar esa primera publicación, en donde se proponen conceptos considerablemente adelantados a su época, y producto de la creciente popularidad de las conexiones remotas, la cooperación entre empresas, y sin duda los servicios en la nube.

Su siguiente documento de posicionamiento, y quizás el más conocido fue el denominado “Mandamientos del Foro Jericó” (*Jericho Forum Commandments*) del año 2007 [7].

En este breve documento blanco de solo dos carillas, el equipo Jericó expuso las premisas fundamentales que ellos consideraban necesarias para abordar un futuro sin perímetro, prediciendo además que ello se haría realidad dentro de la vida corporativa de todos los interesados.

Estos mandamientos se organizaron en cinco áreas de la seguridad informática, y destinados a ser utilizados como punto de referencia para soluciones, estándares y propuestas arquitectónicas.

La primera de ellas denominada “Fundamentos” (*Fundamentals*) establecía que tanto el alcance como el nivel de protección sobre un activo, se debía adecuar al nivel de riesgo inherente al mismo. Que los sistemas de seguridad debían ser simples, escalables y fáciles de administrar. Y que una solución aplicada en un ambiente tal vez no era transferible a otro.

Como segundo principio llamado “Sobrevivir en un Mundo Hostil” (*Surviving in a Hostile World*), recomendaron que los dispositivos y las aplicaciones debían comunicarse utilizando protocolos seguros y de código abierto, manteniendo su política de protección en cualquier tipo de red, interna o externa.

El tercer punto es uno de los que más nos interesa, siendo su título “La Necesidad de Confianza” (*The Need for Trust*). Hay que recordar que el tema de nuestro debate es la no confianza, lo que discutiremos en detalle más adelante.

Aquí lo que se argumentaba era la necesidad de modelos explícitos y transparentes de confianza (*Trust Models*) entre personas, procesos y tecnologías. Y ya se hablaba de autentificación mutua (*Mutual Authentication*).

Como cuarta área de interés se presentaba la administración de identidades, recomendando la modalidad federada, incluyendo otra vez a la confianza, entre organizaciones distintas.

En último lugar también se proponía la administración correcta del acceso a datos, incluyendo el soporte para el cifrado tanto en reposo como tránsito, la separación de responsabilidades y la protección en base a su riesgo y criticidad.

Sin duda estas dos primeras publicaciones del foro Jericó relacionadas con su iniciativa original, el discutir un nuevo tipo de enfoque acerca del perímetro, han sido el basamento fundacional para todo lo que veremos en los capítulos siguientes.

El tema que abordaron a continuación, una vez definido el problema objeto de análisis, fue una arquitectura para la colaboración segura.

Como parte de sus propuestas, elaboraron los conceptos de "Formaciones en la Nube" (*Cloud Formations*) y el "Modelo de Cubo para la Nube" (*Cloud Cube Model*), presentándolos en otro documento de posicionamiento así titulado [8].

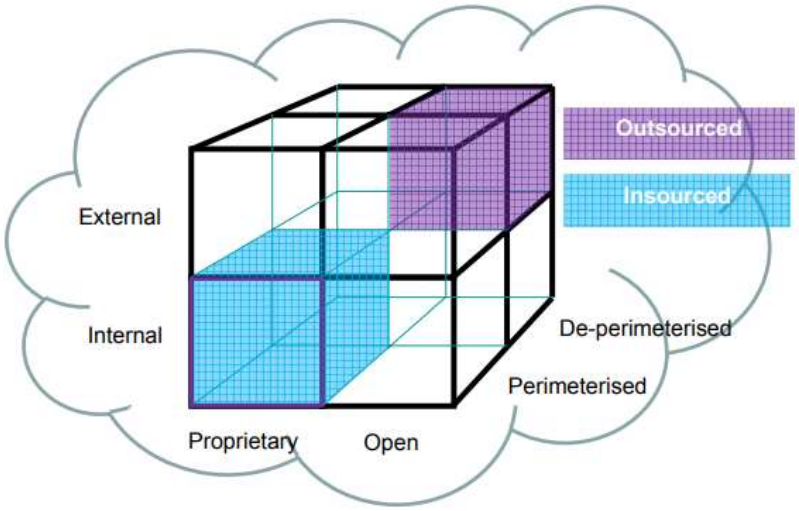


Figura 1 – El "Modelo de Cubo para la Nube".

Este modelo presenta tres dimensiones como se ve en la figura, donde la vertical corresponde a la ubicación externa o interna de los recursos, la horizontal separa los sistemas propios de los de código abierto y la de fondo, la disposición de activos dentro y fuera del perímetro.

Usando este cubo como herramienta gráfica, el documento hace notar que los "Mandamientos" y la arquitectura propuestos por Jericó en conjunto, ayudarían a atravesar la dimensión frontal - el perímetro - hacia la dimensión posterior de forma segura.

Entre 2006 y 2009 desarrollaron una serie de 23 publicaciones con requisitos para esta arquitectura de colaboración segura en la nube y sin un perímetro bien definido.

El resultado de toda esa tarea previa es hoy el marco de trabajo mantenido por *The Open Group* conocido como *O-SCOA* (*Framework for Secure Collaboration-Oriented Architectures*), publicado en 2012 [9].

Asimismo, mucho de este material fue utilizado más tarde por la *Cloud Security Alliance* en su guía para la seguridad en la nube, hoy ya en su cuarta versión [10].

El tercero de los principales temas de trabajo de este foro que sin duda produjo una considerable cantidad de documentos altamente relevantes para su época, fue la administración de identidades y accesos.

Así es como en 2011 hicieron públicos los "Mandamientos para Identidades" (*Identity Commandments*), también expuestos dentro de cinco áreas, pero agregando un importante glosario de términos al final.

Estos mandamientos describían principalmente la transición desde un enfoque tradicional basado en permisos otorgados por cada sistema y aplicación, hacia uno centrado en tipos de usuario y recurso. Sin duda, requiriendo una importante inversión en infraestructura.

No vamos a detenernos mucho en su detalle, o el de las otras importantes contribuciones del equipo Jericó.

Sin embargo, conviene notar que, en esta en particular, se habla de distintos niveles de confianza atribuidos a cada tipo de entidad, y se la define como la dependencia de ellas en el resultado de cada transacción.

Los esfuerzos de Jericó en el ámbito de la administración de identidades y accesos son hoy continuados, como ya mencionamos, por la fundación sin fines de lucro *Global Identity Foundation*. En su sitio, se puede ver la referencia a los mandamientos al principio de la lista de sus referencias de respaldo.

En el año 2007 el Departamento de Defensa de los Estados Unidos y la agencia gubernamental de ese país *DISA* (*Defense Information Systems Agency*) publicaron conjuntamente un informe titulado "Visión Arquitectónica del Sistema Global de Información" (*Global Information Grid Architectural Vision*) [11].

Esta es la segunda fuente importante reconocida como precursora del concepto de Confianza Cero, junto con el trabajo del foro Jericó.

Tampoco haremos aquí un análisis detallado de este documento que ha quedado ya desactualizado. Además, dedicaremos una sección posterior a la nueva propuesta arquitectónica de estos organismos.

Sin embargo, en esta publicación, se presentó la visión conceptual deseada para el futuro de la "Red de Información Global" (*GIG – Global Information Grid*) para la defensa, esquematizada en la siguiente figura.

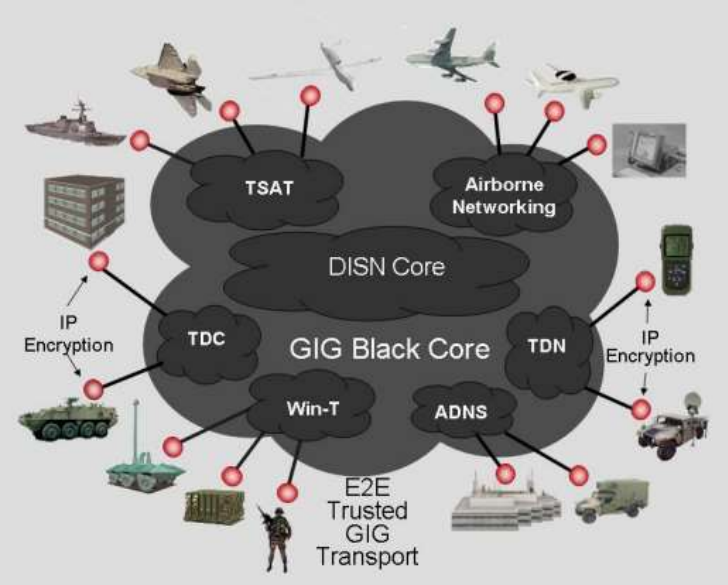


Figura 2 – El "Núcleo Negro".

En su parte interior se puede notar lo que denominaron el "Núcleo Negro" (*Black Core*), en donde todo el tráfico de datos es cifrado de extremo a extremo (*E2E – End to End*).

Finalizamos así esta breve introducción sobre los antecedentes considerados como de mayor relevancia no solo por quien escribe, sino también por la propia organización *NIST* en las referencias que cita para su estándar de arquitectura, del cual nos ocuparemos en detalle en la sección correspondiente.

Si a esta altura se quisiera visualizar una línea de tiempo tentativa para la historia de *Zero Trust*, la siguiente figura sería una opción plausible.

Figura 3 – Una línea de tiempo tentativa para *Zero Trust*.

Nos encontramos en el primer círculo izquierdo, y lo que viene a continuación es sin duda apasionante.

Esta línea de tiempo fue presentada por Daniele Catteddu, *CTO* de la *Cloud Security Alliance*, en su disertación de marzo de 2022 [12].

Pero como veremos en las secciones que siguen, muchos eventos de considerable importancia e impacto sobre la noción y el status de la Confianza Cero han sucedido después del último círculo.

2. Nace la Confianza Cero

El término *Zero Trust* logra su inserción formal en el ámbito de la Seguridad de la Información, a través de una serie de informes de la consultora *Forrester* publicados a partir de septiembre de 2010.

Es así como se adueña del concepto, definiéndolo inicialmente como el "Modelo *Forrester* de Confianza Cero" y su autor, John Kindervag queda asociado ya para siempre como su referente absoluto.

La serie de informes está compuesta por tres entregas, una inicial presentando el basamento conceptual, otra referida a cuestiones de arquitectura y, por último, un conjunto de casos de estudio.

Cabe señalar que estos informes han estado desde su inicio, sujetos a la privacidad definida por el sistema de suscripción que utilizan las consultoras de este tipo, en donde solo podían acceder a ellos sus clientes pagos, es decir, proveedores de soluciones de hardware y software, y grandes empresas capaces de sostener la membresía.

Hoy en día es posible encontrarlos en ciertos sitios relacionados que ofrecen copias, y tanto la propia consultora *Forrester* como el autor mencionado más arriba han comentado sobre el efecto que esta falta de difusión ha tenido en la evolución de *ZT* a través del tiempo.

A continuación, haremos primero una revisión de estos informes que han sido sin duda alguna de fundamental relevancia en el planteo inicial del concepto, iniciando la era de su difusión oficial.

Más adelante, veremos también las primeras propuestas concretas para materializar sus ideas, incluyendo también un primer intento de establecer un marco de trabajo para la Confianza Cero.

2.1 No más “Rellenos Blandos”

La primera de las tres entregas mencionadas lleva como título *No More Chewy Centers: Introducing The Zero Trust Model Of Information Security*, y se trata de la presentación del modelo propuesto por *Forrester* [13] a través de un esquema conceptual.

Su curioso título se basa en el hecho de que, durante mucho tiempo, la comunidad de profesionales de SI ha mantenido la idea de sostener una caparazón dura en el perímetro difícil de penetrar, dejando que los controles sean más permisivos en el centro o relleno.

En este esquema, el autor comienza presentando dos casos de fallas en la seguridad de la información, uno relacionado con espías soviéticos camuflados durante años en diferentes funciones de diversas empresas con el fin de obtener información sobre importantes miembros del gobierno norteamericano y otro conocido como el “problema de Phillip Cummings”.

Este segundo ejemplo trata sobre un empleado de la empresa *TeleData Communications Inc*. el cual permitió el ingreso a la red de una organización criminal nigeriana, proveyéndoles datos sobre informes crediticios de sus clientes y dejando todo preparado para que sigan conectados a la misma incluso luego de su salida, durante un largo tiempo.

Para el caso Cummings amén del indudable y enorme costo financiero resultante, y el hecho de que la situación fue descubierta por una empresa cliente de *TCI*, el autor propone aquí la nueva problemática relacionada con el hecho de que la confianza ha sido vulnerada.

Kindervag señala que, a pesar de los cuantiosos controles existentes diseñados para proteger a las redes, lo que incluye además numerosos dispositivos tales como IPS, WAF, VPN y otros, los ataques en 2010 siguen creciendo y son cada vez más sofisticados.

El autor plantea cuatro trampas (*pitfalls*) que afectan al enfoque de ese momento aplicado a la seguridad de las redes.

La primera, mencionando el hecho de que se acostumbra a etiquetar a ciertas interfaces de los dispositivos de red como “confiables” (*trusted*), y esto es un error, dado que puede haber actores “no confiables” (*untrusted*) en la red interna.

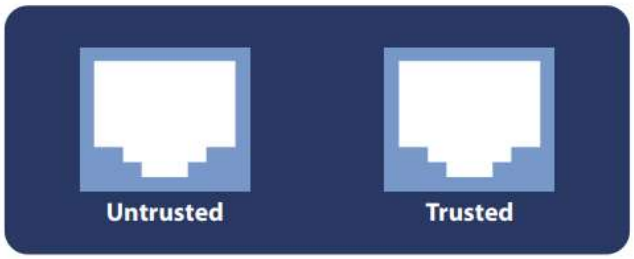


Figura 4 – Interfaces confiables y no confiables en los dispositivos de red.

La segunda, estableciendo que la famosa frase de origen ruso “confiar, pero verificar” (*trust but verify*) es en nuestro ámbito una broma, dado que en la mayoría de los casos se confía, y en pocos de ellos se verifica.

Una tercera y relacionada a la anterior advierte que, en la red “confiable” es donde suelen situarse los atacantes con fines maléficos.

Por último, la cuarta trampa expone que no existe la confianza como un concepto aplicable a los paquetes de red, y que no debemos antropomorfizar al mismo. No se debe confiar en los paquetes, y esto es un problema ontológico que los profesionales deben considerar.

Planteadas así las cuatro trampas, Forrester propone entonces un nuevo modelo de seguridad en el cual no se confíe en los paquetes, y no existan segmentos confiables de la red.

Este nuevo modelo consta de cuatro conceptos, el primero relacionado con la necesidad de proteger los activos en cualquier conexión, sin importar su origen. Esto requiere de aplicar túneles cifrados en todos los casos, autorizando y revisando cada una de ellas, asumiendo siempre que dichas conexiones pueden ser ataques malintencionados.

Un segundo concepto introduce al control de accesos y el mínimo nivel de privilegios como premisas requeridas. Una solución que no sería la única propuesta es la metodología de accesos según roles (*RBAC - Role-Based Access Control*) pudiendo aplicarse nuevas tecnologías en función de su futura aparición.

Asegurarse de que los actores acceden a la red y sus recursos con los mínimos privilegios necesarios, y con su identidad verificada, impide la natural tendencia a moverse lateralmente incluso por mera curiosidad.

El tercer postulado sostiene que, más allá de la verificación de acceso, el modelo exige que se inspeccione qué es lo que el actor está haciendo una vez conectado.

2.2 Seguridad en la Red desde su ADN

La segunda entrega de esta serie de informes [14] está dedicada a proponer un nuevo patrón de arquitectura para las redes, considerando lo planteado en la entrega anterior, en donde se había establecido el problema de la existencia de actores malintencionados operando desde adentro, y el hecho de que no se puede confiar en los paquetes de red.

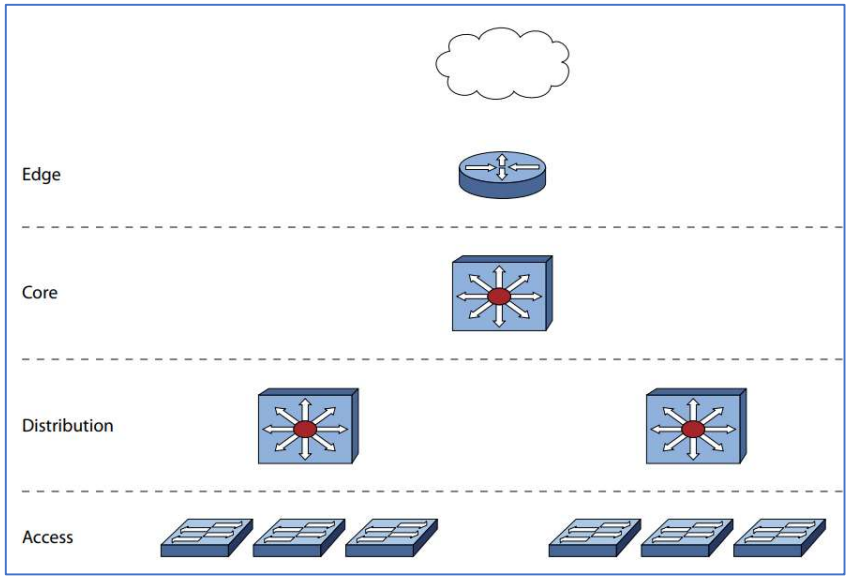


Figura 5 – El diseño tradicional de la red, jerárquico.

Aquí se señala que es necesario repensar el diseño tradicional de las redes, ejemplificado básicamente en la figura.

En este diseño se nota que el énfasis está puesto en habilitar las conexiones desde afuera hacia adentro, comenzando por el ingreso sobre el "borde" (*Edge*), haciendo pasar todo el flujo de datos por el dispositivo principal (*Core*), y desde allí hacia los puntos de distribución (*Distribution*), permitiendo finalmente que cualquier actor "confiable" se conecte utilizando alguno de los puntos de acceso (*Access*).

Una vez concretado el diseño, puesto en funcionamiento y no antes, es cuando se consideran los requerimientos de seguridad.

Y esto ocasiona que se agreguen un sinnúmero de dispositivos de control en forma de capa que cubre al sistema de forma desordenada, y que no termina de solucionar los problemas.

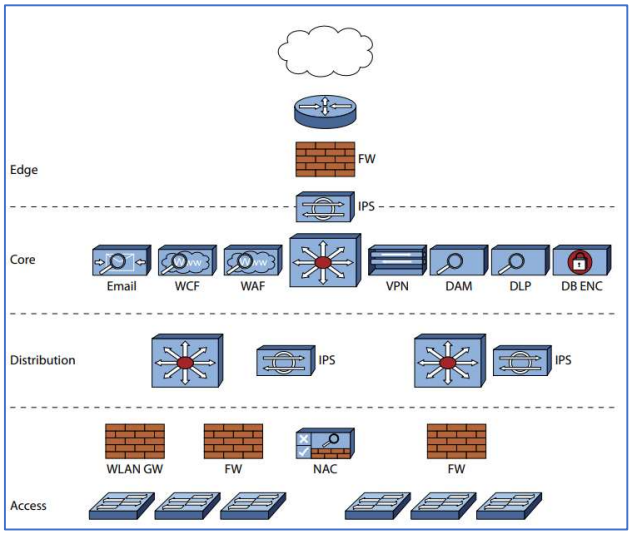


Figura 6 – La capa de seguridad con sus dispositivos.

Nótese en la figura que gran parte de estos dispositivos de control, están ubicados sobre la conexión principal (*Core*) al ingreso y egreso general de todos los datos. Es aquí donde se toman muchas decisiones que refuerzan las políticas de seguridad y cumplimiento.

Se propone entonces una nueva arquitectura, en donde estas decisiones sean efectuadas desde el sector interno de la red en forma centralizada, y que incluya el procesamiento en paralelo de los paquetes, y la segmentación para proteger distintos niveles de criticidad de los recursos que se deban acceder.

Aquí las nuevas tecnologías tales como el acceso a Internet, las redes sociales y la computación en la nube, cambian la disposición del perímetro.

2.2.1 Características del Nuevo Diseño

El nuevo diseño de red propuesto incluye tres conceptos, que cambian de forma fundamental la visión jerárquica tradicional.

El primero de ellos refiere a la segmentación de la red, indicando que ya no se pueden seguir utilizando entretejidos de conmutación (*switch fabrics*) como conductos de bus comunes (*backplanes*) para todo el tráfico.

En referencia a esta segmentación, se enfatiza que la división de la red en forma virtual (*VLAN*) no supone una solución segura y se la equipara a dibujar líneas amarillas en el pavimento, lo que no impide que los vehículos las crucen.

En reemplazo del flujo unificado de los datos desde y hacia el exterior, se plantea la necesidad de reemplazarlo por un sistema de procesamiento de las conexiones en paralelo (*parallelization*).

Esto implica el descartar al *switch* núcleo (*Core*), y usar en cambio múltiples *switches* más económicos y manejables, donde cada uno administre su propio segmento de red. Este segundo concepto, es tomado de la idea de los multiprocesadores ya presentes en los ordenadores de escritorio.

La nueva arquitectura debe, además, poder ser administrada efectivamente en forma centralizada. Y esta centralización debe lograrse a través de una solución específica, logrando que se transforme en el nuevo conducto unificado (*backplane*) de la plataforma.

Utilizando estos tres conceptos, se logra un nuevo enfoque para la construcción de redes que permite soportar en forma segura a las nuevas tecnologías, en donde el perímetro ya no está tan bien definido.

Se trata de pensar en la seguridad al inicio y no por encima de la estructura existente, tomando como premisa el considerar a la confianza como base para el diseño.

2.2.2 Componentes

Es importante tomar en cuenta que lo que se detalla a continuación, corresponde a la aplicación teórica del "Modelo de Confianza Cero" expuesto en el primer documento de esta serie.

A la fecha de estas recomendaciones, el mismo autor señalaba que todavía no existían los dispositivos para cubrir tales expectativas, y entonces las mismas debían ser tomadas en cuenta para la evaluación de futuras ofertas de los proveedores.

Forrester visualiza entonces la creación de un nuevo componente al que llama "puerta de enlace de segmentación" (*SG - Segmentation Gateway*).

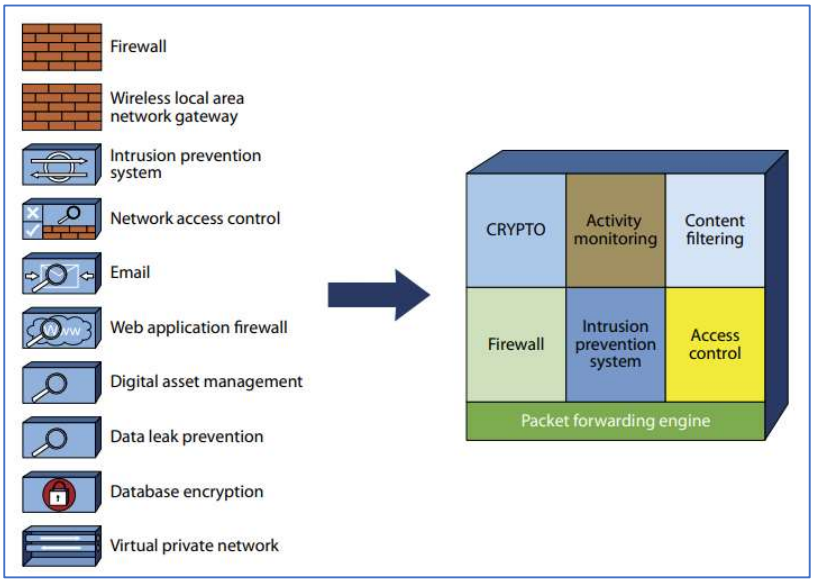


Figura 7 – Puerta de Enlace de Segmentación.

En este nuevo tipo de dispositivo, se combinarían todas las funcionalidades de los elementos habituales que se muestran a la izquierda de la figura, configurando así un motor central de enrutamiento de paquetes (*Packet forwarding engine*).

Ahora desde este dispositivo central y unificado, que va a contar con múltiples interfases de red de alta velocidad y gran poder de procesamiento, se originan los distintos segmentos de red aislados que cuentan cada uno con su micronúcleo (*microcore*) y su respectivo perímetro. A esta combinación la consultora le asigna el acrónimo *MCAP* (*Micro Core and Perimeter*).

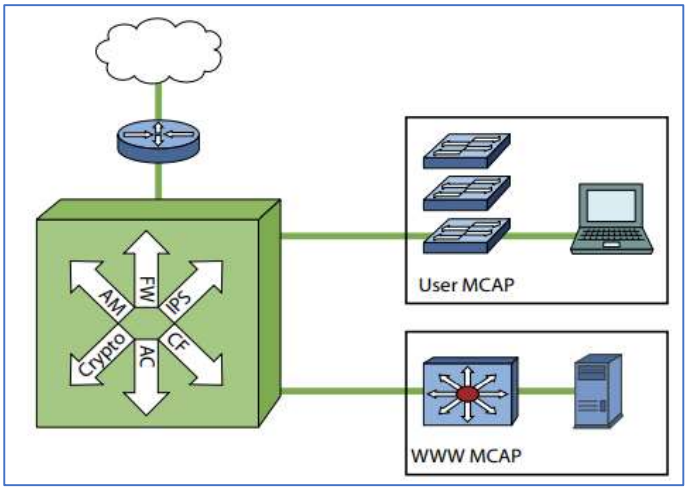


Figura 5 – Micronúcleos y sus perímetros (*MCAP*).

En la figura superior, puede notarse que desde la *SG* se generan dos micro segmentos, uno para la zona de los usuarios, y otro como ejemplo para un servidor de Internet. Cada uno de ellos cuenta con una funcionalidad general para todo su micro perímetro y políticas separadas de seguridad y cumplimiento.

La administración centralizada, que ya no puede consistir en un acceso del tipo consola de comandos, se realiza por sobre la *SG* mediante algún sistema de software integral del cual a la fecha del informe ya existían algunas ofertas de los proveedores.

Una tercera idea para este nuevo diseño que complementa a la *SG* y a los *MCAP*, es la creación de una red de adquisición de datos (*DAN - Data Acquisition Network*), mediante la cual se realice la inspección constante de todo el tráfico.

En la siguiente figura, pueden observarse el servidor de administración centralizada (*MGMT Server*) así como la red *DAN* que opera dentro de su propio *MCAP*.

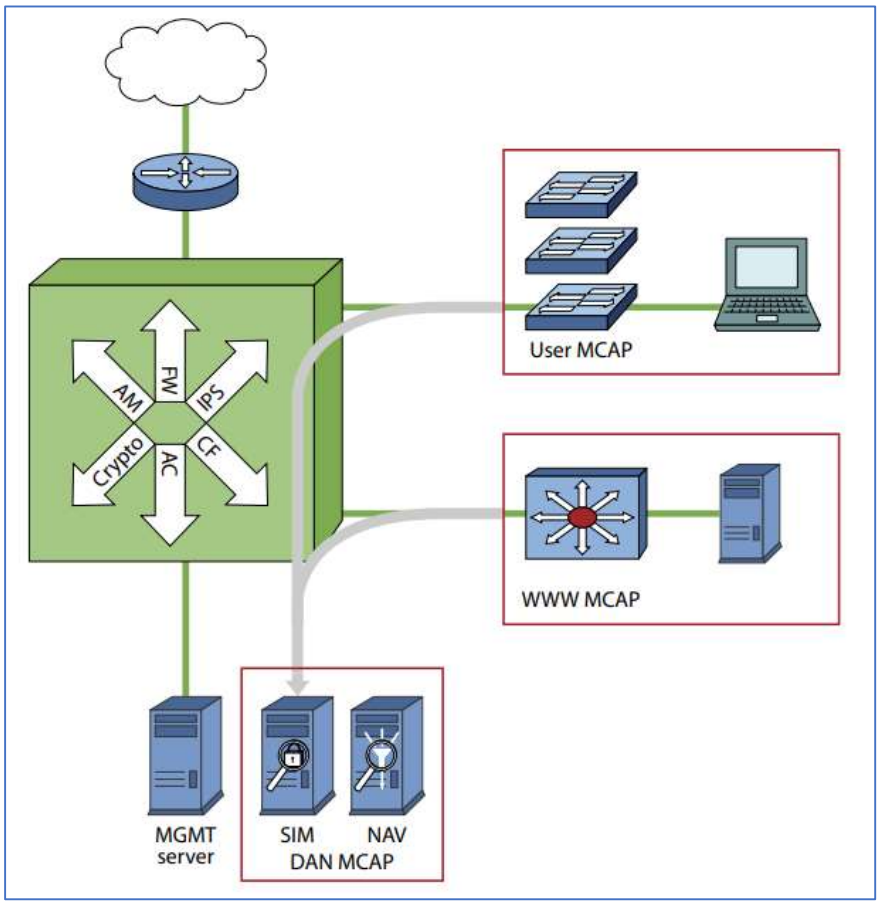


Figura 6 – Servidor de Administración Centralizada y *DAN*.

En este contexto, el servidor de administración se comunica a través del *SG* y mediante una interfaz simplificada y gráfica, con todos los segmentos.

A su vez, la red de adquisición de datos *DAN* controla de forma activa y pasiva el flujo de cada conjunto de datos que circula en los distintos *MCAP*. Esto hace mucho más eficiente la captura de esos datos, cuya dificultad es bien conocida por aquellos a cargo de asegurar las redes.

2.2.3 Beneficios de la Red *ZT*

La arquitectura propuesta que al momento de su exposición es en cierta medida teórica y basada en el modelo de *ZT* de *Forrester*, puede ser llamada de aquí en más la "Red de Confianza Cero" (*Zero Trust Network*). Esta nueva red incluye los siguientes beneficios:

- **Es agnóstica:** No está comprometida con ningún tipo de plataforma, y cada *MCAP* puede contener los dispositivos que sean necesarios, los cuales procesarán un tipo específico de tráfico. En nuestro ejemplo, el *MCAP* que engloba al servidor de Internet, podría estar restringido al protocolo *HTTPS*.
- **Reduce el costo de cumplimiento:** Tomando como ejemplo el caso del conocido marco de trabajo *PCI* [14a] para las tarjetas de crédito, mantener segmentada la red por donde circula ese tipo de información será sin duda más seguro, fácil de implementar y de auditar.
- **Hace que la virtualización sea más segura:** Recomendando el mantener las máquinas virtuales dentro de su propio *MCAP*, incluso si es necesario trasladarlas de un servidor a otro, operación muy frecuente en esta tecnología.
- **Facilita el cumplimiento:** Como se puede ver en la figura de página siguiente, la red inalámbrica también está segmentada y no puede llegar a los otros *MCAP* porque en el medio se encuentra el SG.
- **Es extensible:** Al establecer un diseño modular en donde en cada *MCAP* se administra qué dispositivos forman parte de este, se pueden agregar más *switches* en el caso de un mayor volumen del tráfico, sin tener que hacer grandes inversiones en lo que antes era el núcleo (*core*) de la red.

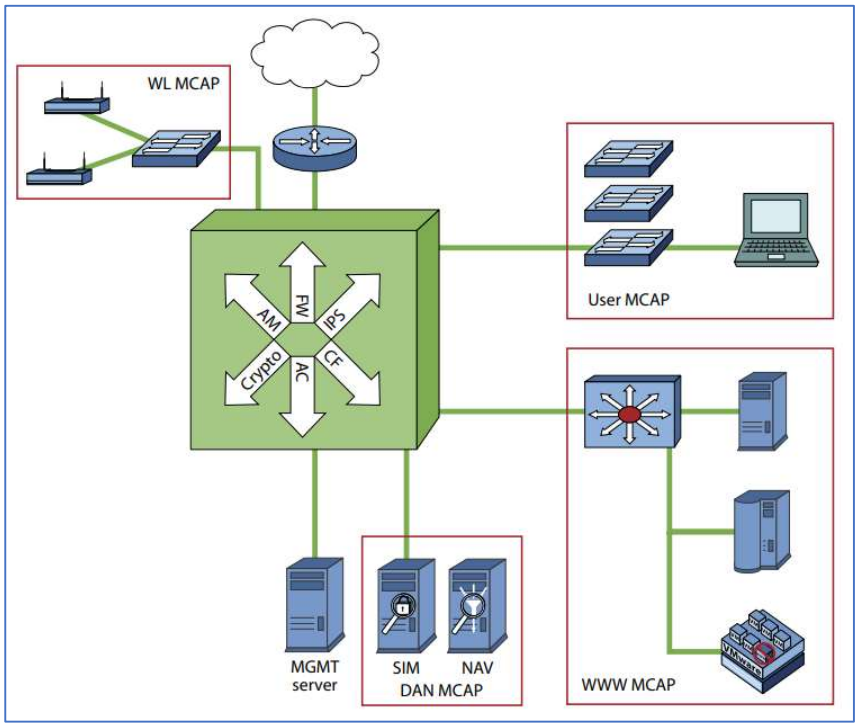


Figura 7 – La red inalámbrica WL segmentada.

- **Favorece los servicios en la nube**: La segmentación propuesta por este modelo es clave para establecer ambientes para múltiples clientes (*multitenant*) aislados entre sí.
- **Descentraliza el balanceo de carga:** Ya que este tipo de dispositivos puede ser ubicado al ingreso de cada *MCAP*.
- **Auspicia nuevas opciones:** Dado que los segmentos no están limitados a la funcionalidad del *SG*, y en cada uno de ellos se pueden agregar nuevos dispositivos que el mercado ofrezca en el futuro.

Un último ítem de esta lista de beneficios merece ser tomado en cuenta de manera especial, y corresponde al hecho de que una red *Zero Trust* puede ser incorporada como anexo a una red tradicional existente.

De esta forma, se lograría incursionar en este nuevo enfoque de trabajo progresivamente, reemplazando la jerarquía existente empezando por los servicios que permitan hacerlo.

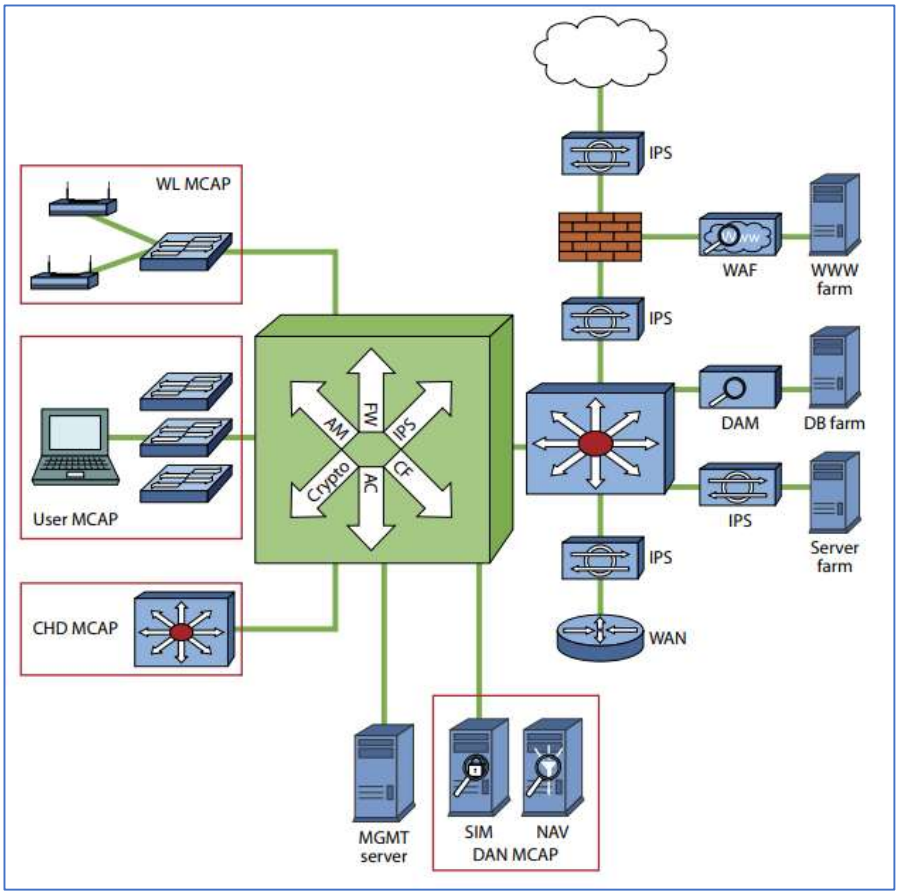


Figura 8 – Agregar *Zero Trust* a una red tradicional existente.

La red *Zero Trust* que propone Forrester es la respuesta a una serie de nuevos desafíos que aparecen de forma casi concurrente alrededor del año 2010.

Entre ellos, se hace referencia a la necesidad de adaptar las redes a mayores velocidades desde los originales 10Mb hacia 10Gb, la Web 2.0 y la aparición de las comunicaciones unificadas incluyendo audio, video y otros servicios que empujan aún más los requerimientos de ancho de banda.

Por su parte la necesidad cada vez mayor de virtualizar recursos, y de moverlos a través de estas redes, también tiene su efecto en la exigencia para aplicar un nuevo enfoque que sustituya al diseño tradicional.

Uno de los problemas que también deben abordarse es la aparición de servicios de red convergente, en donde desde un solo proveedor se logra conectar a la organización con múltiples servicios, y estos pueden transformase en una verdadera caja negra donde sea muy difícil controlar y mantener la postura de seguridad de la organización.

2.3 El Perímetro Definido por Software

En el año 2014 la organización denominada “Alianza para la Seguridad en la Nube” (*CSA - Cloud Security Alliance*) publicó la versión 1.0 de su protocolo *SDP* (*Software Defined Perimeter*). [15].

La propuesta presentada así por la *CSA* pasa a ser entonces una primera formalización de lo concebido por *Forrester*, y se la considera otro hito importante dentro de la historia general del desarrollo de *ZT*.

La idea general que sustentaba a *SDP* no era nueva al momento de su publicación, y se basaba en lo que ya venían haciendo las agencias gubernamentales de los Estados Unidos tales como el Departamento de Defensa, en donde cualquier actor para acceder a un recurso de información clasificado debía primero pasar por un dispositivo tipo “puerta de enlace” que lo autentificaba y autorizaba. El recurso se encontraba siempre escondido detrás del mismo.

El objetivo de este protocolo es el de proporcionar un perímetro lógico alrededor de cualquier recurso, reemplazando a los dispositivos físicos de protección ya utilizados - por estas agencias, por ejemplo - y permitiendo protegerlo de forma dinámica en el contexto de redes no seguras.

SDP es una de las primeras iniciativas concretas orientadas a redefinir el perímetro fijo tradicional de las organizaciones, reemplazando en cierta medida a las ya conocidas redes privadas virtuales (*VPN - Virtual Private Networks*) como se verá más adelante.

Tomando como base al patrón de la RFC 4301 titulada “Arquitectura de Seguridad para IP” [16], su documento promete proveer bajo demanda redes aisladas (*air-gapped*) de las demás inseguras.

2.3.1 Arquitectura

El funcionamiento del perímetro definido por software incluye a tres actores principales que son, en primer lugar, los equipos “iniciadores” o clientes de las conexiones (*IH - Initiating SDP Host*), los que “aceptan” dichos pedidos o servidores (*AH - Accepting SDP Host*), y los controladores (*SDP Controller*) quienes deciden si estas conexiones pueden establecerse o no.

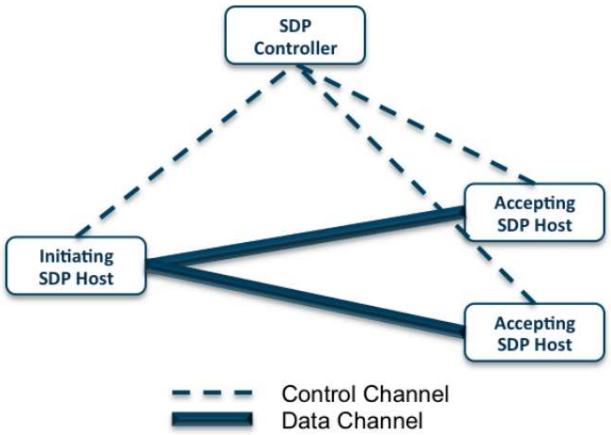


Figura 9 – Arquitectura del protocolo *SDP*.

La comunicación entre clientes y servidores sucede a través de un canal denominado “de datos” (*Data Channel*), separado del que se utiliza entre cualquiera de ellos y el controlador al cual se lo llama “canal de control” (*Control Channel*) y es separado. Este sistema permite su fácil expansión y la inserción de elementos redundantes para mantener la disponibilidad.

Los servidores *AH* no aceptan ninguna conexión salvo desde los controladores, y desde un cliente *IH* autorizado por ellos. Cuando un *IH* se conecta a un controlador, le solicita la lista de los *AH* disponibles. Para obtenerla, deberá presentar sus credenciales, y posiblemente el estado de su software y hardware.

2.3.2 Flujo de Trabajo

Al comienzo (1 en la figura), uno o más controladores se inicializan, conectándose primero a servicios tercerizados de autorización y autentificación [17], tales como *SAML*, *OpenID*, *OAuth*, *LDAP*, *Kerberos*, y otros. Esto también puede incluir a autoridades certificantes de *PKI* [18] y la autentificación multifactorial *MFA* [19].

En el segundo paso (2), los *AH* establecen comunicación con el o los controladores, pero sin permitir todavía ninguna conexión entrante.

En tercer lugar (3), los *IH* se conectan a los controladores, autentificándose. En el paso cuarto (4), los controladores establecen a qué *AH* se puede conectar cada uno de los iniciadores.

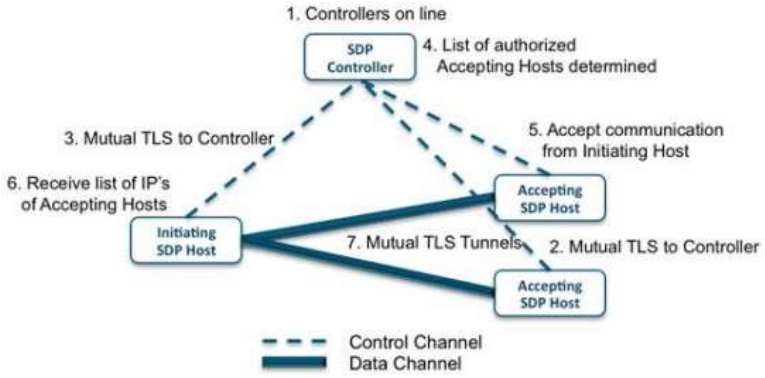


Figura 10 – Flujo de trabajo del protocolo SDP.

Ya en el quinto paso (5), los controladores indican a los *AH* que permitan las conexiones entrantes desde los *IH* junto con cualquier instrucción adicional relacionada con el cifrado de la comunicación. Y en el sexto (6), envían similares instrucciones a los *IH* en cuanto a qué *AH* pueden contactar y con qué parámetros.

En el último paso (7) de este flujo de trabajo (*workflow)*, el cliente *IH* se autentifica frente al servidor *AH* utilizando un paquete único de autorización (*SPA - Single Packet Authorization*) [20] y luego estableciendo una conexión del tipo *TLS* mutuo (*mTLS*) [21] o vía *IPSec* [22].

2.3.3 Tipos de Implementación

Existen diferentes formas de implementar *SDP*, aun cuando el flujo de trabajo es en general siempre el mismo. El documento publicado por la *CSA* expone cuatro de ellas.

En la variante "cliente a puerta de enlace" (*Client-to-Gateway*), se protege a varios servidores detrás de un *AH*. Esta opción puede ser aplicada tanto en instalaciones propias de la organización o en Internet, ayudando a mitigar el movimiento lateral y numerosos tipos de ataques bien conocidos, tales como el aprovechamiento de vulnerabilidades, ataques de intermediario [23], denegación de servicios [24], inyección *SQL* [25], secuencias de comandos entre sitios [26] y otros.

Una segunda opción similar a la anterior es la denominada "cliente a servidor" (*Client-to-Server*), donde el software de *AH* se ejecuta directamente en el sistema a proteger, eliminando la necesidad de una puerta de enlace.

La tercera variante "servidor a servidor" (*Server-to-Server*) se aplica a los servicios presentados como interfaz de programación de aplicaciones (*API – Application Programming Interface*) entre servidores en Internet, tales como *REST*, *SOAP* o *RPC* [27]. Ella también permite la mitigación de ataques en este contexto especial de comunicaciones automatizadas.

Como última propuesta, se presenta la llamada "cliente a servidor a cliente" (*Client-to-Server-to-Client*), aplicable a los casos de comunicaciones punto a punto (*peer-to-peer*) [28] tales como telefonía de voz sobre *IP*, *chat* y videoconferencias. En este caso, lo que se protege es las direcciones *IP* de cada cliente.

2.3.4 Aplicaciones

Es interesante observar cómo el protocolo *SDP* ya menciona en su primera versión (2014), a la mayoría de las modalidades de servicio que al corriente (2023) más nos preocupan. Y esto es razonable, considerando que proviene de la organización *CSA*.

Cabe mencionar que ya se ha publicado una segunda versión [29] en 2022, la cual incluye ahora seis ejemplos de modalidades de implementación, incluyendo adiciones, aclaraciones y extensiones, vinculando expresamente al mismo con *Zero Trust*.

Este protocolo puede utilizarse en instalaciones propias, para prevenir el movimiento lateral de aquellos atacantes que logren ingresar desde el exterior.

También es aplicable a los servicios en la nube [30] tanto privados (*Private Cloud*) como híbridos (*Hybrid Cloud*). Tratándose de un protocolo ejecutado a través de software, provee una capa superior de fácil implementación en cualquiera de estas modalidades.

Para las tres variantes de servicios de nube pública (*Public Cloud*), el protocolo presenta utilidad. En el caso del “software como servicio” (*SaaS - Software as a Service*), el proveedor puede utilizarlo para su propia protección.

En los casos de “infraestructura como servicio” (*IaaS - Infrastructure as a Service*) y “plataforma como servicio” (*PaaS - Plataform as a Service*), los proveedores pueden agregar a *SDP* como una mejora en la seguridad para sus clientes.

El documento incluye también a las tecnologías de interfaz virtual de escritorio (*VDI - Virtual Desktop Interface*) [31] y a los dispositivos de “internet de las cosas” (*IoT - Internet of Things*) [32]. Estos servicios también pueden beneficiarse de la protección y la ofuscación ofrecidas por *SDP*.

2.3.5 *SDP* y las *VPN*

Al principio de esta sección sobre *SDP* se mencionó que una característica de importancia acerca de este protocolo es su propuesta concreta para reemplazar al modelo tradicional de perímetro fijo extendido a través de redes privadas virtuales.

Si bien *SDP* puede utilizar *TLS* mutuo (*mTLS*) o los protocolos *IKE/IPsec* propios de las *VPN* para establecer túneles seguros entre los clientes (*IH*) y los servidores (*AH*), el perímetro definido por software se diferencia de ellas.

En primer lugar, porque el esfuerzo requerido para proteger recursos a través de *SDP* es menor. Una vez que un controlador entra en servicio, se pueden proteger tantos servidores como se desee, y la autentificación de los clientes ocurre a través de asociaciones *LDAP* [33].

En segundo, la obvia diferencia de costo que existe entre la instalación de equipos que operen como puertas de enlace de *VPN*, comparado con *SDP* que es una solución completamente basada en *software*.

Una sutil y tercera disimilitud consiste en que las puertas de enlace de *VPN* no se pueden utilizar al mismo tiempo para seguridad y acceso remoto. El cliente debe conectarse a la puerta de enlace para uno u otro fin, pero no para los dos. *SDP* por su parte, como puede implementarse sobre una *VPN* de acceso remoto, permite las dos alternativas.

Por último, SDP protege contra ataques de denegación de servicio, ya que los servidores (*AH*) pueden situarse topológicamente en una ubicación diferente de los recursos que se están protegiendo. Esta característica es la que logra la ofuscación, es decir, esconder la verdadera ubicación de ese recurso.

2.4 *BeyondCorp* de Google

A raíz de un ataque persistente perpetrado en 2009 por una organización vinculada al gobierno chino sobre sus instalaciones conocido como “Aurora” [34], la empresa Google comenzó una iniciativa dedicada a replantear su arquitectura de seguridad.

En el año 2014 publica el primero de una serie de seis artículos en donde se describen el concepto y la implementación en sus propias redes de lo que ellos denominaron un “nuevo enfoque para la seguridad empresarial”, y al que nombraron *BeyondCorp*.

Si bien podemos considerar a *BeyondCorp* como una de las primeras implementaciones reales de las recomendaciones de *Zero Trust*, curiosamente ninguno de los *papers* originales citados más arriba menciona el término.

Sin embargo, a fecha de hoy, tanto en el sitio oficial de Google [35] como en el que dedica a este tema la empresa Okta utilizando el dominio del mismo nombre [36], se define a *BeyondCorp* como una implementación exitosa de Confianza Cero.

La esencia de la propuesta consiste en eliminar la noción de perímetro fijo sobre las instalaciones de la empresa, y reemplazarlo por un sistema en donde los recursos pueden ser accedidos desde cualquier ubicación, evaluando siempre a los dispositivos y a los usuarios.

A continuación, analizaremos en forma conceptual el contenido de estos artículos, originalmente publicados en la conocida revista digital de *Usenix* “*;login:*” [37] y de dominio público.

2.4.1 El Nuevo Enfoque

El primero de los artículos titulado “Un Nuevo Enfoque para la Seguridad Empresarial” (*A New Approach to Enterprise Security*) [38] presenta la arquitectura de referencia que Google decidió adoptar a partir de 2014.

En esta publicación, los autores Rory Ward y Betsy Beyer inician la discusión reiterando la preocupación por la creciente dificultad en reforzar el perímetro clásico protegido por cortafuegos en un contexto donde los dispositivos móviles y la nube son cada vez más predominantes, y donde un actor que obtiene acceso a través de ese perímetro puede luego realizar operaciones mal intencionadas.

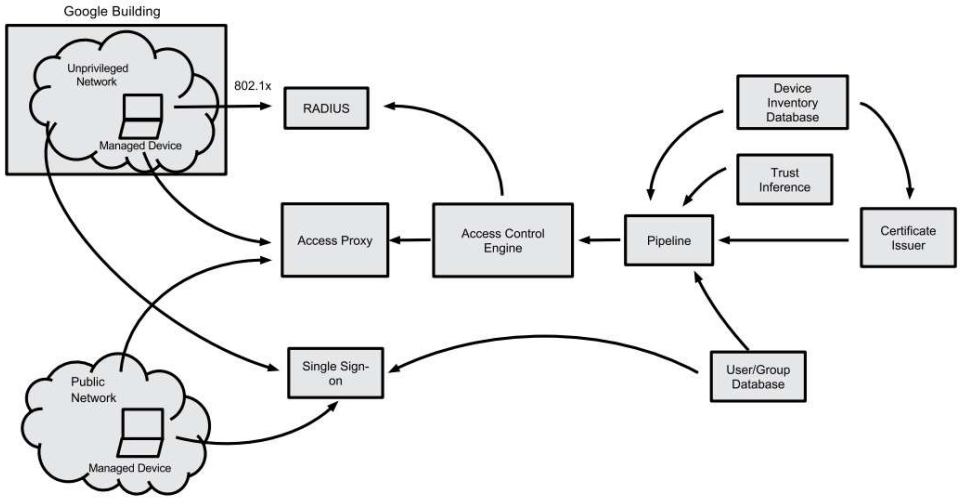


Figura 11 – Componentes y flujo de trabajo de *BeyondCorp*.

Así es como declaran que Google opta por mudar sus aplicaciones corporativas directamente a la red Internet, eliminando la necesidad de conexiones del tipo *VPN*. Todos los dispositivos son evaluados de igual forma, independientemente de dónde estén ubicados, asumiendo siempre que estas conexiones son en principio, no confiables.

En la figura de la página anterior, en el sector izquierdo, puede notarse cómo Google no distingue entre un dispositivo ubicado en los edificios de la empresa (*Google Building*) o en una red pública (*Public Network*). En ambos casos, los considera conectados a una red "no privilegiada" (*Unprivileged Network*).

En el extremo opuesto de la figura, se encuentra un elemento primordial del sistema denominado "Inventario de Dispositivos" (*Device Inventory Database*). En realidad, se trata de un conjunto coordinado de bases de datos alimentadas desde distintas fuentes.

Dado que *BeyondCorp* basa su propuesta de seguridad en la autorización basada en dispositivos y usuarios, los primeros solo pueden ser provistos y administrados por la empresa (*Managed Devices*), y solo ellos pueden acceder a los recursos corporativos.

Estos dispositivos se identifican a través de un certificado, y es por ello por lo que la base de datos de inventario se conecta a una autoridad certificante (*Certificate Issuer*).

En el sector inferior derecho de la figura, se puede notar la otra base de datos de interés para este esquema, la utilizada para identificar usuario y grupos (*User/Group Database*). De más está decir que este recurso se relaciona íntimamente con el departamento de RRHH.

Ambos casos de uso, la conexión desde oficinas propias o desde el exterior, suponen la utilización de un sistema de inicio de sesión único (*Single Sign-On*) multifactorial, que consulta a la base de datos de usuarios y grupos.

En el caso de conexiones dentro de sus oficinas, los dispositivos administrados se conectan a servidores RADIUS [39] y son asignados dinámicamente a distintas *VLAN* conforme a la autentificación 802.1x [40].

Los dispositivos que no son gerenciados por la empresa son directamente redireccionados a una red de invitados. En el centro del diagrama quedan entonces dos componentes que operan en conjunto, y son indispensables para la protección de los recursos accedidos.

Los clientes deben primero pasar por el “intermediario de acceso” (*Access Proxy*) ya sea desde dentro de las oficinas o desde Internet. Luego el “motor de control de acceso” (*Access Control Engine*) provee el nivel adecuado de permisos.

Este motor de control de acceso se alimenta de lo que Google llama una canalización o tubería de datos (*Pipeline*), alimentada de forma dinámica con datos útiles para la toma de decisiones sobre permisos de accesos. Esto incluye listas de certificados válidos, niveles de confianza de usuarios y dispositivos, y sus detalles de inventario.

2.4.2 Del Diseño al Despliegue

El segundo de los *papers* publicados por Google en referencia a *BeyondCorp* describe nuevamente al diseño de su solución, su despliegue, los desafíos encontrados y las lecciones aprendidas.

Este documento, fechado en 2016, tiene como nombre “*Design to Deployment at Google*” [41]. En este trabajo, nos interesa revisar los diagramas adicionales que pueden permitir entender de forma más completa a la propuesta.

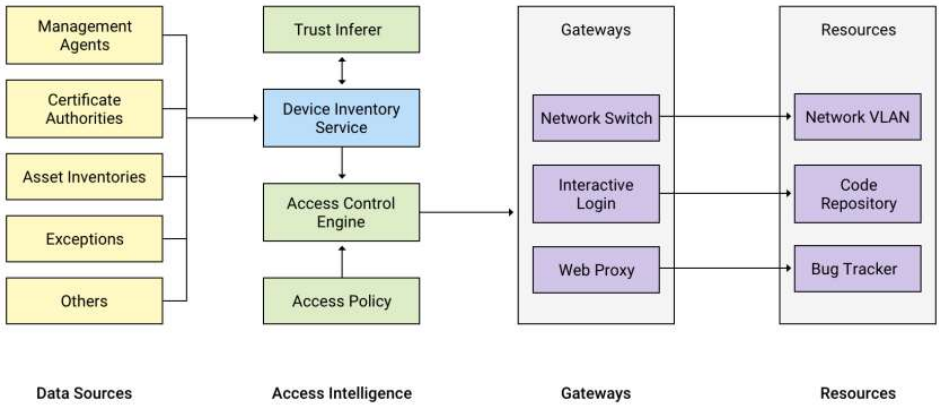


Figura 12 – Arquitectura y Componentes de *BeyondCorp*.

En principio, se aclara que los requerimientos de acceso se encuentran organizados en niveles de confianza (*Trust Tiers*) crecientes.

A la derecha en la figura anterior, se representan los recursos (*Resources*) que incluyen aplicaciones, servicios e infraestructura y cuyo acceso se debe controlar.

A estos recursos, se los accede a través de puertas de enlace (*Gateways*) que ejecutan acciones relacionadas con la autorización, tal como establecer un nivel de confianza mínimo o asignar una *VLAN*.

Para llegar a las puertas de enlace y finalmente acceder a los recursos, cada cliente debe pasar por un sistema de inteligencia de acceso (*Access Intelligence*) que cuenta con varios componentes, de los cuales el más importante es el servicio de inventario de dispositivos (*Device Inventory Service*).

Este servicio se alimenta tanto de los demás componentes de inteligencia de acceso, como de otras fuentes de datos (*Data Sources*) importantes en la columna izquierda de la figura.

El “inferidor de confianza” (*Trust Inferer*) es un sistema que analiza constantemente el estado de los dispositivos clientes, establece su nivel de confianza máximo y a qué *VLAN* de la red corporativa se pueden conectar.

Estos datos se vuelcan al servicio de inventario y se actualizan en base a cambios de estado o por no recibir actualizaciones desde cada dispositivo.

La política de acceso (*Access Policy*) define en forma programática la relación entre los recursos, los niveles de confianza y otros requisitos que deben cumplirse para obtener autorizaciones.

Finalmente, el motor de control de acceso (*Access Control Engine*) es quien toma las decisiones sobre autorización en base a los componentes descritos anteriormente.

En la figura siguiente, se muestra con más detalle cómo el servicio de inventarios es alimentado continuamente desde un amplio conjunto de fuentes de datos.

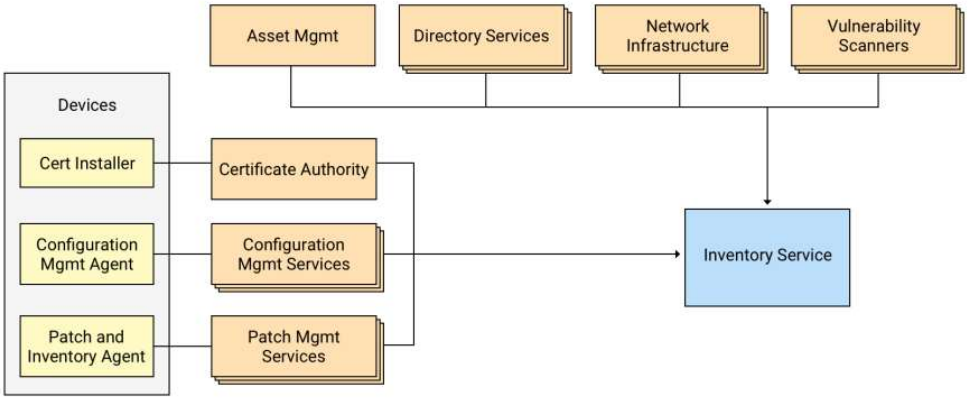


Figura 13 – El servicio de inventario de *BeyondCorp*.

Por ejemplo, los dispositivos (*Devices*) a la izquierda cuentan con agentes de configuración, de inventario y parches (*Patch and Inventory Agent*) y de certificados. Estos agentes se coordinan con los servicios respectivos más a la derecha.

El servicio de inventarios también toma información desde sistemas de administración de activos (*Asset Management*), sistemas de directorio tales como *Active Directory*, la infraestructura de la red y analizadores de vulnerabilidades (*Vulnerability Scanners*).

2.4.3 El *Proxy* de Acceso

El tercero de los documentos publicados por Google [42] acerca de *BeyondCorp* y el último que analizaremos, se centra en la funcionalidad de su componente principal de entrada denominado “Proxy de Acceso” (*Access Proxy*).

En él se explica que implementaron esta solución para hacer más expeditivo el incorporar los numerosos sistemas internos de la compañía, lo que hubiese sido mucho más complejo si se los asociaba al “inferidor de confianza” (*Trust Inferer*) en forma individual.

El *Access Proxy* se encarga de reforzar las políticas de acceso en forma genérica y amplia, tal como qué nivel de confianza permite acceder a qué recurso, trabajando en forma sincronizada con el motor de control de accesos (*Access Control Engine*), como ya pudimos visualizar en el punto 3.4.1. y su primera figura.

Los controles más rigurosos o afinados sobre los accesos, tales como decidir si tal usuario puede acceder tal función en un sistema, los terminan realizando los servidores de las aplicaciones de fondo (*Back End*).

En principio, lo que Google denomina “proxy de acceso” incluye a un conjunto de *proxy* reversos de *HTTP/HTTPS* [43] similar a lo que se dispone para cualquier aplicación expuesta en la red Internet (*Web Application).* Este grupo es denominado “Interfaz de Google” (*GFE – Google Front End*).

El *Access Proxy* agrega a la funcionalidad bien conocida de balanceo de carga y la administración de conexiones *TLS*, prestaciones relacionadas con la autentificación, la autorización, el aprovisionamiento autogestionado y el registro centralizado (*Centralized Logging*) para auditorías y análisis forense.

En el caso de la autentificación de usuarios, el *Access Proxy* se integra con varios protocolos tales como *OpenID Connect* y *OAuth* [44], más otros propietarios. Con respecto a la autorización de estos, se utilizan listas de control de accesos (*ACL - Access Control List*) y un lenguaje específico y extensible para gestionarlas.

Una vez realizadas la autentificación y la autorización de usuarios en el *Access Proxy*, este se comunica con los servidores de fondo a través de conexiones cifradas con *TLS* mutuo. Y toda la actividad se monitorea y registra en almacenamiento persistente, siendo este punto central ideal para tal fin.

Con respecto a la identificación de dispositivos, el mismo documento señala la mayor complejidad en un contexto multiplataforma. Como elementos mínimos indispensables incluye a algún identificador para dispositivo, y una base de datos donde se registre su último estado conocido.

Para los equipos de escritorio y portátiles, un certificado administrado en el sistema operativo es suficiente, mientras que para los dispositivos móviles se utiliza un identificador provisto directamente por su fabricante.

La migración de las aplicaciones *Web* que utilizan el protocolo *HTTP* a este nuevo esquema de trabajo resulta ser sencilla. En el caso de otros sistemas que operan bajo otros protocolos y necesitan cifrado de extremo a extremo requiere de un manejo especial.

La solución encontrada por Google ha sido la de envolver a todo este tráfico en requisiciones *HTTP*, utilizando distintas técnicas. Algunos ejemplos que menciona el trabajo incluyen *SSH* [45], *gRPC* [46] y el escritorio remoto propio (*Google Remote Desktop)* [47].

Por último, para el caso de las aplicaciones de terceros (*Third-Party Software*) que no pueden adecuarse como se comenta arriba, se hace uso de una solución desarrollada internamente que establece túneles punto a punto entre el cliente y el servidor de forma automática.

El documento culmina señalando las lecciones aprendidas durante el proceso de migración, brindado consejos sobre la complejidad de las listas *ACL*, las emergencias de producción y seguridad y la necesidad de combinar múltiples equipos y permitir su autogestión de permisos.

Mayores detalles sobre los distintos desafíos abordados se incluyen en los cuatro papers adicionales que componen a la serie, los cuales detallan cómo se puede encarar la migración [48], cómo se contempló siempre la experiencia del usuario [49], la cuestión relacionada con la seguridad de los dispositivos [50] y los casos de uso más complejos [51], en donde se muestra que para ciertos escenarios, todavía se necesita de las *VPN*.

Google ofrece su servicio de consultoría para que las empresas puedan aplicar este enfoque conocido como *BeyondCorp Enterprise* [52]. Por otra parte, el gigante informático implementa la seguridad en su infraestructura de servicios en la nube mediante una arquitectura denominada *BeyondProd* [53].

2.5 El Ecosistema Extendido *ZTX*

Cerramos este capítulo haciendo referencia nuevamente a un trabajo de la consultora Forrester [54], publicado en enero de 2018, titulado “El ecosistema extendido de *Zero Trust*”.

Este trabajo es relevante debido a que no solo amplía el modelo propio de *ZT* considerando otros aspectos de la plataforma a proteger, sino que además presenta un primer intento de agregar al modelo un marco de trabajo (*framework*) que oficie de guía para la toma de decisiones sobre implementaciones.

El resultado de tal ampliación conceptual es un nuevo acrónimo *ZTX* que la representa, donde la letra X sugiere la palabra “extendido”.

Se explica en el documento que el modelo consideraba originalmente a la eliminación del perímetro fijo, teniendo como protagonista al cortafuegos de última generación (*NGFW – Next Generation Firewall*) [55].

Sin embargo, ZT debe ser más que ello, transformándose en un enfoque holístico que incluya tanto procesos como tecnologías para los siguientes campos de acción:

- **Datos (*Data*):** Haciendo referencia a la seguridad de estos, lo cual supone una solución tecnológica. Se habla aquí de esquemas de clasificación, y de su cifrado tanto en reposo como en tránsito.
- **Redes (*Networks*):** Siendo este el dominio original del modelo de confianza cero, apoyando a la segmentación y el aislamiento de recursos.
- **Personas (*People*):** En donde el minucioso control de accesos y privilegios y su continua observación se suma a la necesidad de proteger sus interacciones con la red a través de las puertas de enlace tradicionales.

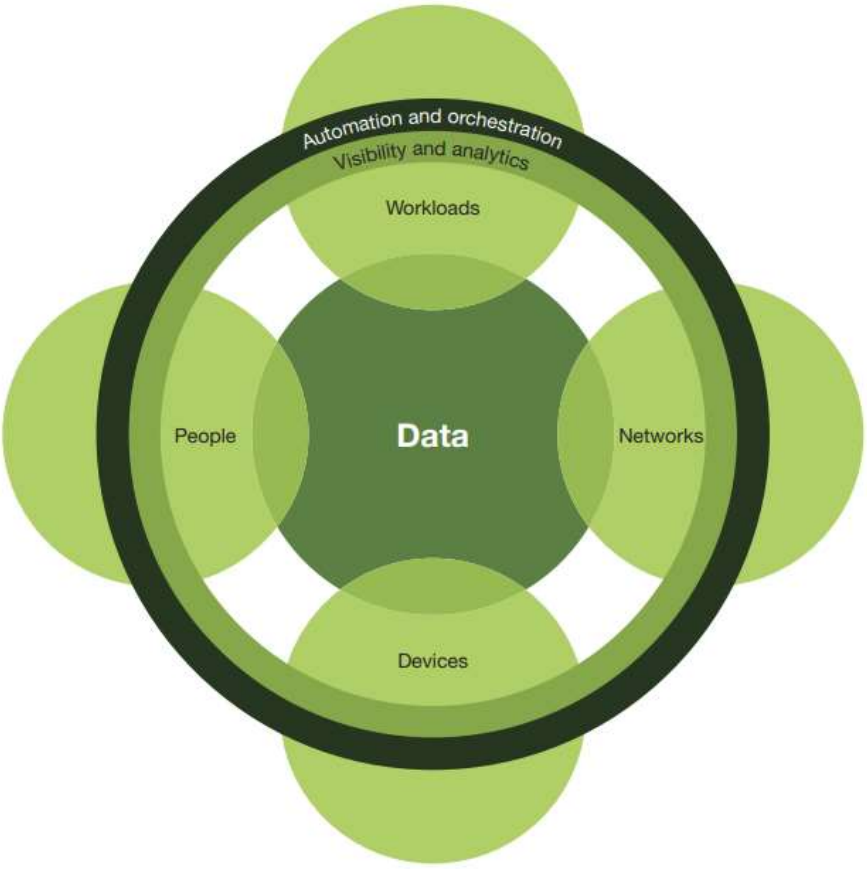


Figura 14 – El Ecosistema Extendido *ZTX*.

- **Aplicaciones (*Workloads*):** El término en inglés en este caso, hace referencia a todo el contexto de cualquier aplicación desde el sistema operativo, pasando por todas las conexiones hasta el código en ejecución.
- **Dispositivos (*Devices*):** Cada uno de los nuevos tipos que se incorporan a la red tales como televisores inteligentes, móviles, y elementos de la "Internet de las Cosas" (*IoT*), es un posible vector de ataque que debe ser vigilado.
- **Monitoreo y Análisis (*Visibility and Analytics*):** Herramientas que son componentes fundamentales en la propuesta de *ZT*.

- **Automatización y Orquestación:** Esencial dados los numerosos elementos que ya componen el ecosistema. Es necesario cada vez más el contar con herramientas para estos fines.

2.5.1 El Marco de Trabajo

Se propone aquí que el ecosistema surgido del modelo de confianza cero debe crecer para ser más inclusivo y prescriptivo.

Es por ello por lo que *Forrester* sugiere un marco de trabajo para el mapeo de controles con la intención de que sirva como guía a los tomadores de decisiones sobre la seguridad de la información en cuanto a qué soluciones elegir de acuerdo con dicho marco.

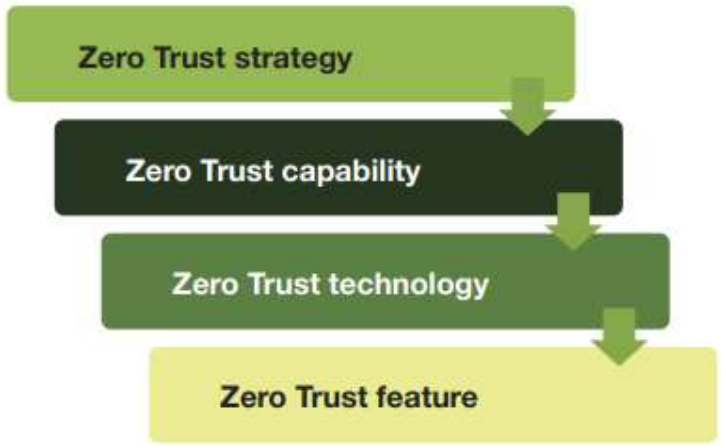


Figura 15 – El marco de trabajo de *ZTX* para el mapeo de controles.

Dentro de este marco, las decisiones estratégicas (*strategy*) se encuentran en la cima de este y no están relacionadas con ninguna solución particular de ningún proveedor. Se trata de planes de alto nivel, tales como "orientarse hacia una arquitectura de Confianza Cero".

En el ecosistema de *ZTX*, existen distintos componentes claves tales como los citados anteriormente: datos, redes, personas, etc.

Para cada uno de esos componentes, se necesitan distintas capacidades (*capability*). Por ejemplo, para los datos, la posibilidad de clasificarlos, cifrarlos, archivarlos o borrarlos. Al seleccionar cualquier proveedor o sus productos, se deben tomar en cuenta los procesos relacionados con tales capacidades.

Recién luego de haber establecido la estrategia e identificado las capacidades necesarias, se puede comenzar a evaluar cada tecnología (*technology*), es decir, herramientas, aplicaciones y plataformas. Y es fundamental el considerar la interconexión de esas soluciones con otras dentro del ecosistema.

El nivel de mayor granularidad en este marco de trabajo es el que corresponde finalmente a cada característica (*feature*). Es preciso analizar cómo una característica de un producto o solución se vincula con los demás niveles del marco y la estrategia en general.

2.5.2 Proveedores Notables

Uno de los aspectos distintivos de este documento es la introducción de una guía de “proveedores notables”, clasificados en base a cada componente del ecosistema extendido.

El hecho de introducir por primera vez nombres específicos de proveedores, algo que tarde o temprano iba a suceder y quizás como un paso estratégico hacia la posibilidad de recomendar ciertas soluciones, es lo que hace a esta publicación ser otro hito en la historia de ZT.

Como parámetro para integrar este selecto listado, Forrester exige a los aspirantes a convertir sus soluciones en “plataformas de Confianza Cero” el cumplir con los siguientes requisitos.

En primer lugar, proveer capacidades que lideren el mercado en al menos tres componentes del ecosistema. Por ejemplo, datos, redes y dispositivos.

En segundo, el ofrecer alguna ventaja única relacionada con la integración de distintas soluciones, tales como la administración unificada de políticas a través de diferentes dispositivos.

Adicionalmente, el proveedor debe contar con un sistema robusto de interfaces de programación de aplicaciones (*API – Application Programming Interface*) o herramientas de desarrollo de software (*SDK – Software Development Kit*) [56] con los que los programadores puedan crear integraciones específicas.

Como último requisito, se debe contar con una visión concreta en relación con la visibilidad, el análisis, la automatización y la orquestación centralizados.

En la página siguiente entonces se muestra una copia de la lista de proveedores clasificados según cada componente del ecosistema.

Como apreciación al margen, recordamos al lector que el espíritu original del modelo de Confianza Cero era primordialmente agnóstico, tal como lo es el de este trabajo académico. En cierta medida, **Forrester** abandona esa premisa en esta publicación, convirtiéndose en otra fuente más de promoción comercial de soluciones.

El motivo por el cual se incluye a esta publicación presentándola como un hito en la línea de tiempo de la confianza cero, es para evidenciar que ya a esta altura en el año 2018, el modelo se había expandido, un marco de trabajo (ciertamente muy elemental) había sido propuesto y un ecosistema de soluciones ya estaba disponible en el mercado, sin hacer foco en ninguna de ellas en particular.

El autor de este trabajo es el Dr. Chase Cunningham [57], otra personalidad relevante y conocido como el “Dr. Zero Trust.”

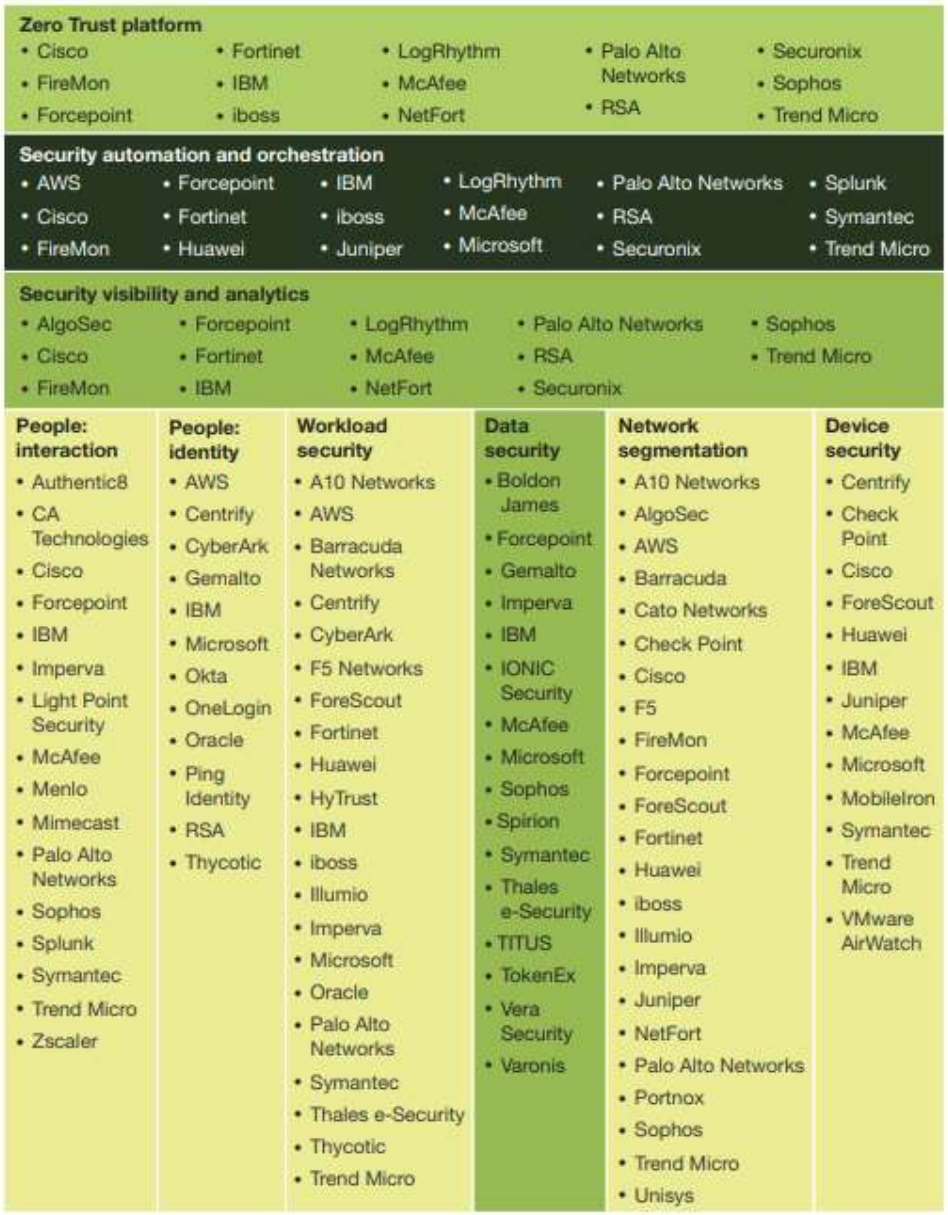


Figura 16 – Proveedores notables en el ecosistema *ZTX*.

3. Desde *NIST* hasta la Actualidad

La línea de tiempo que presentamos en el primer capítulo podría ser interpretada como la cronología "clásica" de nuestro tema de estudio, la cual culmina en el año 2020 con su primera definición formal.

Sin embargo, a partir de esta fecha se produce una serie de eventos adicionales de igual o quizás mayor relevancia, los cuales completan y enriquecen al concepto de Confianza Cero aportándole mayor relevancia, metodología, y hasta ampliando la arquitectura propuesta inicialmente.

Fecha	**Evento / Publicación**
Febrero 2021	*DoD Zero Trust Reference Architecture v1.0.*
Mayo 2021	*Executive Order 14028 Improving the Nation's Cybersecurity.*
Agosto 2021	*CISA Maturity Model v1.0.*
Enero 2022	*Memorandum M-22-09 Federal Zero Trust Strategy.*
Febrero 2022	*Report to the President on Zero Trust and Trusted Identity Management.*
Marzo 2022	*Software-Defined Perimeter (SDP) Specification v2.0.*
Julio 2022	*DoD Zero Trust Reference Architecture v2.0.*
Abril 2023	*CISA Maturity Model v2.0.*

Tabla 1 – La nueva cronología de Confianza Cero.

Estos hitos corresponden principalmente a iniciativas de agencias gubernamentales de los Estados Unidos, y de la *Cloud Security Alliance*, en donde se mantiene la perspectiva agnóstica y la documentación es de dominio público.

La lista no es exhaustiva, e incluye aquellos eventos que se consideran de mayor relevancia en el contexto de este trabajo. A continuación, analizaremos cada uno de ellos con sus respectivas referencias y figuras, intentando completar nuestra comprensión sobre *Zero Trust*.

3.1 La Arquitectura de *NIST*

En agosto de 2020 la reconocida organización de estándares *NIST* (*National Institute of Standards and Technology*) de los Estados Unidos marca uno de los más importantes hitos en la línea de tiempo de *ZT.*

Esto lo realiza ofreciendo su publicación especial 800-207 titulada "Arquitectura de Confianza Cero" (*Zero Trust Architecture*) [58].

Recordando una vez más el paralelismo existente entre el desarrollo de los servicios en la nube y nuestra Confianza Cero, es nuevamente *NIST* quien establece una definición concreta sobre el tema que desde entonces ha sido utilizada en todos los ámbitos como referencia.

De hecho, si existe hoy un documento importante sobre *ZT*, que todos los profesionales informados de la industria de la Seguridad Informática conocen, es sin duda este.

Es interesante observar, y lo veremos a continuación, que *NIST* en el 2020 toma como base para sus definiciones y propuestas, información acumulada que ya hemos visto en los capítulos anteriores, tanto del historial de iniciativas de agencias gubernamentales de su país, como de organizaciones privadas tales como Forrester y *CSA*.

El documento se extiende en 59 páginas, y aquí intentaremos analizar sus puntos más relevantes en relación con el propósito de este trabajo.

3.1.1 Definiciones

Tal como es la costumbre con *NIST* y uno de sus objetivos como organización dedicada a estándares, se ocupa inicialmente de fijar las definiciones básicas con las que trabajar, y respondiendo a la necesidad de industria.

En primer lugar, establece una "definición operativa" para *Zero Trust (ZT)* y para el nuevo término que introduce como *Zero Trust Architecture (ZTA)*. Estas definiciones destacadas a continuación son particularmente extensas y su traducción es de autoría propia:

> *Zero Trust* provee una colección de conceptos e ideas diseñada para minimizar la incertidumbre al hacer cumplir decisiones de acceso precisas, basadas en el menor nivel de privilegios necesario y tomadas por cada petición, en sistemas de información y servicios operando sobre redes consideradas comprometidas.

> *Zero Trust Architecture* es un plan empresarial de ciberseguridad que utiliza conceptos de confianza cero y engloba relaciones entre componentes, planificación de flujos de trabajo y políticas de acceso.

Acompaña finalmente a estas definiciones aclarando que, como resultado de estas, surge la "confianza cero empresarial" (*Zero Trust Enterprise*), que comprende tanto a su infraestructura física o virtual, como a las políticas operativas vigentes.

Sabiendo ahora qué es Confianza Cero según *NIST*, una organización puede adoptarla como estrategia, y desarrollar una arquitectura basada en sus principios. El resultado es un "ambiente" de *ZT*.

Es importante notar algunas definiciones accesorias que el documento utiliza para desarrollar su propuesta.

En primer lugar, resalta que la red tradicional basada en un perímetro fijo es ya obsoleta, tomando como premisa que ese límite ya ha sido superado por un atacante. Esto ya se venía discutiendo hace tiempo.

En segundo lugar, aclara que el enfoque *ZT* si bien se basa primordialmente en la protección de datos y servicios debería extenderse hacia todos los activos de la organización, tales como dispositivos, elementos de su infraestructura, aplicaciones y componentes tanto virtualizados como alojados en la nube.

Finalmente, una distinción relevante entre el término “sujeto” (*subject*), que puede referirse tanto a usuarios como a aplicaciones y a cualquier entidad no humana que solicite servicios a los recursos, y el término “usuario” (*user*) que solo hace referencia a una persona.

Y recordar que el término “recurso” (*resource*) no solo se relaciona con datos sino también con dispositivos, impresoras, computadoras, y elementos de la Internet de las Cosas.

NIST hace hincapié en que el meollo de la cuestión radica en enfocarse tanto en la autorización como en la autentificación, minimizando en la mayor medida factible cada zona de confianza. Las políticas de acceso deben ser lo más granulares posibles reforzando el concepto del menor privilegio.

La primera sección de esta publicación dedicada como venimos observando a sentar las bases conceptuales, introduce un modelo abstracto inicial de acceso con sus dos componentes fundamentales para las políticas de acceso, que son el “punto de decisión” (*PDP – Policy Decision Point*) y el “punto de aplicación” (*PEP – Policy Enforcement Point*).

En la figura a continuación, ambos componentes se muestran unificados en el sector central. Por la izquierda se ve el sujeto que necesita acceder a un recurso, situado a la derecha.

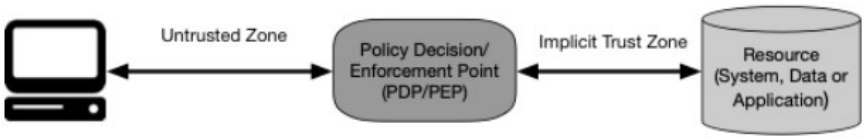


Figura 17 – El modelo abstracto de acceso de *NIST*.

Entre el sujeto que necesita acceso a los servicios y el mecanismo central de acceso, se encuentra la "zona no confiable" (*Untrusted Zone*). Una vez que ese sujeto supera en forma válida al conjunto *PDD/PEP* entonces accede a la "zona de confianza implícita" (*Implicit Trust Zone*).

La idea es posicionar a estos puntos de acceso y aplicación de políticas cerca de los recursos, y para ello *ZT* provee de una serie de principios y conceptos. Los principios (*tenets*) son siete:

1	Todas las fuentes de datos y servicios de cómputo son recursos.
2	Todas las comunicaciones son seguras independientemente de la ubicación en la red.
3	El acceso a cada recurso individual se otorga por cada sesión.
4	El acceso a los recursos se determina por políticas dinámicas.
5	La organización monitorea y mide la integridad y la postura de seguridad de todos los activos propios y asociados.
6	La autenticación y la autentificación se realizan en forma dinámica y estricta antes de otorgar cada acceso.
7	La organización recolecta la mayor cantidad de información posible acerca del estado actual de cada activo, y la utiliza para mejorar su postura de seguridad.

Tabla 2 – Los 7 principios de *Zero Trust* según *NIST*.

Estos siete principios son relativamente sencillos de interpretar y están alineados con todas las discusiones que ya hemos expuesto.

En el caso del cuarto, es de interés notar que las políticas dinámicas mencionadas incluyen al estado observable de la identidad del cliente, de la aplicación que genera la petición, del dispositivo que se utiliza y pueden incluirse otros aspectos conductuales, así como atributos del ambiente.

En cuanto a la dinámica a que hace referencia el punto 6, ya se recomienda una plataforma de gestión de acceso e identidades, y la adopción de autentificación multifactorial.

Otra nota de importancia, y sobre todo para este trabajo, es que la propuesta de *NIST* posiciona a estos principios como tecnológicamente agnósticos, y por supuesto diferenciando a la adopción de Confianza Cero de la compra de cualquier solución integral de un proveedor.

Para cualquier organización que decide utilizar *ZTA* en sus redes, *NIST* plantea una serie de supuestos que deben tomarse en cuenta.

En primer lugar, que su red privada no es confiable y que se la debe considerar comprometida. En segundo, que puede haber dispositivos en la red que no son propios. Asimismo, que ningún sujeto será confiable de manera implícita, y debe ser evaluado antes de otorgarle cualquier acceso.

Como cuarto supuesto, que no todos los recursos se encuentran operando en instalaciones propias. Y que los sujetos no siempre pueden confiar en sus respectivas conexiones de red.

Finalmente, para aquellos activos y flujos de trabajo que se desplazan entre la infraestructura propia y otra externa, la postura de seguridad debe ser siempre la misma.

3.1.2 Componentes Lógicos

A juicio de quien redacta este trabajo, esta sección es sin duda la más importante de todo el documento, ya que no solo describe la arquitectura en términos de componentes lógicos, sino que propone diferentes variantes.

Y es aquí donde más se nota la influencia de los esfuerzos que se han descrito en secciones anteriores, en particular de *BeyondCorp* de *Google* y el protocolo *SDP* de la *Cloud Security Alliance*.

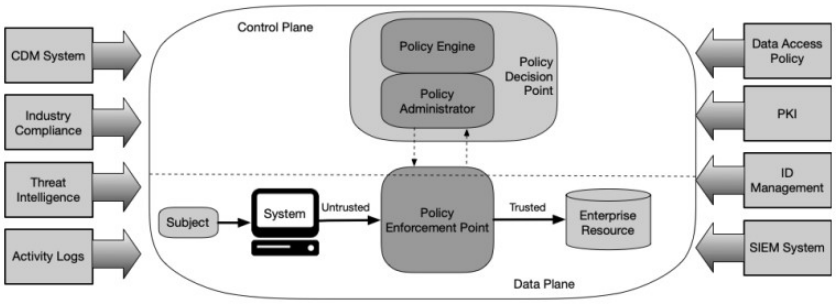


Figura 18 – Componentes lógicos de la *ZTA*.

El diagrama de la figura superior es por supuesto de carácter conceptual. *NIST* ya prevé que este diseño puede ser desplegado tanto en instalaciones propias como en la nube.

En este diagrama, en el sector central, se encuentran los mismos componentes planteados en el modelo abstracto inicial, pero con mayor detalle. Por la izquierda y por la derecha, se disponen todos los otros sistemas que aportan información necesaria para que la toma de decisiones en cuanto a autorizaciones y autentificación.

Dos detalles importantes para notar en este diagrama son los siguientes. En principio se disponen dos canales de comunicación, uno para el control (*Control Plane*) exclusivo para los elementos internos y otro denominado “de datos” (*Data Plane*) para la transferencia de estos.

Además, en la parte superior central de la figura, se encuentra el *PDP* descrito en el modelo abstracto, desglosado en dos elementos funcionales.

El "motor de políticas" (*PE - Policy Engine*) es el encargado de tomar la decisión final en cuanto a otorgar o no a un sujeto el acceso a un recurso. Mientras que el "administrador de políticas" (*PA - Policy Administrator*) se ocupa de establecer o terminar la conexión, configurando al *PEP* para hacerlo.

Por debajo de esta dupla decisoria, se encuentra el *PEP* ya descrito también en el modelo abstracto, intermediario efectivo entre el sujeto y el recurso, el cual no sólo habilita o impide conexiones, sino que además las monitorea.

Ya veremos en las variantes propuestas que el *PEP* puede valerse de ayuda tanto desde el sujeto a través de un agente, como de una puerta de enlace ubicada al frente del recurso.

Con respecto a los componentes adicionales situados por izquierda y por derecha:

- ***CDM System:*** Es un sistema de diagnóstico y mitigación continua (*Continuous Diagnostics and Mitigation*) el cual se ocupa de monitorear el estado de los activos de la organización y aplicarles actualizaciones a su configuración y a su software, más resolver cualquier vulnerabilidad.
- ***Industry Compliance:*** Responsable de asegurar que la organización cumpla con todas las normas y regulaciones a las que debe suscribir, lo que incluye a todas las políticas de cumplimiento.
- ***Threat Intelligence:*** Información de inteligencia sobre amenazas que puede provenir de orígenes múltiples ya sea internos, o desde servicios externos.
- ***Activity Logs:*** Registros de actividad en la red y en los sistemas agregados en tiempo real o con la mayor velocidad posible.

- ***Data Access Policy:*** Este componente fundamental define las políticas de acceso a los recursos las cuales pueden estar almacenadas en el mismo o ser generadas en forma dinámica por el motor. Cada vez que se toma una decisión de acceso, este es el punto de partida.
- ***PKI:*** La organización debe contar con algún sistema de administración de certificados digitales, público o privado, y basado o no en el estándar X.509 [59].
- ***ID Management:*** Elemento esencial para gestión de usuarios e identidades, incluyendo sus permisos de acceso según su rol, y que se apoya en el sistema de certificados digitales.
- ***SIEM System:*** Un sistema para la gestión de la información (*Security Information and Event Management*) [60] sobre eventos de seguridad que es clave para un análisis posterior a los mismos y su aplicación en el refinamiento de las políticas.

3.1.3 Variaciones

NIST no sólo propone la arquitectura conceptual de una solución basada en Confianza Cero, sino que también plantea las diferentes formas en que una organización puede encarar la implementación real, presentando varios modelos posibles.

Para comenzar, enumera tres enfoques que se pueden abordar, dependiendo de cuál sea la principal fuente de reglas para las políticas de acceso. Los tres adhieren a todos los principios (*tenets*) de *ZT*, pero varían en los componentes que incluyen, utilizando uno o dos de ellos como factor conductor principal. Y aclarando que una solución completa de Confianza Cero debería observar a todos los enfoques.

El primero de ellos es el que se centra en el “gobierno mejorado de las identidades” (*Enhanced Identity Governance*). Aquí el foco está obviamente centrado en los permisos otorgados a cada sujeto.

El segundo, pone énfasis en la microsegmentación, ubicando a un recurso o grupo de ellos dentro de un segmento de red protegido a través de una puerta de enlace de seguridad.

La tercera alternativa consiste en la utilización de un “perímetro definido por software” (*SDP*) que ya vimos en la sección correspondiente.

Una vez presentados estos enfoques, *NIST* ofrece 4 variaciones concretas para el despliegue de los componentes de la arquitectura abstracta. Y hace notar que variaciones diferentes podrían ser implementadas en distintos sectores de una misma red organizacional.

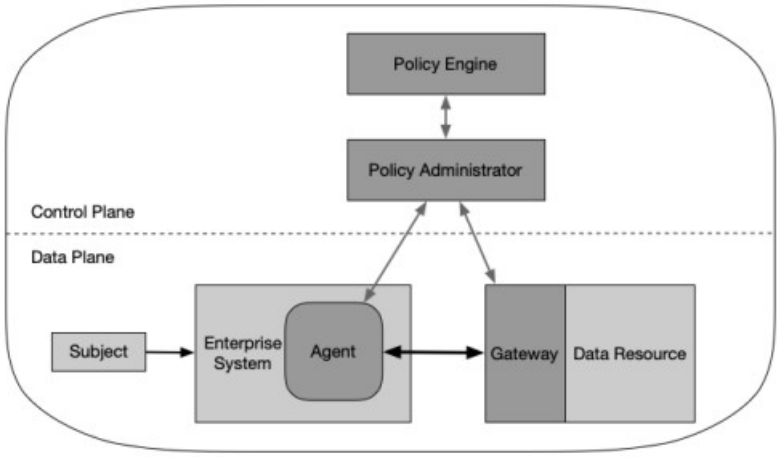


Figura 19 – Modelo de despliegue “Agente / Puerta de Enlace”.

El modelo de despliegue denominado “Agente / Puerta de Enlace” (*Agent / Gateway*) que muestra la figura superior, subdivide al *PEP* en dos componentes. El agente se encuentra instalado en el activo tal como una computadora de la empresa (*Enterprise System*).

La puerta de enlace por su parte puede operar por delante del recurso de datos (*Data Resource*) a proteger, o ser parte de este.

Este modelo depende de un sistema robusto de administración de activos, la disponibilidad de las puertas de enlace y no es compatible con políticas de utilización de dispositivos personales (*BYOD – Bring Your Own Device*).

Para los despliegues apoyados fuertemente en recursos en la nube, se corresponde con la propuesta "cliente-servidor" del protocolo *SDP* de la *Cloud Security Alliance.*

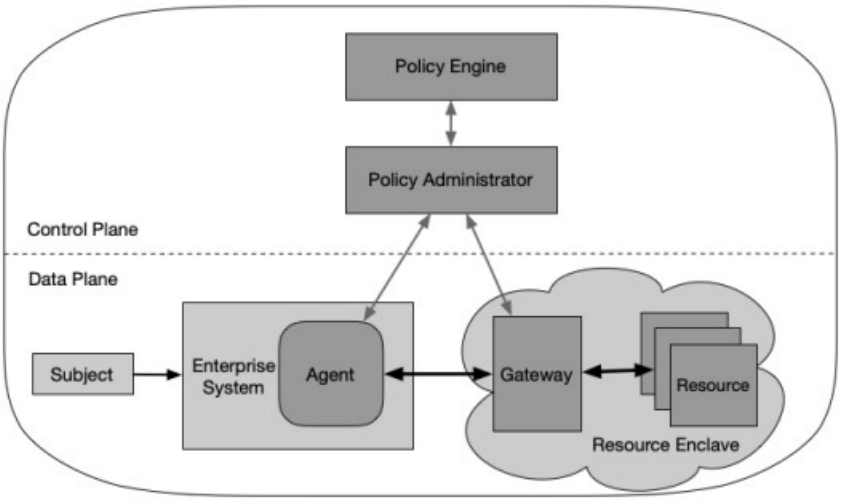


Figura 20 – Modelo de despliegue "Enclave de Recursos".

El modelo siguiente es una variación del anterior, donde la puerta de enlace se encuentra al frente y protegiendo no a un único recurso sino a un grupo o "enclave" de ellos.

Esta opción es aplicable a recursos antiguos (*legacy*) en instalaciones propias, donde quizás no sea posible o recomendable el proteger a cada uno individualmente. Obviamente esto conlleva un efecto en la granularidad de los permisos, y el hecho de que al obtener acceso al enclave se accede a todo.

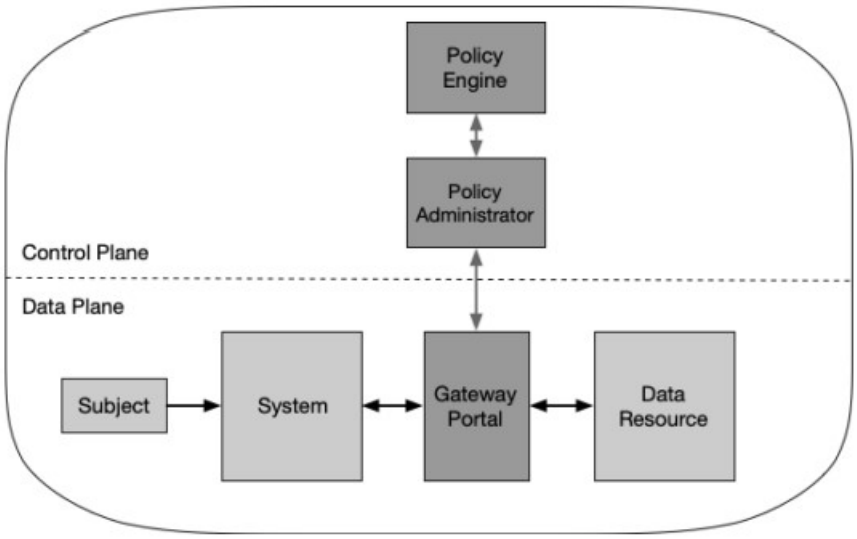


Figura 21 – Modelo de despliegue "Portal de Recursos".

En el modelo "Portal de Recursos" (*Resource Portal*) el *PEP* está compuesto por una única puerta de enlace que protege una o varias fuentes de datos.

En este caso no se utiliza un agente en el sistema donde opera el sujeto y por ende, se habilita la posibilidad de usar dispositivos no provistos por la organización (*BYOD*), haciendo extensivo el acceso a los recursos a terceras partes también.

Como contrapartida, no es posible mantener un control tan estricto sobre la seguridad de los activos, los cuales solo pueden ser auditados al momento de conectarse al portal.

Ejemplos de casos de uso para este modelo incluyen una nube privada o el ya mencionado esquema de protección para un conjunto de fuentes de datos antiguas (*legacy*).

Finalmente se describe una variante en donde el control se realiza sobre el dispositivo que solicita la conexión, como se puede observar en la siguiente figura.

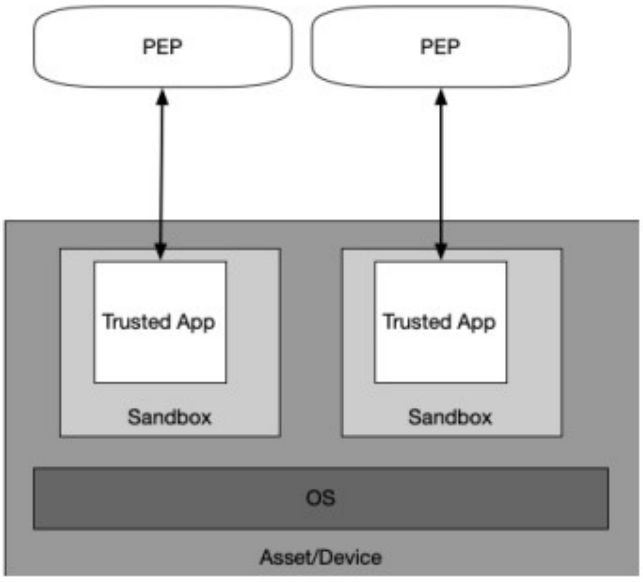


Figura 22 – Modelo de despliegue "Cajas de Arena".

Su nombre es "aplicaciones en cajas de arena" (*Application Sandboxes*) y consiste en encapsular a aquellas aplicaciones confiables (*Trusted Apps*) que vayan a conectarse al *PEP* en un entorno bien protegido (*Sandbox*), que podría ser una máquina virtual segura operando aislada en el dispositivo cliente que podría no serlo.

3.1.4 Casos de Uso

En su cuarta sección, el documento de *NIST* presenta distintos casos de uso aclarando que cualquier ambiente de red organizacional puede ser diseñado en base a los principios de *ZT*, y que es muy probable que la mayoría de ellas ya se encuentre encaminada hacia ese fin.

Muchas organizaciones combinan a la fecha de su publicación elementos de la *ZTA* en combinación con el sistema de perímetro fijo que ya estaba presente.

´+

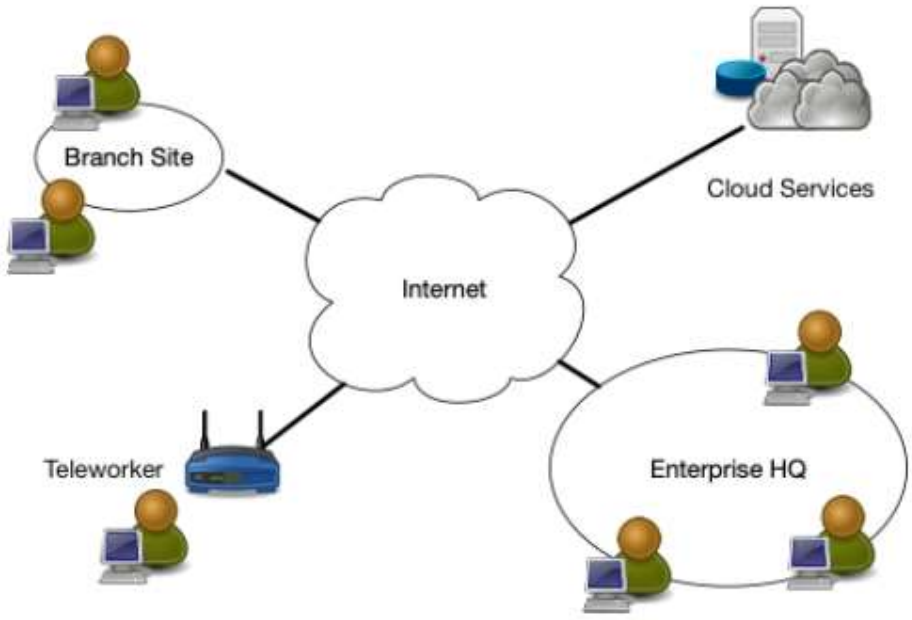


Figura 23 – La organización con empleados remotos.

Sin dudas y tal como lo presenta el documento, el caso de uso de la figura superior es el escenario más común y el más aplicable a la mayoría de las entidades.

Se trata de una organización donde existe una casa matriz (*HQ - Headquarter*s), una o más sucursales (*Branch Site*), empleados que se conectan en forma remota (*Teleworker*) y todo ello combinado con recursos en la nube.

Por distintos motivos no se requiere o no es posible hacer pasar todo el tráfico por la red interna, y además se necesita habilitar el uso de dispositivos personales. Todos los riesgos de seguridad que pretende mitigar una *ZTA* están presentes en este modelo.

Y en base a lo mencionado en el párrafo anterior, es más conveniente en este caso disponer al *PEP* como un servicio en la nube, combinándolo ya sea con agentes instalados en los dispositivos o bien un esquema de portal de recursos.

Algunos servicios serán fácilmente accedidos tales como páginas institucionales o el correo. Pero otros recursos más sensibles como por ejemplo una base de datos necesitarán de permisos más exigentes y granulares.

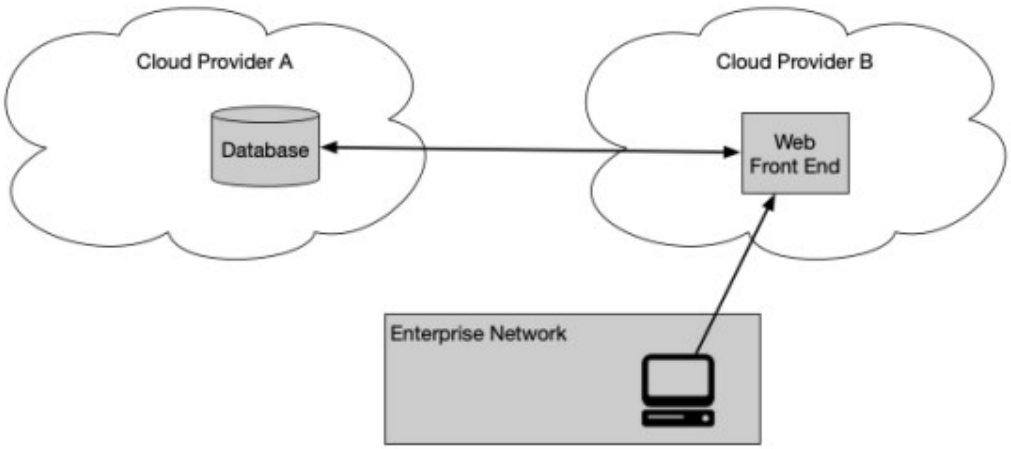


Figura 24 – El uso de nubes múltiples.

El segundo caso de uso corresponde ya a la fecha de publicación del estándar, a un tipo de implementación cada vez más vigente, en donde la organización utiliza más de un proveedor de servicios en la nube.

Aquí sucede que mientras las aplicaciones residen en las instalaciones de un proveedor, los datos que las soportan se encuentran alojados en otro, y se decide establecer una conexión directa entre ambos recursos sin hacerla pasar por la red interna, lo que sería menos eficiente y complicaría su administración.

Se disponen entonces los *PEP* al frente de cada recurso en las respectivas nubes, mientras que el *PE* y el *PA* podrían estar ubicados incluso en un tercer proveedor.

Los dispositivos clientes se conectan directamente a cada *PEP* en forma directa, ya sea contando con un agente instalado en ellos o bien mediante la implementación de un portal.

Cabe recordar, y el mismo documento lo menciona, que este caso corresponde a la variante “servidor a servidor” del protocolo *SDP* que vimos en el punto 2.3.3.

Y, por último, notar que, dado que cada proveedor de servicios en la nube tiene su forma particular de implementar cualquier funcionalidad, hará falta la participación de un arquitecto que diseñe cuidadosamente la solución.

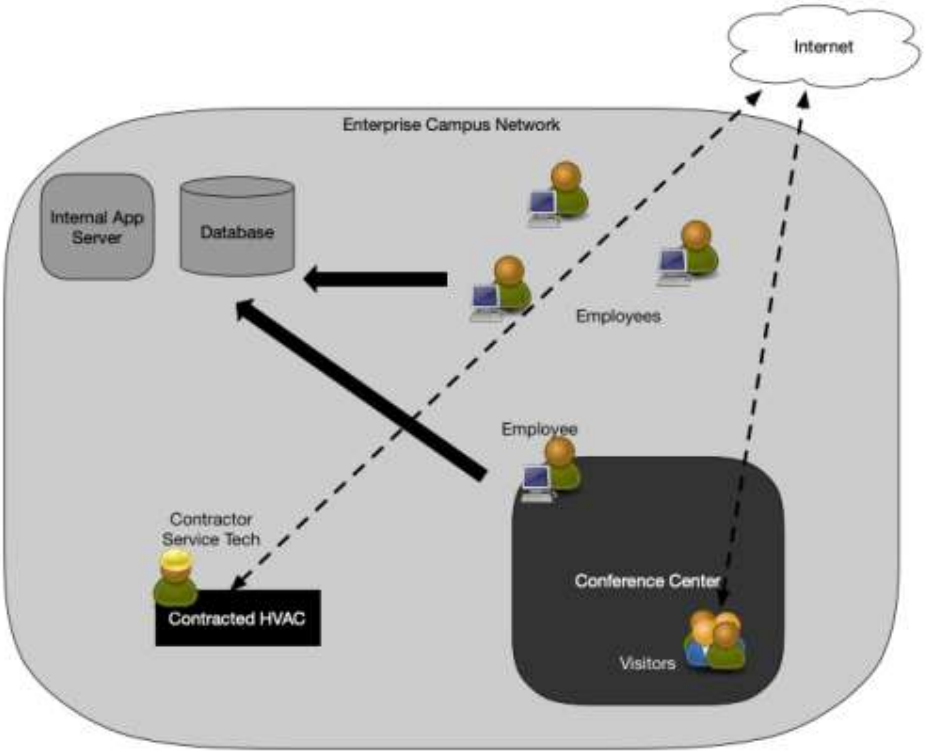


Figura 25 – Contratistas externos.

El tercer caso de uso planteado en la figura superior corresponde a juicio de quien escribe este trabajo a una situación que ya estaba bien prevista antes de la Confianza Cero.

Se trata de la incorporación de terceros contratistas tales como técnicos de un sistema de aire acondicionado, o visitantes que asisten a una conferencia, que necesitan acceso a Internet.

NIST indica que en esta situación el perímetro definido por software puede ayudar a diferenciar empleados de visitantes. Los *PE* y *PA* pueden situarse en la propia red o en un servicio en la nube.

La autorización para utilizar los recursos internos se otorgaría sólo a los dispositivos con un agente instalado o que no puedan conectarse al portal de accesos. Los terceros solo podrían acceder a navegar por Internet.

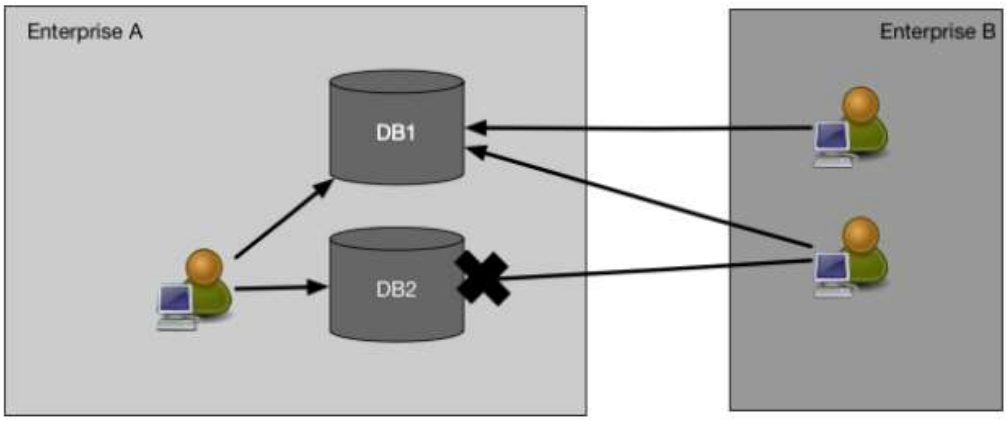


Figura 26 – Colaboración entre distintas empresas.

La figura superior ejemplifica el cuarto caso en el cual dos empresas realizan una tarea en común tal como un proyecto de desarrollo y la empresa A debe brindar acceso a colaboradores de la empresa B.

En vez de establecer complejas reglas en los cortafuegos, que además pueden terminar siendo difíciles de administrar, se puede implementar un sistema federado de manejo de identidades para ambas organizaciones.

Este escenario es similar al primero de los casos planteados en esta sección, correspondiente a los empleados remotos. Y haciendo uso de un servicio en la nube para los *PA* y *PE* se puede lograr cubrir todas las necesidades de conexión, siendo posible que haga falta el instalar en los dispositivos de la empresa B algún agente, o hacerlos pasar por una puerta de enlace.

El último escenario, que no necesita un gráfico descriptivo, es el que corresponde a un servicio bastante común que ofrecen las organizaciones, brindando acceso a cierta información requiriendo o no la registración de los usuarios.

Esa información puede ser completamente pública, datos para clientes o socios de negocios, e incluso destinada a empleados tercerizados.

En todos los casos, las conexiones serán realizadas con dispositivos propios y esto hará difícil el reforzar cualquier política de seguridad.

NIST aclara que, si se trata de un servicio totalmente público y que no exige credenciales, la *ZTA* directamente no aplica. Para aquellos que acceden con permisos, entonces se pueden implementar algunas directivas tales como autentificación multifactorial, y el monitoreo de las conexiones siempre tomando en cuenta las limitaciones regulatorias que apliquen a la información que se pueda recolectar.

3.1.5 La Migración a *ZTA*

En la séptima y última sección del documento de *NIST* se trata la problemática de migrar una plataforma basada en la protección perimetral, haciendo hincapié en el hecho que dicha transformación debe ser incremental, y presentando un esquema con pasos ciertos para abordarla.

Se hace notar aquí que un caso en el que se pudiera implementar una arquitectura de *ZT* desde cero (*greenfield*) sería muy poco factible, sin embargo, podría ocurrir que una organización con instalaciones ya existentes decida inaugurar una nueva unidad operativa donde se pueda diseñar una solución basada en la Confianza Cero desde el inicio.

En los demás casos, se tratará de entidades en donde el proceso se llevará a cabo en varias iteraciones, y probablemente existirán por tiempo indefinido, el enfoque tradicional y la nueva arquitectura.

El proceso de migración propuesto se inicia con tres tareas de relevamiento y evaluación, sobre el inventario de activos (*assets*), los usuarios más los flujos de trabajo (*workflows*) y de datos (*data flows*). Y estas pueden llevarse a cabo en paralelo, pero siempre guiadas por los procesos del negocio.

En el caso de los usuarios, estos pueden incluir tanto personas como otros denominados “entidades no personales” (*NPE - Non Personal Entities*) tales como cuentas de servicios que interactúen con distintos recursos.

Especial énfasis se hace sobre las cuentas de administradores, que pueden tener permisos “amplios” que deben ser auditados.

Para los activos, lo que incluye tanto computadoras, teléfonos y hasta elementos de Internet de las Cosas, como artefactos digitales (cuentas de usuario, aplicaciones y certificados digitales) no solo se debe realizar el relevamiento más completo posible.

Dado que nunca es posible relevar el total de los activos existentes, también se debe habilitar la capacidad de identificarlos, catalogarlos, y administrarlos al momento de su conexión a la red. Y luego actualizarlos y monitorear su comportamiento.

La misma consideración anterior sobre las cuentas de administradores aplica aquí, donde seguramente van a existir activos que ellos usan y no son parte del inventario oficial.

Como tercera evaluación entonces se recomienda la identificación y clasificación de los flujos de trabajo y de datos en el marco de los procesos del negocio y su relación con ellos.

Un detalle relevante y de gran importancia es que *NIST* recuerda que cualquier adopción de *ZTA* es un proceso para reducir riesgos.

Y por ello, determina que los pasos a seguir para completar la evaluación pueden ser mapeados con los que especifica el marco de gestión de riesgos (*RMF- Risk Management Framework*) [61].

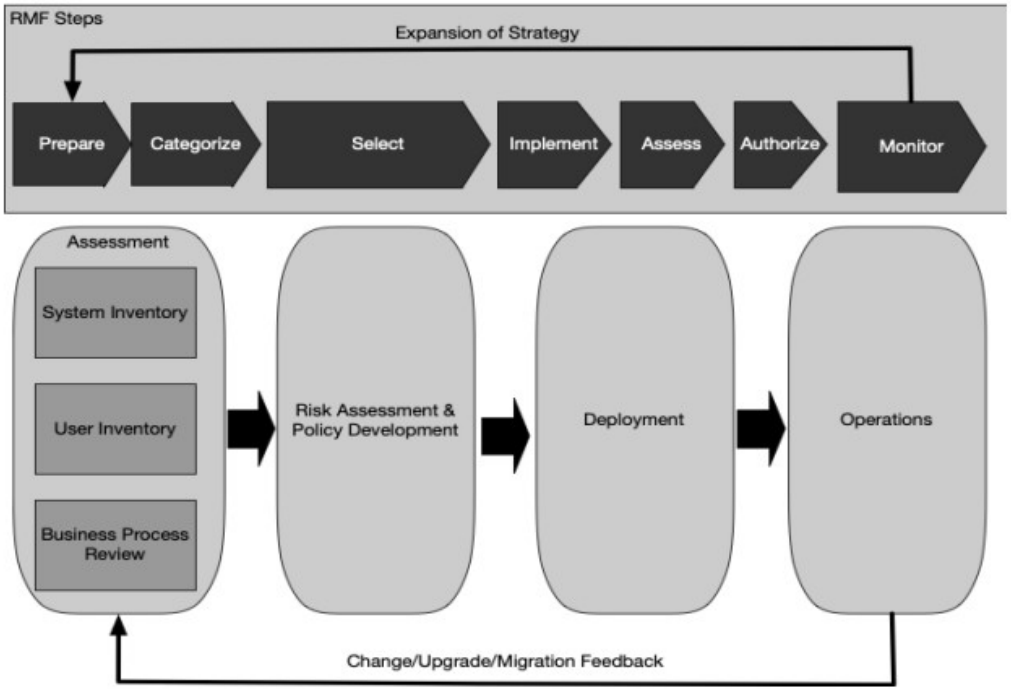


Figura 27 – Equivalencia con el marco de gestión de riesgos.

En la figura, el cuadro superior muestra el esquema que propone el marco de gestión *RMF* de *NIST*. Por debajo, se presenta un paralelo que comienza a la izquierda con los tres relevamientos descritos anteriormente, y sigue con la evaluación de riesgos (*Risk Assessment*), para finalmente concretar el despliegue (*Deployment*) y comenzar el camino hacia la operación sostenida (*Operations*).

Para la etapa de evaluación de riesgos, luego de clasificar los procesos del negocio *NIST* sugiere el comenzar con aquellos que presenten un riesgo menor. Y señala como buenos candidatos para empezar a aquellos procesos que involucren la utilización de recursos en la nube.

Otros factores también deben ser tomados en cuenta al seleccionar los primeros procesos candidatos para la migración, tales como su nivel de impacto sobre sistemas, el monitoreo y las entidades. Se prefiere en este caso a los procesos que impacten menos sobre la plataforma total.

Luego de elegir el o los procesos candidatos para la migración a *ZTA*, se deberá trabajar en la selección de soluciones de hardware y software posibles, y en este caso se consideran los siguientes factores:

- Si la solución requiere de instalar algún agente.
- Si está diseñada para operar en la nube o en instalaciones propias.
- Si permite el monitoreo y la recolección de datos para análisis.
- Su compatibilidad con distintos protocolos, servicios y aplicaciones.
- Si requiere cambios en la conducta del sujeto.

El despliegue inicial entonces, una vez desarrolladas las políticas de acceso preliminares y seleccionadas las herramientas a utilizar, se realiza en modo de prueba piloto y bajo observación.

Durante esta prueba piloto pueden coexistir los procesos tal como operaban anteriormente y bajo su nuevo esquema de funcionamiento, y se registrarán las solicitudes de acceso concedidas para saber si son correctas.

Una vez que la prueba piloto finaliza y existe suficiente confianza en las nuevas políticas desarrolladas, entonces la organización entra en la fase operativa estable y se puede volver al inicio, para abordar otro proceso.

Cabe señalar que, ante cambios de cualquier tipo en un proceso ya migrado, se deberá comenzar otra vez desde el principio realizando los tres relevamientos ya citados.

3.2 La Orden Ejecutiva 14028

En mayo de 2021, el gobierno de los Estados Unidos bajo la administración del presidente Joe Biden emitió la Orden Ejecutiva 14028 [62], instando a las agencias federales de ese país a mejorar la ciberseguridad nacional y en particular, avanzar hacia una arquitectura de *Zero Trust*.

Si la *ZTA* de *NIST* que revisamos en la sección anterior marcó un hito importante en la línea de tiempo de la Confianza Cero, esta orden ejecutiva es sin duda el siguiente.

Figura 28 – La Orden Ejecutiva 14028 de Joe Biden.

A partir de esta publicación, los equipos de seguridad de las agencias federales de ese país no solo cuentan con la formalización conceptual de *NIST*, sino también con una directiva específica gubernamental que respalda al enfoque *Zero Trust* de manera oficial.

La orden ejecutiva, además, no solo impacta a esos organismos públicos, sino también a todos los proveedores que les brindan sus servicios. Y de esa manera, se extiende hacia el sector privado.

Si bien la *EO* 14208 es una disposición estadounidense, bien sabemos que tanto las indicaciones de *NIST* como las directivas de este tipo tienen un alcance a nivel de guía de carácter mundial.

Este decreto presidencial no se centra únicamente en la Confianza Cero y cubre numerosos requerimientos, tales como la adopción de herramientas para el monitoreo continuo de las terminales (*EDR – Endpoint Detection and Response*), autentificación multifactorial *MFA*, y el cifrado de los datos en tránsito y reposo, entre muchos otros.

Es de notar lo que expresa el segundo párrafo de su primera sección, indicando que mejoras incrementales no proveerán la seguridad necesaria, y que el gobierno federal debe realizar "cambios audaces" (*bold changes*) e inversiones significativas a fin de defender las instituciones vitales que apuntalan al sistema de vida norteamericano.

Lo expresado resulta un tanto confuso, dado que la propia recomendación de *NIST* en su apartado séptimo que vimos anteriormente habla sobre una migración gradual hacia *ZT* y, además, los organismos estatales siempre se encuentran retrasados en su avance con respecto a la industria, por lo que las mejoras no pueden ser otras que por incrementos.

La *EO* menciona al término *Zero Trust* en 11 instancias a través de todo el texto, que cubre unas 30 carillas aproximadamente. La primera mención surge en sección tercera, sobre la modernización de la ciberseguridad del gobierno federal. Y luego en la sección décima, que enumera definiciones.

En la sección tercera, se dispone que el gobierno federal debe adoptar las mejores prácticas en seguridad, avanzar hacia una arquitectura de Confianza Cero, acelerar la migración hacia servicios seguros en la nube, coordinar y centralizar el acceso a la información sobre ciberseguridad e invertir en tecnología y personal para el logro de estos objetivos.

Los jefes de cada agencia federal deberán desarrollar un plan para implementar una *ZTA* basada en las recomendaciones de migración de *NIST* dentro de los 60 días de emitido el decreto, e informar mediante un reporte al director de la oficina de gestión y presupuesto (*OMB – Office of Management and Budget*) y al consejero de seguridad nacional (*National Security Advisor*).

En cuanto a la migración de los sistemas hacia la nube, la *EO* establece que dentro de los 90 días, el director de la *OMB*, en conjunto con el secretario de seguridad nacional, el director de la agencia de ciberseguridad y seguridad de la infraestructura (*CISA - Cybersecurity & Infrastructure Agency*), y el programa federal de gestión de riesgo y autorizaciones (*FedRAMP - Federal Risk and Authorization Management Program*) [63], deberá desarrollar una estrategia de seguridad para este tipo de servicios y proveerla al resto de las agencias federales, a fin de que también se acerquen a una *ZTA*.

El decreto en su sección décima párrafo (k), incluye la definición del término *Zero Trust Architecture*, que es de interés para este trabajo.

Esta definición propone que la *ZTA* es un modelo de seguridad, un conjunto de principios sobre el diseño de los sistemas, y una estrategia coordinada de ciberseguridad y gestión de esos sistemas basada en la suposición de que las amenazas existen tanto por dentro y por fuera de los límites de las redes tradicionales.

Es importante notar que esta *EO* 14028 es no solo un hito importante en la línea de tiempo de nuestro tema de estudio, sino que también involucra a diferentes agencias federales y organismos públicos de importancia que están relacionados con la seguridad informática tales como *NIST*, *CISA*, la *OMB*, y el programa *FedRAMP* entre otras.

Y no solo relaciona e involucra a estas agencias, sino que dispara una serie de iniciativas y publicaciones esenciales que veremos en las secciones a continuación. Entre ellas, el modelo de madurez de *CISA*, la arquitectura de referencia del Departamento de Defensa (*DoD*), y más.

Existen opiniones encontradas en los numerosos artículos surgidos a partir de la emisión del decreto. Algunos creen que ha sido un impulso hacia la modernización del sector público en los Estados Unidos, donde el sector privado se encuentra siempre mucho más avanzado.

En todos los casos, se trata de una decisión que eleva al concepto de Confianza Cero al nivel de políticas públicas oficiales.

3.2.1 El Memorándum M-22-09

Acompañando al decreto del presidente Joe Biden en el siguiente año con fecha enero 26, surge este memorándum M-22-09 del director de la *OMB* dirigido a las cabezas de las agencias federales [64].

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

Figura 29 – El memorándum M-22-09.

Su asunto aclara la intención de este, “Moviendo al gobierno de los Estados Unidos hacia los principios de ciberseguridad de Confianza Cero”, y fija plazos ciertos para la concreción de estándares y objetivos específicos.

En particular, declara que establece una estrategia federal basada en la *ZTA*, y requiere que las agencias cumplan con estos objetivos hacia el final de año fiscal 2024.

El memorándum no solo se refiere a la arquitectura de Confianza Cero que es su tema central, sino que además recomienda el aprovechar los beneficios de los servicios en la nube.

Se trata entonces del plan concreto de implementación para la orden ejecutiva que vimos en el punto anterior.

Este documento se vincula con varias fuentes, pero principalmente con dos que analizaremos en las siguientes secciones.

La primera de ellas es la “Arquitectura de Referencia de Confianza Cero del Departamento de Defensa”, de la cual toma sus principios (*tenets*), y la segunda y quizás más importante es el “Modelo de Madurez de Confianza Cero” de la agencia *CISA*, en base al cual organiza los objetivos planteados.

En el memorándum, se describe al enfoque de *ZT* como un verdadero cambio de paradigma. Y se visualiza a un gobierno federal implementando:

- Cuentas de usuario centralmente administradas.
- Dispositivos gestionados y monitoreados.
- Sistemas aislados entre agencias, cifrando el tráfico.
- Aplicaciones verificadas y accesibles en la red Internet.
- Datos categorizados y reglas de acceso para protegerlos.

Esta visión pone énfasis entonces en servicios tales como la autentificación multifactorial, el cifrado de las comunicaciones, la eliminación de los accesos por *VPN*, las pruebas de seguridad para las aplicaciones, y la clasificación de los datos.

Los objetivos que las agencias deben cumplir a fines de 2024 están alineados con esa visión y basados en los cinco pilares del modelo de madurez de *CISA*.

Se reconoce en el memorándum que el plan involucra grandes esfuerzos, cambios de mentalidad y la necesidad de la expresa participación ejecutiva.

Al mismo tiempo, se aclara que esta comunicación propone únicamente un enfoque a grandes rasgos, y se recomienda el usar las referencias que incluye al final como guía para la implementación específica.

3.3 El Modelo de Madurez de *CISA*

La línea de tiempo de la Confianza Cero se vio marcada en el año 2020 por la publicación fundacional de *NIST*, y luego por la orden ejecutiva y el memorándum surgidos en los dos años posteriores.

En agosto de 2021, la agencia de ciberseguridad y seguridad de la infraestructura (*CISA - Cybersecurity and Infrastructure Security Agency*) publica el primer instrumento oficial destinado a medir el nivel de avance en la adopción de *Zero Trust*.

Este documento, denominado "Modelo de Madurez para la Confianza Cero" (*Zero Trust Maturity Model*) [65] , está íntimamente relacionado con la orden ejecutiva y es una de las dos fuentes principales de base para el memorándum. El mismo ha sido actualizado a su versión 2.0 en abril de 2023.

Su nombre es claro en cuanto a la finalidad, que es ofrecer una herramienta para medir de forma progresiva, el nivel de adecuamiento de cada agencia, y ello se hace extensivo también a cualquier organización privada que desee implementar este modelo.

Desde el inicio de la Confianza Cero y hasta este aporte de *CISA* ya se contaba con tres acrónimos. *ZT* para el concepto inicial, *ZTA* para la arquitectura, *ZTX* para el ecosistema según *Forrester* y ahora, *ZTMM* para su madurez.

La propia publicación expresa en sus párrafos iniciales que este *ZTMM* es uno de varios caminos que pueden ser adoptados por las organizaciones para su plan de transición. Más adelante veremos que existe por lo menos un modelo adicional de referencia.

Por otra parte, el trabajo de *CISA* tiene como fundamento a su vez a lo planteado originalmente por Forrester en su ecosistema extendido que ya vimos antes, de donde provienen sus pilares.

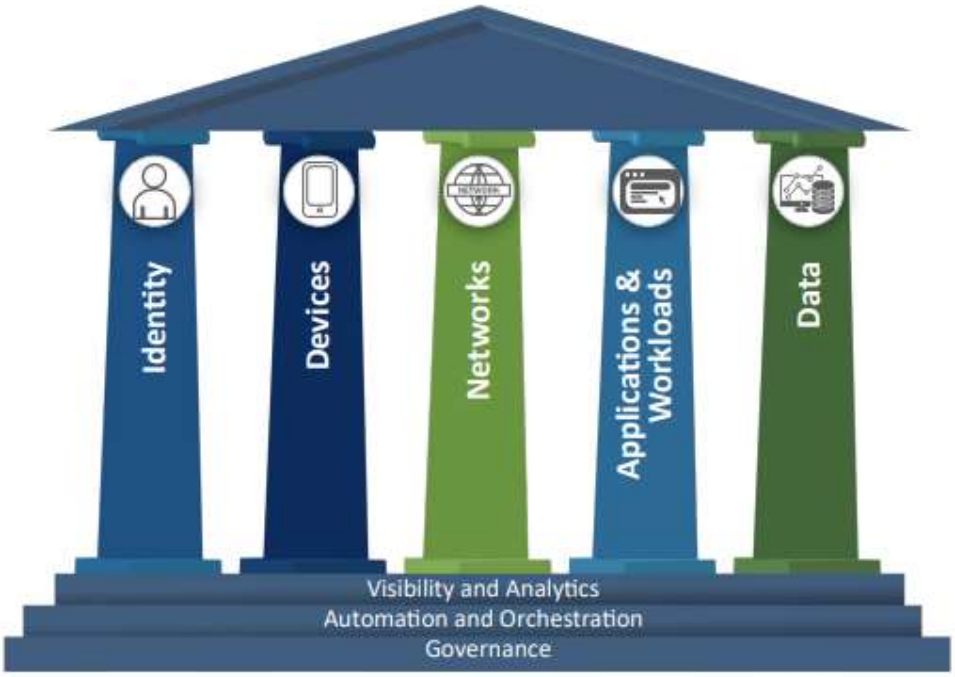


Figura 30 – Los cinco pilares del Modelo de Madurez de *CISA*.

La figura superior esquematiza el modelo propuesto por la agencia estadounidense, el cual consta de cinco pilares, y tres capacidades que los atraviesan transversalmente.

Los cinco pilares son identidad (*Identity*), dispositivos (*Devices*), redes (*Networks*), aplicaciones (*Applications & Workloads*) y datos (*Data*).

Las tres capacidades comunes a todos ellos son visibilidad y análisis (*Visibility and Analytics*), automatización y orquestación (*Automation and Orchestration*), y gobierno (*Governance*).

Este modelo contempla un proceso gradual de implementación en el cual se prevén avances menores hacia el estado óptimo en cada uno de los pilares de forma individual, y alguno puede evolucionar más velozmente que otros. En algún momento, se requerirá el sincronizarlos.

Vale aclarar que tanto los pilares como el resto del modelo están basados en la lista de siete principios que propone *NIST* en la SP 800-207.

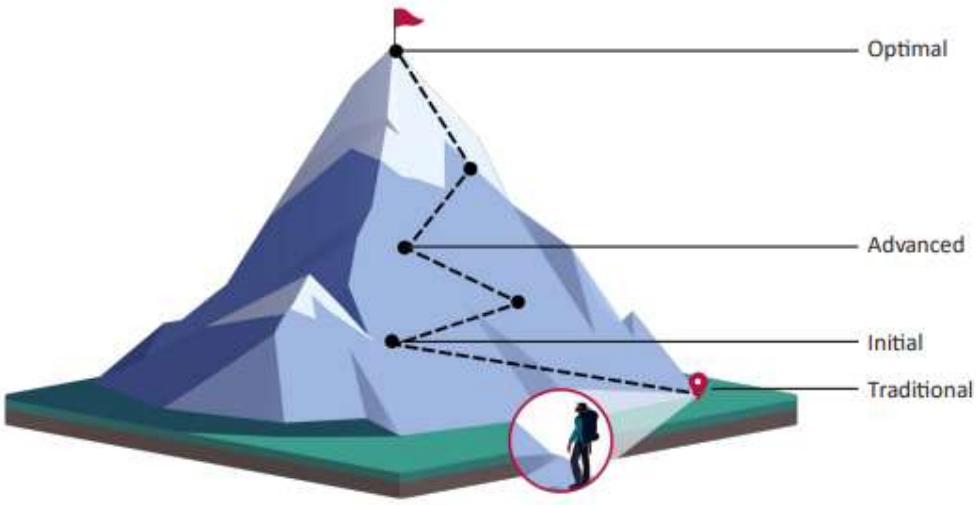


Figura 31 – El camino hacia la madurez.

El *ZTMM* especifica un "camino hacia la madurez" (*maturity journey*) que, como se ve en la figura superior, evoluciona desde el enfoque tradicional y consta de tres etapas. Un estado inicial, uno avanzado, y finalmente el óptimo. El uso de una montaña en el gráfico no es casual.

El enfoque tradicional consiste en ciclos de vida manuales de inicio a fin, políticas estáticas, soluciones y sistemas externos aislados en cada pilar, respuestas manuales y poca correlación entre todos estos componentes, la registración y la telemetría.

El estado inicial supone justamente una primera aproximación hacia la automatización en todos los frentes, y alguna coordinación entre los pilares. Aquí se comienza a integrar las partes antes aisladas.

Un estado avanzado ya significa el uso de controles automatizados, y políticas más configuraciones coordinadas entre los pilares. Visibilidad y control de identidades centralizados. El concepto de menor privilegio ahora dependiendo de forma dinámica del riesgo y de la postura de seguridad, y en general, una acción concurrente a través de toda la organización.

Por último, se encuentra el estado óptimo, al cual quizás nunca se llegue, o que suponga un esfuerzo continuo sin punto final de concreción.

En este estado, los ciclos de vida están completamente automatizados y se completan en modalidad “justo a tiempo” (*just in time*). También lo están la asignación de atributos a los recursos y a los activos, que reportan su estado. Y las políticas son dinámicas y se ajustan en base a disparadores automáticos observados.

El acceso basado en el menor privilegio también se ajusta automáticamente. La interoperabilidad y el monitoreo continuo funcionan a través de los pilares, y la visibilidad es centralizada, obteniendo una visión integral de la situación.

Vale aclarar a qué se refieren las tres capacidades enumeradas anteriormente, de las que dijimos que atraviesan los cinco pilares.

La visibilidad se refiere a la observación de las características de un ambiente y los eventos que allí se generan. El análisis de los datos relacionados con la ciberseguridad puede servir como base para las decisiones sobre políticas, acciones de respuesta y ayudar a componer un perfil de riesgos para desarrollar medidas de seguridad proactivas previas a la ocurrencia de un incidente.

En cuanto a la automatización y la orquestación, se trata de utilizar herramientas automatizadas y flujos de trabajo orquestados para el desarrollo de los productos y servicios incluyendo seguridad, interacción y monitoreo.

El gobierno por su parte corresponde a la definición y el refuerzo de políticas, procedimientos y procesos, dentro y a través de los pilares, para mitigar los riesgos y, en el caso particular de las agencias, para cumplir con requerimientos federales.

Este documento muestra primero una vista de alto nivel de las etapas de evolución para cada uno de los pilares. Incluimos esa vista en la figura siguiente solo a modo ilustrativo, y no haremos una descripción detallada de cada elemento dado que no es la finalidad del presente trabajo.

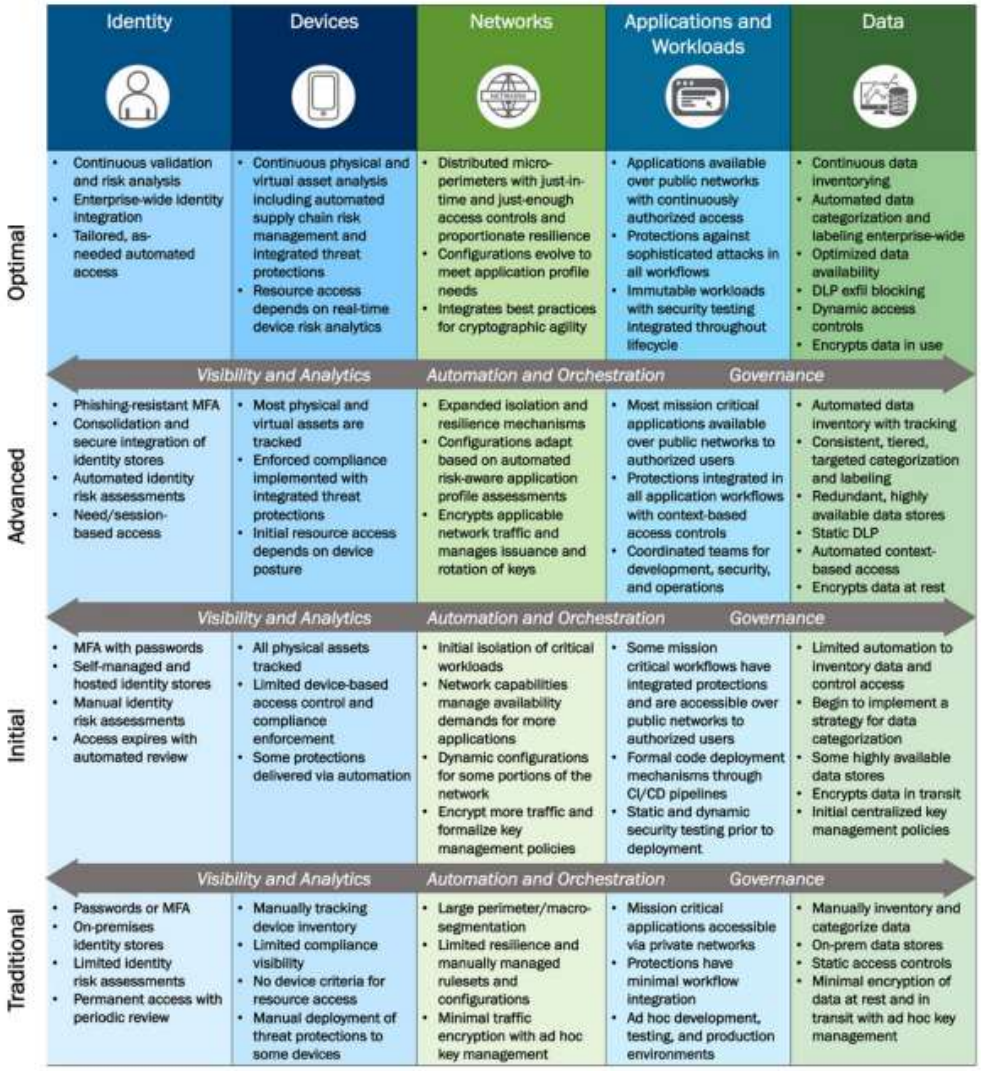


Figura 32 – Una vista de alto nivel del *ZTMM*.

El resto de la publicación describe con más detalle, las etapas de avance para cada pilar, en base a cada una de sus funciones y las tres capacidades que describimos anteriormente. También se incluye una definición de cada pilar al principio.

Al final, en los apartados 6 y 7, se incluyen referencias generales y particulares de *CISA*, algunas de las cuales son de gran relevancia y veremos a continuación.

3.4 La Arquitectura del *DoD*

En febrero de 2021 se publica la primera versión de un trabajo conjunto entre la Agencia de Sistemas de Información de Defensa (*DISA - Defense Information Systems Agency*) y la tan conocida Agencia de Seguridad Nacional (*NSA - National Security Agency*).

Este trabajo, también mencionado en el memorándum que vimos anteriormente, se denomina “Arquitectura de Referencia de Confianza Cero del Departamento de Defensa” (*Department of Defense (DoD) Zero Trust Reference Architecture*) [66].

Tal como viene sucediendo con muchos de los documentos claves que ya componen la “historia oficial” de *Zero Trust* como el modelo de madurez de *CISA*, esta publicación ya cuenta también con su versión 2.0, de Julio de 2022.

Sin duda cualquier organización interesada en tomar alguna arquitectura de referencia para usar como guía de implementación de *ZT*, encontraría a la visión del Departamento de Defensa de los Estados Unidos como una fuente más que valiosa.

Este documento es extenso - 104 páginas - y además complejo, presenta conceptos nuevos e incluye numerosos gráficos. Intentaremos aquí tomar lo más relevante de tamaña exposición, comenzando por analizar su primera sección, la cual describe su propósito y objetivos estratégicos.

En su introducción, un nuevo acrónimo *CS RA* (*Cyber Security Reference Architecture*) refiere a la arquitectura de ciberseguridad, se enumeran los documentos del propio *DoD* utilizados como fuente y se establece que este es el enfoque para adoptar, aclarando también que el mismo estará centrado en los datos y que debe infundir los principios de *ZT*.

Con respecto a su propósito, se explica que la *CS RA* es un marco de trabajo (*framework*) que sirve como guía utilizando pilares y principios. Se trata entonces de una guía conceptual, centrada en las capacidades.

La metodología con la que se organiza la información y los gráficos en esta referencia está basada en el “Marco de Trabajo Arquitectónico del Departamento de Defensa” (*DoDAF – Department of Defense Architectural Framework*) [67].

La arquitectura conceptual entonces se presenta principalmente utlilizando “Vistas Operacionales” (*OV - Operational Views*), y “Vistas de Capacidades” (*CV – Capability Views*).

Las *CV-1* describen la visión estratégica, mientras que las *OV-1* describen el problema y las oportunidades para un ambiente funcional determinado.

Luego las *CV-2* exponen la taxonomía de capacidades relacionadas con las oportunidades y organizadas en base a su relación con pilares y recursos. Finalmente, las *OV-2* explican cómo se relacionan los recursos entre sí en un caso arquitectónico dado.

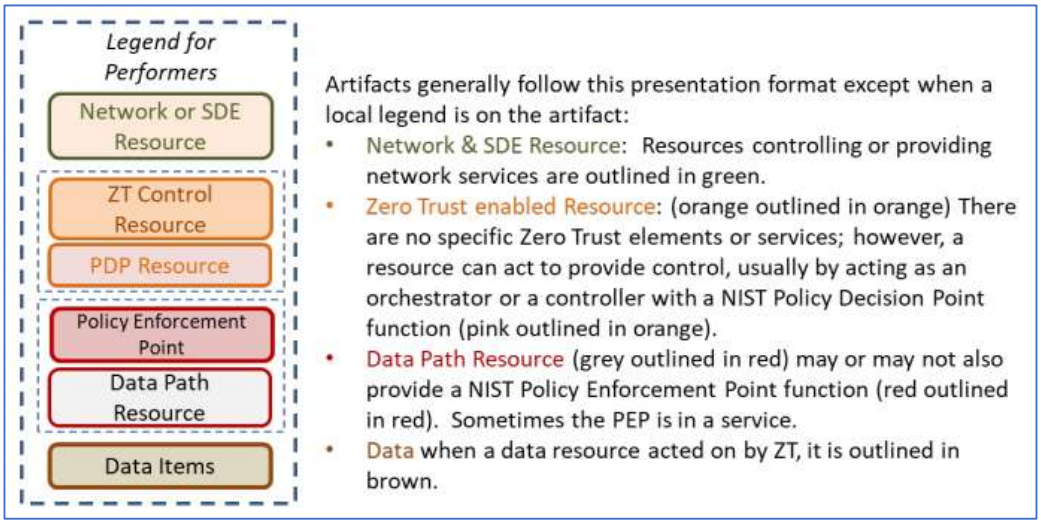


Figura 33 – Referencia de Ejecutantes.

Un primer gráfico describe el formato de presentación para los recursos que participan en cada diagrama en el documento, y su título es “Referencia de Ejecutantes” (*Legend for Performers*).

De arriba hacia abajo la referencia describe a los recursos de red físicos o establecidos por software (*Network and SDE Resource*), recursos que funcionan asociados a un *PDP*, recursos que operan asociados a un *PEP* dentro del camino de datos (*Data Path*), y, por último, los datos (*Data Items*).

Una vez realizadas la introducción y presentada la referencia, comienza la descripción de la visión y los objetivos estratégicos utilizando el marco de referencia y sus vistas.

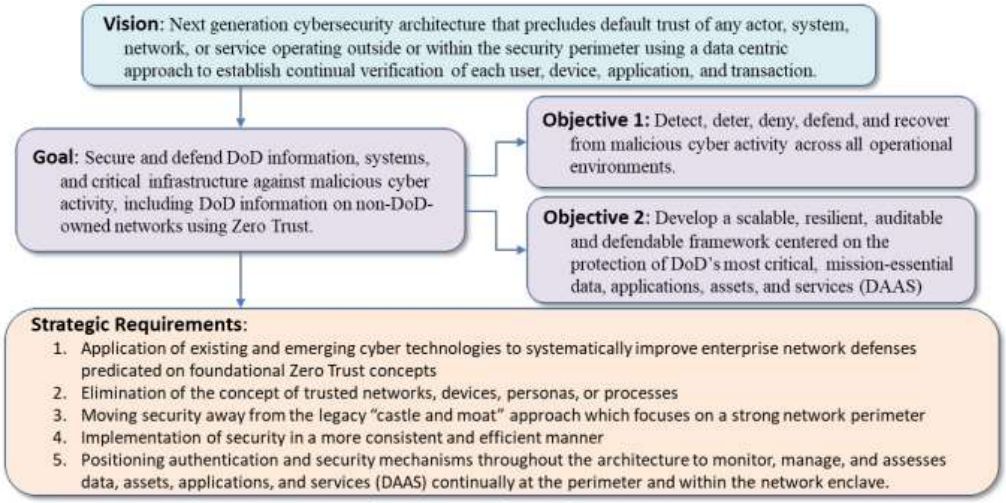


Figura 34 – Visión y Objetivos (*CV-1*).

En cuanto a la visión, se propone una arquitectura de ciberseguridad de "próxima generación" (*next- generation*) que imposibilite una confianza asumida para cualquier actor en la red interna o externa, aplicando verificación continua de usuarios, dispositivo, aplicaciones y transacciones.

El objetivo general es defender redes críticas sean o no del Departamento de Defensa ante ataques cibernéticos. Esto incluye la defensa y recuperación ante cualquier actividad maligna en todos los ambientes operativos. Y desarrollar un marco de trabajo escalable, resiliente, auditable y defendible.

El segundo objetivo de este gráfico introduce un nuevo acrónimo que será de importancia en nuestra discusión sobre *ZT*: Datos, aplicaciones, activos y Servicios (*DaaS – Data, Applications, Assets, and Services*).

Los requisitos estratégicos expuestos en la sección inferior de la figura incluyen el aplicar cualquier ciber tecnología emergente que fortalezca las defensas, basadas en conceptos de la Confianza Cero.

Eliminar el concepto de redes, dispositivos, personas o procesos confiables, y el enfoque del perímetro fijo. Y situar a través de toda la arquitectura mecanismos para efectuar monitoreo y verificación constante.

Cabe aclarar que la nueva arquitectura propuesta con esta visión y estos objetivos tiene asignado también un nuevo acrónimo, *ZT RA*. Y se trata de la evolución del concepto citado al principio, la *CS RA*.

A continuación, aparecen dos gráficos que responden a la categoría *OV-1*, aunque no tan alineados con su definición dado que se están planteando conceptos de muy alto nivel.

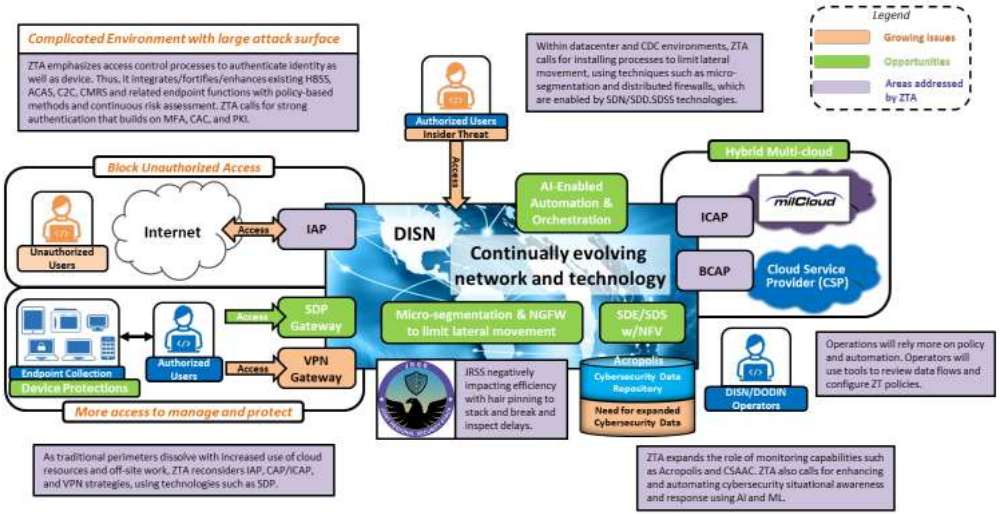


Figura 35 – Declaración del Problema (*OV-1*).

La figura anterior presenta el primero de ellos, denominado “Declaración del Problema” (*Problem Statement*). Aquí se pretende, como su nombre lo indica, definir cuál es la situación que se desea abordar.

No vamos a referenciar en detalle todo su contenido, y se insta al lector a que vea el gráfico con mayor detalle en el propio documento del *DoD*. Sí vamos a comentar sobre sus principales aspectos.

La leyenda situada en el recuadro superior derecho muestra los temas de importancia que aborda este gráfico. En naranja, se señalan los problemas crecientes (*Growing Issues*).

Estos incluyen un ambiente complejo con una gran superficie de ataque, la necesidad de bloquear accesos no autorizados, mayor acceso para administrar y proteger la red, la existencia de actores malignos dentro de la red, y la necesidad de expandir la base de datos de ciberseguridad.

En verde, se indican las oportunidades. Y estas incluyen la protección de dispositivos, el uso de puertas de enlace como parte de un perímetro definido por software, la microsegmentación en la red interna en combinación con cortafuegos de última generación, la automatización y orquestación basadas en inteligencia artificial, más la virtualización de redes.

Se trata de una arquitectura centrada en los datos (*data centric*), con políticas de acceso dinámicas sobre el plano de control, utilizando inteligencia artificial e integrando todas las nuevas tecnologías a través de interfaces de programación de aplicaciones (*API - Application Programming Interface*).

Finalmente, en violeta, se señalan las áreas donde la *ZTA* puede incidir o hacer una diferencia.

Para el ambiente complejo, la autentificación de identidades y de dispositivos, haciendo uso de múltiples factores y cifrado de clave pública. Para bloquear usuarios no autorizados, el control a través de puntos de acceso por Internet (*Internet Access Points*). Para la administración de la red, puertas de enlace de redes privadas virtuales (*VPN Gateway*).

La *ZTA* llama al uso de la inteligencia artificial y el aprendizaje automático (*Machine Learning*) [68] para mejorar las actividades de monitoreo y respuesta. También se considera el uso del perímetro definido por software, la virtualización de redes y nuevas técnicas de acceso a los recursos en la nube.

Los analistas y operadores por su parte utilizarán la automatización y sus herramientas para revisar flujos de trabajo y configurar políticas.

El segundo gráfico que puede verse a continuación describe el "Ambiente Objetivo" (*Target Environment*), es decir, el resultado final esperado al cual no se va a llegar inmediatamente.

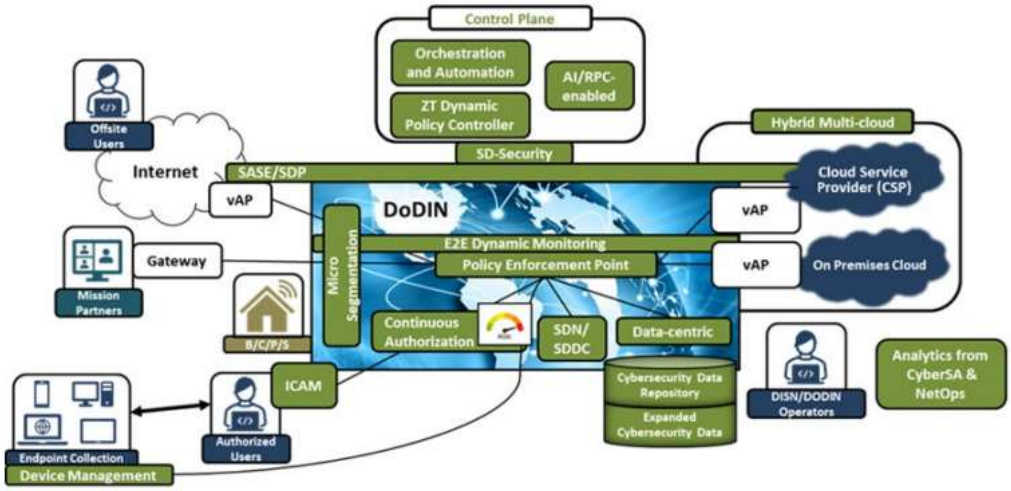


Figura 36 – Ambiente Objetivo (*OV-1*).

Aquí tampoco vamos a describir cada elemento del gráfico, y nuevamente se sugiere al lector verlo en el documento. Mencionaremos algunos de los detalles más relevantes.

Observar que esta propuesta incluye en la parte superior al plano de control (*Control Plane*). En él, se utilizan la orquestación y la automatización en conjunto con inteligencia artificial y robótica (*RPA – Robotic Process Automation*) [69] para lograr políticas de acceso dinámicas y enriquecidas.

Notar también que, a través de todo el ambiente ideal se distribuyen numerosos puntos de control de accesos.

Y el primer paso para las autorizaciones es sin duda la implementación de una solución centralizada de administración de credenciales y accesos (*ICAM – Identity Credential and Access Management*) [70].

Obviamente, estos controles deben incluir a un sistema de verificación de la higiene de los dispositivos, así como un monitoreo continuo de la actividad de cada entidad. Esto resulta en una calificación también dinámica basada en todo ello y la telemetría.

En los puntos de ingreso desde el exterior, correspondientes a usuarios remotos o conexiones con los recursos en la nube, se disponen puntos de acceso virtuales (*vAP - Virtual Access Points*). Y la combinación de redes definidas por software más la microsegmentación, previenen los movimientos laterales.

La protección en sí de los datos, elementos centrales de la arquitectura, se realiza combinando la prevención de pérdida de datos (*DLP – Data Loss Prevention*) [71], y la gestión de permisos (*DRM – Data Rights Management*) [72] para prevenir su exfiltración.

Ya hemos mencionado la importancia del continuo monitoreo sobre las transacciones. Esta observación debe ser unificada, y mejorada a través del análisis de usuarios y entidades (*UEBA – User and Entity Behavior Analysis*) [73].

3.4.1 Pilares y Principios

Esta breve sección dentro del documento del *DoD* es de interés para este trabajo ya que, en cierta medida, extiende o modifica las definiciones ya planteadas por *NIST* y otros actores hasta su publicación.

Comienza enumerando los cinco principios de la Confianza Cero, y nótese que difieren en su orden, cantidad y concepto respecto de los siete originalmente planteados por *NIST*.

1	**Asumir un ambiente hostil**, interno y externo. Todos los dispositivos y entidades son tratados como no confiables.
2	**Suponer que existe una filtración de datos**. Trabajar bajo la presunción de que existe un adversario presente en la red interna.
3	**Nunca confiar, siempre verificar**. El acceso es denegado por defecto, y otorgado en base al menor privilegio.
4	**Aplicar el escrutinio explícito**. El acceso a los recursos es dinámico y consistente, basado en atributos múltiples.
5	**Aplicar el análisis unificado**, incluyendo la conducta y registrando cada transacción.

Tabla 2 – Los 5 principios de *Zero Trust* según el *DoD*.

También se menciona que, la práctica habitual de utilizar la autentificación del cliente o mutua a través de *PKI* será mejorada aplicando esquemas múltiples de autorización y autentificación.

A continuación, se enumeran los pilares de la Confianza Cero tal como es concebida por este organismo público, los cuales provienen tanto de la estrategia que aquí mismo se plantea como de los ya establecidos por la industria.

Los define como áreas claves donde focalizar la implementación de los controles de *ZT*. Y los muestra en la figura como piezas entrelazadas donde el centro corresponde a la protección de los datos, el objetivo más importante.

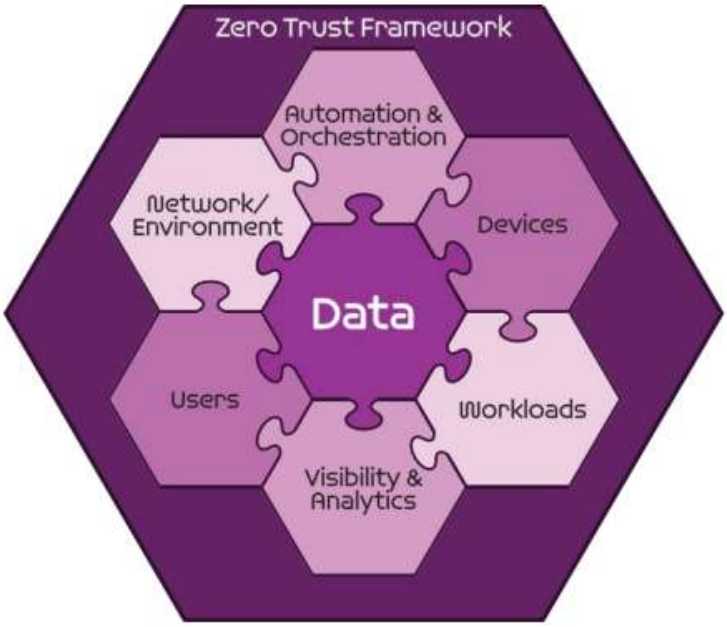


Figura 37 – Los pilares de la Confianza Cero según el *DoD*.

Si se comparan estos pilares con los que vimos anteriormente en el modelo de madurez de *CISA*, se puede inferir que se trata de casi los mismos elementos, salvo el gobierno, ordenados en forma diferente.

En la descripción de los siete componentes del gráfico, donde los datos (*Data*) son el centro de atención, se plantea que un claro entendimiento de los datos, las aplicaciones, los activos y los servicios (*DAAS – Data, Applications, Assets and Services*) es crucial para una implementación exitosa de la arquitectura.

Para lograr ese entendimiento, la organización deberá categorizarlos de acuerdo con su criticidad, desarrollando en base a ello una estrategia de administración de datos.

Y para materializar dicha estrategia, se debe recurrir a soluciones tales como el etiquetado granular de datos, esquemas, el cifrado en tránsito y reposo, ambientes de red definidos por software, la administración de derechos digitales *DRM*, y la prevención de pérdida de datos *DLP*.

Al referirse al componente usuarios (*Users*) se explica que la organización debe contar con la posibilidad de autentificar, autorizar y monitorear el acceso a los *DAAS*, por parte de personas y otras entidades que no lo son. Esto se logra con la autentificación multifactorial, y la asignación de privilegios de acceso (*PAM – Privileged Access Management*) [74].

En cuanto a los dispositivos (*Devices*) las recomendaciones son las ya conocidas, y cubren la capacidad de administrar su postura de seguridad e inspeccionarlos en tiempo real. Una interesante referencia cita al uso de módulos de plataforma confiable (*TFM – Trusted Platform Modules*) [75].

El ambiente de red (*Network / Environment*) debe estar segmentado tanto en forma física como lógica. Aislado y controlado con acceso granular basado en políticas.

Con respecto a las aplicaciones y cargas de trabajo (*Applications and Workloads*) se incluyen en este aspecto tanto las que se desarrollan en instalaciones propias como aquellas que lo hacen en la nube.

Y se aclara que las cargas de trabajo abarcan toda la pila (*stack*) de funciones desde la capa de aplicación hasta el hipervisor, trayendo así a la discusión el importante tema de las máquinas virtuales.

El proceso de desarrollo de aplicaciones internas debe estar regulado por las prácticas de desarrollo, seguridad y operaciones (*DevSecOps*) [76].

En cuanto a la visibilidad y el análisis (*Visibility and Analytics*) las recomendaciones son similares a las de *CISA*. Y para la automatización y la orquestación, se menciona la incorporación de *SOAR* (*Security Orchestration, Automation and Response*) [77] y la utilización de dispositivos *SIEM*.

3.4.2 Capacidades

Esta sección presenta una serie de capacidades y tecnologías que permiten realizar funciones de Confianza Cero en un ambiente determinado.

Estas capacidades se relacionan de forma directa, o en ciertos casos en relación de uno a varios o viceversa, con los pilares vistos en el punto anterior. Algunas capacidades incluso abarcan a todos los pilares.

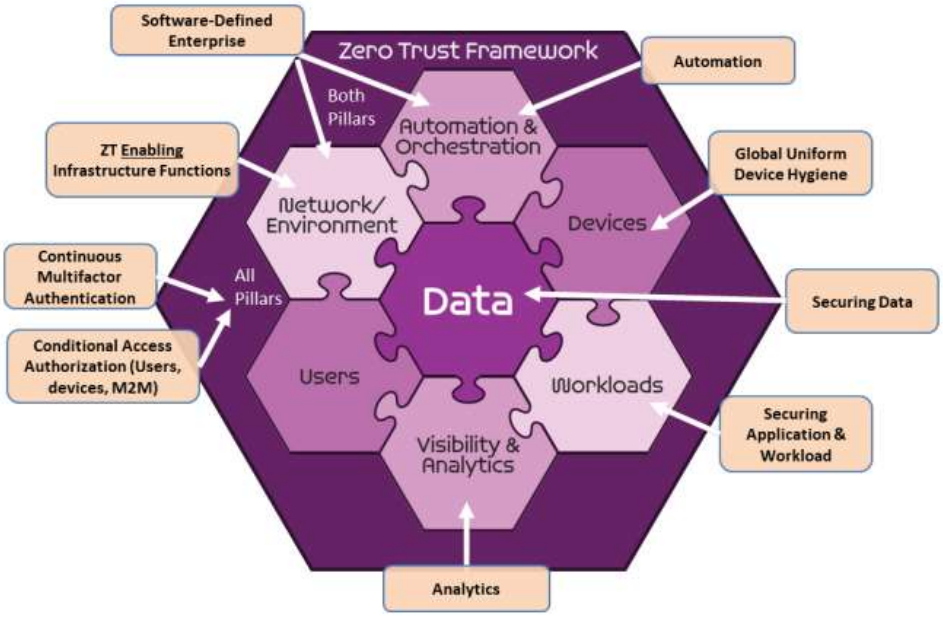


Figura 38 – Mapeo de capacidades a pilares.

Cabe señalar que las capacidades incluidas en la figura representan el nivel de avance tecnológico actual, que puede ser mejorado en las futuras iteraciones de diseño de la arquitectura.

Por otra parte, este diseño con capacidades dispuestas en distintas capas en forma de árbol como se verá a continuación corresponde a una visión de estado final y no a una implementación exacta.

Arriba y a la izquierda del gráfico anterior se puede notar que la capacidad relacionada con el ambiente definido por software (*Software Defined Enterprise*) afecta a dos de los pilares, tanto el de redes como el de automatización y orquestación.

Para los dispositivos más hacia la derecha, se encuentra la higienización de estos en forma global y unificada (*Global Uniform Device Hygiene*). Y para los datos por supuesto, su segurización (*Securing Data*), al igual que para las cargas de trabajo.

Arriba y abajo la automatización y el análisis son dos capacidades que corresponden con pilares de similar nombre. A la izquierda también, se incluyen las funciones de la infraestructura que habilitan a ZT (*ZT Enabling Functions*) sobre el ambiente de red.

Finalmente, dos capacidades afectan a todos los pilares. La autentificación multifactorial continua (*Continuous Multifactor Authentication*) y la autorización condicional de acceso (*Conditional Access Authorization*). Esta última abarcando a usuarios, a dispositivos y a las transacciones de máquina a máquina (*M2M – Machine to Machine*).

En la terminología de la arquitectura de referencia del Departamento de Defensa, lo que veremos a continuación es una serie de gráficos del tipo “Vistas de Capacidades” en nivel *CV-2*, que exponen su taxonomía en más detalle.

El primer gráfico presenta los agregados de autentificación continua y autorización condicional. Para este y los siguientes, solo haremos referencia a los aspectos más relevantes y se invita al lector a verlos con mayor detenimiento desde el documento original.

Aquí la autentificación continua es un concepto claro aplicable a los usuarios e incluye también a la biometría del comportamiento (*Behavioral Biometrics*) [78], mientras que la autorización condicional apunta tanto a aquellos, sean personas o no, como a los dispositivos.

Nótese que, para los dispositivos en la autorización condicional, las sub-capacidades están muy enfocadas en su auditoría constante, evaluando su estado y haciendo uso de la telemetría como apoyo.

Y también se añade el análisis del comportamiento *UEBA,* el control de accesos por atributos *ABAC* y el ya mencionado *PAM*.

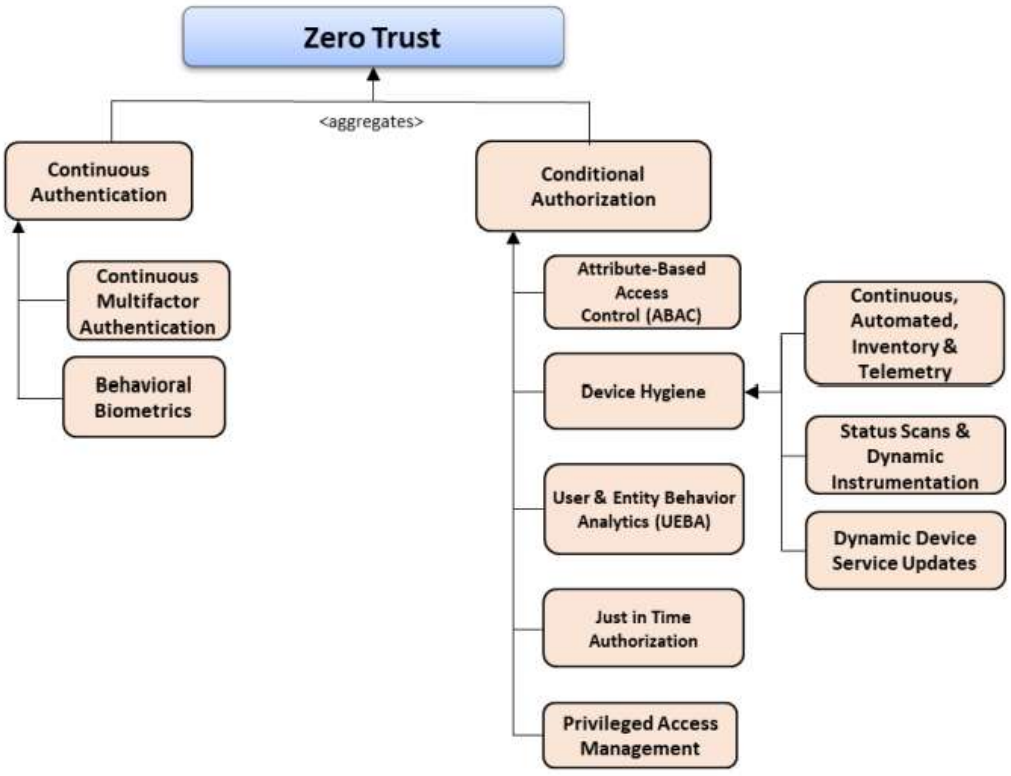


Figura 39 – Taxonomía de capacidades de autentificación y autorización (*CV-2*).

El siguiente gráfico describe tres capacidades agregadas que son la infraestructura que habilita a la Confianza Cero (*ZT Enabling Infrastructure*), la segurización de las aplicaciones y cargas de trabajo (*Securing Applications & Workloads*) y la protección de los datos (*Securing Data*).

En cuanto a la infraestructura, se hace referencia tanto a dispositivos como a nodos en la red, y tanto en instalaciones propias como en la nube, utilizando microsegmentación y perímetros definidos por software.

Para las cargas de trabajo y aplicaciones, los mismos conceptos de microsegmentación, uso de *proxies*, la prevención de movimientos laterales y el correcto desarrollo de software mediante *DevSecOps*.

Se hace hincapié en la futura estandarización de llamadas entre sistemas mediante interfaces de programación de aplicaciones *APIs.*

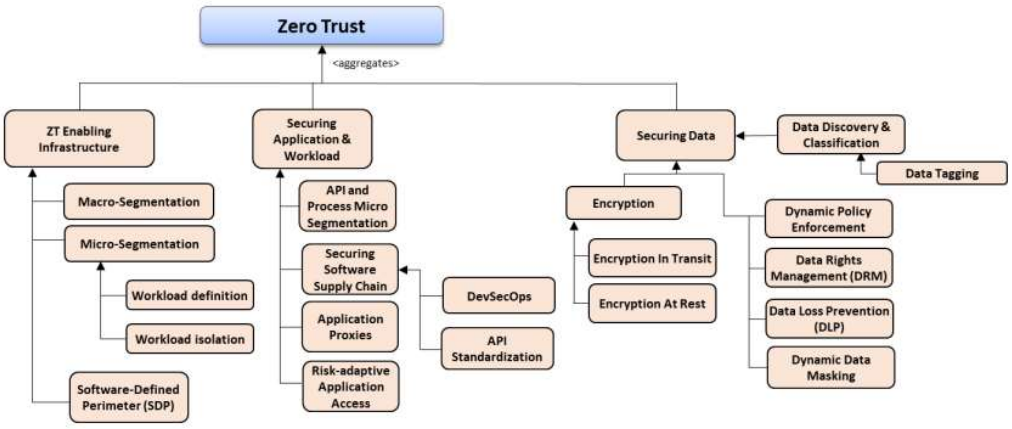


Figura 40 – Infraestructura, cargas de trabajo, aplicaciones y datos (*CV-2*).

En cuanto a los datos, su clasificación y etiquetado (*Data Tagging*), su cifrado en tránsito y reposo, y el uso de técnicas de *DRM* y *DLP* que ya hemos referenciado, junto con el enmascaramiento dinámico (*Dynamic Data Masking*) [79]. En conjunto con políticas también dinámicas.

La tercera figura en este despliegue de la taxonomía de capacidades hace referencia tanto al análisis (*Analytics*) como a la "orquestación de Confianza Cero" (*ZT Orchestration*), a la cual llaman así debido a sus orígenes en las definiciones de *NIST*.

El análisis incluye a la visibilidad, y se compone de una amalgama de funciones para el monitoreo continuo, incluyendo sensores, registros (*logs*), y un aspecto muy importante que es el aprendizaje automático (*Machine Learning*) basado en los eventos observados.

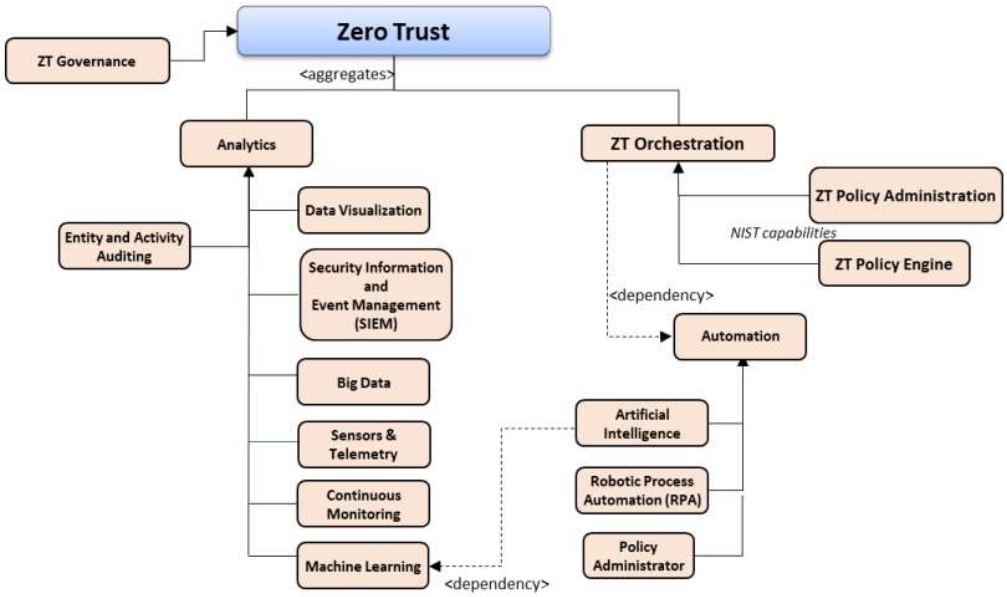


Figura 41 – Taxonomía de capacidades de orquestación *ZT* y análisis (*CV-2*).

Nótese en la figura superior, cómo este aprendizaje automatizado es una fuente de información para la inteligencia artificial aplicada al otro gran agregado, la orquestación *ZT*.

Cuando se hace referencia en este ámbito a la orquestación, se trata de la producción de políticas de acceso de modo dinámico, valiéndose también de la automatización de procesos *RPA*. Esta es la evolución concebida para el futuro.

Una última figura describe las capacidades que habilitan a la Confianza Cero, que son el gobierno de los datos (*Data Governance*) [80], la relación con el marco de trabajo para la administración de riesgos de *NIST* (*RMF - Risk Management Framework*) [81] y lo que este documento llama la "Organización Definida por Software" (*SDE - Software Defined Enterprise*).

Este último concepto *SDE* refiere a la capacidad de crear una capa virtualizada por encima de la infraestructura física, para administrar de forma centralizada y automatizada, todas las funciones de la red, de los sistemas, de la seguridad y los flujos de trabajo.

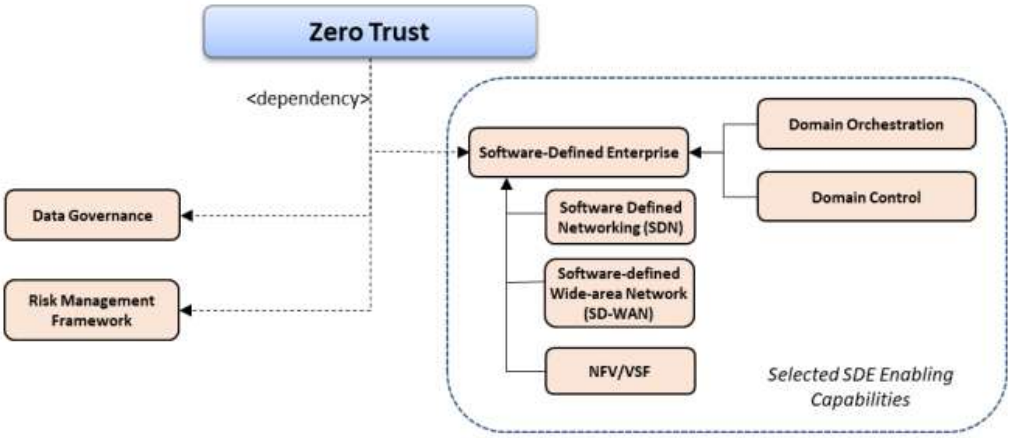


Figura 42 – Taxonomía de capacidades que habilitan a *Zero Trust* (*CV-2*).

A continuación, se presenta una vista operacional de cómo se distribuyen las medidas de seguridad a través de la arquitectura, contando con dos planos separados, uno inferior para la transmisión de los datos, y otro superior para el control y la administración de accesos.

En el sector inferior izquierdo se puede notar que las identidades de personas y las *NPE* se verifican de forma independiente. Las actividades de autorización y autentificación ocurren en numerosos puntos focalizados (*Decision Point*) a través de toda la infraestructura incluyendo usuarios, dispositivos, elementos de la red, aplicaciones y datos.

En cada uno de los *PEP* se envían datos al sistema de análisis que incluye un *SIEM* para desarrollar un nivel de confianza para cada tipo de entidad por separado, lo que luego se combina para obtener la evaluación resultante. El monitoreo de los datos utilizando *DLP* protege contra las exfiltraciones.

El documento del Departamento de Defensa aclara que la línea de base (*Baseline*) para comenzar con cualquier implementación de Confianza Cero consiste simplemente en controlar el acceso a los recursos evaluando el riesgo de los usuarios y los dispositivos.

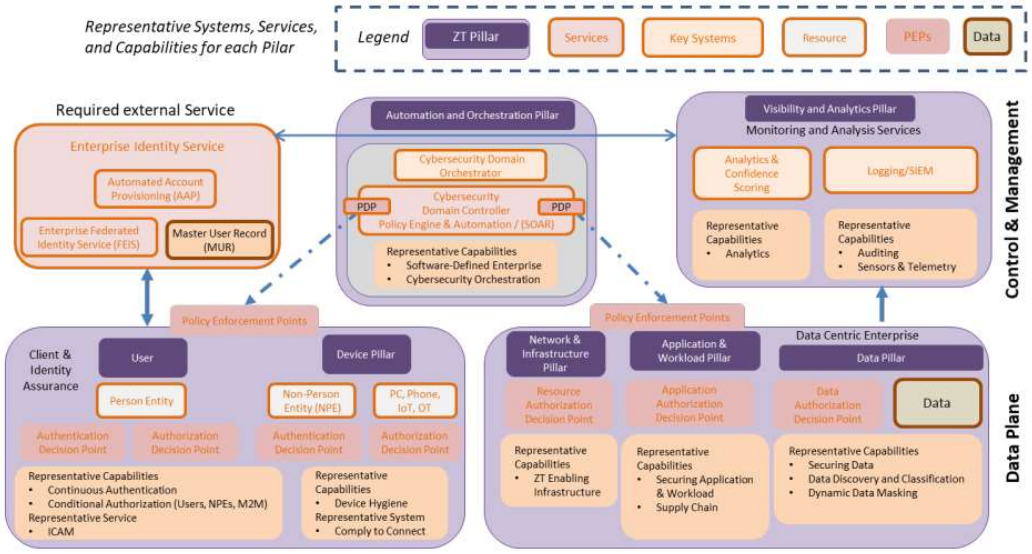


Figura 43 – Mapeo de Pilares, Recursos y Capacidades (*CV-7*).

Como estado final hacia el futuro (*End State*) entonces, se consideran las capacidades que aparecen en el gráfico y que se detallan más en los siguientes párrafos.

El servicio de identidad para la organización (*Enterprise Identity Service*) arriba a la izquierda incluye a las funciones de identidad federada (*FEIS - Federated Enterprise Identity Service*) que permite mantener un registro centralizado y compartido de accesos para habilitar a usuarios y *NPE* de otros organismos a los distintos recursos.

También utiliza el sistema automático de aprovisionamiento de cuentas para los usuarios (*AAP - Automatic Account Provisioning*) y un registro maestro de estos (*MUR - Master User Record*) para llevar un seguimiento de quién tiene acceso a qué recurso.

Volviendo al sector inferior izquierdo además de existir los puntos de decisión para autentificación y autorización, se recomienda implementar un servicio de administración de accesos y credenciales *ICAM*, el cual permite crear representaciones digitales confiables de la identidad de un usuario o *NPE*.

El propio servicio *ICAM* da lugar a la autentificación continua, que combina diferentes estrategias para realizar sus verificaciones repetidamente y casi en tiempo real. Y también habilita la autorización condicional, basada en un chequeo también reiterado de la higiene del dispositivo utilizado, de la conducta del usuario o *NPE*, y otros factores.

Un cuarto componente de este recuadro y relacionado con lo anterior es un concepto propio del *DoD* denominado “cumplir para conectarse” (*C2C - Comply to Connect*) [82] que consiste en un marco de herramientas y tecnologías para monitorear de forma completa a todos los dispositivos que interactúan con la red. Una de sus características es la verificación de su higiene.

Por la derecha y abajo se esquematiza la idea fundamental de la organización centrada en los datos (*Data-Centric Enterprise*). Aquí se siguen implementando puntos de autorización y autentificación, esta vez para los recursos y para las aplicaciones.

Aquí se incluye la capacidad de gestionar la seguridad de las aplicaciones, y la capa de virtualización. Y también la protección de la cadena de suministros de *software* (*Supply Chain*) [83].

Ya hemos comentado que, en el ámbito de los datos, son importantes la clasificación, el proceso de ciclo de vida de la información, y el enmascaramiento de aquellos datos más sensibles.

En la parte central y superior se encuentran los *PDP* administrados a través un sistema de orquestación de la ciberseguridad del dominio (*Cybersecurity Domain Orchestrator*).

Es aquí donde se implementan las políticas de acceso de forma automatizada y dinámica, valiéndose del concepto de organización definida por software *SDE*.

Este centro de control se alimenta por la izquierda de las funciones de monitoreo y análisis, incluyendo la auditoría continua de la actividad a través de sensores y telemetría.

3.4.3 Casos de Uso

La cuarta sección de este documento presenta un total de diecisiete casos de uso para la aplicación de la arquitectura de referencia, lo que a simple vista parece una notable expansión de los que había planteado *NIST*.

Sin embargo, el enfoque es un tanto diferente. Aquí se proponen soluciones para los distintos aspectos de una implementación de Confianza Cero, mientras que en la publicación de *NIST* lo que se analiza es diferentes esquemas completos de aplicación.

Estos casos de uso respetan la codificación del marco de trabajo arquitectónico que ya hemos referenciado anteriormente, exponiendo vistas operacionales (*OV-1*) de alto nivel, de flujo de recursos (*OV-2*) y en algún caso de interfaces entre los sistemas (*SV-1*).

El primero de los casos de uso planteados es el que corresponde a las protecciones de seguridad centradas en los datos (*Data Centric Security Protections*) y no sorprende que sea el punto con mayor detalle en cuanto a sus gráficos.

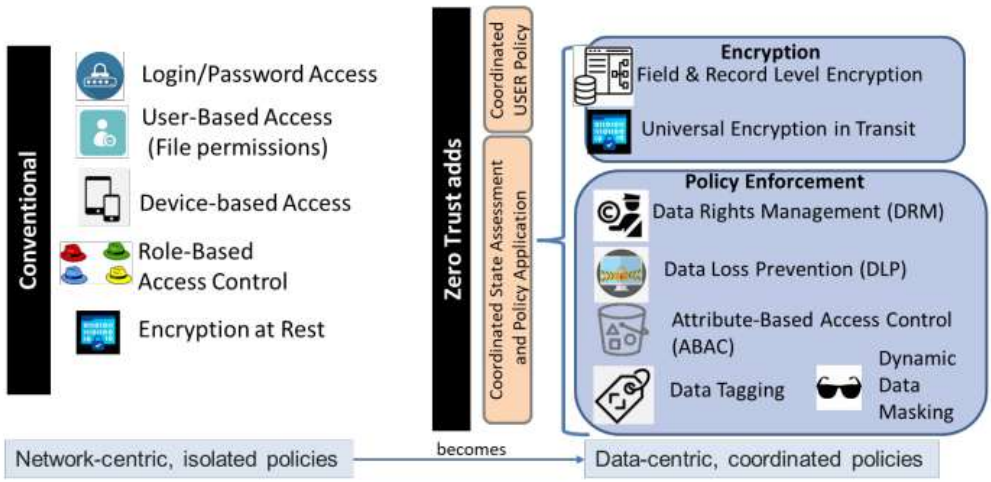


Figura 44 – Protecciones de seguridad centradas en los datos (*OV-1*).

En la vista operacional de alto nivel, se puede notar que por la izquierda se encuentra el enfoque actual, con protecciones aisladas centradas en el perímetro de red. Combinando prácticas básicas tales como usuarios y claves, accesos basados en dispositivos y roles (*RBAC - Role Based Access Controls*) [84] y cifrado de datos en reposo.

La propuesta consiste en aplicar un marco unificado de *ZT* como se ve a la derecha que incluya políticas centradas en los datos, cifrado en tránsito y reposo e incluso más cifrado granular en ciertos registros de las bases de datos.

Todo ello combinado también con el etiquetado y el enmascaramiento de datos, alimentando a sistemas de *DRM* y *DLP* que permitan implementar políticas dinámicas utilizando controles de acceso basados en los atributos (*ABAC - Attribute Based Access Control*) [85].

Este primer caso de uso también incluye tres vistas de flujo de recursos (*OV-2*). En todos los casos, el esquema general es el mismo, y lo importante es notar a grandes rasgos la disposición de los distintos componentes.

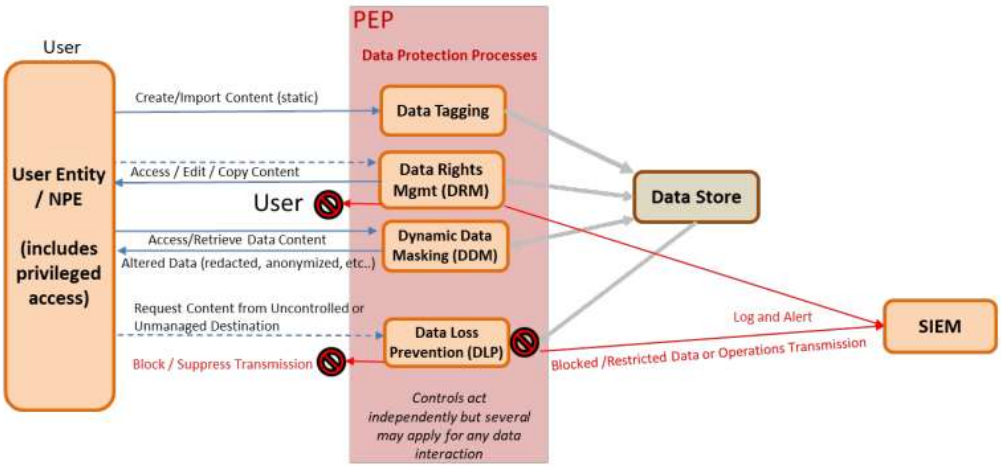


Figura 45 – Protecciones de seguridad centradas en los datos (*OV-2*).

Nótese que por la derecha y en un color diferente al resto se encuentra el elemento central de esta disposición, el repositorio de los datos (*Data Store*). Las protecciones se orientan respecto de este.

Aquí el *SIEM* cumple las importantes funciones de no solo monitorear las operaciones autorizadas sino también de proveer alertas, y registrar también los intentos fallidos de acceso.

En el otro extremo se visualiza el recuadro que corresponde a los usuarios, sean éstos personas o *NPE*, intentando acceder a estos datos de forma autorizada o con el bloqueo resultante de no ser habilitados.

En el sector central, el *PEP* se ocupa de coordinar los procesos que ya hemos mencionado, etiquetando, enmascarando, cuidando los derechos digitales y protegiendo contra la exfiltración.

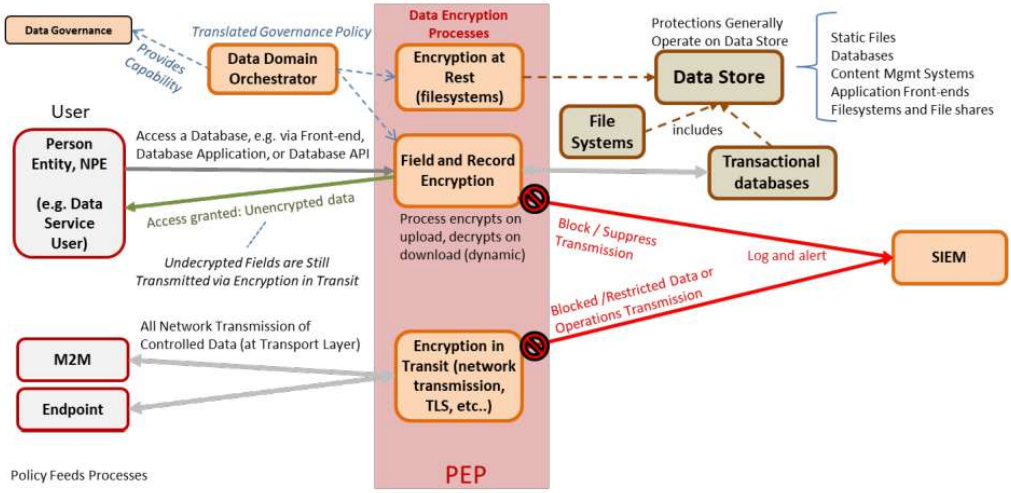


Figura 46 – Protecciones de cifrado de los datos (*OV-2*).

La segunda figura, centra más su atención en cómo se disponen los recursos relacionados con el cifrado. Aquí se puede ver que el repositorio de datos incluye tanto a archivos, como bases de datos, y sistemas de administración de contenidos en línea (*CMS - Content Management Systems*).

Por la izquierda se puede observar también que no solo existen interacciones generadas por parte de los usuarios de todo tipo, sino también las llamadas “de máquina a máquina” (*M2M – Machine to Machine*) siempre respetando el cifrado en tránsito.

Y en el centro, suceden el cifrado y el descifrado según el sentido incluyendo a registros y campos individuales en las bases de datos. Nótese que, aun siendo descifrados, la información sigue viajando por la red con un cifrado general.

La última figura de segundo nivel (*OV-2*) relacionada con la protección de datos, esquematiza la coordinación de políticas entre los puntos de decisión *PDP* y los de refuerzo *PEP*.

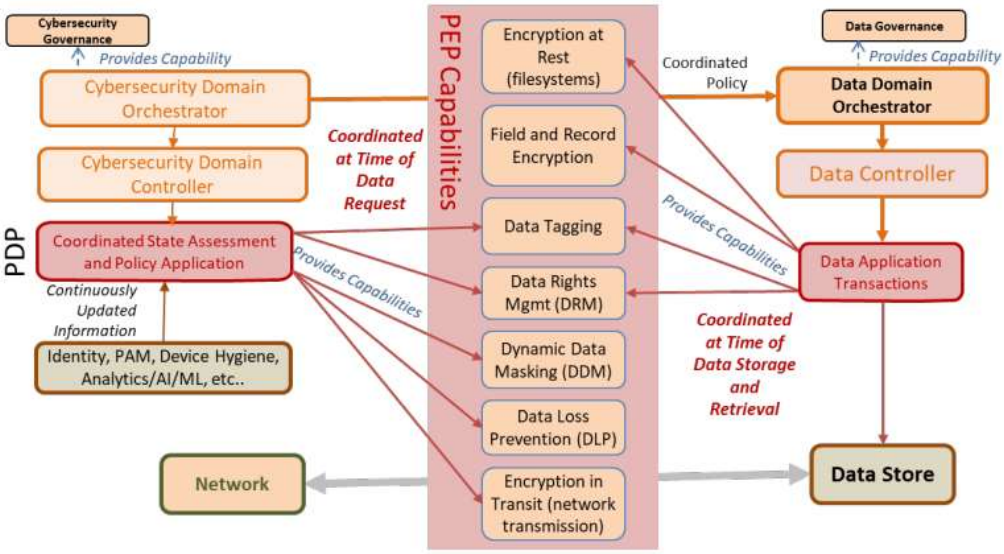


Figura 47 – Coordinación de políticas de protección de datos (*OV-2*).

A grandes rasgos, se puede observar que los *PDP* por la izquierda se alimentan de múltiples fuentes de análisis. Las identidades de los usuarios, la higiene de los dispositivos, el acceso privilegiado a los recursos *PAM,* el monitoreo de eventos, todo combinado con técnicas de aprendizaje automático e inteligencia artificial.

Como lo indica la figura con flechas rojas por izquierda y derecha, esta coordinación sucede tanto cuando se realiza un requerimiento de acceso a los datos (izquierda), como cuando se almacena o se recuperan datos (derecha).

En ambos casos, la figura muestra en el sector superior, que el gobierno de la ciberseguridad [86] se relaciona con las actividades controladas por el *PDP*, mientras que el gobierno de los datos se relaciona con estos.

A través de este esquema de defensa en profundidad (*Defense in Depth*) [87] utilizando todos los recursos mencionados, los *PEP* situados en numerosos puntos de control evalúan de forma continua la seguridad de los datos en el ambiente.

El quinto caso de uso según la numeración propuesta por la arquitectura de referencia corresponde en realidad a la segunda vista operacional de alto nivel y se ocupa del análisis de datos y la inteligencia artificial (*Data Analytics and AI*).

Aquí se propone evolucionar a través del enfoque de *ZT*, desde el estado actual en donde predominan los silos de información en donde se recolectan datos según cada dominio y aplicación, hacia un sistema de análisis, visibilidad, automatización y asistido por la IA.

El problema de los silos de información radica en que, en cada uno de ellos, se recogen datos basados en criterios diferentes, lo que dificulta el lograr un repositorio centralizado para el análisis, exigiendo muchas veces la intervención manual para normalizar la sumatoria de los mismos.

Mediante el análisis y la inteligencia artificial, el enfoque de Confianza Cero permite crear una arquitectura de recolección de datos sistemática y unificada que es mucho más eficiente a la hora de detectar y mitigar riesgos de seguridad.

La primera figura entonces muestra esa evolución, desde los silos hacia la base de conocimientos (*Knowledge Base*) y el lago de datos (*Data Lake*) [88] expandidos.

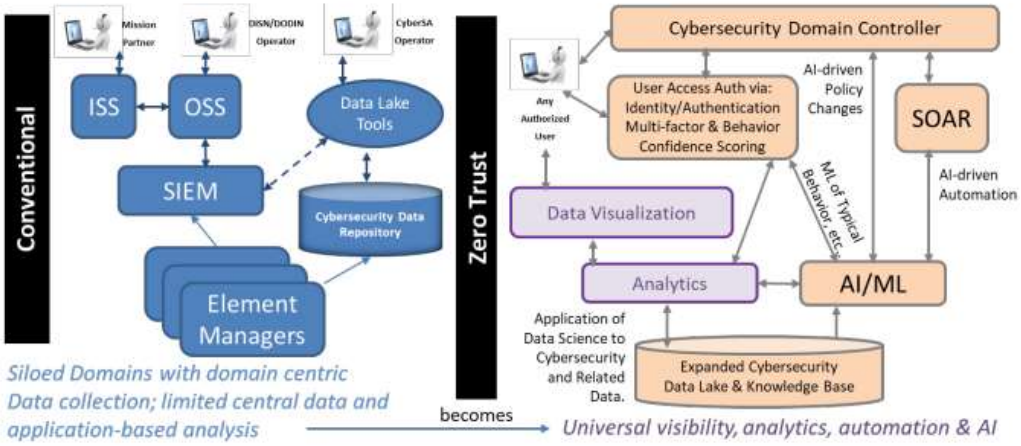


Figura 48 – Análisis de datos e inteligencia artificial (*OV-2*).

En el sector derecho que describe la propuesta de *Zero Trust* del Departamento de Defensa, puede observarse cómo se combinan las ciencias de datos aplicadas sobre este repositorio centralizado y expandido, con la aplicación de inteligencia artificial, el aprendizaje automatizado y alimentando de esa forma a un sistema de orquestación y automatización de seguridad *SOAR*.

Una figura adicional muestra a continuación con mucho más detalle cómo se alimentan de datos tanto el *SIEM* como el sistema *SOAR*.

En el centro del gráfico, se encuentra el ambiente de análisis de datos (*Data Analytics Environment*), que recibe información desde la parte inferior y a través de numerosos sensores (*Sensors*) dispuestos en toda la infraestructura y también en las aplicaciones, tanto en las instalaciones propias como en la nube.

Por izquierda y por derecha, también hacen su contribución la técnica de visualización de datos (*Data Visualization*) y las actualizaciones que se pueden recibir desde fuentes externas tales como un programa de inteligencia sobre amenazas (*Threat Intel Program*) y también la IA provista por terceros.

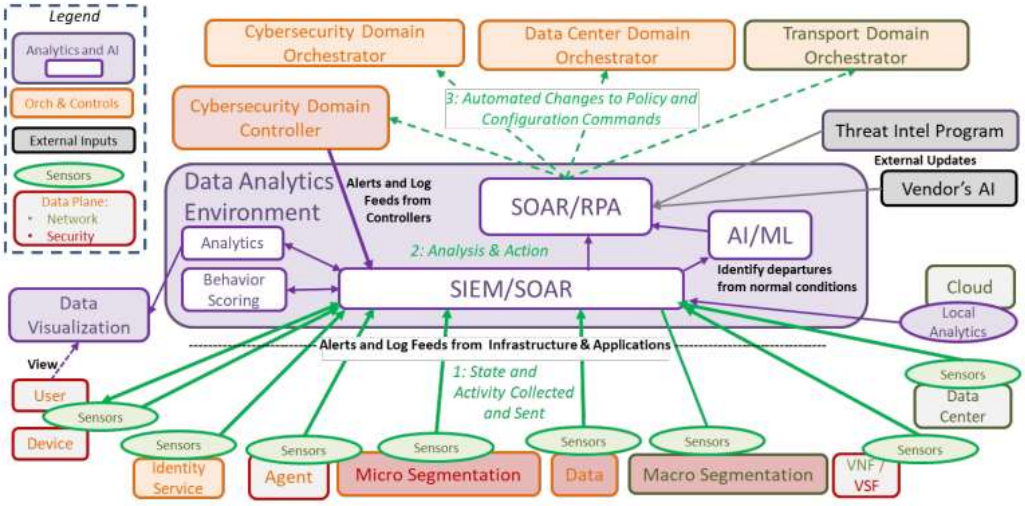


Figura 49 – Análisis de datos e inteligencia artificial (*SV-1*).

Este es el único gráfico del tipo "punto de vista de sistemas" (*SV - Systems Viewpoint*) presente en esta lista de casos de uso, y de nivel 1, que corresponde a la descripción de las interfaces entre los mismos (*Systems Interface Description*).

Lo destacable aquí es que con el enfoque de Confianza Cero que propone el *DoD*, se aumentan considerablemente la visibilidad, la capacidad de análisis y la automatización en todo el ambiente, debido a la mayor cantidad de datos recolectados desde todos sus aspectos.

Los sensores obtienen esta información desde múltiples puntos como muestra la figura, alimentando inicialmente al sistema *SIEM* para su verificación inicial, y luego son remitidos al *SOAR* para profundizar este análisis valiéndose de la inteligencia artificial.

Mantener esta base de información en un repositorio de grandes datos (*Big Data*) [89] permitirá además aplicar posteriormente técnicas de aprendizaje de máquina (*machine learning*) para prevenir futuros incidentes.

El siguiente par de casos de uso 4.7 y 4.8, apuntan a describir cómo *ZT* cambia la perspectiva adoptando la orquestación y administración centralizada de políticas (*Centralized Orchestration & Policy Management*).

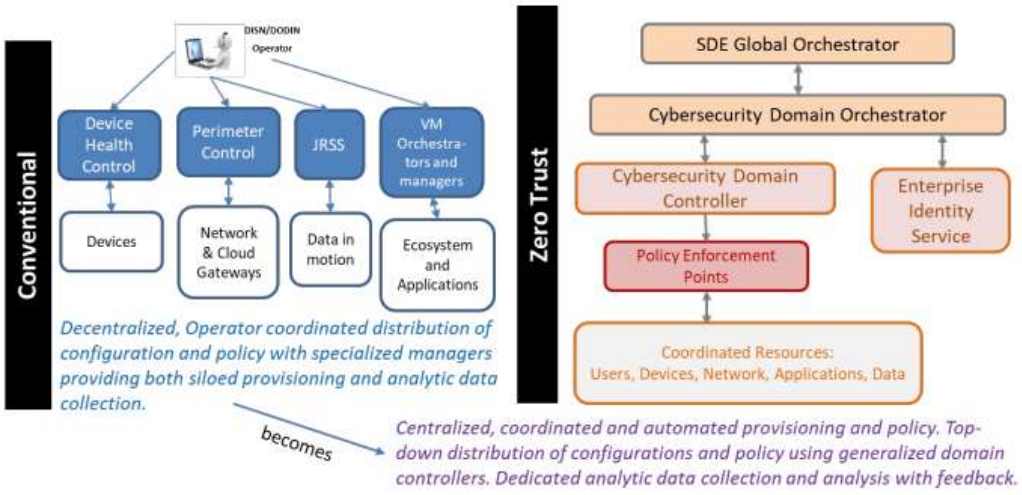


Figura 50 – Orquestación y administración centralizada de políticas (*OV-1*).

Tal como venimos haciendo, aquí lo importante es apreciar la idea general de estos gráficos antes que la detallada terminología.

En este caso, se puede notar a la derecha de la figura, que el enfoque convencional izquierdo en donde las políticas eran administradas por operadores individuales generando distintos silos aislados en cada dominio, se reemplaza por una estructura de control central.

En cada unidad de negocio, funcionará entonces un agente denominado “orquestador de ciberseguridad para el dominio” (*Cybersecurity Domain Orchestrator*).

Este orquestador se comunica en ambos sentidos tanto con un controlador de ciberseguridad para el dominio (*Cybersecurity Domain Controller*) y con el servicio de identidades empresarial (*Enterprise Identity Service*).

A su vez, el controlador de dominio toma información desde los distintos *PEP* distribuidos a través de toda la infraestructura, los cuales supervisan usuarios, dispositivos, elementos de la red, aplicaciones y datos.

Lo importante aquí es que, cada orquestador de dominio obtendrá las actualizaciones de políticas centralizadas desde un "orquestador global para la empresa definida por software" (*SDE Global Orchestrator*).

La segunda figura describe con más detalle el otro caso de uso que tiene el mismo nombre ya que apunta a idéntica cuestión.

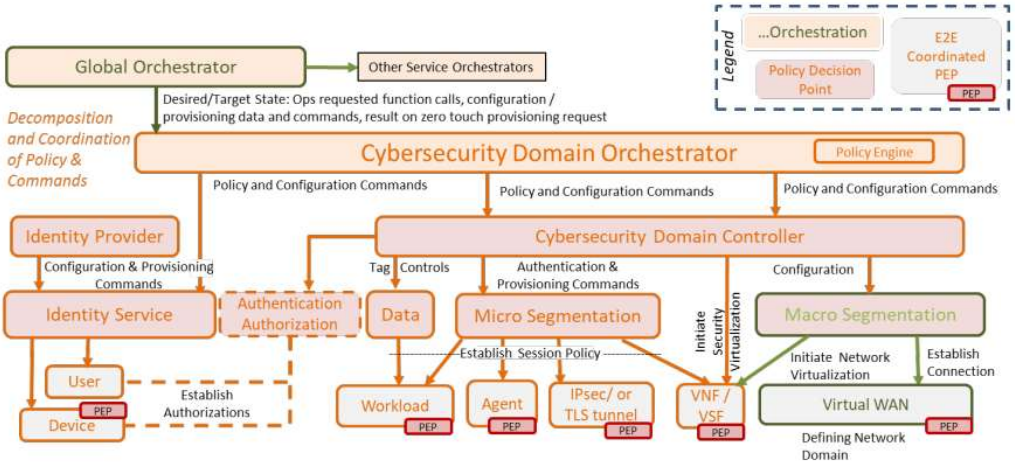


Figura 51 – Orquestación y administración centralizada de políticas (*OV-2*).

Aquí también se puede notar la centralidad en cada unidad de negocio del orquestador de dominio, que toma las instrucciones de un orquestador global, para luego emitir distintos tipos de comandos de políticas y configuración (*Policy and Configuration Commands*) hacia las distintas áreas en el sector inferior.

Por la izquierda abajo, el orquestador de dominio envía estos comandos al sistema de administración de identidades incluyendo opciones de configuración (*Provisioning*) para los dispositivos. También se comunica en el sector central inferior con los repositorios de datos para establecer etiquetas (*Tag Controls*) y su microsegmentación.

Por la derecha, además, también trabaja sobre la macro segmentación, es decir, la administración tradicional de la organización de la red, pero utilizando la virtualización.

A continuación, se presenta el caso de uso número 4.9, que es sin duda una extensión de todos los anteriores, e incluye solo una figura del tipo *OV-1*. Se trata de la aplicación de un bucle de retroalimentación dinámico y adaptativo para las políticas (*Dynamic, Adaptive Policy Feedback Loop*).

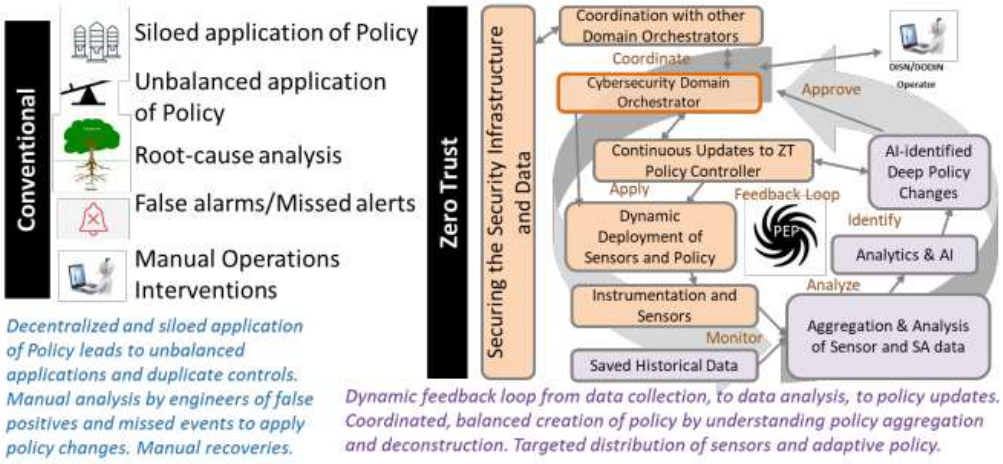


Figura 52 – Bucle de retroalimentación de políticas dinámico y adaptativo (*OV-1*).

La figura superior expone la idea claramente, amén de todo su detalle. Por la izquierda, el modelo convencional se basa en análisis manuales y no coordinados de la información sobre alarmas y alertas, en donde frecuentemente se pierden controles o se trabaja sobre falsos positivos.

La nueva propuesta entonces consiste en mantener este bucle que se adapta y retroalimenta, tomando información de los sensores (*Instrumentation and Sensors*) y de los datos históricos almacenados (*Saved Historical Data*).

Se prevé que un principio, se trabaje con datos guardados para el análisis por medio de inteligencia artificial, pero en un futuro que esto cambie hacia la verificación en línea y directa.

Este análisis entonces retroalimenta al sistema permitiendo la actualización continua de las políticas que el orquestador de dominio comunicará luego a los distintos *PEP* de la plataforma.

El caso de uso número 4.10 se aparta de ya de las consideraciones relacionadas directamente con los datos, y propone un tratamiento idéntico tanto para usuarios locales como remotos, en donde todos deben pasar por un *PEP* para acceder a cualquier recurso.

Esto ya había sido planteado por *NIST* como una premisa fundamental. Aquí se lo denomina “implementación sin VPN” (*VPN-Less Implementation*), y no requiere mayor análisis.

Figura 52 – Implementación sin *VPN* (*OV-1*).

Algo similar ocurre con el siguiente caso de uso número 4.11, que propone la “segmentación este-oeste” (*East-West Segmentation*), y donde el objetivo es prevenir los movimientos laterales.

Esto tampoco merece mayor análisis dado que ya había planteado anteriormente en las diversas fuentes que hemos presentado en este trabajo, y por supuesto se vale de la microsegmentación para establecer perímetros ajustados a cada recurso.

Es interesante notar que, en el documento del *DoD*, también se menciona el control de las comunicaciones no solo entre dispositivos, sino también entre las aplicaciones segmentando las *APIs*.

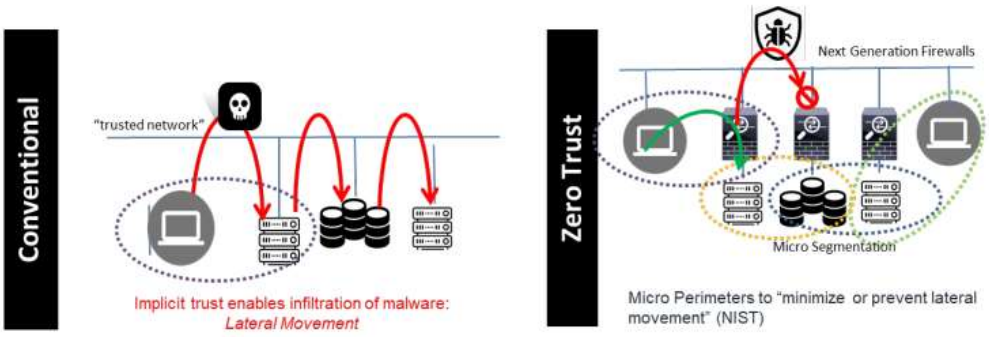


Figura 53 – Segmentación Este-Oeste (*OV-1*).

Los dos casos de uso 4.12 y 4.13 que se plantean a continuación abordan el problema de la higiene global y uniforme de los dispositivos (*Global Uniform Device Hygiene*) en vistas del tipo *OV-1* y *OV-2*.

Aquí la clave reside nuevamente en la evaluación unificada y centralizada tanto del estado de los sistemas como de los eventos que los mismos van generando durante su operación.

Tradicionalmente, la verificación de cada dispositivo se realizaba en silos separados. Si superaba una lista de controles estandarizada, entonces era confiable.

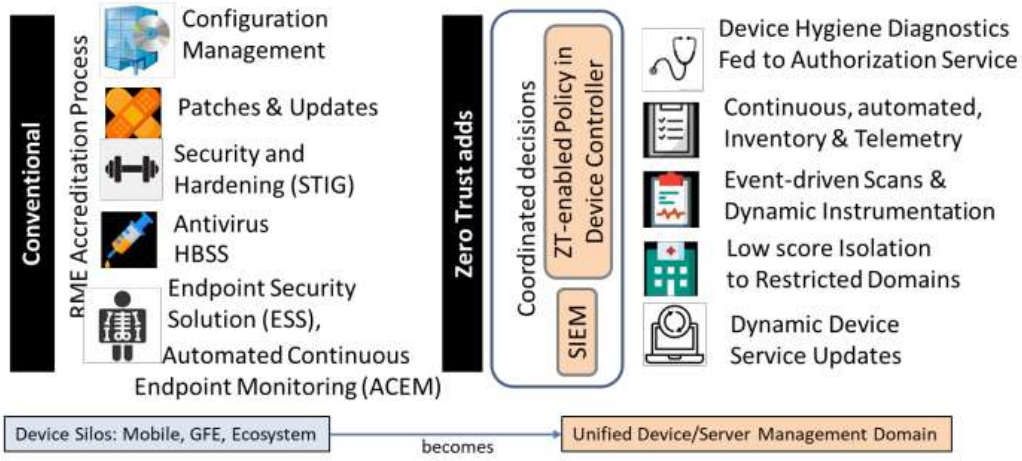


Figura 54 – Higiene global y uniforme de los dispositivos (*OV-1*).

Zero Trust añade entonces al esquema convencional la coordinación centralizada y el análisis continuo de eventos, y las políticas se ajustan en dinámicamente en base a ellos.

De la figura anterior solo hace falta rescatar estos conceptos, en particular la coordinación de las decisiones sobre accesos. La vista de segundo nivel *OV-2*, proporciona un mayor detalle sobre la distribución de los controles de higiene y su relación con el esquema de ciberseguridad general.

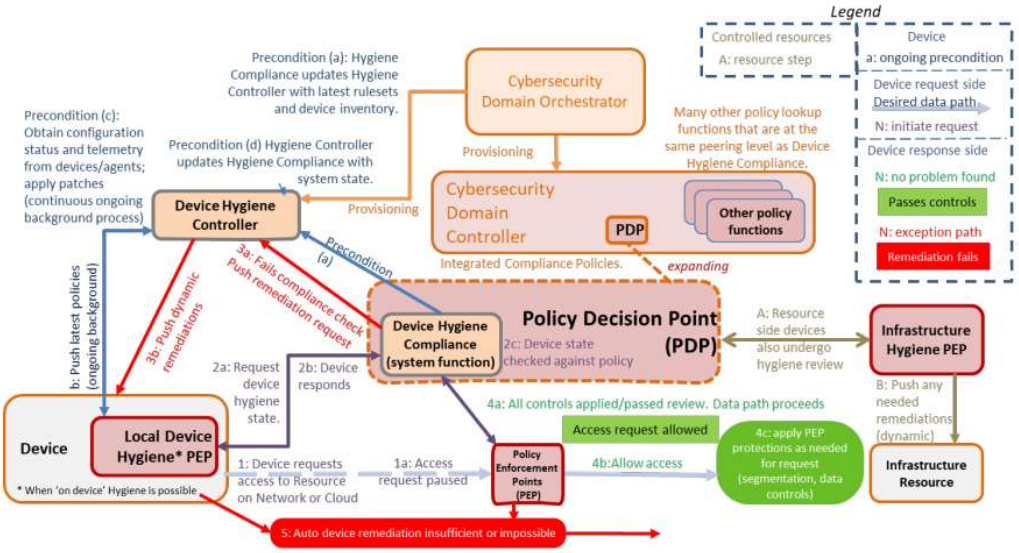


Figura 55 – Higiene global y uniforme de los dispositivos (*OV-2*).

Para comenzar el análisis de esta figura, debemos notar que existen ciertas precondiciones (*Preconditions*) que se deben cumplir para el correcto funcionamiento del esquema. También observar que existe un elemento central denominado “Controlador de Higiene de los Dispositivos” (*Device Hygiene Controller*).

Este controlador de higiene recibe del orquestador de ciberseguridad del dominio que ya conocemos, la lista actualizada de reglas de acceso (*Rulesets*) y el inventario de dispositivos. Esta es la precondición (a).

Abajo a la izquierda, puede notarse que para aquellos dispositivos (*Device*) en donde sea posible, opera un *PEP* local dedicado a la higiene. Si existe, se comunica constantemente con el controlador antes mencionado y recibe sus últimas actualizaciones, en un proceso de segundo plano.

En realidad, esta es una comunicación de doble vía, ya que el *PEP* local envía a su vez información de status y telemetría, colaborando con la continua aplicación de actualizaciones si son necesarias, también en el *background*. Estas son las precondiciones (b) y (c).

El controlador de higiene actualiza a su vez a la función general de cumplimiento del sistema (*Device Hygiene Compliance*) con información sobre el estado de los dispositivos. Corresponde a la precondición (d).

Cumplidas las precondiciones, comienza entonces el proceso habitual (1) de solicitud de acceso ya sea a recursos de la propia red o en la nube. Inmediatamente esa solicitud llega al *PEP* que se encuentra en el sector central inferior y queda en pausa (1a) hasta que se puedan realizar las verificaciones.

El *PEP* como de costumbre le pide al *PDP* que se ve en el centro asistencia para decidir sobre esta solicitud, lo que dispara el paso (2a) en el que se solicita al *PEP* local el estado de higiene del dispositivo.

En el caso en el que en (2b) el dispositivo responda, se verifique su estado (2c) y no cumpla con las pautas requeridas entonces se produce una solicitud de remediación (3a) al controlador de higiene, quien la envía al mismo (3b).

Si por otra parte el dispositivo sí cumple con las condiciones entonces se habilita el acceso en (4a) y (4b). Sin embargo, este acceso permitido debe pasar también por las protecciones regulares (4c) tales como segmentación de la red y controles sobre los datos.

Cabe observar que, en sector derecho, se suma un *PEP* dedicado a la higiene de la infraestructura (*Infrastructure Hygiene*) que también se toma en cuenta y se mantiene.

Pasamos entonces a los siguientes casos de uso 4.14 y 4.15 en donde se propone la autentificación continua y dinámica (*Dynamic, Continuous Authentication*), también en vistas tipo *OV-1* y *OV-2*.

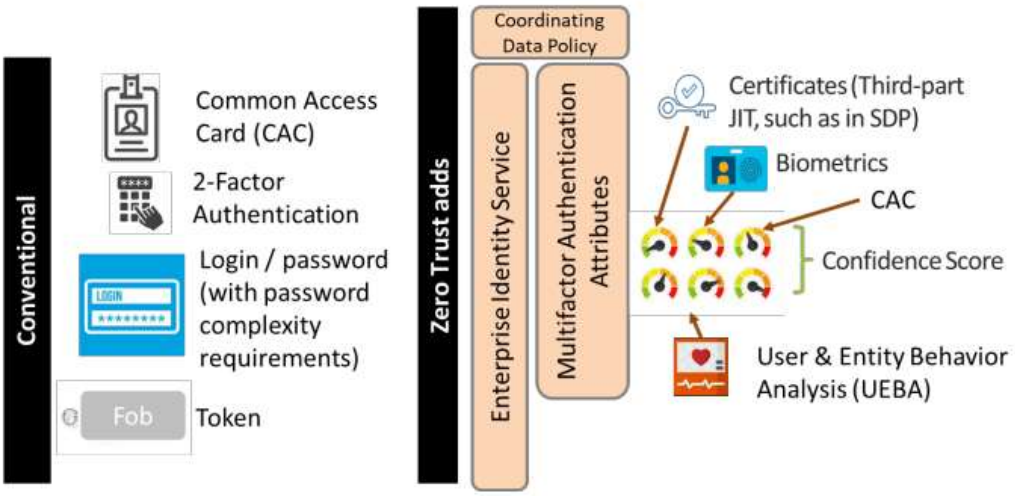


Figura 56 – Autentificación dinámica y continua (*OV-1*).

Lo que agrega *Zero Trust* a los sistemas existentes es un sistema de niveles de confianza basado en atributos de autentificación múltiples (*Multifactor Authentication Attributes*) que incluyen al contexto, y a entidades no personales tales como los robots (*Bots*), dispositivos de *hardware* y aplicaciones.

Para lograr tal combinación como se ve en el sector derecho de la imagen, se suman los certificados emitidos en el momento, datos biométricos, tarjetas de acceso y el análisis de conducta para usuarios y entidades *UEBA*.

Todos estos componentes permiten calcular una puntuación de confianza (*Confidence Score*) en forma dinámica y continua.

Al igual que en los dos casos de uso previos, la figura de la página siguiente esquematiza el flujo de trabajo en una vista operacional de segundo nivel.

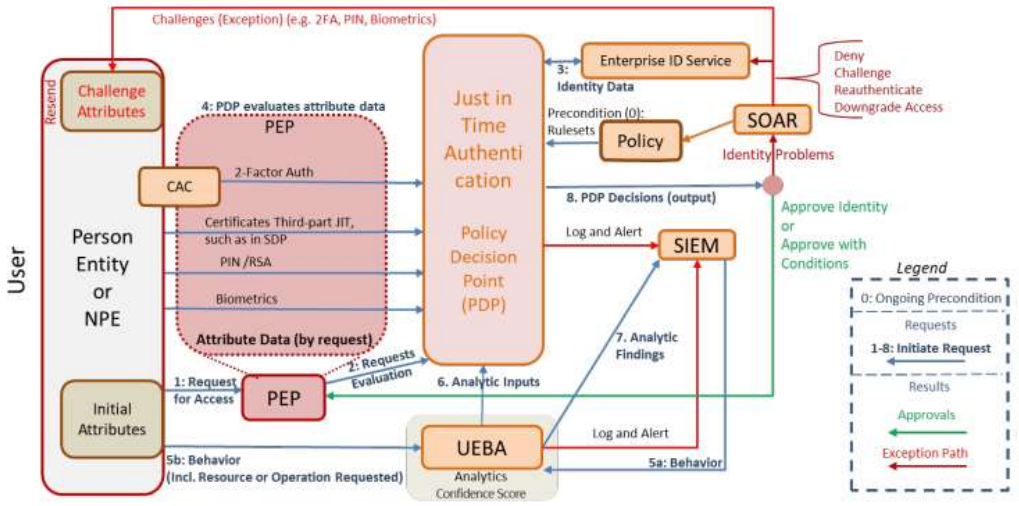


Figura 57 – Autentificación dinámica y continua (*OV-2*).

La única precondición requerida en este flujo es que el sistema de orquestación y automatización de la seguridad (*SOAR*) alimente en forma regular a los *PDP* de conjuntos de reglas de acceso.

El primer paso es la solicitud (1) que realiza la persona o la entidad usando sus atributos iniciales (*Initial Attributes*), que pueden incluir una tarjeta de acceso, un certificado, un pin o un dato biométrico, entre otros.

El *PEP* solicita (2) al *PDP* su evaluación, valiéndose este último de su conexión (3) con el sistema de administración de identidades central para complementar la verificación en (4) de los atributos.

En medio de esta operación, el sistema *UEBA* recibe los datos sobre el comportamiento en (5a) y (5b), actualiza el nivel de confianza y se produce entonces una decisión que combina el aporte de este sistema en (6) y el del *SIEM* en (7). Esto incorpora información sobre el contexto y los eventos generados.

Finalmente, en (8) se produce la decisión de autorización "justo a tiempo" (*JIT – Just In Time*) del *PDP*, que puede resultar favorable, con o sin condiciones.

La otra opción es que el acceso no se conceda, y entonces se informe al sistema *SOAR* que optará por reiterar la verificación o no, y alimentar nuevamente al sistema de políticas, haciendo al proceso dinámico.

Este caso de uso incorpora una imagen adicional que no incluiremos aquí, haciendo referencia a todas las entidades, personas o no, que pueden requerir autentificación.

Entre ellas se citan a los dispositivos en manos de un usuario persona, a los recursos que o bien sostienen alguna aplicación o corresponden a un componente de red, y a cualquier otro elemento en el ámbito de Internet de las Cosas. También se incluye a cualquier tipo de intermediario (*proxy*) que interceda a favor de usuarios o dispositivos.

Llegamos así al último par de casos de uso 4.16 y 4.17, relacionados con la autorización condicional (*Conditional Authorization*), siempre posterior a la autentificación.

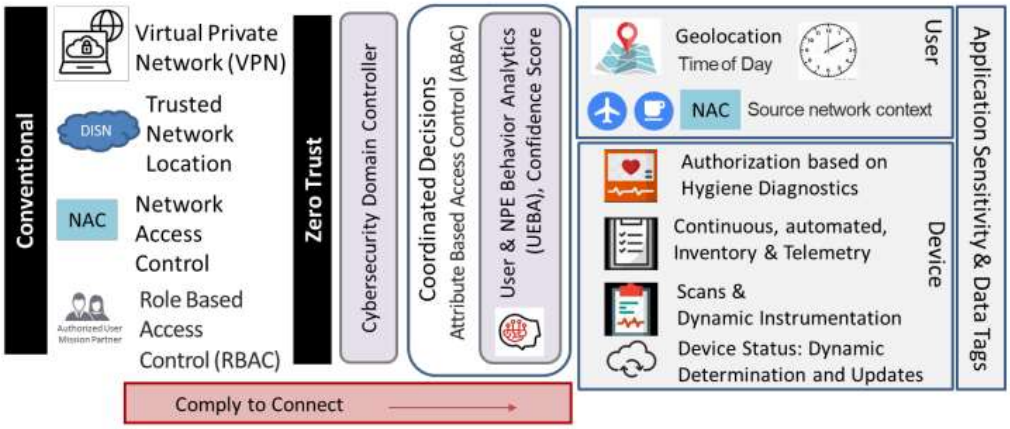


Figura 58 – Autorización condicional (*OV-1*).

Esta autorización en la arquitectura propuesta funciona en combinación con todo lo expuesto en los dos casos de uso anteriores. El sistema convencional decide sobre la autorización de un solicitante en base a los parámetros que se ven a la izquierda en la figura.

Esos parámetros incluyen la ubicación en la red ya sea interna o externa, el rol del usuario o entidad, y su método de autentificación que puede incluir usuario y clave, tarjetas de acceso, certificados, y hasta ser multifactorial.

La propuesta de *ZT* es más integral, considerando también políticas dinámicas, el contexto de la solicitud, la higiene del dispositivo, ubicación, fecha, hora y su comportamiento.

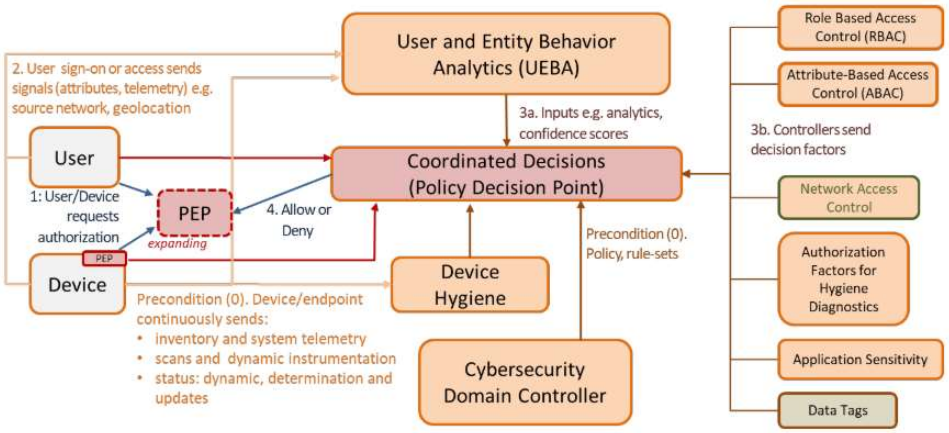


Figura 59 – Autorización condicional (*OV-2*).

El flujo de autorización se muestra en la figura superior, que corresponde al último caso de uso expuesto.

Como en el anterior, todo comienza a partir de una precondición (0), en donde el dispositivo envía en forma continua al *PDP* información sobre su estado, actualizaciones, instrumentación dinámica (*Dynamic Instrumentation*) y telemetría.

Al mismo tiempo, el controlador de ciberseguridad del dominio actualiza al *PDP* con sus conjuntos de políticas y reglas.

Cumplidas estas condiciones previas, el sistema se encuentra listo para recibir los pedidos de autorización desde usuarios y dispositivos (1), que por supuesto deben pasar por el *PEP* tanto local como individual.

En paralelo se ve en la imagen en un color naranja más claro que el usuario envía en el paso (2) junto con su pedido de autentificación, señales que indican su ubicación y los parámetros que mencionamos anteriormente.

Aquí es donde entra en juego el sistema de análisis del comportamiento de usuarios y entidades *UEBA* que examina esas señales y elabora un puntaje de confianza (*Confidence Score*) que es alimentado al *PDP* en el paso (3a).

Nótese que en esta evaluación (3b) se combinan múltiples "controladores" que inciden en el puntaje , tales como el control de acceso por roles *RBAC* y el basado en atributos *ABAC*, la ubicación en la red, el diagnóstico de higiene, la criticidad de la aplicación en uso (*Application Sensitivity*) y hasta las etiquetas de los datos.

Finalmente, si el puntaje obtenido se condice con el nivel de confianza requerido por la organización, se produce la autorización del punto (4).

3.4.4 Patrones Arquitectónicos

Además de ofrecer los casos de uso detallados en el punto anterior, el documento que estamos analizando expone en su capítulo séptimo una serie de cinco patrones arquitectónicos (*Architectural Patterns*).

Tal como lo describe una tabla al inicio que justifica su presentación, cada uno de esos patrones utiliza o provee ciertas capacidades, las cuales señalaremos al comentarlos de forma breve a continuación.

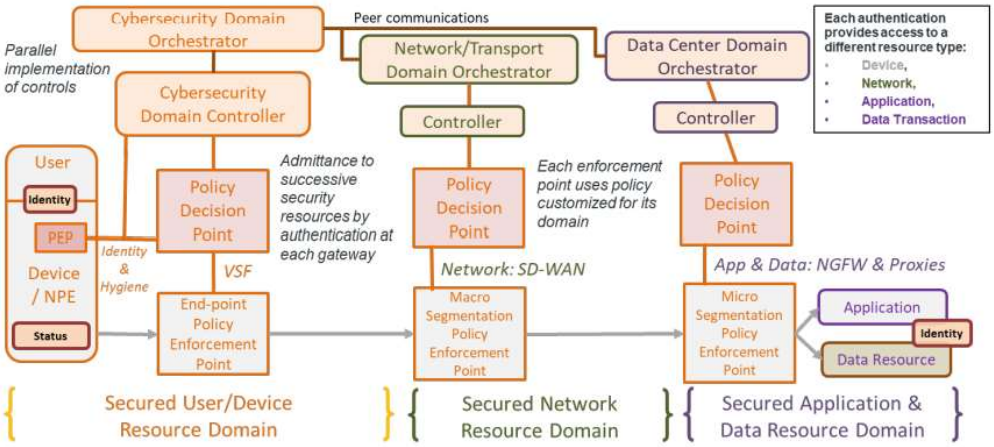


Figura 60 – Aplicación de políticas de dominio para el acceso a recursos (*SV-1*).

El primer patrón describe la aplicación de políticas de dominio para el acceso a los recursos, y se esquematiza en la figura superior en una vista del tipo *SV-1*.

Las capacidades que utiliza o habilita son la autentificación continua, la autorización condicional, más la macro y microsegmentación.

Aquí conviene notar que las políticas son aplicadas utilizando la orquestación de dominios en paralelo. La figura incluye tres dominios que son el de los usuarios y dispositivos (*User / Device*), el de la red (*Network*) y el de las aplicaciones y datos (*Application & Data*).

Cada uno de estos tres dominios maneja sus propias políticas y respuesta automática a través de su controlador (*Controller*) dedicado.

El flujo de controles y protecciones por el que deben pasar un usuario o *NPE* y su correspondiente dispositivo funciona de izquierda a derecha. Primero, en su propio dominio debe cumplir con los requisitos.

Luego, deberá pasar por las verificaciones del segundo dominio que autoriza o no el acceso a la red. Y finalmente, el tercer dominio regula el acceso a datos y aplicaciones, que son el destino final.

Todos los dominios reportan al orquestador de ciberseguridad (*Cybersecurity Domain Orchestrator*) enviándole datos de manera continua para detectar cualquier anomalía en tiempo real, y disparar cambios en las políticas.

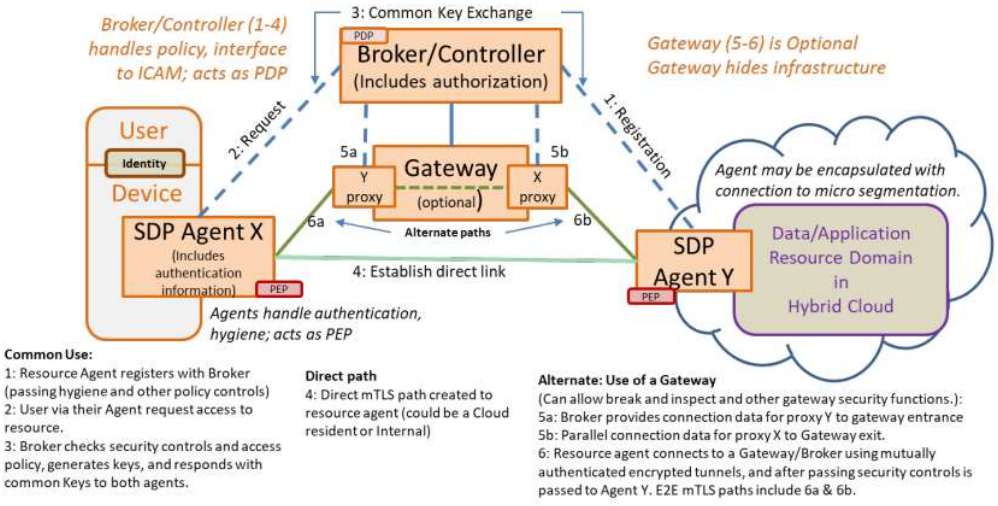


Figura 61 – Patrón para el perímetro definido por *software* (*OV-2*).

El segundo patrón se ocupa del perímetro, estableciendo que el mismo debe ser definido por software y utilizando las capacidades de autorización condicional incluyendo microsegmentación y cifrado.

Conviene observar que, para este caso, se utiliza una vista del tipo operacional *OV-2*, la cual describe el flujo operativo. Y este flujo es muy similar al planteado originalmente por *NIST*.

El primer paso en el flujo (1) es la registración del recurso que se exhibe a la derecha, y el segundo (2) es la solicitud de acceso por parte de un usuario y su dispositivo.

En el sector central, se ubica un gestor (*Broker*) con facultades de *PDP* y que también se ocupa de la autorización, además de generar en el paso (3) las claves requeridas para el cifrado dinámico y bidireccional de cada conexión.

La figura muestra que tanto el extremo solicitante como el receptor cuentan con un agente (*SDP Agent*) que opera como *PEP*. En el caso del usuario, se incluye en el agente la información sobre autentificación.

Para que se establezca finalmente el enlace directo entre ambos (4), el acceso condicional se otorga en base a la identidad del usuario y del dispositivo, y la higiene de este último todo combinado en una puntuación de confianza.

Como una alternativa a este enlace directo, se recomienda el uso de una puerta de enlace (*Gateway*) que habilite los caminos (6a) y (6b) pero siempre en comunicación con el gestor en (5a) y (5b).

Esto permite tanto la inspección del tráfico como el corte del enlace en caso de actividad sospechosa o exfiltraciones.

El siguiente patrón es en cierta medida una extensión del anterior, en donde se detalla cómo se integra el gestor al ambiente de *ZT*.

En general el ambiente esconde a los recursos y requiere que los usuarios finales contacten y se conecten con un gestor que provee como ya se mencionó, autorización condicional basada en un puntaje de confianza.

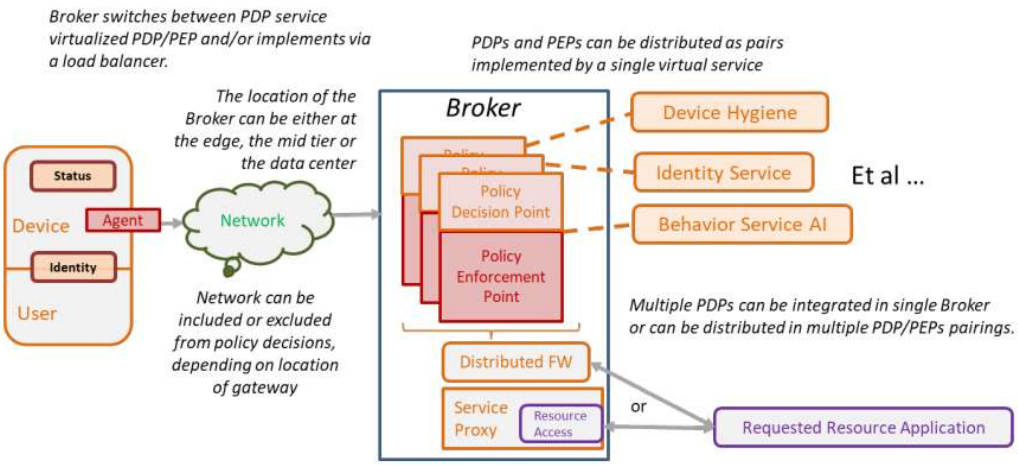


Figura 62 – Integración de un gestor de Confianza Cero (*SV-1*).

Las capacidades que usa o habilita son la autentificación continua, la autorización condicional, y la higiene de dispositivos.

En la figura se exhibe que este gestor podría integrar distintas funciones, tales como la de uno o más pares virtualizados de *PDP / PEP*, cortafuegos y hasta un intermediario (*Proxy*).

Hacia la derecha, puede observarse que el gestor se alimenta de las fuentes ya citadas tales como la higiene, identidades y en combinación con inteligencia artificial aplicada al comportamiento.

Por último, vale la pena agregar que este gestor puede estar situado en el borde (*Edge*), o cercano a la aplicación que protege. Todo depende de los requerimientos del sistema, y esto también influye en la decisión sobre incluir en las políticas de acceso a la red.

Entre los distintos patrones propuestos existe uno en particular relacionado con la microsegmentación que se presenta en tres variantes, todas ellas enfocadas únicamente al nivel de infraestructura.

Se menciona en el documento que la microsegmentación puede ser descompuesta en componentes menores hasta el nivel de procesos, evolucionando en un futuro hacia un esquema de *APIs.*

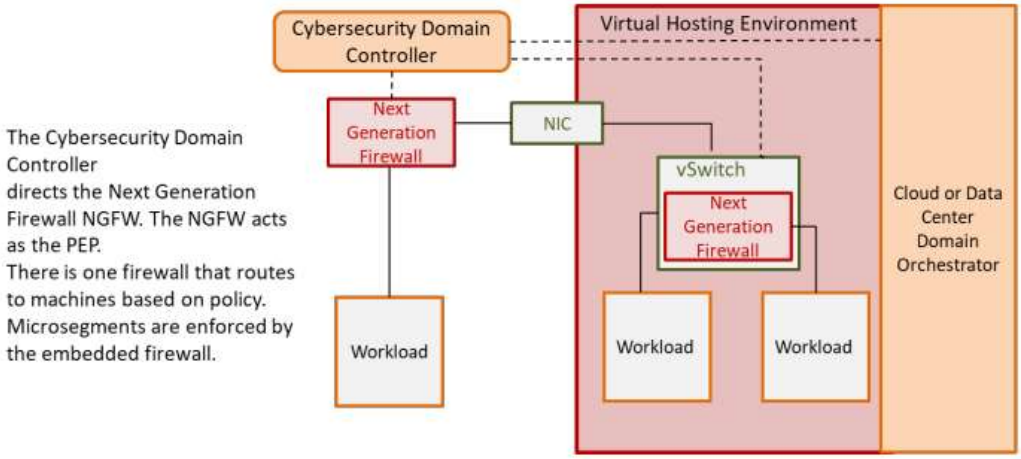


Figura 63 – Microsegmentación a nivel de red (*SV-1*).

La primera variante implementa la microsegmentación al nivel de red, utilizando un cortafuegos de próxima generación (*NGFW - Next Generation FireWall*) [90], ubicado en la red física o como parte de la virtualizada.

El cortafuegos toma el papel de un *PEP* para el refuerzo de políticas, y por sus características avanzadas incluye prevención de intrusiones, inspección profunda de los paquetes, detección de amenazas *(Malware)*, y funcionalidad al nivel de aplicaciones.

Aquí el tráfico debe pasar sí o sí por el *firewall*, y las políticas a reforzar las provee el controlador de ciberseguridad del dominio.

La segunda variante concreta la microsegmentación al nivel del hipervisor, colocando un micro cortafuegos (*Micro Firewall*) por delante de cada recurso virtualizado.

Como se puede ver en la figura siguiente, el controlador de ciberseguridad del dominio efectúa una distribución orquestada de las políticas a ser reforzadas hacia cada uno de estos micro cortafuegos que operan como *PDP*.

Este modelo de trabajo permite mejorar la mitigación de riesgos al prevenir los movimientos laterales.

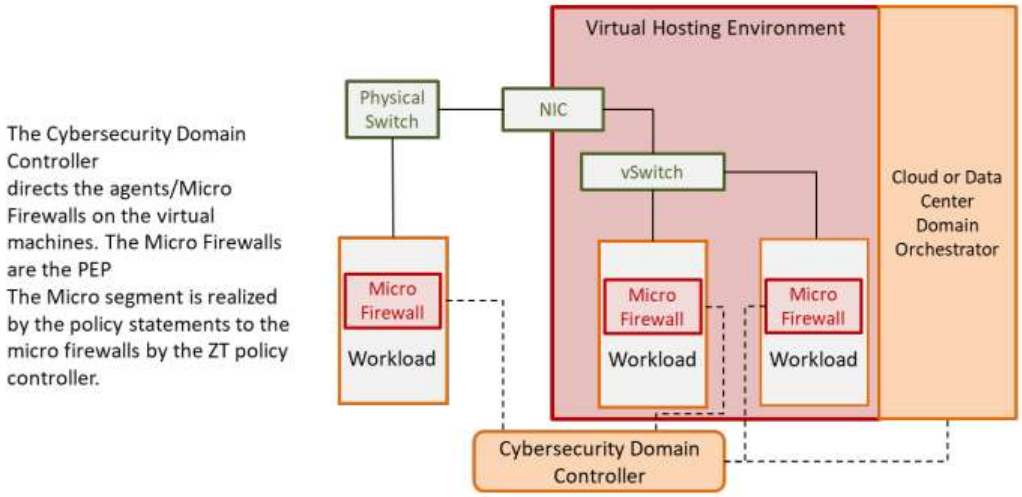


Figura 64 – Microsegmentación a nivel de hipervisor (*SV-1*).

En la tercera y última disposición se utiliza un agente instalado en cada dispositivo (*Endpoint Agent*). Esto permite llevar las protecciones hasta el nivel de los procesos, provee la máxima granularidad y es independiente de la infraestructura.

Todo el tráfico debe ser autorizado por los agentes, orquestados como siempre por el controlador de dominio.

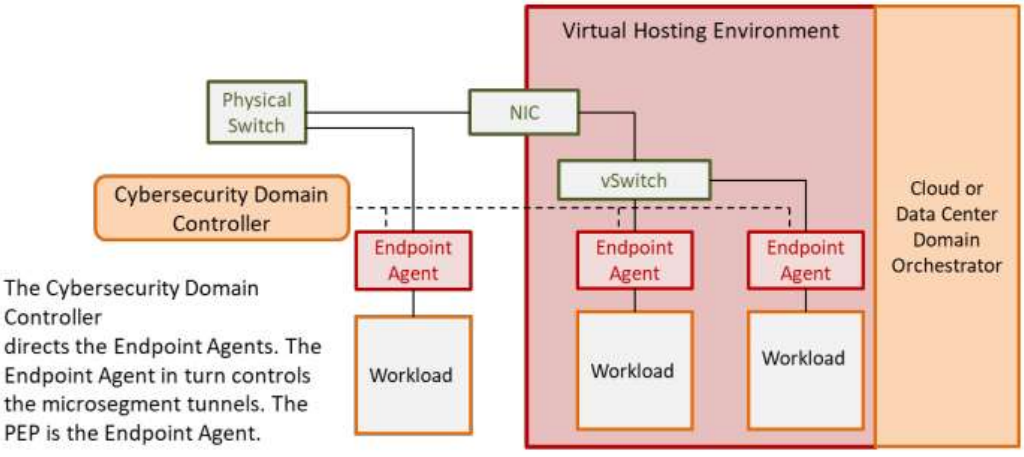


Figura 65 – Microsegmentación a nivel de dispositivo (*SV-1*).

Una aclaración adicional corresponde al escenario en donde una aplicación es parte de un esquema de tres capas *(Three-Tier*) tal como el que se utiliza en sistemas accedidos vía Internet.

En ese caso, se dispone un *PEP* por delante del servidor *web*, otro que protege a la capa de aplicación en sí y un último controlando el acceso a la base de datos.

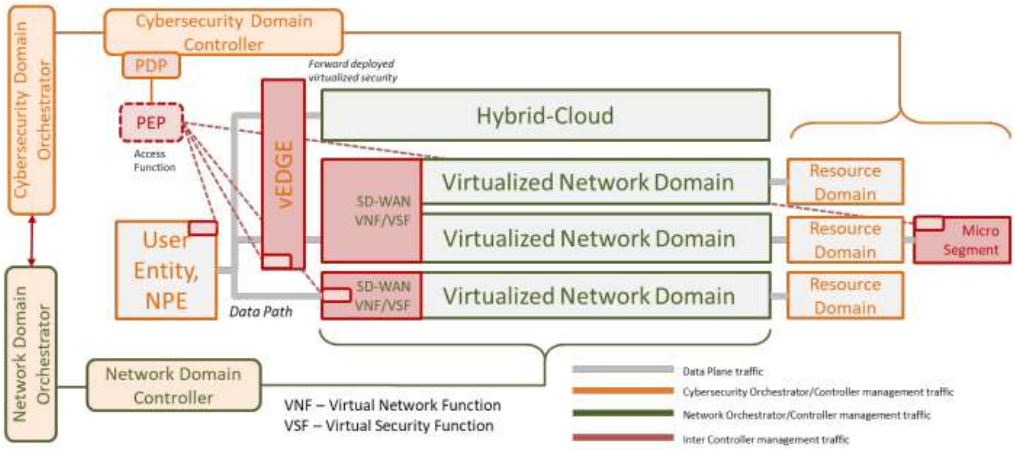


Figura 66 – Macro segmentación (*SV-1*).

La plataforma de red también necesita de una segmentación más general a nivel “macro”, la cual se ejemplifica en la figura superior.

Se pretende aquí mejorar el enfoque tradicional en el cual la división en grandes bloques se logra a través de *VLANs*, y *switches* gestionables, y que solo consigue establecer una protección perimetral.

Zero Trust agrega protecciones destinadas al control de los actores que ya están ubicados dentro del perímetro, primero verificándolos sean usuarios o entidades, y en posiciones estratégicas sobre el borde, y en el ingreso a cada dominio de la red virtualizada, segura y definida por *software*.

Nótese que los caminos de comunicaciones para los datos (*Data Path*) y para la gestión de la seguridad y de la red, son diferentes.

El último patrón arquitectónico corresponde a los servicios externos necesarios para la implementación de un sistema de administración de identidades centralizado.

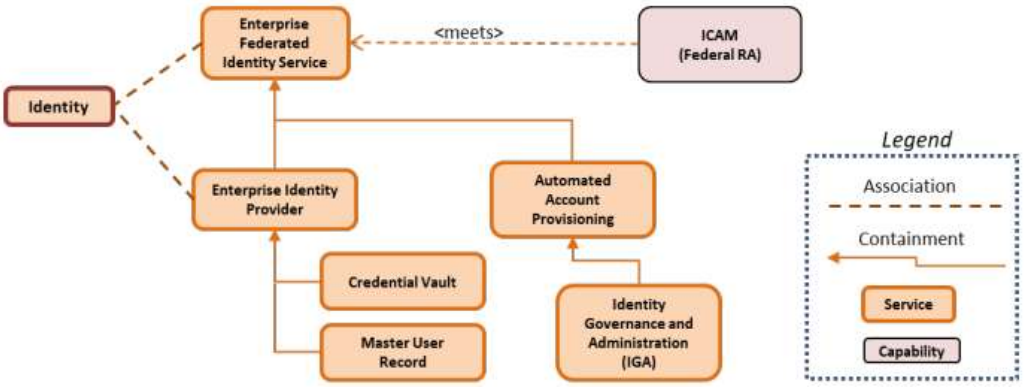


Figura 67 – Servicios externos para administración de identidades (*SvcV-1*).

El patrón es descrito por la figura superior, que corresponde a un tipo de vista que expone el contexto de los servicios (*SvcV-1 - Services Context Description*), y si bien su contenido está relacionado con los sistemas propios del Departamento de Defensa, vale la pena analizarlo.

Por arriba se puede notar que el servicio empresarial federado de identidades (*Enterprise Federated Identity Service*) cumple con los lineamientos del diseño de referencia para este propósito publicado por el propio organismo *ICAM* que ya hemos visto.

Este sistema federado es un elemento fundamental de la visión a futuro de *Zero Trust*, y se nutre de los componentes que se ven por debajo.

Un sistema automatizado de aprovisionamiento de cuentas (*Automated Account Provisioning*) le proporciona servicios de gobierno tales como la administración de permisos, auditoría de roles y el manejo de altas, bajas y modificaciones que resultan de las incorporaciones, cambios de roles y desvinculaciones.

El otro componente importante que se ve más a la izquierda es el proveedor empresarial de identidades (*Enterprise Identity Provider*), que mantiene y administra esta información, y provee servicios de autentificación.

Para habilitar, auditar y reportar quién tiene acceso a qué aplicaciones, se vale de un registro maestro de usuarios (*Master User Record*) encargado de recolectar atributos de las personas y sus permisos otorgados.

Asimismo, se vale de una bóveda de credenciales (*Credential Vault*), para complementar sus funciones en este sentido.

Dos vistas adicionales que describen el flujo de los servicios (*SvcV-2 - Services Resource Flow Description*) esquematizan a muy alto nivel cómo la validación externa de identidades se lleva a cabo mediante una interfaz *API* estandarizada, tal como podría ser *SAML*.

Mostramos aquí solo una de ellas, suficiente para comprender la propuesta, donde por la izquierda se puede notar que cualquier función de autentificación y/o autorización requerida por la arquitectura de Confianza Cero es solicitada al proveedor externo de identidades.

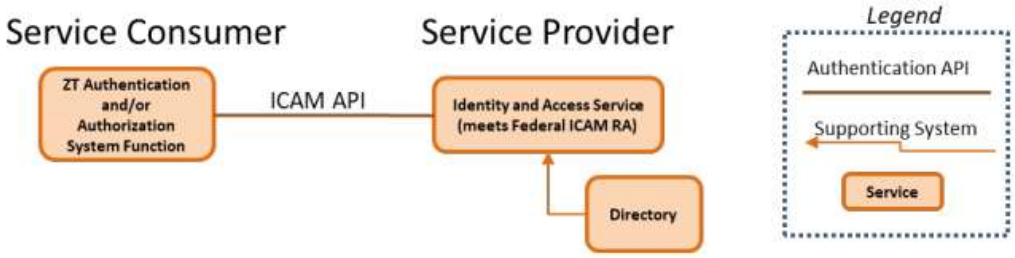


Figura 68 – Servicio *ICAM* (*SvcV-2*).

3.5 La Metodología de su Creador

John Kindervag es sin duda alguna el nombre más prominente en el ambiente de la Confianza Cero, habiendo iniciado su camino en este sentido con las publicaciones realizadas durante su paso por la consultora Forrester [91], que ya analizamos en la sección tercera.

Este egresado de la Universidad de Iowa - curiosamente con un título de *Bachelor of Arts* en comunicaciones - es hoy considerado uno de los más destacados expertos en ciberseguridad, habiendo pasado por la conocida empresa *Palo Alto Networks* [92], siendo miembro directivo de la consultora *ON2IT* [93] *y recientemente unido a la empresa Illumio* [94].

Su extenso currículo incluye publicaciones de gran relevancia sobre el tema, presentaciones en incontables conferencias, haber formado parte del informe *NSTAC* al presidente de los Estados Unidos y ser nombrado personalidad del año en el campo de la ciberseguridad por la revista *CISO*.

Citarlo nuevamente en esta sección es pertinente dado que, habiendo pasado ya más de una década desde su propuesta original, hoy Kindervag ofrece una metodología particular para la adopción de *Zero Trust* en forma simple y sencilla, incluyendo principios, pasos concretos para su implementación y hasta un modelo de madurez.

Esta metodología ha sido expuesta ya en numerosas disertaciones tituladas con el lema “Ganar la guerra cibernética con Confianza Cero” (*Win the Cyberwar with Zero Trust)* [95].

Tales disertaciones ya estandarizadas comienzan con una breve discusión sobre qué significa exactamente el término que nos ocupa, estableciendo que se trata de una estrategia para prevenir exfiltraciones de datos (*data breaches*) e impedir que otros ataques cibernéticos sean exitosos al eliminar la noción de confianza en los sistemas digitales.

A continuación, Kindervag expone sobre las ideas equivocadas que han surgido a través del tiempo en relación con *ZT*. En primer lugar, el considerar qué significa hacer que un sistema sea confiable, recordando que justamente la Confianza Cero supone esa no existencia.

En segundo lugar, descartar que *ZT* esté centrado en la administración de identidades, aclarando que este es solo uno más de los servicios que el modelo consume.

Finalmente, dejar también en claro que no se trata de la adquisición de ningún producto en particular, y que su adopción no tiene por qué ser compleja.

Una vez realizadas las aclaraciones iniciales, se presentan los cuatro niveles de compromiso estratégico que se deben observar al encarar un enfoque de Confianza Cero.

Figura 69 – Los cuatro niveles de la estrategia de *Zero Trust*.

En la parte superior de la figura se puede notar que es imprescindible, como en cualquier planteo estratégico para una organización, el identificar el objetivo fundamental del cual se desprenden todas las iniciativas.

En el caso de la ciberseguridad, este objetivo estratégico fundamental (*Grand Strategy*) es impedir la exfiltración de datos (*Stop Data Breaches*).

La estrategia para implementar entonces es justamente la visión integral de Confianza Cero. Y de esa forma todas las herramientas y técnicas (*Tools and Techniques*) que se utilicen a tal fin quedan relegadas al nivel táctico.

En el nivel operativo finalmente, se posiciona tanto a la plataforma en servicio como a las políticas que se definan y apliquen.

Al comentar sobre qué es estrategia y qué no lo es, Kindervag señala que lo que hoy conocemos como "Defensa en Profundidad" (*Defense in Depth*) se trata simplemente de aumentar el gasto en soluciones parciales y desconectadas entre sí. A tal punto, que a este criterio se lo ha llegado a llamar "Gasto en Profundidad".

Otro tema relacionado es la sobreabundancia de requisitos de cumplimiento (*Compliance*), en donde el profesional de Seguridad Informática se transforma en un burócrata que dedica gran parte de su tiempo al papeleo, y donde además muchos requisitos de un programa se contradicen con los de otros.

También hace referencia a las guías publicadas por las grandes consultoras tales como los "cuadrantes mágicos" (*Magic Quadrant*) de Gartner y los "informes de olas" (*Wave Reports*) de Forrester, argumentando que estas revisiones son individuales para cada tipo de producto, y que no contemplan la necesidad de crear un sistema en donde sus partes interactúen entre sí.

A raíz de toda esta complejidad y trabajo no coordinado, las organizaciones terminan finalmente realizando análisis post mortem, es decir, una vez sucedido el hecho que no se pudo prevenir adecuadamente.

Una definición fundamental que Kindervag reitera es que la confianza es una peligrosa vulnerabilidad que debe ser mitigada, aprovechada por los actores malignos dentro y fuera de la organización.

A efectos de sustentar la afirmación anterior, explica que lo que circula por la red son paquetes de datos, y no personas. Asignar a estos paquetes algún nivel de confianza es antropomorfizar erróneamente a las comunicaciones.

3.5.1 Principios del Diseño

La propuesta simplificada de Kindervag incluye cuatro principios a ser tomados en cuenta de izquierda a derecha al diseñar un sistema de Confianza Cero, que pueden verse en la figura.

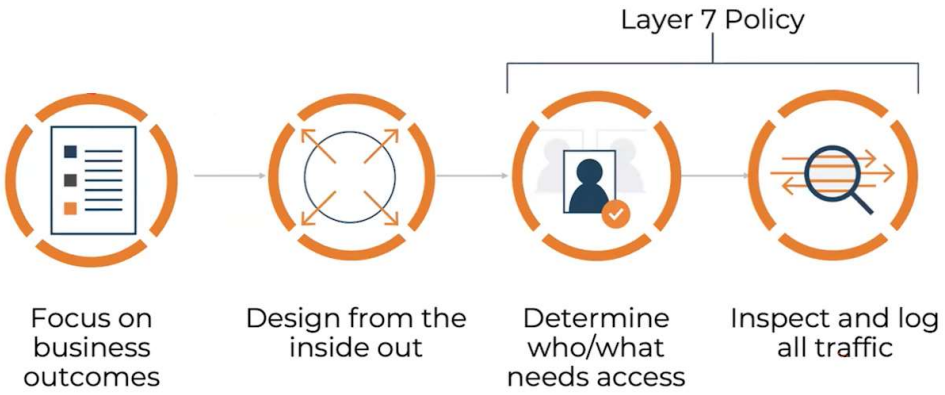


Figura 70 – Los cuatro principios de diseño para *Zero Trust*.

El primero de ellos consiste en determinar cuáles son los objetivos del negocio (*business outcome*) que se desean perseguir, cuál es la gran estrategia, a ser determinada por la alta dirección de la organización.

En base a esos objetivos, se diseña al sistema de protección para cada activo de importancia desde adentro hacia afuera (*inside out*), en claro contraste con la metodología tradicional, focalizada en establecer un perímetro.

Una vez implantado el diseño alrededor de cada activo, se debe determinar qué personas y qué otras entidades necesitan acceso a los mismos (*who/what needs access*).

Estando ya lo diseñado en funcionamiento, se debe inspeccionar y registrar todo el tráfico (*inspect and log*), tomando en consideración que este monitoreo debe producirse hasta la capa séptima (*Layer 7*).

3.5.2 Un Camino de 5 Pasos

El autor de esta metodología comenta que, luego de concretar numerosas implementaciones de *Zero Trust*, ha encontrado que los siguientes cinco pasos son comunes a todas ellas, y son estos los recomendados para cualquier nuevo proyecto.

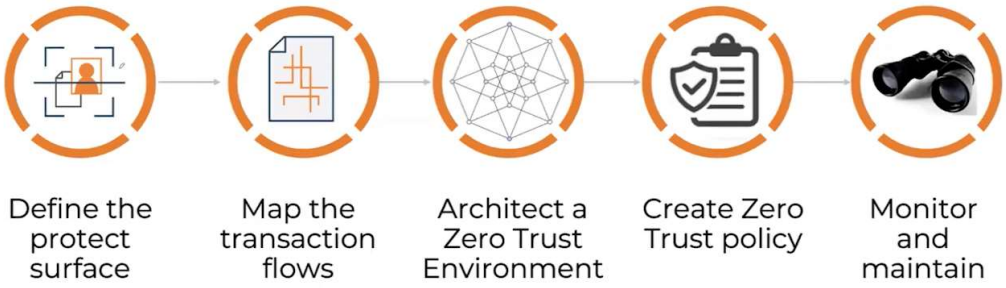


Figura 71 – Los cinco pasos de la metodología.

El primero de estos pasos es sin duda definir cuál es la superficie que debe ser protegida (*protect surface*). Y para explicar cómo hacerlo, Kindervag introduce un acrónimo propio *DAAS (Data, Applications, Assets and Services)* que incluye a todos los elementos que necesitan dicha protección.

El análisis comienza con la identificación de los datos sensibles, y esto se puede lograr considerando a las aplicaciones con las que se los accede. Tenemos además a los activos (*Assets*) con los que se procesan y almacenan, y por último los servicios que permiten que la plataforma funcione, tal como *DNS*, *Active Directory*, *NTP*, entre muchos otros.

Identificado cada elemento perteneciente al conjunto *DAAS*, se crea la superficie de protección alrededor de cada uno en particular, uno a la vez. Esto hace que la metodología sea incremental, iterativa y no disruptiva.

El paso siguiente consiste en realizar un mapeo del flujo de transacciones (*transaction flows*) que involucran al elemento de *DAAS* bajo estudio.

Esto requiere de un entendimiento completo sobre cómo funciona cualquier sistema dentro de la organización. Qué datos se procesan, dónde se almacenan, por qué vías se transmiten. Y en ese proceso, qué activos toman parte en las operaciones, y qué servicios son requeridos.

El tercer paso consiste en la creación de un ambiente de Confianza Cero (*Zero Trust Environment*) alrededor de cada superficie protegida. Y esta es una diferencia sustancial con respecto al enfoque que se propone a través de una arquitectura de referencia, como la que vimos anteriormente del Departamento de Defensa de los Estados Unidos.

En esta metodología, no se puede producir una arquitectura de referencia genérica, dado que al construir el ambiente de Confianza Cero por alrededor de cada elemento *DAAS*, cada implementación es particular.

Una vez organizada la protección de cada superficie individual, se procede entonces a crear las políticas para el acceso a las mismas. Y, por último, se monitorea y se mantiene la plataforma.

El resultado de analizar la información de telemetría con la que se monitorea el ambiente se utiliza para retroalimentar al primer paso del sistema. Kindervag llama a esto el producir un sistema anti frágil [96], que se hace más fuerte a medida que se enfrenta a nuevos sucesos.

La segmentación de la red es el producto de realizar el primer paso, es decir, definir la superficie a proteger. Como ya dijimos, previamente se debe identificar el elemento de *DAAS* sobre el que se desea trabajar.

Un ejemplo muy común en el ámbito de la seguridad informática es el de un ambiente de datos de tarjetas de crédito, en donde sin duda el marco de trabajo a utilizar es el provisto por *PCI*. En la figura siguiente, puede verse cómo funciona la propuesta que estamos describiendo.

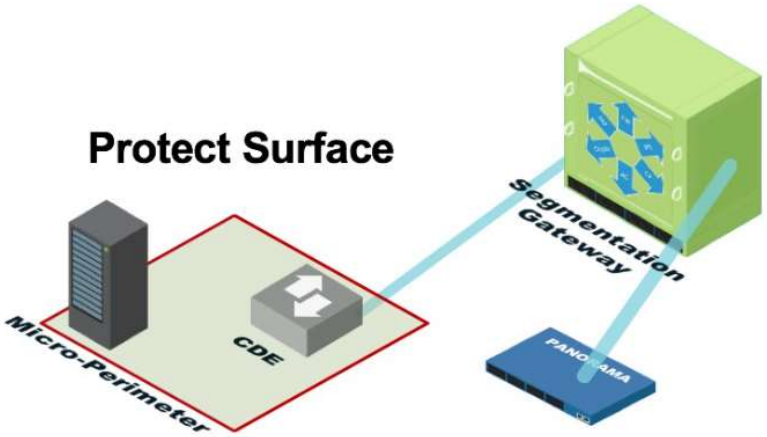


Figura 72 – Segmentación de la red para cada elemento *DAAS*.

El micro perímetro sobre el que vamos a trabajar entonces es el que corresponde a un ambiente de datos de tarjetas de crédito (*CDE - Cardholder Data Environment*).

Identificado este perímetro, se procede a implementar una puerta de enlace para la segmentación (*Segmentation Gateway*). Y esta puede consistir en un cortafuegos de próxima generación, tanto físico como virtual.

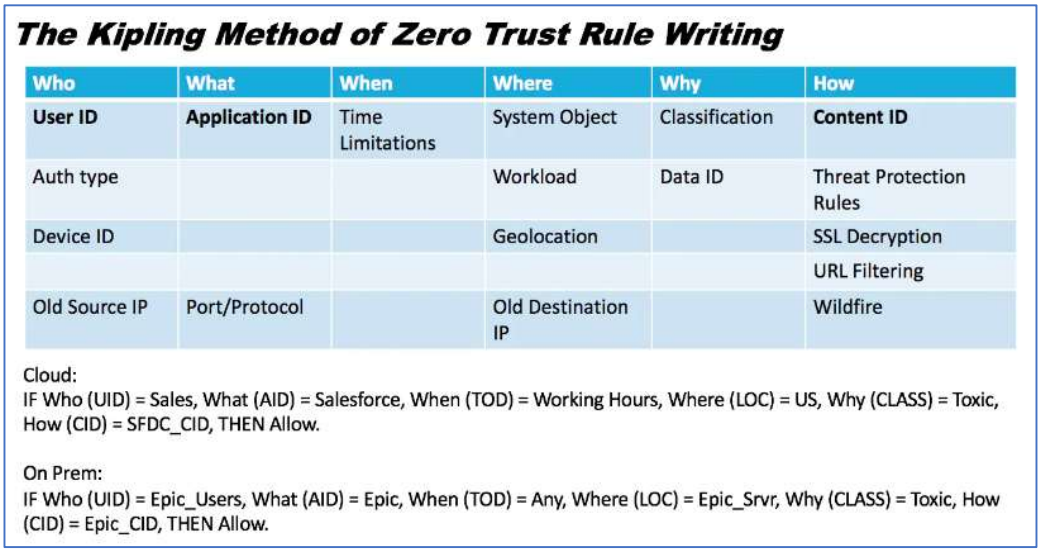
De esta forma la solución puede ubicarse tanto en la nube como en instalaciones propias, pero lo que sí importa es que la puerta de enlace opere sobre todas las capas del modelo *OSI* [97], desde la segunda hasta la séptima.

Este simple esquema es la arquitectura necesaria para Confianza Cero, aplicada a cada recurso en forma individual. El despliegue de la solución completa termina siendo incremental, y en el caso de fallar en algún caso individual, esto no afecta a los demás.

Para complementar adecuadamente este diseño simplificado, es fundamental el considerar que quienes intentan atacar nuestros sistemas, utilizan hoy herramientas cada vez más automatizadas.

Es por ello por lo que según Kindervag, tanto la orquestación como la automatización son imprescindibles.

Lo que se orquesta y automatiza son las políticas, y para reforzar las mismas John ha implementado un método para escribir reglas de acceso que él mismo ha denominado “Método Kipling”, basado en los principios del periodismo derivados del poema escrito en 1902 por ese autor [98].



The Kipling Method of Zero Trust Rule Writing

Who	What	When	Where	Why	How
User ID	**Application ID**	Time Limitations	System Object	Classification	**Content ID**
Auth type			Workload	Data ID	Threat Protection Rules
Device ID			Geolocation		SSL Decryption
					URL Filtering
Old Source IP	Port/Protocol		Old Destination IP		Wildfire

Cloud:
IF Who (UID) = Sales, What (AID) = Salesforce, When (TOD) = Working Hours, Where (LOC) = US, Why (CLASS) = Toxic, How (CID) = SFDC_CID, THEN Allow.

On Prem:
IF Who (UID) = Epic_Users, What (AID) = Epic, When (TOD) = Any, Where (LOC) = Epic_Srvr, Why (CLASS) = Toxic, How (CID) = Epic_CID, THEN Allow.

Figura 73 – El “Método Kipling” para escribir reglas de acceso de *Zero Trust*.

Como se puede ver en el gráfico, para otorgar un permiso de acceso (*Allow*) se verifica el quién (*Who*) incluyendo la identificación del usuario y de su dispositivo, el qué (*What*) que comprende tanto a la aplicación como el puerto y protocolo en uso, y el cuándo (*When*) que refiere al horario en el que se accede a un recurso.

Adicionalmente se verifican datos sobre el dónde (*Where*) relacionados con la ubicación física, la de red, y en qué circunstancias se está trabajando. También el porqué (*Why*) vinculado al motivo del acceso, y por último el cómo (*How*), en donde se detallan las particularidades del permiso tales como el cifrado, y la protección contra código maligno.

Este camino de cinco pasos supone una curva de aprendizaje que se muestra en la figura siguiente [99].

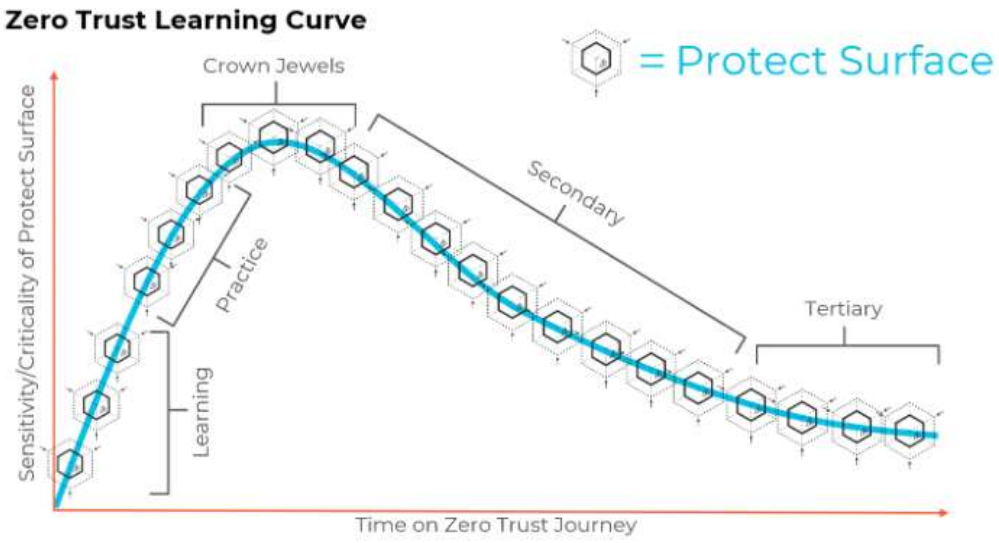


Figura 74 – La curva de aprendizaje de *Zero Trust*.

Lo que Kindervag sugiere para comenzar es trabajar sobre ambientes no críticos a los cuales llama “de aprendizaje” (*Learning*). Con ellos se puede practicar sin mayor disrupción, y las equivocaciones son permitidas.

La etapa de aprendizaje dura poco tiempo, y una vez familiarizado el equipo de implementación con los conceptos de *Zero Trust* bajados al plano real, lo que sigue es trabajar sobre ambientes “de práctica” (*Practice*) que son un poco más delicados que los anteriores, pero no críticos.

Luego de suficiente práctica, llega la hora de trabajar sobre las “joyas de la corona” (*Crown Jewels*), los elementos de *DAAS* de mayor sensibilidad.

Se puede notar en el gráfico que a medida que transcurre el tiempo, la organización irá trabajando luego en sistemas secundarios y terciarios, en un proceso continuo.

Y también se puede determinar un punto de criticidad mínimo a partir del cual no conviene el esfuerzo. No es necesario proteger todo.

3.5.3 Los dos Modelos de Madurez

Toda iniciativa destinada a realizar mejoras en el ámbito de la seguridad de la información necesita de algún mecanismo para medir su progreso y relevar su estado.

La propuesta de John Kindervag también incluye un componente para evaluar la madurez de una organización en cuanto a su adopción del enfoque de Confianza Cero.

En este punto tomaremos como referencia un importante artículo publicado en mayo de 2023 [100], en donde el autor no solo presenta su versión del modelo, sino que además lo compara con el que ya vimos creado por *CISA*.

El artículo comienza enumerando dos errores que cometen quienes inician su camino hacia *Zero Trust*. Uno de ellos, es intentar un despliegue completo de la arquitectura. El otro, es preocuparse demasiado en productos y tecnología, es decir, en el aspecto táctico.

La primera versión del modelo de madurez propuesto por Kindervag y otros fue publicada por Forrester en el año 2017 [101], y en ella se utilizan los cinco pasos que vimos en el punto anterior para concretar su evaluación, asignando a cada paso un puntaje de cero a cinco.

Esta primera versión tomó carácter público en los Estados Unidos al promulgarse el informe "*NSTAC*" al presidente del comité consultivo para la seguridad nacional de las telecomunicaciones (*National Security Telecommunications Advisory Committee*) [102] sobre *Zero Trust* y administración de identidades.

En ese documento, el apéndice A exhibe una tabla que cruza los cinco pasos con igual cantidad de puntajes, como se ve en la figura de la página siguiente. Y en el apéndice B, se ejemplifica un caso específico relacionado con los servicios de directorio.

	Maturity Stage	Initial (1)	Repeatable (2)	Defined (3)	Managed (4)	Optimized (5)
	Description and Characteristics	The initiative is undocumented and performed on an ad hoc basis with processes undefined. Success depends on individual efforts	The process is documented and is predictably repeatable, using lessons learned in the initial phase	Processes for success have been defined and documented	Processes are monitored and controlled; efficacy is measurable	Focus is on continuous optimization
Step of the Five-Step Process	1. **Define the Protect Surface**	The DAAS element is unknown or discovered manually; data classification is not done or is incomplete	The use of automated tools to discover and classify DAAS elements has begun but is not standardized	Data classification training and processes have been introduced and are maturing; protect surface discovery is becoming automated	New or updated DAAS elements are immediately discovered, classified as assigned to the correct protect surface in an automated manner	Discovery and classification processes are fully automated
	2. **Map the Transaction Flows**	Flows are conceptualized-based interviews and workshops	Traditional scanning tools and event logs are used to construct approximate flow maps	A flow mapping process is in place; automated tools are beginning to be deployed	Automated tools create precise flow maps; all flow maps are validated with system owners	Transaction flows are automatically mapped across all locations in real time
	3. **Build a Zero Trust Architecture**	With little visibility and an undefined protect surface, the architecture cannot be properly designed	Protect surface is established based on current resources and priorities	The basics of the protect surface enforcement is complete, including placing segmentation gateways in the appropriate places	Additional controls are added to evaluate multiple variables (e.g., endpoint controls, SaaS and API controls)	Controls are enforced using a combination of hardware and software capabilities
	4. **Create a Zero Trust policy**	Policy is written at Layer 3 (Network)	Additional "who" statements are being identified to address business needs; user IDs of applications and resources are known, but access rights are unknown	The team works with the business to determine who or what should have access to the protect surface	Custom user-specific elements are created and defined by policy, reducing policy space and number of users with access	Layer 7 (Application) policy is written for granular enforcement; only known allowed traffic and legitimate application communication is allowed
	5. **Monitor and Maintain the Network**	Visibility into what is happening on the network is low	Traditional security information and event management or log repositories are available, but the process is still mostly manual	Telemetry is gathered from all controls and is sent to a central data lake	Machine learning tools are applied to the data lake for context into how traffic is used in the environment	Data is incorporated from multiple sources and used to refine steps 1–4; alerts and analyses are automated

Figura 75 – El Apéndice A del "Informe *NSTAC*".

Sin detallar cada uno de los contenidos de cada etapa de madurez (*Maturity Stage*) en cruce con cada paso, podemos notar que en la primera fila de la tabla se describe y enumera las características de estas.

Una etapa “inicial” con puntaje 1 (*Initial*) corresponde a un sistema de trabajo en el cual no se documenta la iniciativa, no están definidos los procesos y los cambios se realizan de manera individual para cada caso.

Una calificación de nivel 2 o “repetible” (*Repeatable*) consiste en la existencia de procesos documentados, que además incluyen lecciones aprendidas. Llegar a un puntaje 3 o “definido” (*Defined*) significa que se documentaron aquellos procesos que suponen el éxito.

La cuarta etapa “administrada” (*Managed*) agrega monitoreo y control a los procesos, y la eficacia de estos es medible. La quinta con el mayor puntaje de cinco es donde la optimización es continua.

Ahora estas definiciones son sin duda muy genéricas y no ofrecen recomendaciones específicas. Sin embargo, el detalle para cada cruce de etapas contra los cinco pasos brinda mayores aclaraciones. Nos ocuparemos de analizar en qué consiste el nivel óptimo en cada etapa.

El primer paso implica definir la superficie a ser protegida. Aquí el nivel óptimo supone que los procesos de descubrimiento y clasificación estén completamente automatizados.

El segundo paso ligado al mapeo de transacciones llega su mayor nivel de madurez cuando esto ocurre en forma también automática a través de toda la plataforma y en tiempo real.

Implementar la arquitectura de Confianza Cero es el tercer paso y para un nivel óptimo los controles se deben hacer cumplir utilizando *software* y *hardware*.

Para la aplicación de las políticas internas en el paso cuarto se deben utilizar reglas granulares que operen en la capa séptima del modelo *OSI*, y utilizando el método Kipling que ya comentamos.

De hecho, el propio “informe *NSTAC*” que es como se lo conoce en el ámbito de *Zero Trust*, lo incluye en el caso de uso expuesto en el apéndice B.

Este caso de uso que el informe utiliza como ejemplo, corresponde a la administración de servicios de directorio tales como el que ofrece el conocido sistema *Active Directory,* y en donde la nomenclatura *DAAS* califica a tal recurso como un activo (*Asset*).

Llegar al directorio de la organización es obviamente un jugoso objetivo para cualquier atacante, y accediendo al mismo puede hacerse de información valiosa o causar daño a la plataforma.

Aquí se pueden distinguir para este ejemplo dos claros casos de uso que son el acceso por parte de un administrador, y el que se otorga a los usuarios. Para establecer las políticas de acceso en ambos casos, se aplica el modelo Kipling.

WHO	WHAT	WHEN	WHERE	WHY	HOW
Admins MFA	Directory Admin Tool App	24/7	Dir_Server_Loc	metadata	IDS/DPI

Figura 76 – Política de acceso para Administradores.

En la figura se muestra la política de acceso para administradores, en donde la identificación (*Who*) de los mismos se realiza evaluando si pertenecen a tal grupo (*Admins*) y si han completado la autentificación multifactorial (*MFA*), y no a través de su ubicación basada en su dirección *IP*.

Una vez identificado, este administrador deberá estar trabajando (*Where*) con alguna herramienta catalogada específicamente como de administración de directorio (*Directory Admin Tool App*), y no en base a su dirección *IP* o puerto.

El horario establecido (*When*) para esta tarea es obviamente amplio, sin restricciones (24/7).

Mientras este administrador inicia su acceso utilizando la herramienta autorizada, su actividad pasa (*How*) por el sistema de detección de intrusiones (*IDS - Intrusion Detection System*) [103] y los chequeos a fondo de paquetes (*DPI - Deep Packet Inspection*) [104].

Este tipo de controles requiere la colocación de un cortafuegos de última generación (*NGFW*) por delante del servicio de directorios en cuestión.

Y aquí se realizará el registro (*metadata*) que brindará la justificación (*Why*) de su solicitud de acceso, y la información necesaria para retroalimentar a la plataforma y permitir la mejora continua.

El ejemplo incluye también una muestra de lo que sería el modelo de madurez aplicado específicamente a los servicios de directorio.

Para conseguir un nivel óptimo y un puntaje de cinco en este caso, la organización deberá contar primero con un inventario exhaustivo de usuarios, dispositivos y grupos.

A partir de ese inventario, se deberá monitorear en tiempo real el total de las actividades tales como cambios en los permisos, reconocimientos, movimientos laterales, y otras, vinculando a los registros estrechamente con el centro de operaciones de seguridad (*SOC - Security Operations Center*) [105].

Por último, las políticas establecidas deben ser dinámicas, y considerar la conducta de cada usuario posterior a su conexión para decidir sobre sus autorizaciones de acceso a los recursos.

El último paso en la metodología propuesta implica monitorear y mantener la plataforma. Para lograr esto, los datos deben ser recolectados desde múltiples fuentes y los mismos deben ser utilizados para la mejora continua, siendo los análisis y el procesamiento de alertas automatizados.

Llegamos entonces al punto en el que presentamos el modelo de madurez simplificado, que Kindervag aclara es el resultado de un refinamiento producto de numerosos proyectos con clientes y casos reales.

Zero Trust Maturity Model

Protect Surface _____
DAAS Element _____

	Initial	Repeatable	Defined	Managed	Optimized
1. Define your Protect Surface	1	2	3	4	5
2. Map the Transaction Flows	1	2	3	4	5
3. Architect a Zero Trust Environment	1	2	3	4	5
4. Create Zero Trust Policy	1	2	3	4	5
5. Monitor and Maintain the Network	1	2	3	4	5

Total Score _____

Figura 77 – El Modelo de Madurez simplificado de John Kindervag.

Lo que importa resaltar aquí es que la evaluación se realiza para cada superficie a proteger (*Protect Surface*) y para cada elemento de *DAAS,* obteniendo cada uno de ellos un puntaje final que tiene un máximo de 25.

Con este método, se logra analizar la plataforma subdividiéndola en porciones manejables, y comparando las distintas evaluaciones se puede decidir sobre cuál conviene invertir un mayor esfuerzo. El valor agregado de todas las evaluaciones dará un nivel de madurez general.

Teniendo entonces ya dos modelos de madurez que hemos visto en este trabajo, el presente y el de *CISA*, surge la inevitable pregunta sobre cuál de ellos es el más adecuado para adoptar.

Kindervag señala como dato de interés, que el modelo de *CISA* tiene como precursor al ecosistema *ZTX* de Forrester que también hemos analizado, y cuyo autor es el Dr. Chase Cunningham, otra de las personalidades de renombre en el ámbito de la Confianza Cero. Y que merece el crédito por su aporte.

Con respecto a la pregunta planteada anteriormente, señala que ambos modelos son complementarios. Hay que recordar que el mismo documento de *CISA* señala que el suyo es solo uno de los caminos para concretar la transición.

El modelo de *CISA* se basa en sus cinco pilares, y el problema es que la mayoría de las organizaciones lo interpretan de forma demasiado literal, lo que a su vez redunda en serios problemas para su implementación.

Por ejemplo, para el caso en que una de ellas decida trabajar sobre el pilar de identidades, pensando en abordar el modelo de izquierda a derecha, entonces se intenta solucionar todos los problemas en este aspecto para toda la plataforma, y esto es un objetivo imposible.

Lo que propone Kindervag para quien desee utilizar los dos modelos, es primero seleccionar una superficie a proteger en particular, y ahí recién analizar cada uno de sus pilares.

4. Últimos Desarrollos

Este trabajo ha sido completado entre el final de 2022 y el de 2023, revisando la línea de tiempo de *Zero Trust* y analizando sus eventos más relevantes desde las publicaciones iniciales de Forrester, seleccionándolos de acuerdo con el propio criterio y los objetivos planteados.

Sin embargo, por obvias razones de espacio y tiempo, muchos otros recursos no han podido ser incluidos, y existen numerosas otras iniciativas, algunas incluso muy recientes, que conviene al menos conocer y citaremos brevemente aquí.

El principal organismo dedicado a fomentar y desarrollar las ideas conceptuales de nuestro tema de estudio y su implementación práctica es hoy sin duda la *Cloud Security Alliance.*

Una interesante observación es que, si bien la *CSA* es una entidad dedicada al desarrollo de estándares para los servicios en la nube, en el caso particular de *ZT* han decidido ocuparse también de las problemáticas que surgen en la instalaciones locales y contextos híbridos.

Ellos ofrecen de forma gratuita un sitio denominado “Centro para el Avance de la Confianza Cero” (*Zero Trust Advancement Center*) [106] que incluye numerosos recursos para la consulta, muchos de los cuales hemos utilizado aquí en este documento.

Asimismo, mantienen un grupo de trabajo (*Zero Trust Working Group*) [107] que se reúne mensualmente, integrado por más de 500 miembros que provienen de importantes empresas de la industria, organizaciones de estándares, la academia y otros interesados, y del cual se formó parte. El propio John Kindervag es uno de sus miembros.

La última reunión antes de nuestra entrega se realizó en forma virtual el 21 de noviembre, y en ella se comentaron los últimos desarrollos en cuanto a eventos, documentos de interés, y otras propuestas.

En principio, se detallaron los eventos más recientes los cuales incluyen la “Cumbre de Investigación Virtual” (*CSA Virtual Research Summit*) [108] llevada a cabo en octubre 17 donde un panel de expertos del cual participó John Kindervag analizaron cuál es el estado actual de la Confianza Cero.

Otro evento de incluso mayor importancia fue la “Cumbre de Confianza Cero” (*CSA Virtual Zero Trust Summit*) [109] realizada el 15 de noviembre, donde se discutieron una variedad de temas encuadrados en implementación, estrategia, planificación y arquitectura, infraestructuras críticas y todo lo relacionado con orquestación, análisis y servicios automatizados.

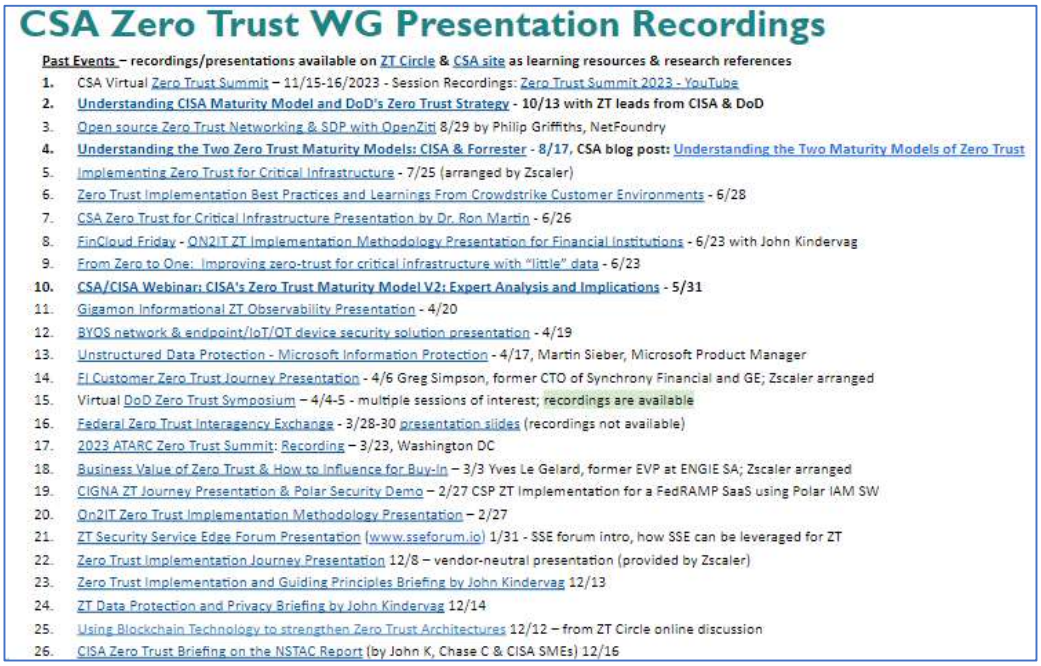
La conferencia denominada “*SECtember*” [110] también tuvo lugar en ese mes, y en ella se reúnen la comunidad de servicios en la nube con la dedicada a la ciberseguridad.

Otros eventos organizados por entidades externas también fueron citados en la reunión mensual de este grupo de trabajo.

La organización denominada “Centro de Investigación Académica para la Tecnología Avanzada” (*ATARC - Advanced Technology Academic Research Center*) [111] sostuvo una conferencia en agosto sobre la transformación y modernización de la ciberseguridad federal con *Zero Trust* en los Estados Unidos, y es de interés el revisar también las otras conferencias que ofrecen en su sitio institucional sobre nuestro tema de estudio.

El volumen de información que ha sido generado en este ultimo tiempo, durante los últimos dos años ha sido realmente notorio, rozando quizás la sobreabundancia de esta.

La figura de la página siguiente muestra un recuento de las presentaciones disponibles las cuales son todas de interés y relacionadas con múltiples temas que hacen al desarrollo del nuevo enfoque para la Seguridad Informática. Todos estos recursos se encuentran disponibles sin cargo desde el sitio que ofrece la *CSA*.



CSA Zero Trust WG Presentation Recordings

Past Events – recordings/presentations available on ZT Circle & CSA site as learning resources & research references

1. CSA Virtual Zero Trust Summit – 11/15-16/2023 - Session Recordings: Zero Trust Summit 2023 - YouTube
2. **Understanding CISA Maturity Model and DoD's Zero Trust Strategy - 10/13 with ZT leads from CISA & DoD**
3. Open source Zero Trust Networking & SDP with OpenZiti 8/29 by Philip Griffiths, NetFoundry
4. **Understanding the Two Zero Trust Maturity Models: CISA & Forrester - 8/17, CSA blog post:** Understanding the Two Maturity Models of Zero Trust
5. Implementing Zero Trust for Critical Infrastructure - 7/25 (arranged by Zscaler)
6. Zero Trust Implementation Best Practices and Learnings From Crowdstrike Customer Environments - 6/28
7. CSA Zero Trust for Critical Infrastructure Presentation by Dr. Ron Martin - 6/26
8. FinCloud Friday - QN2IT ZT Implementation Methodology Presentation for Financial Institutions - 6/23 with John Kindervag
9. From Zero to One: Improving zero-trust for critical infrastructure with "little" data - 6/23
10. **CSA/CISA Webinar: CISA's Zero Trust Maturity Model V2: Expert Analysis and Implications - 5/31**
11. Gigamon Informational ZT Observability Presentation - 4/20
12. BYOS network & endpoint/IoT/OT device security solution presentation - 4/19
13. Unstructured Data Protection - Microsoft Information Protection - 4/17, Martin Sieber, Microsoft Product Manager
14. FI Customer Zero Trust Journey Presentation - 4/6 Greg Simpson, former CTO of Synchrony Financial and GE; Zscaler arranged
15. Virtual DoD Zero Trust Symposium – 4/4-5 - multiple sessions of interest; recordings are available
16. Federal Zero Trust Interagency Exchange - 3/28-30 presentation slides (recordings not available)
17. 2023 ATARC Zero Trust Summit: Recording – 3/23, Washington DC
18. Business Value of Zero Trust & How to Influence for Buy-In – 3/3 Yves Le Gelard, former EVP at ENGIE SA; Zscaler arranged
19. CIGNA ZT Journey Presentation & Polar Security Demo – 2/27 CSP ZT Implementation for a FedRAMP SaaS using Polar IAM SW
20. Qn2IT Zero Trust Implementation Methodology Presentation – 2/27
21. ZT Security Service Edge Forum Presentation (www.sseforum.io) 1/31 - SSE forum intro, how SSE can be leveraged for ZT
22. Zero Trust Implementation Journey Presentation 12/8 – vendor-neutral presentation (provided by Zscaler)
23. Zero Trust Implementation and Guiding Principles Briefing by John Kindervag 12/13
24. ZT Data Protection and Privacy Briefing by John Kindervag 12/14
25. Using Blockchain Technology to strengthen Zero Trust Architectures 12/12 – from ZT Circle online discussion
26. CISA Zero Trust Briefing on the NSTAC Report (by John K, Chase C & CISA SMEs) 12/16

Figura 78 – Múltiples presentaciones disponibles sobre *Zero Trust*.

El grupo de trabajo de *CSA* dedicado a la Confianza Cero opera en conjunto con organizaciones de los Estados Unidos que incluyen a *NIST*, *CISA*, el Departamento de Defensa, *ATARC*, *The Open Group*, *NSTAC*, entre otras, y también con líderes de la industria que participan en distintas modalidades, más otros grupos internos dedicados a temas relacionados.

Lo que sí cabe notar, es que todas las iniciativas de estos grupos y que hemos visto en el presente trabajo, están circunscriptas al ámbito norteamericano. Nos ocuparemos de esto más adelante en esta sección.

Varios documentos importantes producidos por el *ZT Working Group* han sido ya publicados o se encuentran en etapas finales de revisión.

Uno de ellos es el denominado "Guía y Principios para la Administración de Accesos e Identidades" (*Zero Trust Principles and Guidance for Identity and Access Management*) [112].

Otro es uno de carácter más fundacional, con nombre "Principios Rectores de la Confianza Cero" (*Zero Trust Guiding Principles*) [113].

Adicionalmente, una herramienta fundamental para poder sostener conversaciones con el cuerpo directivo en cada organización, titulado "Comunicando el Valor de la Confianza Cero para el Negocio" (*Communicating the Business Value of Zero Trust)* [114].

Como dijimos, muchas otras publicaciones se encuentran en proceso de confección o revisión final. Y en particular, se está trabajando en una guía para cada uno de los cinco pasos de implementación que vimos en el punto 3.5.2.

Por el momento, la guía para el primero de esos pasos, "Definir la Superficie de Confianza Cero a Proteger" (*Defining the Zero Trust Protect Surface*) [115] ya está siendo revisada por los pares.

Las iniciativas de este grupo de trabajo de *CSA* están organizadas en ocho equipos que se ocupan de cada uno de los pilares planteados por *CISA* en su modelo de madurez. Cada equipo liderado por expertos de la industria y con sus respectivos miembros voluntarios.

Un primer equipo se dedica a los temas relacionados con principios, estrategia y gobierno, y ya han producido los principios rectores que mencionamos antes, preparando la versión segunda.

Al corriente se encuentran desarrollando una guía para pequeñas y medianas empresas, y cruzando los controles de la conocida matriz [116] que publica *CSA* desde hace tiempo con los pilares del modelo de madurez de Confianza Cero. Por lo que pronto, se contaría con un sistema de controles específicos para *ZT*, y esto es algo de gran importancia.

Por último, también colaboran con otros equipos en una guía y evaluación para la privacidad.

El siguiente equipo orientado al pilar de identidades, ya produjo el entregable que mencionamos anteriormente, y continúa preparando otros relacionados con el cifrado asimétrico aplicado a los objetivos de *Zero Trust*, el sistema de autentificación *FIDO* [117] y un glosario con terminología específica para este dominio.

Por su parte, el equipo a cargo del pilar de dispositivos, ya se encuentra cerca de publicar una guía de *ZT* para la infraestructura crítica, y otra que estará lista más adelante para Internet de las Cosas.

Con respecto al pilar de redes, un documento que describe cómo realizar el mapeo de los flujos de transacciones (*Mapping Transaction Flows for Zero Trust*) y que corresponde al segundo de los cinco pasos en la metodología de John Kindervag ya se ubica en estado de revisión interna.

Quienes se encuentran vinculados al pilar de aplicaciones y cargas de trabajo no están produciendo documentación propia, pero sí están asistiendo a los demás equipos.

En cuanto al pilar de datos, este grupo ya ha entregado para su revisión el trabajo dedicado a la definición de la superficie a proteger, y está a punto de finalizar la guía sobre privacidad, que ya mencionamos en ambos casos.

Para el tema visibilidad y análisis, se encuentran en progreso un estudio del espacio de soluciones disponibles, y una guía arquitectónica. Es interesante considerar que es aquí donde entrará en juego el enfoque relacionado con la inteligencia artificial.

El último grupo dedicado a la implementación, la arquitectura y el modelo de madurez de *ZT* ya ha entregado la publicación relacionada con comunicar el valor de negocio de la Confianza Cero.

Habíamos comentado que todas estas iniciativas están circunscritas al contexto de los avances realizados dentro de los Estados Unidos.

Sin embargo, *NIST* también trabaja en conexión con organismos internacionales, lo que incluye al Instituto de Ingenieros en Electrónica y Electricidad (*IEEE - Institute of Electrical and Electronics Engineers*), la Organización para Estandarización Internacional (*ISO - International Organization for Standarization*), la Comisión Electrotécnica Internacional (*IEC - International Electrotechnical Commission*) y la Unión Internacional de Telecomunicaciones (*ITU - International Telecommunications Union*).

El nivel de avance de estos organismos con respecto a nuestra temática es reducido, y en cierta medida relacionado con el hecho de que ellos manejan sus propios estándares y terminología.

Algunos de los equipos que se están interesando de a poco en la Confianza Cero son el grupo de estudio SG-17 de la *ITU* [118], y el comité JTC 1/SC 27 [119] de la *ISO*.

El instituto *IEEE* por su parte, se encuentra desarrollando dos proyectos directamente vinculados con *ZT*. Ellos son impulsados por un grupo de trabajo denominado *Zero Trust Security Working Group - ZTSWG* [120] iniciado ya en el año 2020 y dedicado al desarrollo de estándares, guías, capacitación y conferencias.

El primero de ellos se denomina “Práctica Recomendada para la Seguridad” (*Recommended Practice for Zero Trust Security*) y numerado como P2887 [121]. Su foco consiste en recomendar arquitecturas e implementaciones seguras, con cierto interés en el perímetro definido por software. También en establecer terminología, pero al estilo particular de la *ISO* y no utilizando la propuesta por *NIST*.

El segundo es mucho más reciente iniciado en septiembre de 2023, numerado P3409 [122] y denominado “Estándar para un Marco de Trabajo de Seguridad” (*Standard for a Zero Trust Security Framework)*. Como su nombre lo indica, este pasaría a ser el estándar fundacional publicado por *IEEE*.

Volviendo al contexto norteamericano, es imprescindible el incluir una referencia al trabajo que está realizando el Centro de Excelencia para la Ciberseguridad Nacional que depende de *NIST* (*NCCOE - National Cybersecurity Center of Excellence*).

Esta entidad se encuentra desarrollando una serie de documentos de guía para la implementación de una arquitectura de Confianza Cero, agrupados en la denominación SP 1800-35 [123]. El esfuerzo incluye la colaboración de importantes empresas proveedoras de soluciones, profesionales e ingenieros del ámbito de la Seguridad Informática.

La serie de publicaciones de enorme interés todavía reviste el carácter de borrador, en etapas preliminares segunda y tercera.

Se trata de cinco documentos, donde el primero consiste en un resumen ejecutivo, el segundo trata sobre el enfoque, la arquitectura y características de seguridad, el tercero demuestra cómo se implementaron diez soluciones y qué productos se utilizaron, el cuarto describe casos de uso, y el quinto se dedica a las importantes cuestiones relacionadas con el riesgo y el cumplimiento.

En un futuro cercano este paquete de documentos estará terminado y será un recurso invaluable que servirá como guía para toda organización que desee abordar el enfoque de Confianza Cero.

La *Cloud Security Alliance* también ha lanzado recientemente lo que se puede considerar como la primera certificación oficial de la industria asociada a nuestro tema, denominada “Certificado de Competencia” (*CCZT - Certificate of Competence in Zero Trust*) [124].

Por su parte, la organización denominada *The Open Group* también cuenta con su propio grupo de trabajo [125] y sus iniciativas incluyen una arquitectura propia más varios proyectos adicionales orientados a contribuir al cuerpo de conocimientos general.

5. Conclusiones

Se propuso como objetivo general de este trabajo, el desarrollar una guía clara y actualizada sobre el tema “Confianza Cero” que pudiese ser de utilidad para que un profesional de la Seguridad de la Información tome decisiones. Este es el aporte que supone el mismo.

De ese objetivo general, se desprenden como secundarios el encontrar una definición de ser posible única, entender cuál es su utilidad en el ámbito mencionado y cómo debería ser aplicado.

A partir de tales premisas, también se incluyó el determinar si *Zero Trust* consiste únicamente en una expresión de moda (*buzzword*), o si, por el contrario, implica un verdadero cambio de paradigma en cuanto a la concepción de la disciplina que nos ocupa.

En primera medida entonces, afirmaremos que *ZT* es al mismo tiempo una frase de moda, y un nuevo paradigma para la gestión de la Seguridad Informática.

Sin duda el término posee todas las cualidades necesarias para su aprovechamiento en el marco de la comercialización de productos y servicios, y esto está probado por su utilización por parte de todos los actores relevantes en la industria.

Como comprobación de tal afirmación, podemos citar las referencias de líderes tales como Microsoft [126], IBM [127], Crowdstrike [128], AWS [129], Cloudflare [130], Paloalto Networks [131] entre muchos, muchos otros.

Se trata de una expresión compacta y concreta, que sugiere directamente el refuerzo completo de las protecciones eliminando la noción de cualquier tipo de confianza, la cual se reduce directamente a cero.

Confianza Cero como expresión, engloba todas las características de una frase de moda.

Según la definición del diccionario Merriam-Webster [132] se trata de una frase técnica con poco significado utilizada para impresionar al hombre común. Sin duda la expresión bajo análisis tiene ese efecto, el de impresionar.

Pero, además, se trata de una herramienta que es necesaria en el ámbito de los negocios [133] y tiene utilidad en el contexto laboral, como toda expresión de ese tipo, brindando el beneficio de un entendimiento mutuo.

Lo que no ocurre con *Zero Trust* es la pérdida de significado o su relevancia a través del tiempo, y eso lo hemos comprobado a través de todo el análisis cronológico realizado en este trabajo.

Como frase de moda, Confianza Cero cumple entonces con todos los requisitos para esa finalidad, pero el concepto comprende un significado mucho más amplio.

En relación con el primero de los objetivos secundarios planteados, el de encontrar una definición única y concreta para el término en cuestión, podemos afirmar que no la hemos encontrado.

En cada uno de los documentos que hemos tomado como referencia para el análisis temporal de su evolución se han expuesto distintas definiciones.

Forrester define a *Zero Trust* en sus documentos originales como un "nuevo modelo para la Seguridad Informática" y una nueva forma de pensar sobre la misma. Google también lo considera un modelo.

NIST por su parte lo describe como una "colección de conceptos e ideas" en una definición que realmente no es muy precisa. Esta afirmación, es un juicio personal de quien redacta este trabajo.

El resto de los actores que hemos analizado aquí coinciden de una u otra forma en que se trata de un modelo. Así lo caracteriza la Orden Ejecutiva 14028 aunque esta refiere directamente a la arquitectura, mientras que *CISA* replica la definición de *NIST*.

El Departamento de Defensa también habla de un modelo, pero lo enfoca en las políticas de acceso dinámicas y la verificación del estado observable de los agentes que solicitan acceso a los recursos.

En este trabajo hemos adoptado como base para el análisis aquellos recursos que no suponen relación alguna con ningún fabricante, consultor o proveedor de servicios en particular, es decir, manteniendo una perspectiva agnóstica.

Es por ello por lo que no se han tomado en cuenta las incontables definiciones que a través del tiempo han aportado los numerosos actores de la industria, donde cada uno ha desarrollado su propia concepción de lo que significa *Zero Trust*, a veces para su beneficio.

Solo como ejemplos, citamos nuevamente la definición de Microsoft [126] que lo posiciona tanto como un modelo y como una estrategia, mientras que IBM [134] lo describe además como un marco de trabajo.

La conocida Paloalto Networks [135] lo ve como un enfoque estratégico, y Okta [136] indica también que se trata de un marco.

Podríamos continuar de manera casi indefinida, pero se invita al lector a ejecutar una simple búsqueda en el omnisciente navegador usando el término que nos ocupa para encontrar incontables y distintos puntos de vista.

Por su parte John Kindervag el denominado padre fundador de la Confianza Cero expone que se trata de una estrategia.

Nos encontramos entonces envueltos en este dilema de más de dos opciones donde debemos determinar si *ZT* es sólo una colección de ideas, un marco de trabajo, un modelo, o un enfoque o visión de carácter estratégico.

Desde ya descartamos la definición de *NIST* relacionada con la colección de ideas, la cual consideramos imprecisa.

En cuanto a la noción de “marco de trabajo” (*framework*), nos basamos en la definición del diccionario Merriam-Webster [137] en donde se lo describe como una estructura conceptual de base.

Y en ese sentido, se podría pensar en *Zero Trust* como un marco, si se consideran los principios básicos y pilares enumerados por *NIST* y extendidos por *CISA* y el Departamento de Defensa.

La única salvedad que se podría hacer en este sentido es que, a diferencia de otros marcos de trabajo mucho más definidos que se utilizan en nuestro ámbito y en otros, *ZT* todavía no cuenta con una estructura documental bien delineada.

Un ejemplo de un marco bien definido podría ser justamente, el que utiliza el Departamento de Defensa para sus arquitecturas *DoDAF* que vimos en el punto 3.4.

En cuanto a la interpretación de ZT como un "modelo" (*model*), y tomando en cuenta que existen numerosas definiciones para este término, revisamos sus múltiples significados desde el diccionario Oxford [138].

Aceptamos que pudiera tratarse de una representación simplificada o idealizada de un sistema de Seguridad de la Información, y lo entendemos también en el contexto de "modelo a seguir".

Y en cuanto a los motes de "enfoque" (*approach*) [139] que es una forma particular de ver las cosas, y "visión" (*vision*) [140] que consiste en una imagen futura de la realidad, también podemos aprobarlos, pero en el contexto que expondremos a continuación.

Coincidimos con la interpretación de John Kindervag en cuanto al carácter estratégico del concepto de Confianza Cero. Y no estando conformes con ninguna de las definiciones estudiadas, incluso con la de este autor que la considera simplemente una estrategia, proponemos la nuestra:

Zero Trust comprende tanto una visión como un enfoque estratégicos sobre la Seguridad de la Información, en continua evolución y cuya finalidad es prevenir la exfiltración de datos.

Contando ahora con una definición concreta de propia autoría, podemos pasar al siguiente objetivo que es el determinar cuál es la utilidad de esta visión o enfoque.

Desde ya lo que elaboramos lo expresa claramente, y es importante notar que existe una diferencia entre la concepción clásica basada en el perímetro fijo donde lo que se pretendía era impedir los accesos no autorizados.

Aquí conviene recordar que el cambio de paradigma propuesto significa abandonar el proverbio ruso “confiar, pero verificar” (*trust but verify*) por la premisa “nunca confiar, siempre verificar” (*never trust, always verify*) [141].

El nuevo enfoque de la Confianza Cero, y así lo expresa su creador como vimos en sus exposiciones, da por sentado que esos accesos no autorizados son inevitables, y por otra parte, también existen actores malintencionados por dentro de la organización.

Por lo tanto, lo que se quiere lograr con *ZT* es impedir las exfiltraciones, considerando que la plataforma puede estar siempre comprometida. Es una forma muy diferente de concebir a la Seguridad Informática.

Pasamos entonces al tercer objetivo, que es el determinar cómo se aplica este enfoque en el contexto práctico.

Hemos observado a lo largo de este trabajo que no existe una referencia arquitectónica única para el despliegue de *Zero Trust*, sino que existen sucesivas propuestas en continua evolución, lo que da soporte adicionalmente a nuestra particular definición.

La *ZTA* ha mejorado desde su planteo conceptual inicial por parte de Forrester, pasando por una primera aproximación por parte de *BeyondCorp* y el intento fundacional de *NIST*, donde solo la solución desarrollada por Google consiste en una arquitectura puesta en funcionamiento.

Hemos dedicado una sección entera por otra parte al diseño arquitectónico también conceptual del Departamento de Defensa.

Y sostenemos que este diseño y su documento descriptivo son sin duda la propuesta más completa y de mayor complejidad disponible hoy, siempre haciendo referencia a soluciones agnósticas no presentadas por un proveedor de software o hardware en particular.

Si bien no existe entonces una arquitectura única de referencia para cualquier organización interesada en implementar la Confianza Cero, podemos afirmar que existe una serie de componentes necesarios para que la misma sea exitosa.

En primer lugar, y antes de implementar cualquiera de esos componentes en particular, se debe realizar un relevamiento de todas las superficies a proteger (*protect surface*) existentes.

Una vez determinadas todas ellas, es fundamental el realizar el estudio de su seguridad de a una por vez, empezando por las menos críticas como práctica inicial y luego trasladando lo aprendido hacia lo que se conoce como "joyas de la corona" (*crown jewels*).

Habiendo hecho esa salvedad inicial, podemos mencionar que el centro de nuestra atención debe ser puesto en los datos, ya que toda la estrategia de *Zero Trust* se despliega para que no se produzcan exfiltraciones.

El foco en los datos evoluciona luego hacia el concepto de *DAAS*, incluyendo entonces a los activos, las aplicaciones y los servicios. Y con estos cuatro elementos podemos definir cada una de las superficies a ser protegidas, siguiendo la mecánica descrita por John Kindervag.

Para cada una de estas superficies entonces, debemos considerar los pilares planteados por el Departamento de Defensa que no son más que una extensión de lo ya propuesto por el Modelo de Madurez de *CISA*. Y en base a los mismos, desplegar las capacidades necesarias asociadas.

Una implementación exitosa de *Zero Trust* debería comenzar entonces por el tratamiento seguro de los datos, lo que incluye el cifrado en tránsito, reposo y a nivel de campos, clasificación, etiquetado, más la prevención de exfiltraciones y administración de sus derechos.

Como requisito siguiente los dispositivos deben ser adecuadamente gestionados a través de un sistema centralizado de higiene.

La infraestructura de red debe habilitar a las funciones de Confianza Cero aplicando micro y macro segmentación, y un perímetro definido por software. La administración de usuarios y *NPE* debe ser federada y los controles de acceso deben incluir la autentificación multifactorial, el análisis de comportamiento y su combinación con elementos biométricos.

Las aplicaciones y las cargas de trabajo (*workloads*) deben adecuarse a los mejores estándares de *DevSecOps,* observar las protecciones sobre la cadena de abastecimiento y mantener una segmentación de procesos, orientándose en un futuro hacia un esquema de *API*.

El objetivo final de todo el despliegue citado más arriba debe ser el de su implementación y actualización completamente automatizada, asistida por un sistema de monitoreo que se apoye en herramientas de aprendizaje máquina e inteligencia artificial para gestionar todas las políticas.

Para cumplir con tal requerimiento, es necesario contar con una considerable base de datos de eventos y/o una conexión a un servicio de inteligencia de amenazas provisto por un tercero especializado.

Este monitoreo constante debe favorecer la continua retroalimentación de toda la arquitectura de Confianza Cero para transformarla en un verdadero sistema “anti-frágil”.

La utilización de sistemas de orquestación automatizada basados en aprendizaje máquina e inteligencia artificial son indispensables debido a que los atacantes también los utilizan. Es la única forma de mantener su ritmo.

Ahora como comentario final, se debería tomar en cuenta la posibilidad de que los sistemas utilizados sufran “alucinaciones” tal como las que ocurren con los grandes modelos de lenguaje (*LLM - large language models*) [142], y que ello tenga serias implicancias sobre el funcionamiento de las plataformas adecuadas a *Zero Trust*.

Si esas plataformas son críticas, los resultados de un error en el otorgamiento o denegación de acceso podrían ser desastrosos.

La configuración correcta de los modelos de aprendizaje máquina utilizados será crucial para conseguir la protección y funcionalidad deseada, y es sin duda un nuevo campo de acción para los profesionales de la Seguridad de la Información. [143] [144].

Por otra parte, el continuo avance del conocimiento y del desarrollo de herramientas para todos los pilares y capacidades que hemos analizado es lo que hace que el estado óptimo de madurez para la Confianza Cero sea un objetivo en constante redefinición.

6. Bibliografía

[1] Marsh S., “Formalizing Trust as a Computational Concept”, University of Stirling, 1994. https://dspace.stir.ac.uk/handle/1893/2010#.Y7HRE3bMI2w (Consultada el 29/11/2022).

[2] Lacey D., Biography, https://certinfosec.org/?speaker=david-lacey (Consultada el 21/10/2023).

[3] The Open Group, Jericho Forum Publications, https://publications.opengroup.org/catalogsearch/result/?q=jericho (Consultada el 21/10/2023).

[4] The Global Identity Foundation, https://www.globalidentityfoundation.org/ (Consultada el 21/10/2023).

[5] Cloud Security Alliance, https://cloudsecurityalliance.org/ (Consultada el 21/10/2023).

[6] Jericho Forum, “What is the Jericho Forum”, https://collaboration.opengroup.org/jericho/vision_wp.pdf, (Consultada el 28/10/2023).

[7] Jericho Forum, “Jericho Forum Commandments”, https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf, (Consultada el 28/10/2023).

[8] Jericho Forum, “Cloud Cube Model”, https://collaboration.opengroup.org/jericho/cloud_cube_model_v1.0.pdf, (Consultada el 29/10/2023).

[9] The Open Group, “Framework for Secure Collaboration-Oriented Architectures (O-SCOA)”, https://publications.opengroup.org/g127, (Consultada el 29/10/2023).

[10] Cloud Security Alliance – “Security Guidance for Critical Areas of Focus in Cloud Computing v4.0”, https://cloudsecurityalliance.org/research/guidance/, (Consultada el 29/10/2023).

[11] U.S. Department of Defense, “Global Information Grid Architectural Vision”, https://www.acqnotes.com/Attachments/DoD%20GIG%20Architectural%20Vision,%20June%2007.pdf, (Consultada el 14/10/2023).

[12] Catteddu D, “Searching for Zero Trust”, https://www.brighttalk.com/webcast/10415/534258?utm_source=cvent (Consultada el 29/10/2023).

[13] Kindervag J., “No more chewy Centers: Introducing the Zero Trust Model of Information Security”, https://crystaltechnologies.com/wp-content/uploads/2017/12/forrester-zero-trust-model-information-security.pdf, (Consultada el 4/11/2023).

[14] Kindervag J., “Build Security Into Your Network’s DNA: The Zero Trust Network Architecture”, https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf, (Consultada el 4/11/2023).

[14a] PCI Security Standards Council, “Document Library”, https://www.pcisecuritystandards.org/document_library/?category=pcidss (Consultada el 26/11/2023).

[15] Cloud Security Alliance – “SDP Specification v1.0”, https://cloudsecurityalliance.org/artifacts/sdp-specification-v1-0/, (Consultada el 4/11/2023).

[16] IETF RFC 4301, “Security Architecture for the Internet Protocol”, https://www.rfc-editor.org/rfc/rfc4301, (Consultada el 4/11/2023).

[17] kisi, “Authentication Protocols: LDAP vs Kerberos vs OAuth2 vs SAML vs RADIUS”, https://www.getkisi.com/blog/authentication-protocols-overview, (Consultada el 6/11/2023).

[18] KEYFACTOR, “What is PKI? A Public Key Infrastructure Definitive Guide”, https://www.keyfactor.com/education-center/w(Consultada el 6/11/2023).hat-is-pki/, (Consultada el 6/11/2023).

[19] AWS, “¿Qué es la autenticación multifactor (MFA)?”, https://aws.amazon.com/es/what-is/mfa/, (Consultada el 6/11/2023).

[20] Conran M., “Zero Trust: Single Packet Authorization | Passive authorization”, https://network-insight.net/2019/06/18/zero-trust-single-packet-authorization-passive-authorization/, (Consultada el 11/11/2023).

[21] Cloudflare, “¿Qué es el TLS mutuo (mTLS)?”, https://www.cloudflare.com/es-es/learning/access-management/what-is-mutual-tls/, (Consultada el 11/11/2023).

[22] Cloudflare, "¿Qué es IPsec? | Cómo funcionan las VPN IPsec", https://www.cloudflare.com/es-es/learning/network-layer/what-is-ipsec/, (Consultada el 11/11/2023).

[23] Tidmarsh D., "Man-in-the-Middle (MitM) Attack: Definition, Types, & Prevention Methods", https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/man-in-the-middle-attack-mitm/, (Consultada el 11/11/2023).

[24] Cloudflare, "¿Qué es un ataque de denegación de servicio (DoS)?", https://www.cloudflare.com/es-es/learning/ddos/glossary/denial-of-service/, (Consultada el 11/11/2023).

[25] Lenaerts-Bergmans B., "SQL INJECTION", https://www.crowdstrike.com/cybersecurity-101/sql-injection/, (Consultada el 11/11/2023).

[26] Lenaerts-Bergmans B., "CROSS SITE SCRIPTING (XSS)", https://www.crowdstrike.com/cybersecurity-101/cross-site-scripting-xss/, (Consultada el 11/11/2023).

[27] IBM Topics, "What is an API?", https://www.ibm.com/topics/api, (Consultada el 11/11/2023).

[28] Camarillo G., RFC 5694, "Peer-to-Peer (P2P) Architecture: Definition, Taxonomies, Examples, and Applicability", https://www.rfc-editor.org/rfc/rfc5694.html, (Consultada el 11/11/2023).

[29] Cloud Security Alliance, "Software-Defined Perimeter (SDP) Specification v2.0", https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-zero-trust-specification-v2/, (Consultada el 11/11/2023).

[30] Mell P., Grance T., NIST SP 800-145, "The NIST Definition of Cloud Computing", https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf, (Consultada el 11/11/2023).

[31] VMWare Topics, "What is VDI (Virtual Desktop Infrastructure)?", https://www.vmware.com/topics/glossary/content/virtual-desktop-infrastructure-vdi.html, (Consultada el 11/11/2023).

[32] IBM Topics, "What is internet of things?", https://www.ibm.com/topics/internet-of-things, (Consultada el 11/11/2023).

[33] Sermersheim J., RFC 4511, “Lightweight Directory Access Protocol (LDAP): The Protocol”, https://www.rfc-editor.org/rfc/rfc4511,
(Consultada el 11/11/2023).

[34] Google, “A new approach to China”,
https://googleblog.blogspot.com/2010/01/new-approach-to-china.html,
(Consultada el 11/11/2023).

[35] Google, “¿Qué es BeyondCorp?”,
https://cloud.google.com/beyondcorp,
(Consultada el 11/11/2023).

[36] Okta, “A New Approach to Enterprise Security”,
https://www.beyondcorp.com,
(Consultada el 11/11/2023).

[37] Usenix, “Revista Digital ;login:”,
https://www.usenix.org/publications/loginonline;
(Consultada el 12/11/2023).

[38] Ward R., Beyer B., “BeyondCorp: A New Approach to Enterprise Security”,
https://storage.googleapis.com/pub-tools-public-publication-data/pdf/43231.pdf,
(Consultada el 12/11/2023).

[39] Cisco, “Examine how the RADIUS Works”,
https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html, (Consultada el 12/11/2023).

[40] Fruhlinger J., Snyder J., “802.1X: What you need to know about this LAN-authentication standard”, https://www.networkworld.com/article/2216499/wireless-what-is-802-1x.html,
(Consultada el 12/11/2023).

[41] Osborn B. y otros, “BeyondCorp: Design to Deployment at Google”,
https://storage.googleapis.com/pub-tools-public-publication-data/pdf/44860.pdf,
(Consultada el 12/11/2023).

[42] Cittadini L. y otros, “BeyondCorp Part III: The Access Proxy”,
https://storage.googleapis.com/pub-tools-public-publication-data/pdf/45728.pdf,
(Consultada el 12/11/2023).

[43] Cloudflare, “What is a reverse proxy? | Proxy servers explained”,
https://www.cloudflare.com/learning/cdn/glossary/reverse-proxy/,
(Consultada el 12/11/2023).

[44] OpenID, “What is OpenID Connect”,
https://openid.net/developers/how-connect-works/,
(Consultada el 12/11/2023).

[45] SSH Academy, “What is SSH (Secure Shell)?”,
https://www.ssh.com/academy/ssh,
(Consultada el 12/11/2023).

[46] gRPC, “About gRPC”,
https://grpc.io/about/,
(Consultada el 12/11/2023).

[47] Google Chrome Remote Desktop,
https://remotedesktop.google.com/?pli=1,
(Consultada el 12/11/2023).

[48] Peck J. y otros, “Migrating to BeyondCorp”,
https://storage.googleapis.com/pub-tools-public-publication-data/pdf/f29b3e764b1122d508b7b53544a3bbadd6cd1101.pdf, (Consultada el 12/11/2023).

[49] Escobedo V. y otros, “BeyondCorp 5 – The User Experience”,
https://storage.googleapis.com/pub-tools-public-publication-data/pdf/c8da594124dab1f91e6750995e2b7805403b19f1.pdf, (Consultada el 12/11/2023).

[50] King H. y otros, “BeyondCorp – Building a Healthy Fleet”,
https://storage.googleapis.com/pub-tools-public-publication-data/pdf/b9b4a09a913e410b7c45f3fbacec4d350e38146f.pdf, (Consultada el 12/11/2023).

[51] Goncalves G. y otros, “BeyondCorp and the long tail of Zero Trust”,
https://www.usenix.org/publications/loginonline/beyondcorp-and-long-tail-zero-trust,
(Consultada el 12/11/2023).

[52] BeyondCorp Enterprise,
https://cloud.google.com/beyondcorp-enterprise?hl=en,
(Consultada el 12/11/2023).

[53] BeyondProd,
https://cloud.google.com/docs/security/beyondprod,
(Consultada el 12/11/2023).

[54] Cunningham C., “The Zero Trust eXtended (ZTX) Ecosystem”,
https://www.cisco.com/c/dam/m/en_sg/solutions/security/pdfs/forrester-ztx.pdf,
(Consultada el 16/11/2023).

[55] Cisco, “What Is a Next-Generation Firewall?”, https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html, (Consultada el 16/11/2023).

[56] Okta, “What Is an SDK? Software Development Kits Explained”, https://www.okta.com/identity-101/what-is-an-sdk/, (Consultada el 16/11/2023).

[57] Cunningham C., “Dr. Zero Trust”, https://www.drzerotrust.com/, (Consultada el 7/10/2023)

[58] Rose S. y otros, NIST SP 800-207, “Zero Trust Architecture”, https://csrc.nist.gov/publications/detail/sp/800-207/final, (Consultado el 18/11/2023).

[59] Jean-Mary C., Harrison L., “An Overview of X.509 Certificates”, https://www.ibm.com/support/pages/system/files/inline-files/An_Overview_of_x.509_certificates.pdf, (Consultada el 18/11/2023).

[60] IBM Topics, “What is SIEM?”, https://www.ibm.com/topics/siem, (Consultada el 18/11/2023).

[61] Varios Autores, NIST SP 800-37, “Risk Management Framework”, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf (Consultada el 18/11/2023).

[62] Biden J., “Executive Order 14028 on Improving the Nation’s Cybersecurity”, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, (Consultada el 18/11/2023).

[63] FedRAMP, Federal Risk and Authorization Management Program, https://www.fedramp.gov/, (Consultada el 18/11/2023).

[64] Young S., OMB M-22-09, “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles”, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf, (Consultada el 18/11/2023).

[65] CISA, “Zero Trust Maturity Model v2.0”, https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf, (Consultada el 19/11/2023).

[66] Department of Defense, “Zero Trust Reference Architecture v2”, https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf, (Consultada el 20/11/2023).

[67] Department of Defense, “DoDAF Architectural Framework v2.02”, https://dodcio.defense.gov/Library/DoD-Architecture-Framework/, (Consultada el 20/11/2023).

[68] IBM Topics, “What is machine learning?”, https://www.ibm.com/topics/machine-learning, (Consultada el 20/11/2023).

[69] IBM Topics, “What is robotic process automation (RPA)?”, https://www.ibm.com/topics/machine-learning, (Consultada el 20/11/2023).

[70] Department of Defense, “Enterprise (ICAM), Reference Design v1”, https://dodcio.defense.gov/Portals/0/Documents/Cyber/DoD_Enterprise_ICAM_Reference_Design.pdf, (Consultada el 20/11/2023).

[71] IBM Topics, “What is data loss prevention (DLP)?”, https://www.ibm.com/topics/data-loss-prevention, (Consultada el 20/11/2023).

[72] Roach C., “What is Digital Rights Management (DRM)? (The Definitive Guide)”, https://www.digitalguardian.com/blog/what-digital-rights-management, (Consultada el 22/11/2023).

[73] IBM Topics, “What is UEBA (user and entity behavior analytics)?”, https://www.ibm.com/topics/ueba, (Consultada el 22/11/2023).

[74] Microsoft, “What is privileged access management (PAM)?”, https://www.microsoft.com/en/security/business/security-101/what-is-privileged-access-management-pam, (Consultada el 22/11/2023).

[75] Trusted Computing Group, “Trusted Platform Module (TPM) Summary”, https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary/, (Consultada el 22/11/2023).

[76] Red Hat, “What is DevSecOps?”, https://www.redhat.com/en/topics/devops/what-is-devsecops, (Consultada el 22/11/2023).

[77] IBM Topics, “What is SOAR?”, https://www.ibm.com/topics/security-orchestration-automation-response, (Consultada el 22/11/2023).

[78] International Biometrics + Identity Association, “Behavioral Biometrics”, https://www.ibia.org/download/datasets/3839/Behavioral, (Consultada el 22/11/2023).

[79] Microsoft, “Dynamic data masking”, https://learn.microsoft.com/en-us/sql/relational-databases/security/dynamic-data-masking?view=sql-server-ver16, (Consultada el 22/11/2023).

[80] Data Governance Institute, “The Data Governance Basics”, https://datagovernance.com/the-data-governance-basics/, (Consultada el 22/11/2023).

[81] Varios Autores, NIST SP 800-37, “Risk Management Framework”, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf (Consultada el 25/11/2023).

[82] MeriTalk, “Comply-to-Connect is Key to Zero Trust for DoD”, https://www.meritalk.com/2023/02/23/comply-to-connect-is-key-to-zero-trust-for-dod, (Consultada el 25/11/2023).

[83] Red Hat, “What is software supply chain security?”, https://www.redhat.com/en/topics/security/what-is-software-supply-chain-security, (Consultada el 25/11/2023).

[84] CSO Online, “What is RBAC? Role-based access control explained”, https://www.csoonline.com/article/572177/what-is-rbac-role-based-access-control-explained.html, (Consultado el 25/11/2023).

[85] Okta Blog, “What Is Attribute-Based Access Control (ABAC)?”, https://www.okta.com/blog/2020/09/attribute-based-access-control-abac/, (Consultada el 25/11/2023).

[86] CISA, “Cybersecurity Governance”, https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-governance, (Consultada el 25/11/2023).

[87] Cloudflare, “What is defense in depth? | Layered security”, https://www.cloudflare.com/learning/security/glossary/what-is-defense-in-depth/, (Consultada el 25/11/2023).

[88] Oracle, “What is a Data Lake?”,
https://www.oracle.com/big-data/data-lake/what-is-data-lake/,
(Consultada el 25/11/2023).

[89] Oracle, “What is Big Data?”,
https://www.oracle.com/big-data/what-is-big-data/,
(Consultada el 25/11/2023).

[90] Cisco, “What Is a Next-Generation Firewall?”,
https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html, (Consultada el 25/11/2023).

[91] Forrester, “Analyst: John Kindervag”,
https://www.forrester.com/staticassets/staticPDF_back/BIO1960.pdf,
(Consultada el 26/11/2023).

[92] Paloalto Networks, “Get to know John Kindervag”,
https://www.paloaltonetworks.com/blog/author/john-kindervag/,
(Consultada el 26/11/2023).

[93] ON2IT, “John Kindervag”,
https://on2it.net/john-kindervag/,
(Consultada el 26/11/2023).

[94] Illumio, “Zero Trust Creator John Kindervag Joins Illumio…”,
https://www.illumio.com/news/illumio-appoints-john-kindergav-chief-evangelist,
(Consultada el 26/11/2023).

[95] Kindervag J., “Win the Cyberwar with Zero Trust”,
https://media.dau.edu/media/t/1_r4me8hbp,
(Consultada el 26/11/2023).

[96] Taleb, N., “Antifragile: Things That Gain from Disorder”,
Random House, New York, 2012.

[97] ISO-IEC 7498-1, “Information Technology – Open Systems Interconnection – Basic Reference Model: The Basic Model”,
http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip, (Consultada el 26/11/2023).

[98] Kindervag J., “All Layers are not Created Equal”,
https://www.paloaltonetworks.com/blog/2019/05/network-layers-not-created-equal/
(Consultada el 26/11/2023).

[99] Kindervag J., “The Zero Trust Learning Curve: Deploying Zero Trust One Step at a Time”, https://www.paloaltonetworks.com/blog/2020/04/network-zero-trust-learning-curve/ (Consultada el 28/11/2023).

[100] Kindervag J., “Understanding the Two Maturity Models of Zero Trust”, https://cloudsecurityalliance.org/blog/2023/05/17/understanding-the-two-maturity-models-of-zero-trust/ (Consultada el 28/11/2023).

[101] Balaouras S. y otros, “Assess Your Network Security Architecture with Forrester’s Zero Trust Maturity Model”, https://silo.tips/download/res136187 (Consultada el 28/11/2023).

[102] NSTAC, “Zero Trust and Trusted Identity Management” https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management.pdf, (Consultada el 28/11/2023).

[103] Paloalto Networks, “What is an Intrusion Detection System?”, https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids, (Consultada el 29/11/2023).

[104] Fortinet, “What Is Deep Packet Inspection (DPI)?”, https://www.fortinet.com/resources/cyberglossary/dpi-deep-packet-inspection, (Consultada el 29/11/2023).

[105] IBM Topics, “Security Operations Center (SOC)”, https://www.ibm.com/topics/security-operations-center, (Consultada el 29/11/2023).

[106] CSA, “Zero Trust Advancement Center”, https://cloudsecurityalliance.org/zt/, (Consultada el 9/12/2023).

[107] CSA, “Zero Trust Working Group”, https://cloudsecurityalliance.org/research/working-groups/zero-trust/, (Consultada el 9/12/2023).

[108] CSA, “Virtual Research Summit”, https://www.csaresearchsummit.com/event/17e14892-a68e-4db9-82a9-528bf4bdbb4e/summary, (Consultada el 9/12/2023).

[109] CSA, “Zero Trust Summit”, https://csazerotrustsummit.com/, (Consultada el 9/12/2023).

[110] CSA, “SECtember”,
https://www.sectember.com/event/a39529bd-b9b2-4019-9fd4-b75d59bfabc4/summary,
(Consultada el 9/12/2023).

[111] ATARC, “Zero Trust: Driving Transformation and Modernization in Federal Cybersecurity”, https://atarc.org/event/zero-trust-modernization/,
(Consultada el 9/12/2023).

[112] CSA, “Zero Trust Principles and Guidance for Identity and Access Management (IAM)”,
https://cloudsecurityalliance.org/artifacts/zero-trust-principles-and-guidance-for-iam/,
(Consultada el 9/12/2023).

[113] CSA, “Zero Trust Guiding Principles”,
https://cloudsecurityalliance.org/artifacts/zero-trust-guiding-principles/,
(Consultada el 9/12/2023).

[114] CSA, “Communicating the Business Value of Zero Trust”,
https://cloudsecurityalliance.org/artifacts/communicating-the-business-value-of-zero-trust/,
(Consultada el 9/12/2023).

[115] CSA, “Defining the Zero Trust Protect Surface”,
https://cloudsecurityalliance.org/artifacts/defining-the-zero-trust-protect-surface/,
(Consultada el 9/12/2023).

[116] CSA, “Cloud Controls Matrix (CCM)”,
https://cloudsecurityalliance.org/research/cloud-controls-matrix/,
(Consultada el 9/12/2023).

[117] FIDO Alliance, “How FIDO Works”,
https://fidoalliance.org/how-fido-works/,
(Consultada el 9/12/2023).

[118] ITU, “SG17: Security”,
https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx,
(Consultada el 9/12/2023).

[119] ISO/IEC JTC 1/SC 27, “Information security, cybersecurity and privacy protection”,
https://www.iso.org/committee/45306.html,
(Consultada el 9/12/2023).

[120] IEEE, “Zero Trust Security Working Group (ZTSWG)”,
https://development.standards.ieee.org/myproject-web/public/view.html#/interest/8425,
(Consultada el 9/12/2023).

[121] IEEE P2887, “Recommended Practice for Zero Trust Security”,
https://standards.ieee.org/ieee/2887/10278/,
(Consultada el 9/12/2023).

[122] IEEE P3409, “Standard for a Zero Trust Security Framework”,
https://standards.ieee.org/ieee/3409/11386/,
(Consultada el 9/12/2023).

[123} NCCOE, “Implementing a Zero Trust Architecture”,
https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture,
(Consultada el 9/12/2023).

[124] CSA, “Certificate of Competence in Zero Trust (CCZT)”,
https://cloudsecurityalliance.org/education/cczt/,
(Consultada el 9/12/2023).

[125] The Open Group, “Zero Trust Architecture”,
https://www.opengroup.org/forum/security-forum-0/zerotrustsecurityarchitecture,
(Consultada el 9/12/2023).

[126] Microsoft Security, “Embrace proactive security with Zero Trust”,
https://www.microsoft.com/en-us/security/business/zero-trust,
(Consultada el 2/12/2023).

[127] IBM Topics, “Qué es Zero Trust”,
https://www.ibm.com/es-es/topics/zero-trust,
(Consultada el 2/12/2023).

[128] Raina K., “What is Zero Trust”,
https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/,
(Consultada el 2/12/2023).

[129] Amazon Web Services, “Confianza Cero en AWS”,
https://aws.amazon.com/es/security/zero-trust/,
(Consultada el 2/12/2023).

[130] Cloudflare, “Cloudflare Zero Trust”,
https://developers.cloudflare.com/cloudflare-one/,
(Consultada el 2/12/2023).

[131] Paloalto Networks, “What is a Zero Trust Architecture”,
https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture,
(Consultada el 2/12/2023).

[132] Merriam-Webster, “buzzword”,
https://www.merriam-webster.com/dictionary/buzzword,
(Consultada el 2/12/2023).

[133] Etorre B., “What’s the next business buzzword?”,
https://www.proquest.com/docview/206683339,
(Consultada el 2/12/2023).

[134] IBM Topics, “What is Zero Trust”,
https://www.ibm.com/topics/zero-trust,
(Consultada el 2/12/2023).

[135] Paloalto Networks, “Zero Trust”,
https://www.paloaltonetworks.com/zero-trust,
(Consultada el 2/12/2023).

[136] Shepherd J., “What is Zero Trust Security?”,
https://www.okta.com/blog/2019/01/what-is-zero-trust-security/,
(Consultada el 2/12/2023).

[137] Merriam-Webster, “framework”,
https://www.merriam-webster.com/dictionary/framework,
(Consultada el 2/12/2023).

[138] Oxford English Dictionary, “model”,
https://www.oed.com/dictionary/model_n?tl=true,
(Consultada el 2/12/2023).

[139] Cambridge Dictionary, “approach”,
https://dictionary.cambridge.org/dictionary/english/approach,
(Consultada el 4/12/2023).

[140] Cambridge Dictionary, “vision”,
https://dictionary.cambridge.org/dictionary/english/vision,
(Consultada el 4/12/2023).

[141] Kerman A., “Zero Trust Cybersecurity: ‘Never Trust, Always Verify’”,
https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify,
(Consultada el 6/12/2023).

[142] Heyer S., “Generative AI - Understand and Mitigate Hallucinations in LLMs”,
https://medium.com/google-cloud/generative-ai-understand-and-mitigate-hallucinations-in-llms-8af7de2f17e2, (Consultada el 6/12/2023).

[143] Markets and Markets, “Artificial Intelligence in Cybersecurity Market”, https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-security-market-220634996.html, (Consultada el 6/12/2023).

[144] Goss A., “Will AI Replace Cyber Security Jobs? The New Cyber Future”, https://www.stationx.net/will-ai-replace-cyber-security-jobs, (Consultada el 6/12/2023).