NIST Publicación especial 800-207

Arquitectura de confianza cero

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

Esta publicación se encuentra disponible en inglés de forma gratuita en
https://doi.org/10.6028/NIST.SP.800-207

S E G U R I D A D I N F O R M Á T I C A

NIST

National Institute of Standards and Technologies

U. S. Department of Commerce

NIST Publicación especial 800-207

Arquitectura de confianza cero

Scott Rose
Oliver Borchert
División de Tecnologías Avanzadas de Red
Laboratorio de Tecnologías de la Información

Stu Mitchell
Stu2Labs
Stafford, VA

Sean Connelly
Agencia de Ciberseguridad y Seguridad de las Infraestructuras
Departamento de Seguridad Nacional

Esta publicación se encuentra disponible en inglés de forma gratuita en:
https://doi.org/10.6028/NIST.SP.800-207

Traducción al español
Dreamlab Technologies Chile
Yanina Ángela Bettati (2023)

Departamento de Comercio de EE. UU.
Wilbur L. Ross, Jr., Secretario

Instituto Nacional de Normas y Tecnología Walter Copan, Director del NIST y Subsecretario de Comercio para Normas y Tecnología

Autoridad

Esta publicación ha sido desarrollada por NIST de conformidad con sus responsabilidades estatutarias en virtud de la Ley Federal de Modernización de la Seguridad de la Información (FISMA) de 2014, 44 U.S.C. § 3551 y siguientes, Ley Pública (P.L.) 113-283. NIST es responsable de desarrollar normas y directrices de seguridad de la información, incluidos los requisitos mínimos para los sistemas de información federales, pero dichas normas y directrices no se aplicarán a los sistemas de seguridad nacional sin la aprobación expresa de los funcionarios federales apropiados que ejercen la autoridad política sobre dichos sistemas. Esta directriz es coherente con los requisitos de la Circular A-130 de la Oficina de Gestión y Presupuesto (OMB).

Nada de lo que figura en esta publicación debe interpretarse como contradictorio con las normas y directrices que el Secretario de Comercio ha hecho obligatorias y vinculantes para los organismos federales en virtud de la autoridad legal. Estas directrices tampoco deben interpretarse como una alteración o sustitución de las autoridades existentes del Secretario de Comercio, el Director de la OMB o cualquier otro funcionario federal. Esta publicación puede ser utilizada por organizaciones no gubernamentales de forma voluntaria y no está sujeta a derechos de autor en los Estados Unidos. No obstante, el NIST agradecerá que se cite su procedencia.

Publicación especial 800-207 del Instituto Nacional de Estándares y Tecnología (NIST)
Inst. Nac. Est. Technol. Publ. Espec. 800-207, 59 páginas (agosto de 2020)
CODEN: NSPUE2

Esta publicación está disponible en inglés de forma gratuita en:
https://doi.org/10.6028/NIST.SP.800-207

Los comentarios sobre esta publicación pueden enviarse a

Instituto Nacional de Estándares y Tecnología
A la atención de: Advanced Network Technologies Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8920) Gaithersburg, MD 20899-8920
Correo electrónico: zerotrust-arch@nist.gov
Todos los comentarios están sujetos a la Ley de Libertad de Información (FOIA).

Informes sobre tecnología de sistemas informáticos

El Laboratorio de Tecnología de la Información (ITL, por su nombre en inglés, Information Technology Laboratory) del Instituto Nacional de Estándares y Tecnología (NIST) promueve la economía y el bienestar público de Estados Unidos a través de su liderazgo técnico en la infraestructura de medición y normalización del país. El ITL desarrolla pruebas, métodos de prueba, datos de referencia, implementaciones de pruebas de concepto y análisis técnicos para avanzar en el desarrollo y el uso productivo de la tecnología de la información. Las responsabilidades del ITL incluyen el desarrollo de normas y directrices de gestión, administrativas, técnicas y físicas para la seguridad rentable y la privacidad de la información no relacionada con la seguridad nacional en los sistemas de información federales. La serie de publicaciones especiales 800 informa sobre las investigaciones, directrices y actividades de divulgación del ITL en materia de seguridad de los sistemas de información, así como sobre sus actividades de colaboración con organizaciones industriales, gubernamentales y académicas.

Resumen

La confianza cero (ZT) es el término que designa un conjunto de paradigmas de ciberseguridad en evolución que desplazan las defensas de los perímetros estáticos basados en la red para centrarse en los usuarios, los activos y los recursos. Una arquitectura de confianza cero (ZTA) utiliza principios de confianza cero para planificar la infraestructura y los flujos de trabajo industriales y empresariales. La confianza cero asume que no hay confianza implícita concedida a activos o cuentas de usuario basada únicamente en su ubicación física o de red (es decir, redes de área local frente a Internet) o basada en la propiedad de los activos (propiedad de la empresa o personal). La autenticación y la autorización (tanto del sujeto como del dispositivo) son funciones discretas que se realizan antes de establecer una sesión con un recurso de la empresa. La confianza cero es una respuesta a las tendencias de las redes empresariales que incluyen usuarios remotos, dispositivos personales (BYOD, por su nombre en inglés *bring-your-owned-device*) y activos basados en la nube que no se encuentran dentro de los límites de una red propiedad de la empresa. La confianza cero se centra en proteger los recursos (activos, servicios, flujos de trabajo, cuentas de red, etc.), no los segmentos de red, ya que la ubicación de la red ya no se considera el componente principal de la postura de seguridad del recurso. Este documento contiene una definición abstracta de la arquitectura de confianza cero (ZTA) y ofrece modelos generales de despliegue y casos de uso en los que la confianza cero podría mejorar la postura global de seguridad de las tecnologías de la información de una empresa.

Palabras claves

Arquitectura, ciberseguridad, empresa, seguridad de la red, confianza cero.

Agradecimientos

Este documento es fruto de la colaboración entre múltiples agencias federales y está supervisado por el Consejo Federal de CIO. El subgrupo de arquitectura es responsable del desarrollo de este documento, pero hay personas concretas que merecen reconocimiento. Entre ellas se encuentran Greg Holden, director del proyecto ZTA del Consejo Federal de CIO; Alper Kerman, director del proyecto ZTA del NIST/Centro Nacional de Ciberseguridad; y Douglas Montgomery.

En la traducción, un especial reconocimiento a las personas que colaboraron de alguna u otra forma con la gestión, redacción, terminología específica y compaginación: Fabien Spychiger, CEO Dreamlab Technologies Chile; Javier Toro Rodríguez, Cybersecurity Service Manager, Dreamlab Tecnologies Chile; Stéphane Bürgi, Senior Technical Writer Dreamlab Technologies Chile y Celeste Gauna, Cyberintelligence Analyst Dreamlab Technologies Chile.

Audiencia

Este documento pretende describir la confianza cero para los arquitectos de seguridad empresarial. Se intenta ayudar a la comprensión de la confianza cero para los sistemas civiles no clasificados y proporcionar una hoja de ruta para migrar y desplegar conceptos de seguridad de confianza cero a un entorno empresarial. Los responsables de ciberseguridad de las agencias, los administradores de red y los directivos también pueden obtener información sobre la confianza cero y la ZTA a partir de este documento. Esta guía no pretende ser un plan de despliegue único para la ZTA, ya que cada empresa tendrá sus propios casos de uso y activos de datos que requieran protección. Si se parte de un conocimiento sólido del negocio y los datos de la organización, se obtendrá un enfoque sólido de la confianza cero.

Información sobre marcas registradas

Aviso de divulgación de patentes

AVISO: el laboratorio de tecnologías de la información (ITL) ha solicitado que los titulares de registros de patentes cuyo uso pueda ser necesario para el cumplimiento de las orientaciones o requisitos de esta publicación comuniquen dichos registros de patentes al ITL. Sin embargo, los titulares de patentes no están obligados a responder a las solicitudes de patentes del ITL y el ITL no ha realizado una búsqueda de patentes para identificar cuáles, si las hubiera, pueden aplicarse a esta publicación.

Tras la convocatoria del ITL para la identificación de reclamaciones de patentes cuyo uso pueda ser necesario para el cumplimiento de las orientaciones o requisitos de esta publicación, se ha recibido notificaciones de una o más de dichas reclamaciones.

Mediante la publicación, el ITL no adopta posición alguna con respecto a la validez o el alcance de cualquier reivindicación de patente o de cualquier derecho relacionado con ella. No obstante, el o los titulares conocidos de patentes han facilitado a NIST una carta de garantía en la que declaran o bien (1) una renuncia general en el sentido de que no poseen y no tienen actualmente la intención de poseer ninguna reivindicación esencial de patente, o bien (2) que negociarán licencias libres de cánones o que devenguen cánones con otras partes sobre una base no discriminatoria demostrable con términos y condiciones razonables.

Para más detalles se puede consultar en **zerotrust-arch@nist.gov.**

No se declara ni se da a entender que esta sea la única licencia necesaria para evitar la infracción de patentes en el uso de esta publicación.

Tabla de contenidos

Lista de apéndices

Lista de figuras

Lista de tablas

1 Introducción

La infraestructura de una empresa típica se ha convertido en algo cada vez más complejo. Una única organización puede gestionar varias redes internas, oficinas remotas con su propia infraestructura local, personas a distancia o móviles y servicios en la nube. Esta complejidad ha superado los métodos tradicionales de seguridad de red perimetral, puesto que no existe un perímetro único y fácilmente identificable para la compañía. También, esta seguridad ha demostrado su insuficiencia, ya que una vez que los atacantes han traspasado la barrera, el movimiento lateral no tiene obstáculos.

Esta difícil tarea ha impulsado el desarrollo de un nuevo modelo de ciberseguridad conocido como «confianza cero» (ZT, por su denominación en inglés *zero trust*). El enfoque ZT se centra, fundamentalmente, en la protección de los datos y los servicios, pero puede y debe ampliarse para incluir todos los activos de la empresa (dispositivos, aplicaciones, componentes de infraestructura, virtuales y de la nube) y los sujetos (usuarios finales, aplicaciones y otras entidades no humanas que solicitan información de los recursos). A lo largo de este documento, se utilizará la palabra *sujeto* a menos que la sección se refiera directamente a un usuario final humano, en cuyo caso, se utilizará específicamente *usuario* en lugar del término más genérico *sujeto*. Los modelos de seguridad de confianza cero parten de la base de que el atacante está presente en el entorno y que el ambiente de la compañía no es diferente (o no es más confiable) a cualquier otro que no sea de la organización. En este nuevo paradigma, se debe asumir que no hay seguridad implícita. Se deben analizar y evaluar continuamente los riesgos para los activos y actividades corporativas y luego promulgar protecciones para mitigarlos. En la confianza cero, estas protecciones implican, por lo general, restringir el acceso a los recursos (como los datos, los medios informáticos y las aplicaciones o servicios) solo a aquellos sujetos y activos identificados como necesarios para el acceso. Además, consiste en autenticar y autorizar continuamente la identidad y la postura de seguridad de cada solicitud de acceso.

Una arquitectura de confianza cero (ZTA, por su nombre en inglés *zero trust architecture*) es una estrategia de ciberseguridad empresarial basada en los principios de la confianza cero y concebida para prevenir las violaciones de datos y limitar los movimientos laterales internos. Esta publicación analiza la ZTA, sus componentes lógicos, los posibles escenarios de implementación y las amenazas. Asimismo, presenta una guía general para las organizaciones que deseen migrar a un diseño de confianza cero y examina las políticas federales[1] pertinentes que pueden afectar o influir en una arquitectura de confianza cero.

La ZT no es una simple arquitectura, sino un conjunto de principios orientativos para el flujo de trabajo, el diseño del sistema y las operaciones que pueden utilizarse para mejorar la postura de seguridad de cualquier clasificación o nivel de sensibilidad (FIPS199)[2]. La transición a la ZTA es

[1] N. del T.: en este ejemplo y cada vez que se mencionen las políticas o agencias federales, se estará haciendo referencia a entidades de Estados Unidos.

[2] N. del T.: el FIPS199 es un documento publicado por NIST que presenta las normas para la categorización de la seguridad de la información federal y del sistema de información en Estados Unidos. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

un proceso en el que una organización evalúa el riesgo de esa misión y no puede lograrse simplemente con una sustitución masiva de la tecnología. Ahora bien, muchas organizaciones ya cuentan con elementos de la ZTA en su infraestructura empresarial. Estas deben tratar de implementar gradualmente los principios de confianza cero, cambios en los procesos y soluciones tecnológicas para proteger sus datos y funciones empresariales mediante casos de uso. La mayoría de las infraestructuras funcionarán en un modo híbrido, al tiempo que seguirán invirtiendo en iniciativas de modernización de TI (tecnologías de la información) y mejorando los procesos de negocio de la organización.

Para que este sistema sea efectivo, se deben implementar prácticas exhaustivas de seguridad y recuperación de la información. Si se equilibra con las orientaciones y las políticas de ciberseguridad existentes, la gestión de la identidad y del acceso, el monitoreo continuo y las mejores prácticas, la ZTA puede proteger contra las amenazas comunes y mejorar la postura de seguridad de las empresas mediante un enfoque de riesgo gestionado.

1.1 Historia de los programas de confianza cero relacionados con las agencias federales

El concepto de confianza cero ha estado presente en la ciberseguridad antes de que se acuñara el término *confianza cero*. La Agencia de Sistemas de Defensa de la Información (DISA, por su nombre en inglés Defense Information Systems Agency) y el Departamento de Defensa publicaron un trabajo sobre una estrategia empresarial más segura denominada «núcleo negro» (BCORE, por su nombre en inglés *black core*), la cual implicaba pasar de un modelo de seguridad basado en el perímetro a uno focalizado en la seguridad de las transacciones individuales (JERICHO). El Foro Jericho —organización para proteger los sistemas y datos empresariales— del 2004 dio a conocer la idea de desperimetrización: los límites de la seguridad implícita basada en la ubicación de la red y las limitaciones de confiar en defensas únicas y estáticas en un gran segmento de red. El concepto de desperimetrización evolucionó y mejoró hasta convertirse en el término más amplio de confianza cero, que fue acuñado posteriormente por John Kindervag[3] mientras trabajaba en Forrester[4]. Luego, se convirtió en el término utilizado para describir diversas soluciones de ciberseguridad que se alejaban de la seguridad basada en la ubicación de la red y, en cambio, se centraban en la evaluación de la confianza en cada transacción. Tanto la industria privada como la enseñanza superior también han experimentado esta evolución desde la seguridad basada en el perímetro hacia una estrategia sustentada en los principios de la confianza cero.

Desde hace más de una década se insta a los organismos federales a cambiar hacia una protección basada en estos nuevos principios, mediante la creación de prestaciones y políticas como la Ley Federal de Gestión de Seguridad de la Información (FISMA por su nombre en inglés Federal Information Security Modernization Act); seguida del Marco de Gestión de Riesgos (RMF por su apelación en inglés Risk Management Framework); la Gestión Federal de Identidades, Credenciales y Accesos (FICAM, por su nombre en inglés Federal Identity,

[3] https://go.forrester.com/blogs/next-generation-access-and-zero-trust/
[4] Cualquier mención de productos o servicios comerciales dentro de los documentos de NIST es solo para información y no implica una recomendación o respaldo por parte de NIST.

Credential, and Access Management); la Conexión a Internet de confianza TIC (por su nombre en inglés Trusted Internet Connections), y los programas de Diagnóstico y Mitigación Continuos (CDM por su denominación en inglés Continuous Diagnostics and Mitigation). Todos estos planes tienen como objetivo restringir el acceso a los datos y a los recursos a las partes autorizadas. Cuando se iniciaron estos programas, estaban limitados por las capacidades técnicas de los sistemas de información. Las políticas de seguridad eran mayormente estáticas y se aplicaban en grandes «cuellos de botella» al alcance de la empresa para obtener el mejor resultado posible. A medida que la tecnología se consolida, se están pudiendo analizar y evaluar continuamente las solicitudes de acceso de forma dinámica y granular, sobre una base de «necesidad de acceso» que permite mitigar la exposición de los datos ocasionada por cuentas comprometidas, atacantes que monitorean las redes y otras amenazas.

1.2 Estructura del documento

El resto del documento se encuentra organizado de la siguiente manera:

- **Sección 2:** define la ZT y la ZTA al mismo tiempo que enumera algunos postulados a la hora de diseñar una ZTA para una empresa. Esta sección también incluye una lista de los principios del diseño de ZT.
- **Sección 3:** documenta los componentes lógicos o bloques de construcción de la ZT. Es posible que algunas implementaciones únicas conformen los componentes de la ZTA de forma diferente, pero que sirvan para la misma funcionalidad lógica.
- **Sección 4:** enumera algunos posibles casos de uso en los que una ZTA puede hacer que los entornos empresariales sean más seguros y menos propensos a ataques exitosos. Entre ellos, se encuentran las empresas con empleados remotos, servicios en la nube y redes para invitados.
- **Sección 5:** analiza las amenazas de una empresa que utiliza una ZTA. Muchas de ellas son similares a las de cualquier red con arquitectura perimetral, pero pueden requerir técnicas de mitigación diferentes.
- **Sección 6:** comenta cómo los principios de la ZTA se adaptan o se complementan con las orientaciones existentes para las agencias federales.
- **Sección 7:** presenta el punto de partida del proceso de transición de una empresa (como una agencia federal) a una ZTA, en el que se incluye una descripción de los pasos generales necesarios para planificar e implementar aplicaciones e infraestructuras empresariales que se guíen por los principios de la ZT.

2 Conceptos básicos de la confianza cero

La confianza cero es un paradigma en ciberseguridad centrado en la protección de los recursos y con la premisa de que la confianza nunca se concede de forma implícita, sino que debe evaluarse continuamente. La ZTA es un enfoque integral de la seguridad de los recursos y de los datos de las empresas, que engloba la identidad (entidades personales y no personales), las credenciales, la gestión del acceso, las operaciones, los puntos finales, los entornos de alojamiento y la infraestructura de interconexión. El punto de partida debe ser la restricción de los recursos a los que se necesita acceder y conceder solo los privilegios mínimos (como leer, escribir y borrar) necesarios para llevar a cabo las tareas. Históricamente, las agencias (y las redes empresariales en general) se han centrado en la defensa del perímetro y una vez que los sujetos autenticados se encontraban en la red interna, se les daba un acceso autorizado a una amplia gama de recursos. Como resultado, el movimiento lateral no permitido dentro del entorno ha sido uno de los mayores desafíos para las agencias federales.

Las conexiones a Internet de confianza (TIC) y los cortafuegos perimetrales de un organismo proporcionan sólidas puertas de enlace a Internet. De este modo, ayudan a bloquear a los atacantes que provienen de la red, pero son ineficaces al momento de detectar y detener los ataques desde el interior. Tampoco pueden proteger a los sujetos que se encuentran fuera del perímetro de la empresa (por ejemplo, los trabajadores remotos, los servicios basados en la nube, los dispositivos periféricos, etc.).

Una definición operativa de la confianza cero y de su arquitectura es la siguiente:

> La *confianza cero* (ZT) es un conjunto de conceptos e ideas diseñados para minimizar la inseguridad mediante la aplicación de decisiones de acceso precisas y de mínimos privilegios por solicitud, tanto en los sistemas de información como en los servicios ante una red que se considera comprometida. La *arquitectura de confianza cero* (ZTA) es el plan de ciberseguridad de una empresa que utiliza los conceptos de confianza cero y engloba las relaciones de los componentes, la planificación del flujo de trabajo y las políticas de acceso. Por consiguiente, un emprendimiento de este tipo comprende la infraestructura de red (física y virtual) y las políticas operativas que aplica una empresa como producto de un plan de arquitectura de confianza cero.

Cuando una entidad decide adoptarla, toma como modelo su estrategia principal y genera la arquitectura mediante el desarrollo de un plan que tiene en cuenta sus principios (véase la sección 2.1). El programa se implementa, entonces, con el fin de generar un entorno de confianza cero aplicable en la organización.

Esta definición se enfoca en el eje de la problemática, cuyo objetivo es *prevenir el acceso no autorizado a los datos y servicios* junto con *la implementación de un control de acceso lo más granular posible*. Concretamente, los sujetos autorizados y aprobados (una combinación de usuario, aplicación o servicio y dispositivo pueden acceder a los datos con exclusión de todos los demás sujetos (es decir, los atacantes). Para profundizar, la palabra *recurso* no puede limitarse solo a *datos*, de modo que ZT y ZTA se refieren al acceso a los recursos (por ejemplo,

impresoras, medios informáticos, actuadores del Internet de las cosas [IdC]) y no solo al acceso a los datos.

Para disminuir la inseguridad (puesto que no se puede eliminar), se hace hincapié en la autenticación, la autorización y la reducción de las zonas de confianza implícitas, mientras se mantiene la disponibilidad y se minimizan los retrasos temporales en los mecanismos de autenticación. Las reglas de acceso se hacen de la manera más granular posible con el fin de aplicar los mínimos privilegios necesarios al momento de realizar la solicitud.

En el modelo abstracto de acceso en la Figura 1, se presenta un sujeto que necesita acceder a un recurso de la empresa. El acceso se concede a través de un punto de decisión de políticas (PDP por su nombre en inglés *policy decision point*) y el correspondiente punto de aplicación de políticas (PEP por *policy enforcement point*). [5]

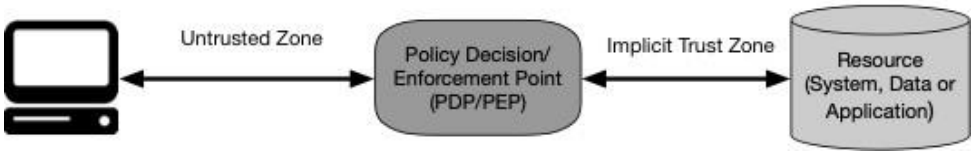

Figura 1
Accesos de la confianza cero
Untrusted Zone (zona no confiable). *Implicit Trust Zone* (zona de confianza implícita). *Policy Decision/Enforcement Point (PDP/PEP)* (punto de decisión y aplicación de políticas). *Resource (System, Data or Application)* (recurso; sistema, datos o aplicación).

El sistema debe garantizar que el sujeto sea auténtico y que la solicitud sea válida. Los PDP y los PEP emiten un dictamen para permitir que el sujeto acceda al recurso. Esto implica que la confianza cero abarca dos áreas básicas: la autenticación y la autorización. ¿Cuál es el nivel de confianza sobre la identidad del sujeto para esta solicitud en particular? ¿Está permitido el acceso al recurso dado el nivel de confianza en la identidad del sujeto? ¿El dispositivo utilizado para la solicitud dispone de la configuración de protección adecuado? ¿Existen otros factores que deberían considerarse y que modificarían el nivel de confianza (por ejemplo, la hora, la ubicación y la postura de seguridad del sujeto)? En general, las empresas deben desarrollar y mantener políticas dinámicas basadas en el riesgo al momento de acceder a los recursos, así como establecer un sistema que garantice que dichas políticas se apliquen de forma correcta y coherente para las solicitudes de acceso a los recursos individuales. Estas afirmaciones suponen que una organización no debe basarse en la fiabilidad implícita en la que si el sujeto ha cumplido un nivel de autenticación básico (por ejemplo, iniciar sesión en un recurso), todas las solicitudes de recursos posteriores se considerarán igualmente válidas.

Lo que se entiende como «zona de confianza implícita» constituye un área en la que todas las unidades presentan, al menos, un nivel de confianza equivalente al de la última puerta de enlace del PDP y del PEP. Por ejemplo, si se toma como modelo el control de pasajeros en un aeropuerto, todas las personas que viajan pasan por el control de seguridad (PDP y PEP) para acceder a las puertas de embarque. Los viajeros, los empleados que trabajan en las instalaciones,

[5] Concepto definido en OASIS XACML 2.0 https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-specos.pdf

la tripulación del avión, etc. circulan por la zona de la terminal y todos estos individuos se consideran confiables. En este modelo, la zona de confianza implícita es el área de embarque.

El PDP y el PEP aplican un conjunto de controles para que todo el tráfico más allá del PEP tenga un nivel de confianza común y no se puedan aplicar políticas adicionales fuera de su ubicación en el flujo del tráfico. Para permitir que el PDP y el PEP resulten lo más específicos posible, la zona segura implícita debe ser lo más pequeña que se pueda.

La confianza cero proporciona un conjunto de principios y conceptos que acercan el PDP y el PEP al recurso. La idea es autenticar y autorizar explícitamente a todos los sujetos, activos y flujos de trabajo que conforman la empresa.

2.1 Principios de la confianza cero

Muchas definiciones y debates sobre la ZT destacan como factor el concepto de eliminación de las defensas perimetrales de la zona amplia (por ejemplo, los cortafuegos de la empresa). Sin embargo, la mayoría de estos conceptos siguen de alguna manera definiéndose en relación con los perímetros (como la microsegmentación o los microperímetros; véase la sección 3.1) y como parte de las capacidades funcionales de una ZTA. Lo que se presenta a continuación es un intento de definir la ZT y la ZTA en términos de principios básicos que deberían contemplarse, en lugar de lo que se descarta. Estos fundamentos representan la meta ideal; aunque hay que reconocer que no todos los preceptos pueden aplicarse plenamente en su forma más pura para todas las estrategias.

Una arquitectura de confianza cero se debe diseñar e implementar respetando los siguientes principios básicos:

1. **Todas las fuentes de datos y los servicios informáticos se consideran recursos.** La red puede estar compuesta por múltiples tipos de dispositivos y también tener aparatos de pequeño alcance que envían datos a agregadores/almacenamiento, *software* como servicio (SaaS, por su desarrollo en inglés *software as a service*), sistemas que envían instrucciones a los actuadores y otras funciones. Además, si existen dispositivos de propiedad personal con acceso a las fuentes de la empresa, esta puede clasificarlos como recursos de la organización.
2. **Toda comunicación debe protegerse independientemente de la ubicación de la red**. La localización de la red por sí sola no implica confianza. Las solicitudes de acceso procedentes de activos situados en la infraestructura de la red de la empresa (por ejemplo, dentro de un perímetro de red tradicional) deben reunir los mismos requisitos de seguridad que las solicitudes de acceso y las comunicaciones procedentes de cualquier otra que no sea de la entidad. En otras palabras, la confianza no tiene que concederse automáticamente por el hecho de que el dispositivo está en la infraestructura de red de la compañía. Toda comunicación debe realizarse de la manera más segura posible, mediante la protección de la confidencialidad e integridad, y el suministro de una autenticación de la fuente.

3. **El acceso a los recursos individuales de la empresa se concede por sesión**. Antes de conceder el acceso se evalúa la confianza en el solicitante; a su vez, este acceso se otorga con los privilegios mínimos necesarios para completar la tarea, lo que podría significar solo «en un momento dado» para esa transacción en particular y podría no ocurrir directamente antes de iniciar una sesión o realizar una transacción con un recurso. Sin embargo, esta autenticación y autorización no concederá automáticamente el acceso a otro diferente.
4. **El acceso a los recursos está determinado por una política dinámica, que incluye el estado visible de la identidad del cliente, de la aplicación o servicio y del activo solicitante, y puede incluir otros rasgos de comportamiento y del entorno.** La organización protege los recursos definiendo, en primer lugar, cuáles tiene, quiénes son sus miembros (o la capacidad de autenticar a los usuarios de una comunidad federal) y a qué recursos necesitan acceder esos miembros. Para la confianza cero, la identidad del cliente puede incluir la cuenta de usuario (o la identidad del servicio) y cualquier otra característica asociada asignada por la empresa a esa cuenta o artefacto para autenticar las tareas automatizadas. El estado de los activos solicitados puede incluir características del dispositivo como las versiones de *software* instaladas, la ubicación de la red, la hora y la fecha de la solicitud, el comportamiento observado previamente y las credenciales instaladas. Los factores de comportamiento incluyen, entre otros, análisis automatizados del sujeto, análisis del dispositivo y mediciones de las desviaciones de los patrones de utilización observados. La política es el conjunto de reglas de acceso basado en los atributos que una organización asigna a un sujeto, a una base de datos o a una aplicación. Las características del entorno pueden incluir factores como la ubicación de la red del solicitante, la hora, los ataques activos notificados, etc. Estas reglas y particularidades se basan en las necesidades del desarrollo empresarial y en un nivel de riesgo aceptable. Las políticas de acceso a los recursos y los permisos de acción pueden variar en función de la sensibilidad de estos y de los datos. Además, se aplican los principios de mínimo privilegio para restringir tanto la visibilidad como la accesibilidad.
5. **La empresa supervisa y mide la integridad y la postura de seguridad de todos los activos propios y de los asociados.** Ningún activo es intrínsecamente confiable, por lo que la empresa examina la postura de seguridad de cada uno de ellos cuando evalúa la solicitud de un recurso. Una organización que implemente una ZTA debe establecer un programa de Diagnóstico y Mitigación Continuos (CDM) o un sistema similar para supervisar el estado de los dispositivos y las aplicaciones. A su vez, debe aplicar parches o correcciones si es necesario. Cuando se descubren activos alterados, con vulnerabilidades conocidas o no gestionados por la empresa, estos pueden tratarse de forma distinta (incluida la denegación de todas las conexiones a los recursos de la organización) a los dispositivos de propiedad de la compañía o asociados a ella y que se consideran en su estado más seguro. Este trato diferente puede aplicarse también a los dispositivos asociados (por ejemplo, dispositivos de propiedad personal) a los que se les permitirá tener acceso a algunos recursos, pero no a otros. Asimismo, se requiere un sólido sistema de supervisión e información en curso que proporcione datos procesables sobre el estado actual de los activos de la organización.

6. **Toda autentificación y autorización a un recurso es dinámica y se aplica de forma estricta antes de permitir el acceso**. Se trata de un ciclo constante de acceso, escaneo y evaluación de amenazas, adaptación y reevaluación continua de la confianza en permanente comunicación. Así, se espera que la empresa que implemente una ZTA cuente con una gestión de la identidad, credenciales y acceso (ICAM, por su nombre en inglés Identity, Credential, and Access Management) y sistemas establecidos de gestión de activos. Entre ellos, se incluye el uso de la autenticación multifactor (MFA, por su denominación en inglés *multifactor authentication*) para el acceso a algunos o todos los recursos de la empresa. La supervisión continua con posibles reautenticación y reautorización se produce a lo largo de las transacciones de los usuarios, según lo definido y aplicado por la política (por ejemplo, basada en el tiempo, modificación o nuevo recurso solicitado, actividad anómala de sujeto detectada), la cual procura establecer un equilibrio entre la seguridad, la disponibilidad, la usabilidad y la rentabilidad.
7. **La empresa recopila toda la información posible sobre el estado actual de los activos, la infraestructura de la red y las comunicaciones, y la utiliza para mejorar la postura de seguridad.** Una empresa debe reunir y procesar los datos sobre la postura de seguridad de sus bienes, el tráfico de red y las solicitudes de acceso. Además, tomará cualquier información obtenida para mejorar la creación y la aplicación de las políticas. Estos datos también servirán como contexto para las solicitudes de acceso de los sujetos (consultar la sección 3.3.1).

Los principios mencionados anteriormente intentan ser agnósticos en cuanto a la tecnología. Por ejemplo, la «identificación del usuario» (ID) podría incluir varios factores como el nombre de usuario y contraseña, certificados y contraseña de un solo uso. Estos postulados se aplican al trabajo que se realiza dentro de una organización o en colaboración con una o más entidades asociadas, y no al público anónimo o a los procesos empresariales de cara al consumidor. Una organización no puede imponer políticas internas a terceros (por ejemplo, clientes o usuarios de Internet en general), en cambio, puede aplicar algunas políticas basadas en ZT a usuarios no pertenecientes a la empresa, pero que tienen una relación especial con ella (por ejemplo, clientes registrados, dependientes de empleados, etc.).

2.2 Visión de confianza cero de una red

Para cualquier organización que utilice la ZTA en la planificación y el despliegue de la red, existen algunos supuestos básicos para su conectividad. Parte de estos fundamentos se aplican a la infraestructura que es propiedad de la empresa y otros a los recursos propios que operan en una infraestructura de red que no le pertenece (por ejemplo, wifi público o proveedores de nube pública). Estos conceptos se utilizan para determinar la creación de una ZTA. La red de una empresa que implemente este modelo debería desarrollarse con los principios descritos anteriormente y con las premisas que se exponen a continuación.

1. **La red privada de la empresa no constituye por sí sola una zona de confianza.** Los activos deben actuar siempre como si un atacante estuviera presente en la red de la empresa y la comunicación debe realizarse de la manera más segura posible (véase el

principio 2 mencionado más arriba), lo que implica llevar a cabo acciones como la autenticación de todas las conexiones y el cifrado de todo el tráfico.

2. **Los dispositivos integrados a la red pueden ser ajenos a la empresa o estar configurados por terceros.** Los visitantes o los servicios contratados pueden incluir activos que no son propiedad de la organización y que necesitan acceso a la red para desempeñar sus funciones. Este punto incluye las políticas basadas en el principio de trae tu propio dispositivo (BYOD) que permite a los miembros de la empresa utilizar artefactos que le pertenecen para acceder a sus recursos.
3. **Ningún recurso es confiable por naturaleza**. Se debe evaluar la postura de seguridad de cada activo a través de un PEP antes de que se conceda una solicitud a un recurso de propiedad de la empresa (similar al principio 6 anterior para los activos, así como para los sujetos). Esta evaluación debe mantenerse durante toda la sesión. Los dispositivos que son de la empresa deben tener artefactos que permitan la autenticación y proporcionen un nivel de confianza más alto que si la misma solicitud procediera de dispositivos que no pertenecieran a la compañía. Las credenciales del sujeto por sí solas son insuficientes para la autenticación a un recurso de la organización.
4. **No todos los recursos de la empresa se encuentran dentro de su infraestructura.** Los recursos incluyen sujetos remotos, así como servicios en la nube. Los activos propios o gestionados por la empresa pueden necesitar utilizar sus redes locales (es decir, no de la empresa) para la conectividad básica y los servicios de red (por ejemplo, la resolución del Sistema de nombre de dominio DNS, por su nombre en inglés Domain Name System).
5. **Los sujetos y activos de la empresa que operan a distancia no pueden confiar plenamente en su conexión de red local.** Los sujetos remotos deben asumir que la red local (es decir, la que no es propiedad de la empresa) es hostil y deben considerar que todo el tráfico puede ser monitoreado y potencialmente modificado. Todas las solicitudes de conexión deben ser autenticadas y autorizadas, y todas las comunicaciones deben realizarse de la manera más segura posible (es decir, proporcionar confidencialidad, protección de la integridad y autenticación de la fuente). Véanse los principios de la ZTA más arriba.
6. **Los activos y los flujos de trabajo que se mueven entre la infraestructura perteneciente a la empresa y una externa deben adoptar una política y una postura de seguridad coherentes.** Los activos y las operaciones deben mantener una postura de seguridad cuando se mueven hacia o desde la infraestructura de la empresa, como los dispositivos que se trasladan desde redes pertenecientes a la organización hacia otras externas (es decir, usuarios remotos). Estas medidas también incluyen las operaciones que migran desde los *data centers* (centros de datos) locales hacia un servidor en la nube que no pertenece a la compañía.

3 Componentes lógicos de la arquitectura de confianza cero

Existen numerosos componentes lógicos que conforman el montaje de una ZTA en una empresa. Estos elementos pueden funcionar como un servicio local o a través de un servicio en la nube. El modelo de marco conceptual de la Figura 2 presenta la relación básica entre los componentes y sus interacciones. Obsérvese que se trata de un modelo ideal. A partir de la Figura 1, el punto de decisión de políticas (PDP) se desglosa en dos componentes lógicos: el motor de políticas (*policy engine*) y el administrador de políticas (*policy administrator*) (definidos más adelante). Los componentes lógicos de la ZTA utilizan un plano de control separado para comunicarse, mientras que los datos de las aplicaciones se comunican en un plano de datos (véase la sección 3.4).

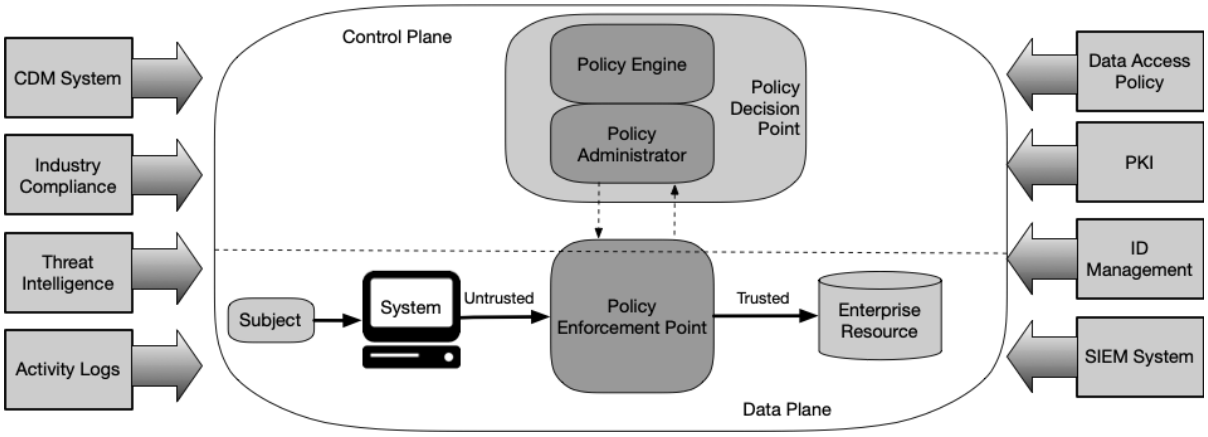

Figura 2
Componentes lógicos del núcleo de la confianza cero

CDM System (sistema CDM). *Industry Compliance* (cumplimiento de la industria). *Threat Intelligence* (inteligencia sobre amenazas). *Activity Logs* (registros de actividades). *Control Plane* (plano de control). *Policy Engine* (motor de políticas). *Policy Administrator* (administrador de políticas). *Policy Decision* Point (punto de decisión de políticas). *Data plane* (plano de datos). *Subject* (sujeto). *System* (sistema). *Untrusted* (no confiable). *Policy Enforcement Point* (punto de aplicación de políticas). *Trusted* (confiable). *Enterprise Resource* (recurso de la empresa). *Date Access Policy* (política de acceso a los datos). *PKI, public key infrastructure* (infraestructura de clave pública). *ID Management* (gestión de identidades). *SIEM System* (sistemas de seguridad de la información y gestión de eventos).

Descripción de los componentes

- **Motor de políticas (PE, *policy engine*):** este componente es responsable de la decisión final de conceder el acceso a un recurso para un sujeto determinado. El PE utiliza la política de la empresa, así como la información procedente de fuentes externas (por ejemplo, los sistemas CDM y los servicios de inteligencia sobre amenazas que se describen más adelante) como el ingreso a un algoritmo de confianza (referirse a la sección 3.3 para más detalles) para conceder, denegar o revocar el acceso al recurso. El PE está vinculado con el componente administrador de políticas. El motor de políticas toma y registra la decisión (como aprobada o denegada), y el administrador de políticas ejecuta la decisión.

- **Administrador de políticas (PA, *policy administrator*):** este componente se encarga de establecer o cerrar la vía de comunicación entre un sujeto y un recurso (a través de comandos a los PEP correspondientes). Es el responsable de generar cualquier autenticación específica de sesión y de *token* o de credencial que utilice un cliente para acceder a un recurso de la empresa. Se encuentra estrechamente vinculado al PE y se basa en su decisión para, en última instancia, permitir o denegar una sesión. Si se autoriza la sesión y se autentifica la solicitud, el PA configura al PEP para permitir el inicio de la sesión. Si se deniega esta última (o una autorización anterior se anula), el PA avisa al PEP para que cierre la conexión. Es posible que algunas configuraciones traten al PE y al PA como un servicio único; en este caso, el PA se divide en dos componentes lógicos. El PA se comunica con el PEP cuando se crea la ruta de comunicación que se realiza a través del plano de control.

- **Punto de aplicación de políticas (PEP, *policy enforcement point*):** este sistema se encarga de habilitar, supervisar y, eventualmente, terminar las conexiones entre un sujeto y un recurso de la empresa. El PEP se comunica con el PA para reenviar las solicitudes o recibir las actualizaciones de las políticas del PA. Se trata de un único componente lógico en la ZTA, pero puede dividirse en dos componentes diferentes: el lado del cliente (por ejemplo, un agente en un computador portátil) y el lado del recurso (por ejemplo, un componente de puerta de enlace frente al recurso que controla el acceso) o puede constituir un único portal que actúa como guardián de las vías de comunicación. Más allá del PEP se encuentra la zona de confianza (véase la sección 2) que alberga el recurso empresarial.

Al momento de tomar decisiones de acceso, además de los componentes principales en una empresa que implementa una ZTA, existen varias fuentes de datos que proporcionan reglas de entrada y de políticas utilizadas por el motor de políticas: fuentes de datos locales, así como externas (es decir, no controladas o creados por la empresa). Estas pueden incluir:

- **Sistema de Diagnóstico y Mitigación Continuos (CDM):** reúne información sobre el estado actual del activo de la empresa y aplica actualizaciones a los componentes de configuración y *software*. Un sistema CDM de una empresa proporciona al motor de políticas la información sobre el activo que realiza una solicitud de acceso como, por ejemplo, si está ejecutando el sistema operativo (SO) con los parches adecuados, si posee la integridad de los componentes de *software* aprobados o no por la empresa y si el activo tiene alguna vulnerabilidad conocida. Los programas CDM también se encargan de identificar y eventualmente hacer cumplir un subconjunto de políticas en los dispositivos que no pertenecen a la empresa y que actúan en su infraestructura.
- **Sistema de cumplimiento de la industria:** garantiza que la empresa cumpla con los regímenes normativos a los que pueda atenerse (por ejemplo, la FISMA o los requisitos de seguridad de la información del sector sanitario o financiero). Es decir, incluye todas las reglas de políticas que una empresa desarrolla para lograr el cumplimiento requerido.
- **Fuentes de inteligencia sobre amenazas:** proveen información de fuentes internas o externas que ayudan al motor de políticas a tomar las decisiones de acceso. Puede tratarse

de múltiples servicios que toman datos de fuentes internas o diversas externas e informan sobre nuevos ataques o vulnerabilidades descubiertos. Estos avisos también incluyen fallas de *software* y programas malignos recién identificados, así como ataques notificados a otros activos a los que el motor de políticas denegará el acceso a la empresa.

- **Registros (*logs*) de actividad de la red y del sistema:** este sistema recopila los registros de activos, el tráfico de red, las acciones de acceso a los recursos y otros eventos que proporcionan información en tiempo real (o casi) sobre la postura de seguridad de los sistemas de información de la empresa.
- **Políticas de acceso a los datos:** constituyen las características, reglas y políticas sobre el acceso a los recursos de la empresa. Este conjunto de normas puede ser codificado (a través de la interfaz de gestión) o generado de manera dinámica por el PE y constituyen el punto de partida para autorizar el acceso a un recurso, ya que proporcionan los privilegios de acceso básicos para las cuentas, las aplicaciones y los servicios de la empresa, y deben basarse en los protocolos de gestión definidos, así como en las necesidades de la organización**.**
- **Infraestructura de clave pública de la empresa (PKI, por su nombre en inglés *public key infrastructure*):** este sistema es responsable de generar y registrar los certificados emitidos por la empresa a los recursos, los sujetos, los servicios y las aplicaciones. También incluye el ecosistema de la autoridad de certificación global y la PKI[6] federal, que puede o no estar integrada en la PKI de la empresa. Además, puede tratarse de una PKI que no se base en el formato estándar de certificado X.509.
- **Sistema de gestión de identidades:** se encarga de crear, almacenar y gestionar las cuentas de usuario de la empresa y los registros de identidad (por ejemplo, el servidor del protocolo ligero de acceso a directorio, LDAP, por su nombre en inglés Lightweight Directory Access Protocol). Este sistema contiene la información necesaria del sujeto (como el nombre, la dirección de correo electrónico y los certificados) y otras características relacionadas con la empresa, como la función, los privilegios de acceso y los derechos asignados. Con frecuencia, utiliza otros sistemas (como una PKI) para los dispositivos asociados a las cuentas de usuario. Además, puede formar parte de una comunidad federada más amplia e incluir empleados que no son de la empresa o vincularse a activos que tampoco pertenecen a la organización para trabajar en colaboración.
- **Sistema de seguridad de la información y gestión de eventos (SIEM, por Security Information and Event Management):** recoge información basada en la seguridad para su posterior análisis. Estos datos se utilizan para afinar las políticas y advertir sobre posibles ataques contra los activos de la empresa.

3.1 Variaciones de los enfoques de la arquitectura de confianza cero

Existen varias formas en que una empresa puede establecer una ZTA para los flujos de trabajo. Estas varían en los componentes que se utilizan y en la fuente principal de las reglas de las

[6] https://www.idmanagement.gov/topics/fpki/

políticas de una organización. Cada enfoque implementa todos los principios de la ZT (véase la sección 2.1), pero puede utilizar uno o dos (o un componente) como principal impulsor. Una solución ZT completa incluirá elementos de estos tres enfoques: una mejor gobernanza de la identidad, una microsegmentación lógica y una segmentación basada en la red.

Algunos enfoques se prestan más a ciertos casos de uso que a otros. Una organización que desee desarrollar una ZTA para su empresa puede encontrar que su forma de acción elegida y las políticas existentes apuntan a un enfoque más que a otros; lo que no significa que los demás abordajes no funcionen, sino que algunos podrían ser más difíciles de implementar y requerir cambios más fundamentales en la forma en que la empresa realiza habitualmente los flujos comerciales.

3.1.1 ZTA basada en una gobernanza de la identidad mejorada

Para desarrollar una ZTA, el enfoque de la gobernanza de la identidad mejorada utiliza la identidad de los actores como el componente clave de la creación de las políticas. Si no fuera por los sujetos que solicitan acceso a los recursos de la empresa, no habría necesidad de crear políticas de acceso. Para este abordaje, estas políticas se basan en la identidad y en los atributos asignados. El requisito principal para el acceso a los recursos se establece en función de los privilegios de acceso que se conceden a cada sujeto. Otros factores como el dispositivo utilizado, el estatus de los activos y los factores del entorno pueden alterar el cálculo final del nivel de confianza (y la autorización de acceso definitiva) o adaptar el resultado de algún modo, como conceder solo un acceso parcial a una determinada fuente de datos en función de su ubicación en la red. Los recursos individuales o los componentes PEP que protegen el recurso deben tener una forma de reenviar las solicitudes a un servicio del motor de políticas o autenticar al sujeto y aprobar la solicitud antes de conceder el acceso.

Los esquemas basados en la gobernanza de la identidad mejorada utilizan, a menudo, un modelo de red abierta o una red de la organización accesible a visitantes o con conexión frecuente de dispositivos que no le pertenecen (como en el caso de la sección 4.3 que se describe debajo). El ingreso a la red se concede en principio a todos los activos; sin embargo, el acceso a los recursos de la empresa se limita a las identidades con los privilegios adecuados. La autorización a la conectividad básica a la red tiene un inconveniente, puesto que agentes maliciosos podrían intentar reconocerla o utilizarla para lanzar ataques de denegación de servicio, ya sea a nivel interno o contra terceros. Las empresas deben supervisar y responder a este comportamiento antes de que afecte los flujos de trabajo.

El enfoque basado en la identidad funciona correctamente con un modelo de portal de recursos (véase la sección 3.2.3), ya que la identidad y el estado del dispositivo proporcionan datos de referencia secundarios para las decisiones de acceso. Otros enfoques también sirven, según las políticas que se apliquen. Los que se basan en la identidad además resultan adecuados para las empresas que utilizan aplicaciones o servicios en la nube que no permiten el uso de componentes de seguridad ZT propios o gestionados por la empresa, como muchas ofertas de SaaS. La organización puede utilizar la identidad de los solicitantes para crear y aplicar políticas en estas plataformas.

3.1.2 ZTA y el uso de la microsegmentación

Una empresa puede optar por implementar una ZTA basada en el emplazamiento de los recursos individuales o grupos de recursos en un único segmento de red protegido por un componente de seguridad denominado puerta de enlace (*gateway*). Así, la empresa instala dispositivos de infraestructura, como conmutadores (*switches*) inteligentes (o rúteres), cortafuegos de nueva generación (NGFW, por su nombre en inglés *next generation firewalls*) o dispositivos de puertas de enlace de uso especial para que actúen como PEP y protejan cada recurso o pequeños grupos de recursos relacionados. De manera alternativa (o adicional), la empresa puede optar por implementar la microsegmentación del alojamiento utilizando agentes de *software* (consultar la sección 3.2.1) o cortafuegos en el o los puntos finales. Estas puertas de enlace conceden de manera dinámica el acceso a las solicitudes individuales del cliente, activo o servicio. De acuerdo con el modelo, la puerta de enlace será el único componente PEP o parte de un PEP múltiple que consistirá en la puerta de enlace por un lado y el agente del lado del cliente (véase la Sección 3.2.1).

Este enfoque se aplica a una variedad de casos de uso y patrones de implementación, donde el dispositivo de protección actúa como PEP junto con la gestión de los dispositivos que trabajan como componentes PE y PA. Además, requiere un programa de gobernanza de la identidad (IGP, por *identity governance program*) para funcionar plenamente, pero se basa en los componentes de la puerta de enlace para actuar como PEP al proteger los recursos de accesos o descubrimientos no autorizados.

Por último, la condición fundamental es que los componentes PEP se gestionen y puedan reaccionar y reconfigurarse según sea necesario para responder a las amenazas o a los cambios en el flujo de trabajo. Una empresa con microsegmentación puede implementar algunas prácticas utilizando dispositivos de puerta de enlace menos avanzados e incluso cortafuegos sin estado, pero el costo de administración y la dificultad para adaptarse rápidamente a los cambios hacen que esta sea una opción muy poco recomendable.

3.1.3 ZTA y el uso de una infraestructura de red y perímetros definidos a través de *software*

El último modelo utiliza la infraestructura de red para implementar una ZTA. Esta ejecución podría lograrse mediante el uso de una red superpuesta (es decir, la capa 7, pero también podría establecerse más abajo de la pila de red OSI [por su nombre en inglés Open System Interconnection, interconexión de sistemas abiertos]). Estos métodos se denominan a veces perímetro definido por *software* (SDP, por su nombre en inglés *software defined perimeter*) y, a menudo, incluyen conceptos de redes definidas por *software* (SDN, por *software defined network*) (SDNBOOK) y redes basadas en la intención (IBN, por su nombre en inglés *intent-based networking*) (IBNVN). En este esquema, el PA actúa como el controlador de la red, el cual la configura y reconfigura a partir de las decisiones tomadas por el PE. Los clientes siguen solicitando el acceso a través de los PE, que son gestionados por el componente PA.

Cuando este enfoque se implementa a la capa de red de la aplicación (es decir, la capa 7), el modelo de despliegue más común es el de agente y puerta de enlace (referirse a la sección 3.2.1).

En esta implementación, el agente y la puerta de enlace del recurso (que actúan como el único PEP y son configurados por el PA) establecen un canal seguro utilizado para la comunicación entre el cliente y el recurso. Puede haber otras variaciones de este modelo, así como para redes virtuales en la nube, redes no basadas en IP (protocolo de Internet, por su nombre en inglés *internet protocol*), etc.

3.2 Variantes implementadas de la arquitectura abstracta

Todos los elementos anteriores son componentes lógicos. No necesariamente deben ser sistemas únicos. Un solo activo puede desempeñar las funciones de varios componentes lógicos y, del mismo modo, un componente lógico puede constar de varios elementos de *hardware* o *software* para realizar las tareas. Por ejemplo, una PKI gestionada por la empresa puede constar de un componente responsable de la emisión de certificados para los dispositivos y otro utilizado para la emisión de certificados a los usuarios finales, pero ambos utilizan certificados intermedios emitidos por la misma autoridad de certificado raíz de la empresa. En algunas ofertas de productos ZT disponibles actualmente en el mercado, los PE y PA se encuentran combinados en un único servicio.

Existen diversas variaciones en el desarrollo de determinados componentes de la arquitectura que se describen en las secciones siguientes. De acuerdo con la configuración de la red de la empresa, podrán utilizarse diversos modelos de aplicación de la ZTA para diferentes procesos empresariales en una misma compañía.

3.2.1 Despliegue basado en agentes y puertas de enlace de los dispositivos

En este modelo de implementación, el PEP se divide en dos elementos, uno que se encuentra en el recurso y otro como un componente directamente frente a él. Por ejemplo, cada activo de la empresa tiene instalado un agente de dispositivo que coordina las conexiones, y cada recurso tiene un componente (es decir, una puerta de enlace) que se coloca directamente delante para que comunique solo con él, y sirva esencialmente como un *proxy* para el recurso. El agente es un componente de *software* que dirige parte del tráfico (o todo) al PEP apropiado con el fin de evaluar las solicitudes. La puerta de enlace se encarga de comunicarse con el administrador de políticas y de permitir únicamente las vías de comunicación aprobadas y configuradas por este (véase la Figura 3).

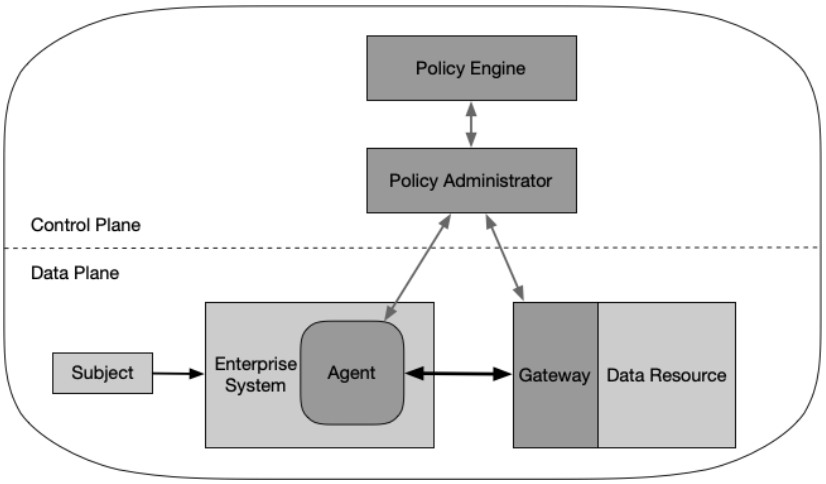

Figura 3
Modelo de agente y puerta de enlace de los dispositivos
Control Plane (plano de control). *Policy Engine* (motor de políticas). *Policy Administrator* (administrador de políticas). *Data plane* (plano de datos). *Subject* (sujeto). *Enterprise System* (sistema de la empresa). *Agent* (agente). *Gateway* (puerta de enlace). *Data Resource* (recurso de datos).

Como ejemplo, se toma un escenario típico en el que un sujeto con un computador portátil desea conectarse a un recurso de la empresa (por ejemplo, una aplicación o base de datos de recursos humanos). El agente local toma la solicitud de acceso y la reenvía al administrador de políticas (este último y el motor de políticas pueden ser un recurso local de la empresa o un servicio alojado en la nube), el cual remite nuevamente la solicitud al motor de políticas para su evaluación. Si se autoriza, el administrador de políticas configura un canal de comunicación entre el agente de dispositivo y la puerta de enlace del recurso correspondiente a través del plano de control. Esta acción puede incluir información como la dirección de protocolo de Internet (IP), referencias sobre el puerto, la clave de la sesión o mecanismos de protección similares. Luego, el agente de dispositivo y la puerta de enlace se conectan y comienzan los flujos de datos cifrados de las aplicaciones o servicios. La conexión finaliza cuando se completa el flujo de trabajo o cuando el administrador de políticas activa el cierre debido a un evento de seguridad (por ejemplo, el tiempo de espera de la sesión o la falta de reautenticación).

Este modelo se adapta mejor a las empresas que cuentan con un sólido programa de gestión de dispositivos y con recursos separados que consiguen comunicarse con la puerta de enlace. Para las organizaciones que utilizan en gran medida los servicios en la nube, existe una implementación, entre el cliente y el servidor, el perímetro definido por *software* (SDP) desarrollado por la Alianza de Seguridad en la Nube (CSA, por su nombre en inglés Cloud Security Alliance). Esta estrategia también es apropiada para las empresas que no quieren una política BYOD. El acceso solo es posible a través del agente de dispositivo, que puede encontrarse en los activos que son propiedad de la empresa.

3.2.2. Implementación basada en enclaves

Este esquema es una variación del enfoque anterior de agente de dispositivos y puerta de enlace, en el que los componentes de la puerta de enlace pueden no situarse en los activos o frente a los recursos individuales, sino en el límite de un enclave de recursos (por ejemplo, un centro de datos *in situ*) como se muestra en la Figura 4. En general, estos recursos desempeñan una única función empresarial o no pueden comunicarse directamente con una pasarela (por ejemplo, un sistema de base de datos tradicional que no tiene una interfaz de programación de aplicaciones [API, Application Programming Interface] que pueda utilizarse para comunicarse con una puerta de enlace). Asimismo, este enfoque es útil para las empresas que utilizan microservicios basados en la nube para un proceso de negocio único (por ejemplo, notificación de usuarios, búsqueda en la base de datos, pago de salarios). En este patrón, toda la nube privada se encuentra detrás de una puerta de enlace.

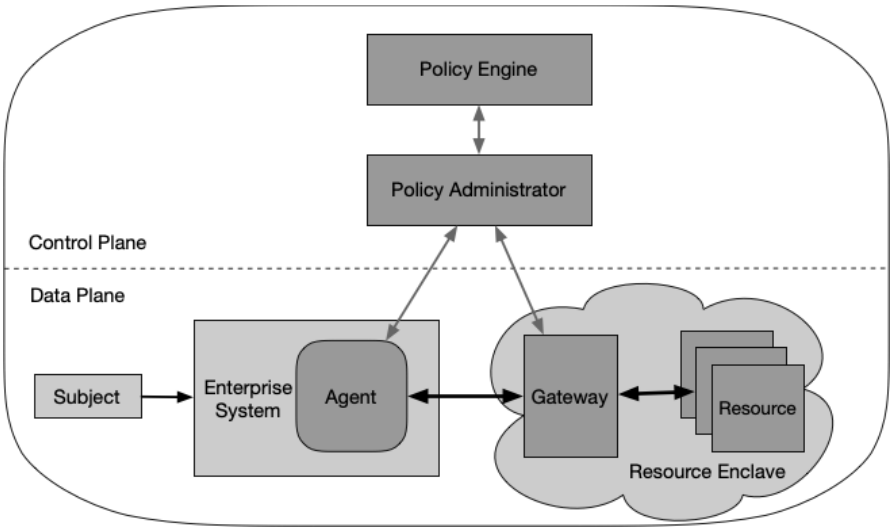

Figura 4
Modelo de puerta de enclave
Control Plane (plano de control). *Policy Engine* (motor de políticas). *Policy Administrator* (administrador de políticas). *Data Plane* (plano de datos). *Subject* (sujeto). *Enterprise System* (sistema de la empresa). *Agent* (agente). *Gateway* (puerta de enlace). *Resource* (recurso). *Resource Enclave* (enclave de recursos).

Este modelo puede funcionar como un híbrido junto con el esquema de agente de dispositivo y puerta de enlace. Así, los activos de la empresa tienen un agente de dispositivo que se utiliza para conectarse a las puertas de enlace del enclave, pero estas conexiones se crean utilizando el mismo proceso que el enfoque básico de agente de dispositivo y puerta de enlace.

Este arquetipo es útil para las empresas que tienen aplicaciones heredadas o centros de datos locales que no pueden tener puertas de enlace individuales. En este caso, se necesita un sólido programa de gestión de activos y de configuración para instalar y adaptar los agentes de dispositivos. El inconveniente de este modelo es que la puerta de enlace protege un conjunto de recursos y no cada uno individualmente, lo que permite a algunos sujetos visualizar recursos a los que no tienen privilegios para acceder.

3.2.3 Despliegue basado en un portal de recursos

En este tipo de implementación, el PEP es un componente único que actúa como puerta de enlace para las solicitudes de los sujetos. Este portal puede operar para un recurso individual o actuar como un enclave seguro para un conjunto de recursos utilizados con una sola función empresarial. Un ejemplo podría ser un portal de puerta de enlace dentro de una nube privada o en un centro de datos que contengan aplicaciones heredadas, como se muestra en la Figura 5.

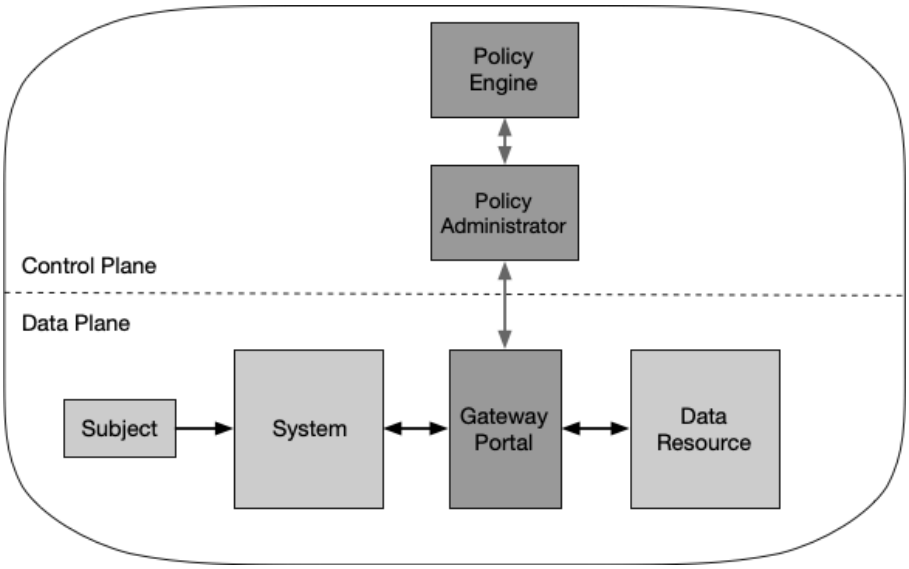

Figura 5
Modelo de portal de recursos
Control Plane (plano de control). *Policy Engine* (motor de políticas). *Policy Administrator* (administrador de políticas). *Data Plane* (plano de datos). *Subject* (sujeto). *System* (sistema). Gateway Portal (portal de puerta de enlace). *Data Resource* (recurso de datos).

La principal ventaja de este modelo sobre los demás reside en que no es necesario instalar un componente de *software* en todos los dispositivos de los clientes. Asimismo, es más flexible para las normativas BYOD y los proyectos de colaboración entre organizaciones, y los administradores de la empresa no necesitan asegurarse de que cada equipo disponga del agente de dispositivo adecuado antes de usarlo. No obstante, se puede extraer información limitada de los dispositivos que solicitan el acceso y solo permite escanear y analizar los activos y dispositivos una vez que se conectan al portal PEP. Tampoco es posible supervisarlos continuamente en busca de programas maliciosos, vulnerabilidades sin parches o verificar una configuración adecuada.

La principal diferencia con este modelo es que no existe un agente local que gestione las solicitudes, con lo que la empresa no llega a tener una visibilidad total o un control arbitrario sobre los activos, ya que solo puede verlos o escanearlos cuando se conectan a un portal. La compañía debería poder emplear medidas como el aislamiento del navegador para mitigar o compensar. Además, estos activos pueden ser invisibles entre las sesiones. Por otra parte, este modelo permite a los atacantes descubrir e intentar acceder al portal o probar un ataque de denegación de servicio (DoS, por su nombre en inglés *denial of service*) contra este último. Es

por lo expuesto, que los sistemas deben estar bien equipados para garantizar la disponibilidad contra un ataque DoS o una interrupción de los servicios de la red.

3.2.4 Entorno de pruebas (*sandbox*) para aplicaciones en dispositivos

Otra variación del modelo de despliegue de agente y puerta de enlace es hacer que las aplicaciones o procesos examinados se ejecuten en compartimentos independientes dentro de los activos. Estos segmentos pueden ser máquinas virtuales, bloques o cualquier otra implementación, pero el objetivo es el mismo: proteger la aplicación o las instancias de las aplicaciones de un alojamiento posiblemente comprometido o de otras aplicaciones que se ejecuten en el activo.

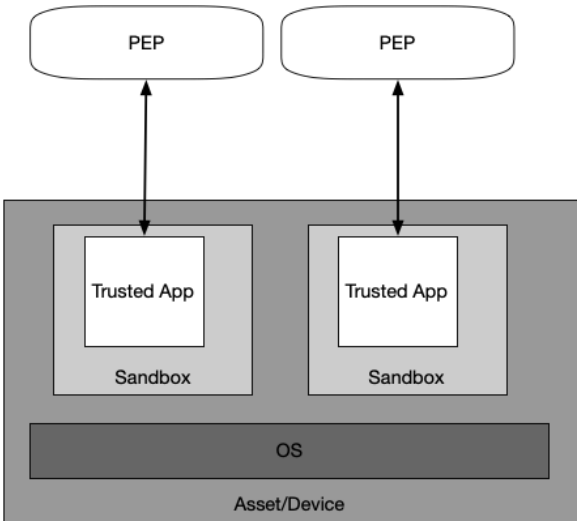

Figura 6
Entorno de prueba de la aplicación
PEP (*policy enforcement point*, punto de aplicación de políticas). *Trusted App* (aplicación *de confianza). Sandbox (entorno de pruebas). OS (operative system*, sistema operativo). *Asset/Device* (activo, dispositivo).

En la Figura 6, el dispositivo del sujeto usa aplicaciones aprobadas y verificadas en un entorno de pruebas, las cuales se comunican con el PEP para solicitar acceso a los recursos; sin embargo, el PEP rechazará las solicitudes de otras aplicaciones en el activo. En este modelo, el PEP puede ser un servicio local de la empresa o un servicio en la nube.

La principal ventaja de esta variante consiste en que cada aplicación se encuentra segmentada del resto del activo, y si este no puede escanearse en busca de vulnerabilidades, estas aplicaciones individuales dentro del entorno de pruebas estarán protegidas de una posible infección a causa de un programa maligno en el alojamiento. Una de las desventajas es que las empresas deben mantener estas aplicaciones en un entorno de pruebas para todos los activos y, en consecuencia, no logran tener una visibilidad completa sobre los que pertenecen a los clientes. Además, las organizaciones deben asegurarse de que cada aplicación alojada en un entorno de pruebas sea segura, lo que suele requerir más esfuerzo que la simple supervisión de los dispositivos.

3.3 Algoritmos de confianza

Para una empresa con una implementación de ZTA, el motor de políticas puede considerarse como el cerebro y el algoritmo de confianza del PE como el procesador principal de pensamientos. El algoritmo de confianza (TA, por su nombre en inglés *trust algorithm*) es el proceso mediante el cual el motor de políticas, en última instancia, concede o deniega el acceso a un recurso. Para realizar esta acción, toma información de múltiples fuentes (consultar la sección 3): la base de datos de las políticas con información sobre los sujetos (sus atributos, sus roles y patrones históricos de comportamiento), las fuentes de inteligencia de amenazas y otros metadatos. El proceso puede agruparse en grandes categorías como se representa en la Figura 7.

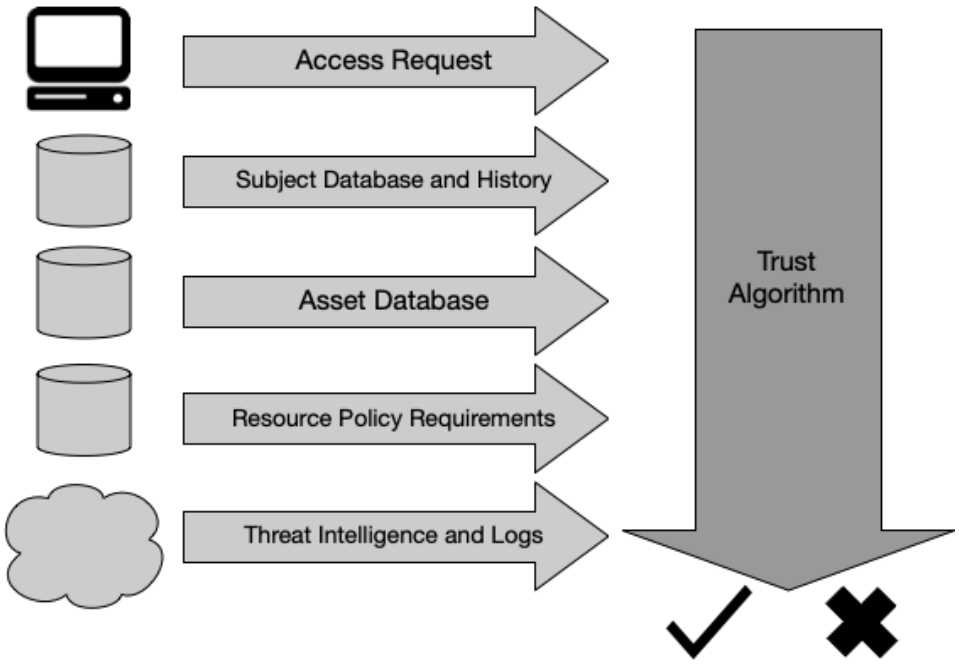

Figura 7
Proceso del algoritmo de confianza
Access Request (solicitud de acceso). *Subject Database and History* (datos e historial del sujeto). *Asset Database* (datos del activo). *Resource Policy Requirements* (requerimientos de la política de recursos). *Threat Intelligence and Logs* (inteligencia de amenazas y registros). *Trust Algorithm* (algoritmo de confianza).

En la figura, las variables pueden clasificarse por categorías en función de lo que aportan al algoritmo de confianza.

- **Solicitud de acceso:** es la solicitud real del sujeto. El recurso solicitado es la información principal utilizada, pero también se usa lo que se conoce sobre el solicitante. Estos datos pueden incluir la versión del SO, el *software* utilizado (por ejemplo, ¿el programa solicitante aparece en una lista de aplicaciones aprobadas?) y el nivel de parches. En función de estos factores y de la postura de seguridad de los activos, se podría restringir o denegar el acceso a estos

- **Base de datos de los sujetos**: corresponde a *quién* solicita el acceso al recurso (*SP 800-63*). Es decir, es el conjunto de sujetos (humanos y procesos) de la empresa o colaboradores, así como los atributos y privilegios que se les asignan. Estos sujetos y atributos forman la base de las políticas de acceso a los recursos (*SP 800-162*) (*NISTIR 7987*)[7]. Las identidades de los usuarios pueden incluir una mezcla de identidades lógicas, por ejemplo, la identificación (ID, por su nombre en inglés *identity document*) de la cuenta y los resultados de las comprobaciones de autenticación realizadas por los PEP. Los parámetros de la identidad que se consideran para derivar el nivel de confianza incluyen la hora y la geolocalización. Se podría considerar una serie de privilegios otorgados a varios sujetos con un mismo rol; sin embargo, los permisos deben asignarse al sujeto de forma individual y no simplemente porque detiene un papel determinado en la organización. Esta selección de privilegios debería codificarse y almacenarse en un sistema de gestión de ID y en una base de datos de políticas. También podrá incluir información sobre el comportamiento anterior del sujeto observados en algunas variantes del TA (véase la sección 3.3.1).
- **Base de datos de los activos (y observación del estatus):** se trata de la base de datos que contiene el estado registrado de cada uno de los activos (físicos y virtuales, hasta cierto punto) que son propiedad de la empresa (y posiblemente de los que no lo son, es decir, los BYOD). Este estado se compara con el estatus del activo que realiza la solicitud y puede incluir la versión del SO, el *software* presente y su integridad, la ubicación (de la red y la geolocalización) y el nivel de parches. En función de la comparación entre el estado del activo y esta base de datos, se restringirá o denegará el acceso.
- **Condiciones de los recursos:** este conjunto de políticas complementa la base de datos de ID y los atributos del usuario (*SP 800-63*) y define los requisitos mínimos para el acceso al recurso, los que pueden incluir los niveles de garantía del autentificador, como la localización de la red de MFA (por ejemplo, denegar el acceso desde direcciones IP extranjeras), la sensibilidad de la información y los requerimientos para la configuración de los recursos. Tanto el administrador de los datos (es decir, los responsables de ellos) como los encargados de los procesos empresariales que los utilizan (es decir, los responsables de la misión) deben establecer estos requerimientos.
- **Análisis de inteligencia sobre amenazas:** se trata de uno o varios suministros de información sobre las amenazas generales y programas malignos activos que operan en Internet. También, puede incluir información específica sobre la comunicación detectada en el dispositivo que puede resultar sospechosa (como las consultas de posibles comandos de programas malignos y nodos de control). Estas fuentes de información pueden ser servicios externos o escaneos y descubrimientos internos, y pueden incluir firmas de ataques y mitigaciones. Este aspecto es el único componente que probablemente estará bajo el control de un servicio y no de la empresa.

[7] N. del T.: los *NISTIR* (por su nombre en inglés NIST Internal Reports) son reportes internos periódicos que corresponden a investigaciones que realiza el instituto y que pueden descargarse desde su sitio «https://www.nist.gov/search?s=NISTIR».

La importancia de cada fuente de datos puede corresponder a un algoritmo propio o puede estar configurada por la empresa. Esta valoración puede utilizarse para reflejar la relevancia que la organización otorga a sus datos.

Luego, la determinación final se pasa al PA para su ejecución. El trabajo del PA consiste en configurar los PEP necesarios para permitir la comunicación autorizada. Según cómo esté implementada la ZTA, esta acción puede implicar el envío de los resultados de la autenticación y la información sobre la configuración de la conexión a las puertas de enlace y a los agentes o bien a los portales de los recursos. Los PA también pueden poner en pausa una sesión de comunicación para volver a autenticar y autorizar la conexión de acuerdo con los requisitos de la política. El PA, además, es responsable de emitir el comando para terminar la conexión según las políticas implementadas (por ejemplo, después de un tiempo de espera, cuando el flujo de trabajo ha sido completado o cuando existe una alerta de seguridad).

3.3.1 Variaciones del algoritmo de confianza

Existen diferentes maneras de aplicar un TA. Los diferentes implementadores pondrán más o menos énfasis en los factores mencionados, según la importancia que les atribuyan. Por otra parte, existen otras dos características relevantes que permiten diferenciar los TA. La primera corresponde a cómo se evalúan los factores, ya sea como decisiones binarias o como partes ponderadas según una *puntuación* total o nivel de confianza. La segunda es cómo se evalúan las solicitudes en relación con otras del mismo sujeto, aplicación, servicio o dispositivo.

- **Criterios versus puntuación:** un TA basado en criterios supone un conjunto de propiedades definidas que deben cumplirse antes de que se conceda el acceso a un recurso o se permita una acción (por ejemplo, lectura o escritura). La empresa configura estos criterios y debe hacerlo de forma independiente para cada recurso. Solo concederá el acceso o se aplicará una acción a uno de ellos si se cumplen todos los requisitos. Un TA establecido según la puntuación calcula un nivel de confianza basado en los valores de cada fuente de datos y de acuerdo con el peso que le otorga la compañía. Si la puntuación es mayor al valor del umbral configurado para el recurso, se concede el acceso o se realiza la acción. En caso contrario, se deniega la solicitud o se reducen los privilegios de acceso (por ejemplo, para un archivo, se concede el acceso de lectura, pero no el de escritura).
- **Particular versus contextual:** un TA particular trata cada solicitud de forma individual y no tiene en cuenta el historial del sujeto a la hora de evaluarlo. De este modo, puede permitir exámenes más rápidos, pero existe el riesgo de que un ataque pase desapercibido si se mantiene dentro del rol permitido del sujeto. Un TA contextual toma en consideración el historial reciente del sujeto o del agente de red cuando evalúa las solicitudes de acceso. Por consiguiente, el PE debe contar con cierta información sobre el estado de todos los sujetos y las aplicaciones, pero es más probable que detecte a un atacante que utiliza credenciales falsas para acceder a la información con un patrón atípico al que el PE considera para el sujeto en cuestión, lo que también significa que los PA (y los PEP) con los que los sujetos interactúan al comunicar deben informar al PE sobre el comportamiento de los usuarios. El análisis de las acciones de los sujetos puede utilizarse para proporcionar

un modelo de uso apropiado y las desviaciones podrían desencadenar comprobaciones de autenticación adicionales o denegaciones de solicitudes de recursos.

Ambos factores no siempre dependen el uno del otro. Se puede contar con un TA que asigne un nivel de confianza a cada sujeto o dispositivo y que siga considerando cada solicitud de acceso de forma independiente (es decir, de forma particular). Sin embargo, los TA contextuales, basados en la puntuación, tendrán la capacidad de ofrecer un control de acceso más dinámico y granular, pues la puntuación proporciona un nivel de confianza actualizado para la cuenta solicitante y se adapta a los factores cambiantes más rápido que las políticas estáticas modificadas por los administradores humanos.

Lo óptimo sería que un algoritmo de confianza de una ZTA sea contextual, aunque no siempre es viable con las infraestructuras que disponen las empresas. Un TA contextual puede mitigar las amenazas cuando un atacante se mantiene cerca de un cuadro «normal» de solicitudes de acceso para la cuenta comprometida de un sujeto o para un ataque interno. En el momento de definir e implementar los algoritmos de confianza, es importante equilibrar la seguridad, la usabilidad y la rentabilidad. El hecho de solicitar continuamente la reautenticación de un sujeto frente a un comportamiento que es coherente con el historial y las normas de su función y rol dentro de la organización puede conducir a problemas de usabilidad. Por ejemplo, si un empleado del departamento de recursos humanos de una agencia consulta normalmente entre 20 y 30 registros de empleados en un día de trabajo normal, un TA contextual podría enviar una alerta si las solicitudes de acceso superan repentinamente los 100 registros en un día. Asimismo, un TA contextual podría enviar una alarma si alguien realizara solicitudes de acceso fuera del horario laboral normal, ya que podría tratarse de un atacante que extrae registros utilizando una cuenta de RR. HH. comprometida. Las situaciones presentadas son ejemplos en los que un TA contextual podría detectar un ataque mientras que un TA particular no lograría descubrir el nuevo comportamiento. Se presenta otro ejemplo: un contador que suele acceder al sistema financiero durante las horas normales de trabajo intenta ingresar al sistema en medio de la noche desde un emplazamiento desconocido. Un TA contextual puede desencadenar una alerta y requerir que el sujeto cumpla con un nivel de confianza más estricto u otros criterios, como se describe en la *Publicación especial 800-63A* (*SP 800-63A*) de NIST.

El desarrollo de un conjunto de criterios o valores de ponderación o umbral para cada recurso requiere una planificación y realización de pruebas. Los administradores de la empresa pueden encontrar problemas durante la implementación inicial de una ZTA, donde las solicitudes de acceso que deberían aprobarse se deniegan debido a una configuración errónea. De esta manera, se deberá realizar una fase inicial de «ajuste» de la implementación en la que será necesario arreglar los criterios o las ponderaciones de puntuación para garantizar que las políticas se apliquen al mismo tiempo que permitan el funcionamiento de los procesos de negocio de la empresa. La duración de esta fase de ajustes dependerá de las métricas definidas por la empresa con respecto al progreso y la tolerancia por denegaciones o aprobaciones de acceso incorrectas para los recursos utilizados en el flujo de trabajo.

3.4 Componentes de la red y el entorno

En un entorno ZT, debe haber una separación (lógica y eventualmente física) de los flujos de comunicación utilizados para controlar y configurar por un lado la red y por el otro los flujos de comunicación de las aplicaciones y de los servicios utilizados para realizar el trabajo real de la organización. Este entorno se suele desglosar en un *plano de control* para monitorizar la comunicación de la red y en un *plano de datos* para los flujos de comunicación de las aplicaciones y los servicios (Gilman, 2017).

El plano de control utilizado por varios componentes de la infraestructura (tanto de la empresa como de los proveedores de servicios) se encarga de mantener y configurar los activos, examinar, conceder o denegar el acceso a los recursos, así como de realizar las operaciones necesarias para establecer las vías de comunicación entre estos últimos. El plano de datos se utiliza para la comunicación real entre los componentes de *software*. Este canal de comunicación solo es posible cuando se ha creado la ruta a través del plano de control. Por ejemplo, el plano de control podría ser utilizado por el PA y el PEP para establecer la vía de comunicación entre el sujeto y el recurso de la empresa. Las tareas que realizan las aplicaciones o los servicio utilizarán entonces la ruta del plano de datos que se ha establecido.

3.4.1 Requisitos de la red para admitir una ZTA

1. **Los activos de la empresa disponen de una conectividad de red básica**. La red de área local (LAN, por su nombre en inglés *local network area*), ya sea controlada por la organización o no, proporciona un enrutamiento e infraestructura básicos (por ejemplo, DNS). El activo empresarial remoto no utilizará necesariamente todos los servicios de la infraestructura.

2. **La empresa debe ser capaz de distinguir entre los activos que le pertenecen o gestiona y el estado de seguridad vigente de los dispositivos.** Este requerimiento se determina mediante credenciales emitidas por la compañía y sin utilizar información que no pueda autenticarse como, por ejemplo, direcciones de control de acceso a medios MAC (por su nombre en inglés Media Access Control) que puedan falsificarse.

3. **La empresa puede observar todo el tráfico de la red.** La organización registra los paquetes observados en el plano de datos, a pesar de que no pueda realizar una inspección de la capa de aplicación (es decir, la capa 7 de OSI) en todos los paquetes. La compañía filtra los metadatos relacionados con la conexión (por ejemplo, el destino, la hora, la identidad del dispositivo) para actualizar continuamente las políticas e informar al PE mientras evalúa las solicitudes de acceso.

4. **Se debería acceder a los recursos de la empresa solo por medio del PEP**. Los recursos de la organización no aceptan conexiones entrantes arbitrarias desde Internet, sino las conexiones configuradas personalizadas solo después de que un cliente haya sido autenticado y autorizado. Por lo tanto, es el PEP el que configura estas vías de comunicación y los recursos no deberían ser localizables sin acceder antes a este. Así, se evita que los atacantes identifiquen los objetivos a través de un escaneo o lancen ataques de DoS contra los recursos ubicados detrás de los PEP. Es importante tener en cuenta que

no todos ellos deben estar ocultos de esta manera; algunos componentes de la infraestructura de la red (por ejemplo, los servidores DNS) deben ser accesibles.

5. **El plano de datos y el plano de control se deben encontrar separados en lógicas distintas.** El motor de políticas, el administrador de políticas y los PEP se comunican en una red que está separada de manera lógica y a la que no pueden acceder directamente los activos y los recursos de la empresa. El plano de datos se utiliza para el tráfico de datos de las aplicaciones y servicios. El motor de políticas, el administrador de políticas y los PEP utilizan el plano de control para comunicarse y gestionar las vías de comunicación entre los activos. Los PEP deben ser capaces de enviar y recibir mensajes de los planos de datos y de control.

6. **Los activos de la empresa pueden acceder al componente PEP.** Los sujetos de la empresa deben poder acceder al componente PEP para llegar a los recursos. Este acceso podría adoptar la forma de un portal web, un dispositivo de red o un agente de *software* en el activo de la organización que permita la conexión.

7. **En el flujo empresarial, el PEP es el único componente que se comunica con el administrador de políticas.** Cada PEP que opera en la red de la empresa tiene una conexión con el administrador de políticas con el fin de establecer rutas de comunicación entre los clientes y los recursos. Todo el tráfico de los procesos de negocio dentro de la empresa pasa a través de uno o más PEP.

8. **Los activos empresariales remotos deben poder acceder a los recursos de la compañía sin necesidad de atravesar primero su infraestructura de red.** Por ejemplo, un sujeto remoto no debería estar obligado a utilizar un enlace hacia la red de la organización, es decir, una red privada virtual (VPN, por su nombre en inglés, *virtual private network*) para acceder a los servicios utilizados por la empresa y alojados en un proveedor de nube pública (por ejemplo, el correo electrónico).

9. **La infraestructura utilizada para respaldar el proceso de decisión de acceso a la ZTA debe ser escalable para poder contabilizar los cambios en la carga del proceso.** Los PE, PA y PEP utilizados en una ZTA se convierten en los componentes claves de cualquier proceso empresarial. El retraso o la imposibilidad de llegar a un PEP (o la incapacidad de los PEP para llegar al PA o al PE) impacta de forma negativa en el desarrollo del flujo de trabajo. Una compañía que implemente una ZTA necesita equipar los componentes para la carga de trabajo prevista o ser capaz de escalar rápidamente la infraestructura para manejar un incremento del uso cuando sea necesario.

10. **Se debe considerar que algunos activos de la empresa no podrán llegar a ciertos PEP debido a las políticas o a ciertos factores observables.** Por ejemplo, puede haber una política que establezca que los activos móviles no consigan llegar a ciertos recursos si el solicitante se encuentra fuera del país de origen de la organización. Estos factores podrían basarse en la ubicación (geolocalización o ubicación de la red), el tipo de dispositivo u otros criterios.

4 Escenarios de implementación y casos de uso

Cualquier entorno empresarial puede diseñarse teniendo en cuenta los principios de la confianza cero. La mayoría de las organizaciones ya cuentan con algunos elementos de confianza cero en su infraestructura o se encuentran en proceso de introducir políticas de seguridad de la información y resiliencia, así como buenas prácticas. Varios escenarios de implementación y casos de uso se adaptan fácilmente a una arquitectura de confianza cero. Por ejemplo, la ZTA tiene sus raíces en las organizaciones que no están centralizadas o que tienen una fuerza de trabajo con gran movilidad. No obstante, cualquier organización puede sacar provecho de una arquitectura de confianza cero.

En los casos de uso que se exponen a continuación, la ZTA no se señala de manera explícita, ya que es probable que las empresas cuenten con infraestructuras basadas en el perímetro y posiblemente en la ZTA. Como se explica en la sección 7.2, es factible que haya un periodo en el que los componentes de ambos sistemas estén funcionando simultáneamente en una misma organización.

4.1 Empresa con instalaciones satélites

El escenario más común consiste en una empresa con una única sede y una o más antenas dispersas geográficamente que no están unidas por una conexión de red física propiedad de la organización (ver Figura 8). Es posible que los empleados a distancia no dispongan de una red local completa que pertenezca a la compañía, pero necesitarán acceder a sus recursos para realizar las tareas que les correspondan. La sucursal puede tener una conmutación de etiquetas multiprotocolo (MPLS, por su nombre en inglés Multiprotocol Label Switch) vinculada con la red de la sede central, pero quizás no tenga el ancho de banda adecuado para todo el tráfico o no desee que el flujo destinado a las aplicaciones y servicios basados en la nube atraviese la red de la sede central. Asimismo, los empleados pueden hacer teletrabajo o estar en una ubicación remota y utilizar dispositivos de la organización o personales. En estos casos, la compañía puede querer conceder acceso a algunos recursos (por ejemplo, el calendario de los empleados, el correo electrónico), pero denegar el acceso o restringir las acciones a los más sensibles (por ejemplo, la base de datos de RR. HH.).

En este caso, los PE y PA suelen estar alojados como un servicio en la nube (lo que generalmente proporciona una disponibilidad superior y no requiere que los trabajadores remotos dependan de la infraestructura de la empresa para acceder a los recursos en la nube) con activos finales con un agente instalado (consultar la sección 3.2.1) o con acceso a un portal de recursos (consultar la sección 3.2.3). Quizás no sea lo más adecuado tener los PE y PA alojados en la red local de la empresa, ya que las oficinas y los trabajadores remotos deben enviar todo el tráfico de vuelta a la red para poder acceder a las aplicaciones y a los servicios alojados en la nube.

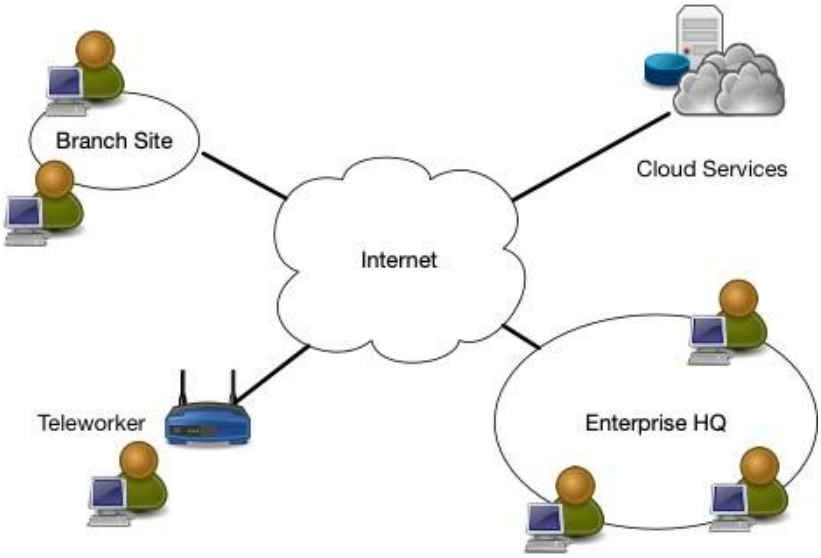

Figura 8
Empresa con empleados remotos
Teleworker (trabajador a distancia). *Branch Site* (sitio de la sucursal). *Cloud Services* (servicios en la nube). *Enterprise HQ* (sede de la empresa). *Internet* (Internet).

4.2 Empresa multinube o nube a nube

Un caso de uso cada vez más común para el despliegue de una ZTA es el de una empresa que utiliza múltiples proveedores en la nube (ver Figura 9). En este ejemplo, la compañía tiene una red local pero utiliza dos o más proveedores en la nube para alojar aplicaciones, servicios y datos. A veces, los dos primeros se alojan en la nube, separados de la fuente de datos. Por razones de rendimiento y facilidad de gestión, la aplicación alojada en el proveedor de nube A debería poder conectarse directamente a la fuente de datos alojada en el proveedor de nube B en lugar de obligarla a hacer un túnel a través de la red de la empresa.

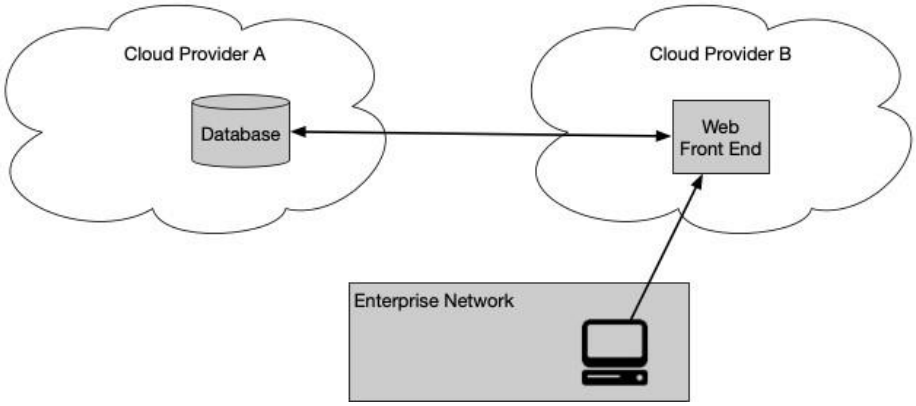

Figura 9
Ejemplo de multinube
Cloud Provider A (proveedor de nube A). *Database* (base de datos). *Cloud Provider B* (proveedor de nube B). *Web Front End* (*front end* de la web). *Enterprise Network* (red de la empresa).

Este caso de uso consiste en la implementación de servidor-servidor que corresponde a la especificación del perímetro definido por *software*, SDP, de CSA (CSA-SDP). A medida que las empresas se orientan cada vez más hacia las aplicaciones y servicios alojados en la nube, es evidente que confiar en el perímetro de la empresa para la seguridad se convierte en un riesgo. Como se ha comentado en la sección 2.2, los principios de la ZT establecen que no debería haber diferencia entre la infraestructura de red propiedad de la compañía, operada por ella, y la infraestructura propiedad de cualquier otro proveedor de servicios, manejada por él. La estrategia de confianza cero con el uso de nubes múltiples consiste en colocar a los PEP en los puntos de acceso de cada aplicación, servicio y fuente de datos. Los PE y PA pueden ubicarse en cualquiera de las dos nubes o incluso en un tercer proveedor de nubes; así, el cliente (a través de un portal o de un agente local instalado) accede directamente a los PEP. De este modo, la organización puede seguir gestionando el acceso a los recursos incluso cuando están alojados fuera de ella. Uno de los desafíos consiste en que los diferentes proveedores de la nube tienen formas particulares de implementar funcionalidades similares. Los arquitectos de la empresa tendrán que ser conscientes de cómo implementar la ZTA con cada proveedor de nube que utilicen.

4.3 Empresa con servicios contratados o acceso de personal externo

Otro escenario común sería el de una empresa que recibe visitantes *in situ* o contrata proveedores de servicios que necesitan un acceso limitado a los recursos para trabajar (véase la Figura 10). Por ejemplo, una compañía tiene sus propias aplicaciones y servicios internos, bases de datos y activos, entre los cuales se encuentran los servicios contratados a proveedores que a veces trabajan en las instalaciones para realizar el mantenimiento (por ejemplo, sistemas inteligentes de calefacción e iluminación que son propiedad de proveedores externos y están gestionados por ellos). Estos visitantes y proveedores de servicios necesitarán conectividad de red para realizar sus tareas. Una empresa de confianza cero podría facilitar este requisito y permitir a estos dispositivos y a cualquier técnico de servicio visitante el acceso a Internet, al mismo tiempo que se protegerían los recursos de la organización.

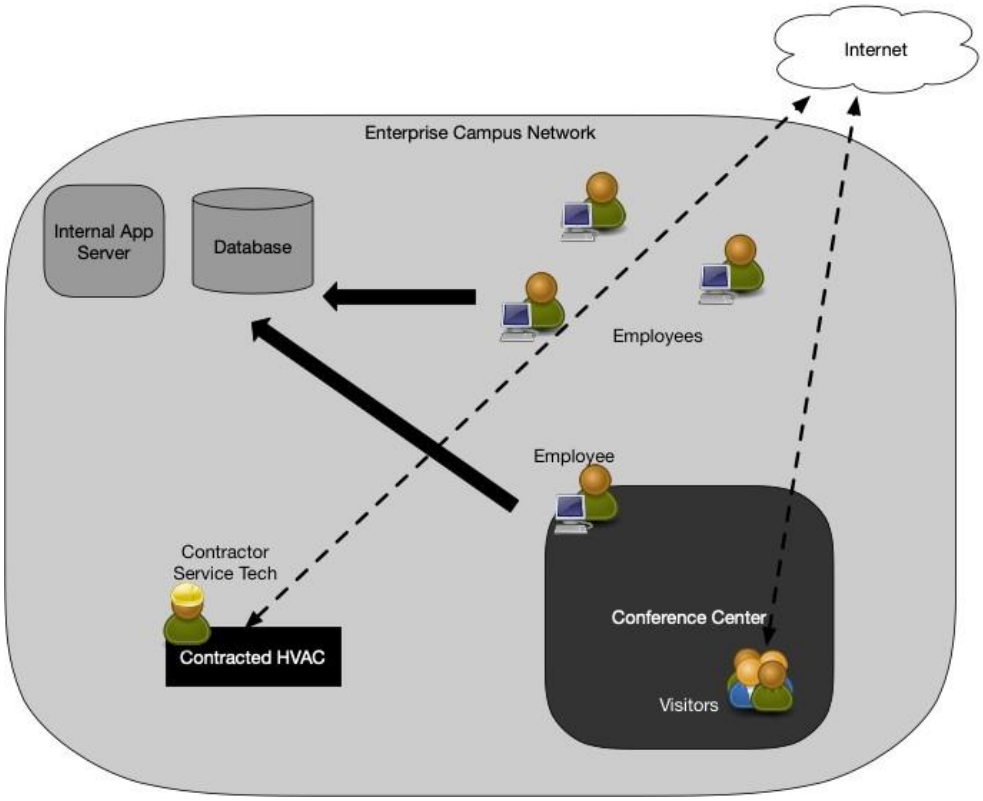

Figura 10
Empresa con acceso para personal externo
Enterprise Campus Network (red de las instalaciones de la empresa). *Internal App Server* (servidor de aplicaciones interno). *Database* (base de datos). Internet (Internet). *Employees* (empleados). *Employee* (empleado). *Contractor Service Tech* (técnico de servicio de contratistas*). Contracted HVAC* (contratación de climatización). *Conference Center* (centro de conferencias). *Visitors* (visitantes).

En este ejemplo, la organización también dispone de un centro de conferencias donde los visitantes interactúan con los empleados. Una vez más, con un enfoque de ZTA de SDP, los dispositivos de los empleados y los sujetos se diferencian y tienen acceso a los recursos adecuados de la empresa. Los visitantes del campus pueden acceder a Internet, pero no a los recursos de la organización e incluso no podrían acceder a los servicios de la empresa a través de los escaneos de la red (es decir, se previene el reconocimiento activo de la red y el movimiento lateral).

En este caso de uso, los PE y los PA podrían estar alojados como servicio en la nube o en la LAN (lo que supone un uso escaso o nulo de servicios alojados en la nube). Los activos de la empresa podrían tener un agente instalado (véase el apartado 3.2.1) o acceder a los recursos a través de un portal (véase el apartado 3.2.3). El o los PA garantizan que todos los activos no empresariales (los que no tienen agentes instalados o no pueden conectarse a un portal) no puedan acceder a los recursos locales, pero sí a Internet.

4.4 Colaboración más allá de los límites de la empresa

El cuarto caso de uso es la colaboración entre empresas. Por ejemplo, en un proyecto participan empleados de la empresa A y B (ver la Figura 11), las cuales pueden ser organismos federales distintos (G2G, por su significado *government to government*) o incluso una organización federada y una privada (G2B, por su significado *government to business*). A gestiona la base de datos utilizada para el proyecto, pero debe permitir el acceso a los datos a determinados miembros de B. De este modo, la empresa A puede configurar cuentas especializadas para que los empleados de B accedan a los datos necesarios y denegar el acceso a todos los demás recursos; sin embargo, este requerimiento puede convertirse rápidamente en algo difícil de gestionar. El hecho de que ambas organizaciones estén inscriptas en un sistema de gestión de identificación federada permitiría establecer estas relaciones de un modo ágil, a condición de que los PEP de ambas organizaciones puedan autenticar a los sujetos en una comunidad de identificación federada.

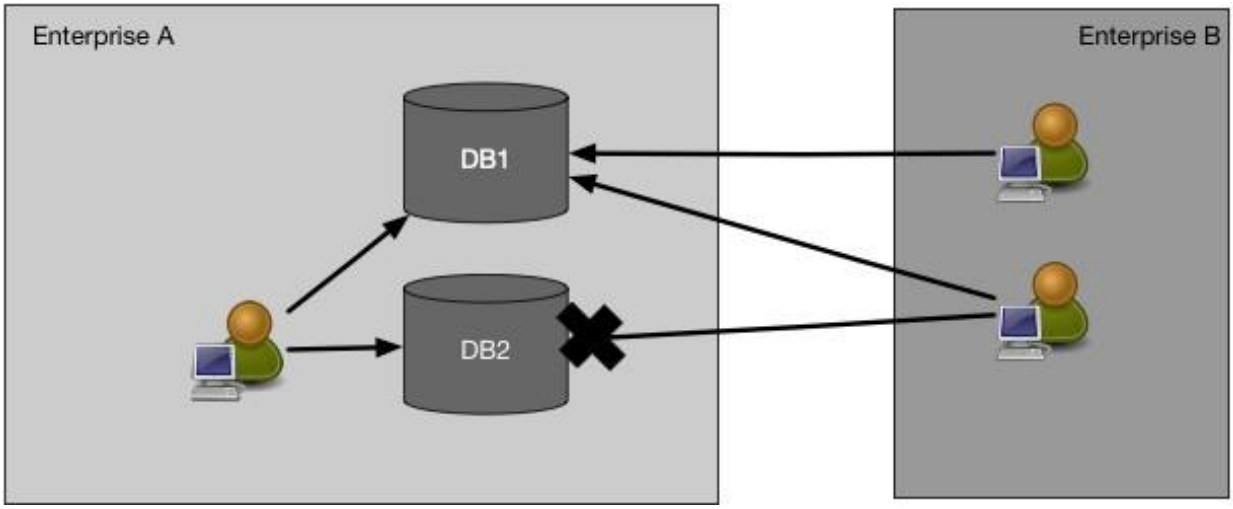

Figura 11
Colaboración entre empresas
Enterprise A (empresa A*). DB1* (base de datos 1). *DB2* (base de datos 2). *Enterprise B* (empresa B).

Este escenario puede ser similar al caso de uso 1 (sección 4.1), ya que los empleados de ambas empresas podrían no estar ubicados en las infraestructuras de red de sus respectivas organizaciones y el recurso al que necesitan acceder podría estar dentro de un entorno empresarial o alojado en la nube. De este modo, no es necesario que existan reglas complejas de cortafuegos o listas de control de acceso (ACL, por su nombre en inglés *access control list*) en toda la empresa para permitir que determinadas direcciones IP pertenecientes a la empresa B accedan a los recursos de la empresa A, en función de las políticas de acceso de esta última. La forma en que se efectúa este acceso dependerá de la tecnología utilizada. Al igual que en el primer caso de uso, un PE y un PA alojados como servicio en la nube pueden ofrecer disponibilidad a todas las partes sin tener que establecer una VPN o algo similar. Así, se les pedirá a los empleados de la empresa B que instalen un agente de *software* en sus activos o que accedan a los datos necesarios a través de una puerta de enlace (ver sección 3.2.3).

4.5 Empresa con servicios orientados al público o al cliente

Una característica común en muchas empresas consiste en un servicio dirigido al público que puede o no incluir el registro del usuario (es decir, crear o tener credenciales de acceso). Estos servicios pueden ofrecerse al público en general, a clientes con una relación comercial o a usuarios no pertenecientes a la empresa, como los que dependen de los empleados. En todos los casos mencionados, es probable que los activos solicitados no sean propiedad de la empresa y que esta se vea limitada en cuanto a las políticas internas de ciberseguridad que deba aplicar.

En el caso de un recurso general y público que no requiere credenciales de acceso (por ejemplo, una página web pública), los principios de la ZTA no se aplican directamente. La empresa no puede controlar con rigor el estado de los activos solicitados puesto que los recursos de este tipo son anónimos (como los de una página web pública) y no se necesitan credenciales para acceder.

Las empresas pueden establecer políticas para los usuarios públicos registrados, como los clientes (es decir, con los que tienen una relación comercial) y los usuarios especiales (por ejemplo, los que dependen de los empleados). Si se exige a los usuarios que presenten o se les expiden credenciales, la empresa puede instituir políticas relativas a la longitud de la contraseña, su ciclo de vida y otros detalles, además de proporcionar una autenticación multifactor (MFA) como opción o requisito. Sin embargo, las organizaciones se ven limitadas en las políticas que pueden implementar para esta clase de usuarios. La información sobre las solicitudes entrantes puede ser útil para determinar el estado del servicio público y detectar posibles atacantes que se hagan pasar por usuarios legítimos. Por ejemplo, si se sabe que los clientes registrados acceden a un portal de usuarios utilizando uno de los navegadores web más comunes, un aumento repentino de las solicitudes de acceso desde tipos de navegadores desconocidos o desde versiones obsoletas conocidas podría indicar un ataque automatizado de algún tipo. En este caso, la empresa podría adoptar medidas para limitar las solicitudes de estos clientes identificados; además, debería ser consciente de los estatutos o reglamentos relativos a la información que se pueden recopilar y registrar sobre los usuarios y activos solicitantes.

5 Amenazas asociadas a la arquitectura de confianza cero

Ninguna empresa puede eliminar el riesgo de ciberseguridad. Una ZTA correctamente implementada y actualizada puede reducir el peligro general y protegerse contra las amenazas más comunes si se complementa con las políticas y directrices de ciberseguridad existentes, la gestión de la identidad y el acceso, la supervisión continua y la ciberhigiene general. Ahora bien, cuando se implementa una ZTA, se presentan ciertos riesgos con características únicas.

5.1 Subversión del proceso de decisiones de la ZTA

En la ZTA, el motor y el administrador de políticas son los componentes clave de toda la empresa. Ninguna comunicación entre sus recursos se produce a menos que sea aprobada y posiblemente configurada por el PE y el PA, lo que significa que estos componentes deben configurarse y mantenerse correctamente. No obstante, cualquier administrador de la empresa con acceso a la configuración de las reglas del PE podría realizar cambios no aprobados o cometer errores que provocarían la interrupción de las operaciones de la compañía. Del mismo modo, un PA comprometido permitiría el acceso a recursos que de otro modo no se aprobarían (por ejemplo, a un dispositivo subvertido de propiedad personal). La mitigación de los riesgos asociados implica una configuración y una supervisión adecuadas de los componentes PE y PA, los cuales deberán registrarse y someterse a una auditoría ante cualquier cambio de configuración.

5.2 Denegación de servicio o alteración de la red

En la ZTA, el PA es el componente clave para el acceso a los recursos de la empresa; es decir, estos últimos no pueden conectarse entre sí sin el permiso del PA y, posiblemente, sin una acción de configuración. Si un atacante interrumpe o niega el acceso al (o los) PEP o a los PE y PA (por ejemplo, un ataque DoS o un secuestro de ruta), se podrían afectar de forma negativa las operaciones de la empresa. Las organizaciones pueden mitigar esta amenaza mediante la aplicación de políticas en un entorno de nube lo más seguro posible o replicado en varias ubicaciones, conforme a las directrices sobre resiliencia cibernética (*SP 800-160v2*).

Sin embargo, estas políticas mitigan el riesgo, pero no lo eliminan. Las redes de ordenadores infectados, *botnets*, como Mirai, producen ataques masivos de DoS contra los principales proveedores de servicios de Internet e interrumpen el servicio a millones de usuarios de Internet[8]. También puede ocurrir que un atacante intercepte y bloquee el tráfico hacia un PEP o PA desde una parte o todas las cuentas de usuario de una empresa (por ejemplo, una sucursal o incluso un solo empleado remoto). En estos casos, solo una parte de los sujetos de la empresa se vería afectada. Estos hechos también suceden en las VPN de acceso remoto heredadas y no es un riesgo exclusivo de la ZTA.

También puede suceder que un proveedor de alojamiento desconecte accidentalmente un PE o PA basado en la nube. Los sistemas en la nube han experimentado alteraciones en el pasado, tanto a nivel de infraestructura como servicio IaaS[9] (por su nombre en inglés *infrastructure as a*

[8] https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/
[9] https://aws.amazon.com/message/41926/

service) como de *software* como servicio SaaS[10]. Por ejemplo, un error operativo podría impedir el funcionamiento de toda una empresa si el motor de políticas o el administrador de políticas se volvieran inaccesibles desde la red.

También existe el riesgo de que no se pueda acceder a los recursos de la empresa desde el PA; así, aunque se conceda el acceso a un sujeto, el PA no logrará configurar la vía de comunicación desde la red. Esta situación podría producirse debido a un ataque de denegación distribuida de servicio DDoS (por su nombre en inglés *distributed denial of service*) o tan solo a un uso intenso e inesperado, y es similar a cualquier otra interrupción de la red en la que algunos o todos los sujetos de la empresa no pueden acceder a un recurso particular debido a que este no se encuentra disponible por alguna razón.

5.3 Robo de credenciales y amenaza de infiltración

Si se dispone de una implementación adecuada de ZT, de políticas de seguridad de la información y de resiliencia, y de las mejores prácticas existentes, se puede reducir el riesgo de que un atacante obtenga un amplio acceso a través de credenciales robadas o de un ataque interno. El principio de ZT fundado en la ausencia de confianza implícita basada en la ubicación de la red significa que los agresores necesitan comprometer una cuenta o un dispositivo existente para conseguir entrar en una empresa. Una ZTA bien desarrollada e implementada debería impedir que una cuenta o activo comprometido acceda a otros recursos fuera de su ámbito o patrones de acceso normales. En consecuencia, las cuentas con políticas de acceso a los recursos serían los objetivos principales de los agresores.

Los atacantes pueden utilizar el Phishing, la Ingeniería Social o una combinación de ataques para obtener las credenciales de cuentas con valor, y el significado de *valor* será diferente en función de la motivación. Por ejemplo, las cuentas de administrador de la empresa pueden ser valiosas, pero los interesados en obtener beneficios económicos considerarán que aquellas cuentas que tienen acceso a los recursos financieros o de pago tienen el mismo valor que las mencionadas anteriormente. La implementación de un MFA para las solicitudes de acceso puede reducir el riesgo de pérdida de información de una cuenta afectada. Sin embargo, un atacante con credenciales válidas (o un usuario malintencionado) podría acceder a los recursos de una cuenta para la que se le hubiese concedido el acceso. Por ejemplo, un agresor o un colaborador afectado que tuviese las credenciales y el acceso al activo propiedad de la empresa de un empleado válido de recursos humanos podría acceder a su base de datos.

La ZTA reduce el riesgo y evita que cualquier cuenta o activo comprometido se desplace lateralmente por la red. Si las credenciales afectadas no están autorizadas para acceder a un recurso concreto, se les denegará el acceso. Además, es más probable que un algoritmo de confianza contextual (véase la sección 3.3.1) detecte y responda rápidamente a este ataque que cuando se produce en una red heredada basada en el perímetro. Así, el TA contextual puede detectar patrones de acceso que están fuera del comportamiento normal y negar el acceso de la cuenta comprometida o de la amenaza interna a los recursos sensibles.

[10] https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=12286870

5.4 Visibilidad en la red

Como se explicó en la sección 3.4.1, todo el tráfico se inspecciona, se registra en la red y se analiza con el fin de identificar y reaccionar ante posibles ataques contra la empresa. No obstante, como también se mencionó, parte (y posiblemente la mayoría) del tráfico en la red de la empresa puede permanecer oculto a las herramientas de análisis de red de la capa 3. Además, este flujo puede provenir de activos que no son propiedad de la empresa (por ejemplo, servicios contratados que utilizan la infraestructura de la organización para acceder a Internet) o de aplicaciones y servicios que se resisten a una supervisión pasiva. La compañía que no pueda realizar una inspección profunda de los paquetes o examinar el tráfico cifrado debería utilizar otros métodos para evaluar la presencia de un posible atacante en la red.

Lo expuesto anteriormente no significa que la empresa sea incapaz de analizar el tráfico cifrado que ve en la red; por el contrario, puede recopilar metadatos (por ejemplo, direcciones de origen y destino, etc.) sobre este y utilizarlos para detectar un atacante activo o un posible programa maligno que estuviera comunicando en la red. Las técnicas de aprendizaje automático (Anderson, 2017) pueden utilizarse para analizar el flujo que no puede desencriptarse y examinarse; además, permitiría a la organización clasificar el tráfico como válido o posiblemente malicioso y proceder, de este modo, a una corrección.

5.5 Almacenamiento de la información del sistema y de la red

Una amenaza relacionada con la monitorización y el análisis del tráfico de red es el propio análisis. Si los escaneos de monitorización, el tráfico y los metadatos se almacenan para crear políticas contextuales, análisis forenses o posteriores, esos datos se convierten en un objetivo para los atacantes. Al igual que los diagramas de red, los archivos de configuración y otros documentos de la arquitectura de la red, estos recursos deben protegerse. Si un atacante lograse acceder a esta información, podría tomar conocimiento de la arquitectura de la empresa e identificar los activos para su posterior reconocimiento y ataque.

Otra fuente de información para un atacante, en una empresa de ZT, es la herramienta de gestión utilizada para codificar las políticas de acceso. Al igual que el tráfico almacenado, este componente contiene políticas de acceso a los recursos y puede dar información a un atacante sobre qué cuentas son más valiosas para vulnerar (por ejemplo, las que tienen acceso a los datos deseados).

Con respecto a toda la información valiosa de la empresa, deben implementarse protecciones adecuadas para evitar el acceso no autorizado y los intentos de ingreso. Como estos activos son vitales para la seguridad, deben contar con las políticas de acceso más restrictivas y ser accesibles solo desde cuentas de administrador designadas o dedicadas a tal fin.

5.6 Confianza en los formatos o en las soluciones de datos patentados

La ZTA se basa en varias fuentes de datos diferentes para tomar decisiones de acceso, incluida la información sobre el sujeto solicitante, el activo utilizado, la inteligencia empresarial y externa y el análisis de las amenazas. A menudo, los activos utilizados para almacenar y procesar esta información no tienen un modelo común y abierto sobre cómo interactuar e intercambiar. En

consecuencia, la empresa puede quedar atrapada en un subsistema de proveedores debido a problemas de interoperabilidad. Si un proveedor tiene un problema de seguridad o una interrupción, migrar hacia uno nuevo representará un gran costo para la compañía (por ejemplo, el reemplazo de varios activos) o el paso por un largo período de un programa de transición (como traducir las reglas de política del formato propio a otro). Al igual que los ataques DoS, este riesgo no es exclusivo de la ZTA, pero debido a que esta depende en gran medida del acceso dinámico a la información (tanto de la organización como de los proveedores de servicios), la interrupción puede afectar las operaciones principales de la empresa. Para mitigar los riesgos asociados, las organizaciones deben evaluar a los proveedores de servicios de forma holística teniendo en cuenta factores como sus controles de seguridad, los costos de cambio de empresa y la gestión de riesgos de la cadena de suministro, además de factores más típicos como el rendimiento, la estabilidad, etc.

5.7 Uso de entidades no personales (NPE, por su nombre en inglés *non-person entities*) en la administración de la ZTA

Para gestionar los problemas de seguridad en las redes de las empresas, se están implementando la inteligencia artificial y otros operadores basados en *software*. Estos componentes necesitan interactuar con los mecanismos de gestión de la ZTA (por ejemplo, el motor de políticas y el administrador de políticas) y a veces toman el lugar de un administrador humano. El modo en que estos componentes se autentifican en una empresa que implementa una ZTA todavía es un asunto pendiente. Se supone que la mayoría de los sistemas tecnológicos automatizados utilizan algún medio para autenticarse cuando usan una API hacia los componentes de los recursos.

El mayor riesgo cuando se utiliza tecnología automatizada para la configuración y la implementación de políticas es la probabilidad de que los falsos positivos (acciones inofensivas que se confunden con ataques) y los falsos negativos (ataques que se confunden con actividades normales) afecten la postura de seguridad de la empresa. Este problema puede reducirse con un análisis regular de reajustes con el fin de corregir las decisiones erróneas y mejorar el proceso de decisión.

El peligro que este sistema supone es que un atacante pueda inducir o forzar a una NPE a realizar alguna tarea para la que no tiene privilegios. El agente de *software* puede tener una barra de autenticación más baja en comparación con un usuario humano (por ejemplo, una clave de API frente a un MFA) para realizar tareas administrativas o relacionadas con la seguridad. Si un atacante pudiera interactuar con el agente NPE, teóricamente podría engañarlo para que le permita un mayor acceso o para que realice alguna tarea en nombre del agresor. También existe el riesgo de que este último pueda acceder a las credenciales del agente de *software* y realice tareas en su nombre.

6 Arquitectura de confianza cero y posibles interacciones con las normas federales existentes

Varias políticas y orientaciones federales existentes se entrecruzan con la planificación, la implementación y el funcionamiento de la ZTA. Estas políticas no prohíben que una empresa pase a una arquitectura más orientada a la confianza cero, pero pueden influir en el desarrollo de su estrategia. Cuando se complementa con las políticas y directrices de ciberseguridad existentes; con la Identidad, Credencial y Manejo del Acceso ICAM (por su nombre en inglés Identity, Credential, and Access Management); la supervisión continua, y la ciberhigiene general, la ZTA puede reforzar la postura de seguridad de una organización y protegerla contra las amenazas comunes.

6.1 ZTA y el Marco de Gestión de Riesgos de NIST

La puesta en funcionamiento de una ZTA implica el desarrollo de políticas de acceso basadas en un riesgo aceptable para la misión o el proceso empresarial designado (véase el apartado 7.3.3). Aunque se le podría denegar a un recurso todo el acceso a la red y permitir el ingreso solo a través de un terminal conectado, este método sería desproporcionadamente restrictivo en la mayoría de los casos e impediría la realización del trabajo. Para que una agencia federal pueda llevar a cabo su labor, debe existir un nivel de amenaza razonable. Los riesgos asociados al desempeño de la misión deben identificarse y evaluarse, para luego aceptarlos o mitigarlos. En este sentido, se ha desarrollado el Marco de Gestión de Riesgos (RMF) de NIST (SP 800-37).

La planificación e implementación de una ZTA puede cambiar los límites de autorización definidos por la empresa. Esta modificación se debe a la adición de nuevos componentes (por ejemplo, el motor de políticas, el administrador de políticas y los PEP) y a la reducción de la confianza en las defensas del perímetro de la red. El proceso general descrito en el RMF no cambiará en una ZTA.

6.2 Confianza cero y Marco de Privacidad de NIST

Una de las principales preocupaciones de las organizaciones es la protección de la privacidad de los usuarios y de la información confidencial (por ejemplo, la relacionada con la identificación personal). La protección de la privacidad y de los datos se incluye en programas de cumplimiento como la FISMA y la Ley de Portabilidad y Responsabilidad del Seguro Médico HIPAA (por su nombre en inglés Health Insurance Portability and Accountability Act).
Como respuesta, NIST elaboró un Marco de Privacidad para uso de las organizaciones (NISTPRIV). Esta herramienta ofrece un cuadro para describir los riesgos asociados a la privacidad y a las estrategias de mitigación, así como el proceso para que una empresa pueda identificar, medir y mitigar los riesgos relacionados con la privacidad de los usuarios y la información confidencial almacenada y procesada por una organización, tales como los datos personales utilizados por la empresa para apoyar las operaciones de la ZTA y los atributos biométricos utilizados en las evaluaciones de las solicitudes de acceso.

Una parte de los requisitos básicos de la ZT consiste en la inspección y el registro del tráfico en el entorno de la empresa (o al menos de los metadatos cuando se trata de flujo que no puede ser descifrado por los sistemas de supervisión). Parte de este tráfico puede contener información

privada o tener riesgos de privacidad asociados. Las organizaciones tendrán que identificar cualquier posible riesgo vinculado con la interceptación, el escaneo y el registro del tráfico de red (*NISTIR 8062*) mediante acciones como informar a los usuarios, obtener el consentimiento (a través de una página de inicio de sesión, un anuncio o procedimiento similar) y educar a los usuarios de la empresa. El Marco de Privacidad de NIST (NISTPRIV) podría ayudar a desarrollar un proceso formal para identificar y mitigar cualquier riesgo relacionado con la privacidad en una empresa que desarrolle una arquitectura de confianza cero.

6.3 ZTA y la Arquitectura Federal de la Gestión de Identidades, Credenciales y Accesos

La información sobre los sujetos es un componente clave de la ZTA. Si el motor de políticas no dispone de la información suficiente para identificar a los sujetos y a los recursos asociados, no puede determinar la autorización a los intentos de conexión para acceder. Antes de pasar a una implementación más alineada con la confianza cero, es necesario contar con sólidas referencias sobre los sujetos y las políticas de autenticación. Las empresas necesitan un sistema claro de atributos de los sujetos y políticas para que el PE pueda evaluar las solicitudes de acceso.

La Oficina de Gestión y Presupuesto (OMB, por su nombre en inglés Office of Management and Budget) publicó la norma M-19-17 sobre la mejora de la gestión de la identidad para el Gobierno Federal. El objetivo de la política es desarrollar «...una visión común de la identidad como facilitadora del cumplimiento de la misión, de la confianza y de la seguridad de la Nación» (M-19-17). El memorando convoca a todas las agencias federales a formar una oficina de ICAM para dirigir los esfuerzos relacionados con la emisión y la gestión de la identidad. Muchas de estas políticas de gestión deberían utilizar las recomendaciones de NIST SP 800-63-3 (Guías de la Identidad Digital, SP 800-63). Como la ZTA depende en gran medida de la gestión precisa de la identidad, cualquier esfuerzo de ZTA tendrá que integrar la política ICAM.

6.4 ZTA y la conexión a Internet de confianza 3.0

La TIC es una iniciativa de ciberseguridad federal gestionada conjuntamente por la OMB, el Departamento de Seguridad Nacional de los Estados Unidos DHS (por su nombre en inglés United States Department of Homeland Security) y la Administración de Servicios Generales (GSA, por su nombre en inglés General Services Administration), con el objetivo de establecer una base de seguridad de la red que abarque todo el Gobierno Federal. Históricamente, la TIC era una estrategia de ciberseguridad basada en el perímetro que exigía a los organismos consolidar y supervisar sus conexiones de redes externas. Las TIC 1.0 y TIC 2.0 asumen que el interior del perímetro es de «confianza», mientras que la ZTA declara que la ubicación de la red no supone «confianza» (es decir, no hay «confianza» en la red interna de una agencia). La TIC 2.0 proporciona una lista de condiciones de seguridad basadas en la red (por ejemplo, el filtrado de contenidos, el monitoreo, la autenticación y otras acciones) que deben desplegarse en el punto de acceso TIC dentro del perímetro de la agencia; muchos de estos requisitos están alineados con los principios de la ZT.

La TIC 3.0 se ha actualizado con un nuevo memorando (M-19-26) para incorporar los servicios en la nube y los dispositivos móviles. En la TIC 3.0 se reconoce que la definición de confianza

puede variar en contextos informáticos específicos y que los organismos tienen diferentes tolerancias de riesgo para definir las zonas de confianza. Además, la TIC 3.0 provee un *Manual de Capacidades de Seguridad TIC* actualizado, que define dos tipos de categorías de seguridad: la primera, las capacidades de seguridad universales que se aplican a nivel de empresa y, la segunda, las capacidades de seguridad del PEP que son a nivel de red y que se emplean en múltiples puntos de aplicación de políticas (PEP), tal y como se definen en los casos de uso TIC. La segunda categoría puede aplicarse a cualquier PEP apropiado situado a lo largo de un flujo de datos determinado, en lugar de limitarse a un único PEP en el perímetro de la agencia. Muchas de estas condiciones de seguridad de la TIC 3.0 apoyan directamente a la ZTA (por ejemplo, el tráfico encriptado, la autenticación robusta, la microsegmentación, el inventario de redes y sistemas y otros). La TIC 3.0 define casos de uso específicos que describen la implementación de zonas de confianza y capacidades de seguridad en aplicaciones, servicios y entornos específicos. También se centra en las protecciones basadas en la red, mientras que la ZTA es una arquitectura más inclusiva que aborda las protecciones de las aplicaciones, los usuarios y los datos. A medida que la TIC 3.0 desarrolle sus casos de uso, es probable que se genere un escenario de ZTA TIC para definir las protecciones de red que se desplegarán en los puntos de aplicación de la ZTA.

6.5 ZTA y Einstein (Sistema de Protección de Seguridad Nacional, NCPS)

El NCPS (por su nombre en inglés National Cybersecurity Protection System y conocido operativamente como Einstein) es un sistema integrado que incluye subsistemas. Este ofrece servicios de detección de intrusiones, análisis avanzados, intercambio de información y prevención de intrusiones para defender al Gobierno Federal de las ciberamenazas. Los objetivos del NCPS, que se alinean con los objetivos generales de la confianza cero, consisten en gestionar el riesgo cibernético, mejorar la ciberprotección y capacitar a los socios para asegurar el ciberespacio. Los sensores de Einstein permiten al Centro Nacional de Integración de la Ciberseguridad y las Comunicaciones (NCCIC, por su nombre en inglés National Cybersecurity and Communications Integration Center) de la Agencia de Seguridad de Infraestructura y Ciberseguridad CISA (por su nombre en inglés Cybersecurity and Infrastructure Security Agency) responder a incidentes significativos en las agencias federales y defender sus redes.

Dentro del Gobierno Federal se encuentran los sensores NCPS para el reconocimiento de la situación del DHS, los cuales se basan en una defensa de la red perimetral, mientras que la ZTA sitúa las protecciones más cerca de los activos, los datos y todos los demás recursos. El programa NCPS está mejorando para garantizar la conservación del conocimiento de la situación mediante la utilización de información de seguridad sobre el tráfico basado en la nube, lo que ayuda a sentar las bases para una ampliación de la telemetría del conocimiento de la situación desde los sistemas de la ZTA. Las funciones de prevención de intrusiones de los NCPS también requerirían una evolución para poder informar sobre la aplicación de políticas tanto en las actuales ubicaciones de los NCPS como en los sistemas ZTA. A medida que se adopte la ZTA en todo el Gobierno Federal, la implementación del NCPS deberá evolucionar continuamente, o será necesario desplegar nuevas capacidades para cumplir los objetivos del NCPS. Los responsables de respuesta a incidentes podrían aprovechar la información procedente de la autenticación, de la inspección y del registro del tráfico disponibles de las agencias para las entidades federales que

hayan implementado una arquitectura de confianza cero. La información generada en una ZTA podría contribuir a la cuantificación del impacto del evento; mientras que las herramientas de aprendizaje automático permitirían utilizar los datos de la ZTA para mejorar la detección. Asimismo, los registros adicionales de la ZTA podrían guardarse para que los responsables de la respuesta a incidentes realicen un análisis después de los hechos.

6.6 ZTA y programa de Diagnóstico y Mitigación Continuos (CDM) del DHS

El programa CDM del DHS es un proyecto para mejorar la tecnología de la información (TI) de las agencias federales. En este contexto, es fundamental que los organismos conozcan los activos, la configuración y los sujetos que los componen; para proteger sus sistemas, necesitan establecer procesos que les permitan descubrir y comprender los componentes y actores básicos de su infraestructura:

- **¿Qué está conectado?** ¿Qué dispositivos, aplicaciones y servicios utiliza la organización? Se trata de observar y mejorar la postura de seguridad de estos artefactos a medida que se descubren vulnerabilidades y amenazas.
- **¿Quién utiliza la red?** ¿Qué usuarios forman parte de la organización o son externos y pueden acceder a los recursos de la empresa? Entre ellos se encuentran las NPE que pueden estar realizando acciones autónomas.
- **¿Qué ocurre en la red?** La empresa necesita conocer los patrones de tráfico y los mensajes entre sistemas.
- **¿Cómo se protegen los datos?** La empresa necesita una política establecida sobre cómo se protege la información en reposo, en tránsito y en uso.

La clave para el éxito de la ZTA consiste en contar con una sólida implementación del programa CDM. Por ejemplo, una empresa que quiera pasar a la ZTA debe tener un sistema para descubrir y registrar los activos físicos y virtuales a fin de crear un inventario útil. El sistema CDM del DHS ha iniciado varios pasos para crear las capacidades necesarias dentro de las agencias federales y así poder pasar a una ZTA. Por ejemplo, el programa DHS de Gestión de Activos de Hardware (HWAM), (HWAM, por su nombre en inglés Hardware Asset Management) tiene por objeto ayudar a los organismos a identificar los dispositivos de su infraestructura de red para implementar una configuración segura, lo que es similar a los primeros pasos en el desarrollo de una hoja de ruta hacia la ZTA. Las agencias deben tener visibilidad de los activos de la red (o de aquellos que acceden a los recursos de forma remota) para categorizar, configurar y supervisar su actividad.

6.7 ZTA, Cloud Smart y la Estrategia Federal de Datos

La estrategia Cloud Smart[11] (nube inteligente), la política actualizada de Data Center Optimization Initiative (Iniciativa de Optimización de Centros de Datos) (M-19-19) y la Federal

[11] Federal Cloud Computing Strategy: https://cloud.cio.gov/strategy/

Data Strategy[12] (Estrategia Federal de Datos) determinan algunos requisitos para los organismos que planifican una ZTA. Estas políticas exigen que las agencias hagan un inventario y evalúen cómo recogen, almacenan y acceden a los datos, tanto en las instalaciones como en la nube.

Este inventario es fundamental para determinar qué procesos y recursos empresariales se beneficiarían de la implantación de una ZTA. Los datos, así como las aplicaciones y los servicios que se encuentran principalmente en la nube o que son utilizados sobre todo por trabajadores remotos resultan buenos candidatos para un enfoque de ZTA (véase la sección 7.3.3), ya que los sujetos y los recursos se encuentran fuera del perímetro de la red de la empresa y es probable que obtengan los mayores beneficios en cuanto a uso, escalamiento y seguridad.

Una consideración adicional con la Estrategia Federal de Datos es cómo hacer que los activos datos de la agencia sean accesibles a otras agencias o al público. La solución corresponde al caso de la ZTA de colaboración interempresarial (véase la sección 4.4). Los organismos que utilicen una ZTA para estos activos deberían tener en cuenta los requisitos de colaboración o publicación a la hora de desarrollar la estrategia.

[12] Federal Data Strategy: https://strategy.data.gov/

7 Migración hacia una arquitectura de confianza cero

La implantación de una ZTA es un viaje, más que una sustitución total de la infraestructura o de los procesos. Una organización debe intentar implementar gradualmente los principios de confianza cero, los cambios en los procesos y las soluciones tecnológicas que protegen sus datos de mayor valor. La mayoría de las empresas continuarán operando en un modo híbrido durante un período indefinido, al mismo tiempo que seguirán invirtiendo en iniciativas de modernización de las TI. Contar con un plan de modernización de TI que incluya el paso a una arquitectura basada en los principios de ZT puede ayudar a las empresas a elaborar hojas de ruta para migraciones de flujos de trabajo a pequeña escala.

El modo en que una empresa migra a una estrategia depende de su postura y de las operaciones de ciberseguridad en las que se encuentra. Además, debería alcanzar una línea de base de competencias antes de que pueda desplegar un entorno significativo centrado en la ZT (Consejo Americano para la Tecnología [ACT] por su nombre en inglés American Council for Technology y Consejo Consultivo de la Industria [IAC], por su nombre en inglés Industry Advisory Council). Este punto de partida incluye una identificación y un inventario de los activos, los sujetos, los procesos de negocio, los flujos de tráfico y los mapeos de dependencia. La empresa necesita esta información antes de poder desarrollar una lista de procesos de negocio potenciales al igual que los sujetos y los activos que estarán involucrados.

7.1 Arquitectura de confianza cero pura

En un contexto nuevo, sería posible construir una arquitectura de confianza cero desde el principio. En el supuesto de que la empresa conozca las aplicaciones, los servicios y los flujos de trabajo que desee utilizar para sus operaciones, podría elaborar una arquitectura basada en los principios de la confianza cero para esos flujos. Una vez identificados estos procedimientos, la empresa podría delimitar los componentes necesarios y comenzar a determinar cómo interactuarían los individuales. A partir de ahí, se trata de un ejercicio de ingeniería y organización para construir la infraestructura y configurar los componentes. En función de la configuración y el funcionamiento actual de la empresa, podría ser necesario introducir cambios organizativos adicionales.

En la práctica, esta no suele ser una opción viable para las agencias federales o cualquier organización con una red existente. No obstante, puede haber ocasiones en las que se pida a una agencia que cumpla con una nueva responsabilidad que requiera la construcción de su propia infraestructura. En estos casos, se podrían introducir los conceptos de ZT en cierto grado. Por ejemplo, un organismo puede recibir una nueva responsabilidad que implique la construcción de una nueva aplicación, servicio o base de datos. La agencia podría diseñar la nueva infraestructura necesaria en torno a los principios de ZT y la ingeniería de sistemas seguros (*SP 8900-160v1*), como la evaluación de la confianza de los sujetos antes de conceder el acceso y el establecimiento de microperímetros alrededor de los nuevos recursos. El grado de éxito variará en función de cuánto dependerá esta nueva infraestructura de los recursos ya existentes (por ejemplo, los sistemas de gestión de identidad).

7.2 Arquitectura híbrida basada en la ZTA y en el perímetro

Es poco probable que cualquier empresa importante pueda migrar a la confianza cero en un solo ciclo de actualización tecnológica. Puede haber un periodo indefinido en el que los flujos de trabajo de la ZTA coexistan con los que no lo son. El cambio a este nuevo enfoque se realiza gradualmente, pasando de un proceso de negocio a otro. La entidad debe asegurarse de que los elementos comunes (por ejemplo, la gestión de la identidad, la de los dispositivos e incluso el registro de eventos) sean lo suficientemente flexibles como para funcionar en una arquitectura de seguridad híbrida basada en la ZTA y en el perímetro. Por otro lado, los arquitectos de la compañía quizás quieran limitar las soluciones candidatas a ZTA en favor de aquellas que puedan interactuar con los componentes actuales.

La migración de un flujo de trabajo ya existente a una ZTA requerirá probablemente (al menos) un rediseño parcial. Las empresas pueden aprovechar esta oportunidad para adoptar prácticas de ingeniería de sistemas seguros (*SP 800-160v1*) si aún no lo han hecho para la organización de sus tareas.

7.3 Pasos para introducir la ZTA en una red con arquitectura basada en el perímetro

La migración a una ZTA requiere de un conocimiento detallado de los activos (físicos y virtuales), de los sujetos (incluidos los privilegios de los usuarios) y de los procesos empresariales. El PE accede a esa información cuando evalúa las solicitudes de los recursos. Un conocimiento incompleto suele conducir a una falla en los procedimientos del negocio en el que el PE deniega las solicitudes por falta de información, lo que representa especialmente un problema si se desconocen los despliegues de «TI en la sombra» que operan dentro de una organización.

Antes de emprender el esfuerzo para implantar una ZTA en una empresa, se debe realizar el estudio de los activos, los sujetos, los flujos de datos y los de trabajo. Este reconocimiento constituye los cimientos que deben establecerse antes de que sea posible la implementación de una ZTA. Una organización no puede determinar qué nuevos procesos o sistemas deben implantarse si desconoce el estado actual de sus operaciones. Estas investigaciones pueden realizarse en paralelo, pero todas están vinculadas al examen de los procedimientos empresariales de la organización. Estos pasos pueden relacionarse con los del RMF (*SP 800-37*), ya que cualquier adopción de una ZTA implica un protocolo para reducir el riesgo de las funciones empresariales de la agencia. El camino hacia la implantación de una ZTA puede visualizarse en la Figura 12.

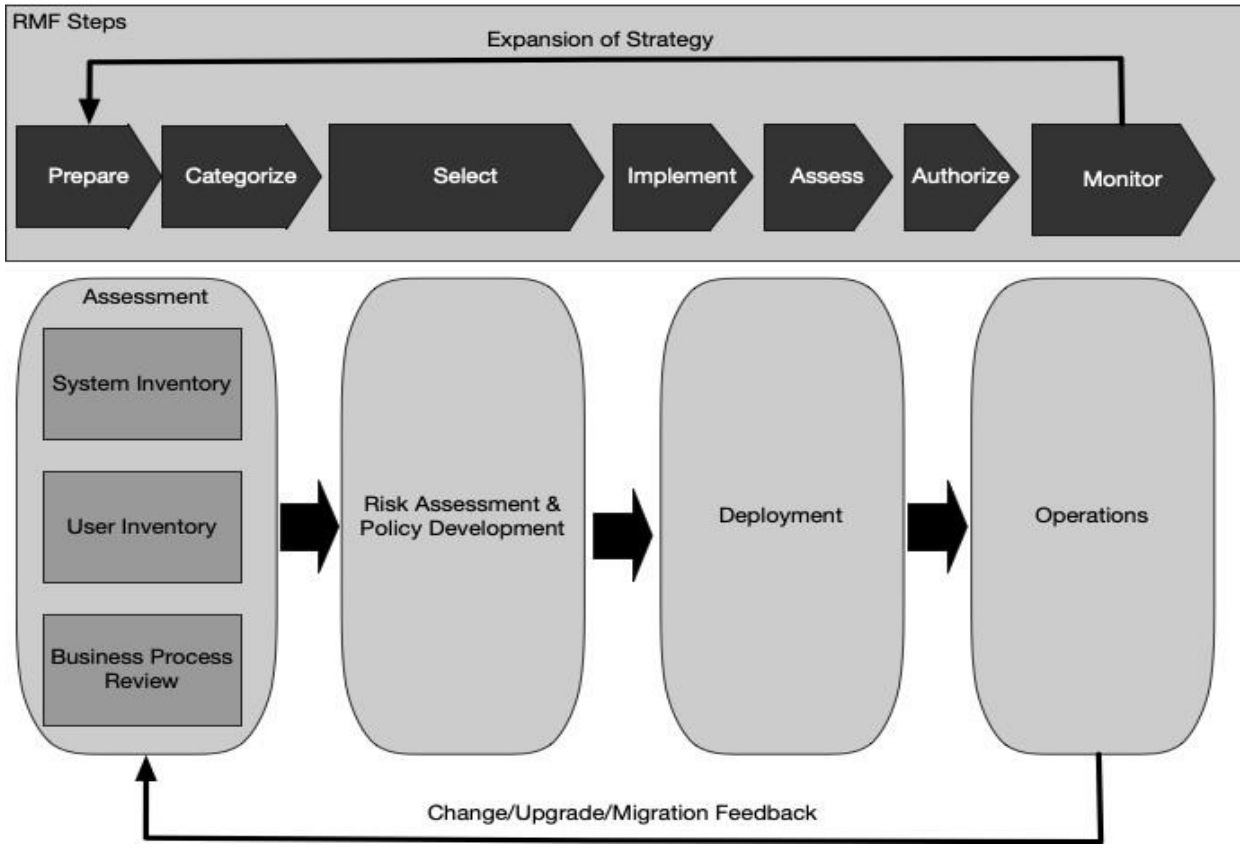

Figura 12
Ciclo de implantación de una ZTA

RMF Steps (pasos del RMF). *Expansion of Strategy* (desarrollo de la estrategia). *Prepare* (preparar). *Categorize* (clasificar). *Select* (seleccionar). *Implement* (implementar). *Assess* (evaluar). *Authorize* (autorizar). *Monitor* (monitorear).
Assessment (evaluación). *System Inventory* (inventario del sistema). *User Inventory* (inventario de usuarios). *Business Process Review* (revisión de los procesos del negocio). *Risk Assessment and Policy Development* (evaluación del riesgo y desarrollo de las políticas). *Deployment* (implementación). *Operations* (operaciones).
Change/Upgrade/Migration Feedback (cambio/actualización/retroalimentación de la migración).

Tras la creación del inventario inicial, existe un ciclo regular de mantenimiento y actualización. Esta última puede cambiar los procesos de negocio o no tener ningún impacto, pero, en todo caso, estos procedimientos deben evaluarse. Por ejemplo, un cambio en los proveedores de certificados digitales puede parecer no tener un impacto significativo, pero quizás implique la gestión del almacenamiento del certificado raíz, la supervisión del registro de Certificate Transparency y de otros factores que no son visibles al principio.

7.3.1 Identificación de los miembros de la empresa

Para que una empresa de confianza cero funcione, el PE debe tener conocimiento de los sujetos involucrados en ella, los cuales pueden abarcar tanto humanos y posibles NPE como cuentas de servicios que interactúan con los recursos.

Los usuarios con privilegios especiales, como los desarrolladores o los administradores de sistemas, requieren un examen adicional cuando se les asignan atributos o funciones. En muchas arquitecturas de seguridad heredadas, estas cuentas pueden tener un permiso total para acceder a todos los recursos de la compañía. La ZTA debe otorgarles la flexibilidad suficiente para cumplir con los requisitos del negocio y a la vez poder utilizar los registros y realizar las acciones de auditoría para identificar patrones de comportamiento de acceso. Las implementaciones de ZTA pueden requerir que los administradores obtengan un nivel de confianza más estricto o que cumplan con los criterios descritos en *SP 800-63A*, Sección 5.

7.3.2 Identificación de los activos propiedad de la empresa

Como se mencionó en la sección 2.1, uno de los requisitos clave de la ZTA es la capacidad de identificar y gestionar los dispositivos, así como de reconocer y supervisar los que no son propiedad de la empresa y que se encuentran en su infraestructura de red o acceden a sus recursos. La capacidad de manejar los activos de la organización es clave para el éxito de la implementación de una ZTA. Su puesta en funcionamiento incluye componentes de *hardware* (por ejemplo, computadores portátiles, teléfonos, dispositivos IdC) y artefactos digitales (como cuentas de usuario, aplicaciones, certificados). Quizás no sea posible realizar un censo completo de todos los pertenecientes a la entidad, por lo que esta debe poder identificar, categorizar y evaluar rápidamente los que se vayan descubriendo en su infraestructura.

Las acciones mencionadas van más allá de la catalogación y el mantenimiento de una base de datos de los activos de la empresa; también incluyen la gestión de la configuración y la supervisión. La capacidad de observar sus estados actuales forma parte del proceso de evaluación de las solicitudes de acceso (véase la sección 2.1). Por tanto, la compañía debe ser capaz de configurarlos, supervisarlos y actualizarlos, tanto los virtuales como los contenedores, lo que también incluye la ubicación física (según la mejor estimación) y de la red. El PE debe disponer de esta información a la hora de tomar las decisiones sobre el acceso a los recursos.

Los activos que no son propiedad de la empresa y la «TI en la sombra» que se encuentra en ella también deben clasificarse lo mejor posible. Este proceso puede incluir todo lo que es visible para la organización (por ejemplo, la dirección MAC y la ubicación de la red) y puede ampliarse con los datos del administrador. Esta información no solo se utiliza para las decisiones de acceso (pues los colaboradores y los bienes BYOD pueden necesitar contactarse con los PEP), sino también para la supervisión y el registro forense. La TI en la sombra presenta un problema especial, en tanto que estos recursos son propiedad de la compañía, pero no se gestionan como los demás. En algunos enfoques de ZTA (principalmente basados en la red) los componentes de la TI en la sombra quedan inutilizables, ya que puede suceder que la organización no los reconozca ni los incluya en las políticas de acceso a la red.

Muchos organismos federales ya han comenzado a identificar sus activos. Las agencias que han establecido programas de CDM, como la gestión de los activos de *hardware* HWAM (por su nombre en inglés, Hardware Assets Management) y la gestión de activos de *software* (SWAM, por su nombre en inglés, Software Asset Management), disponen de un valioso repertorio de datos a los que recurrir a la hora de adoptar una ZTA. Además, pueden tener una lista de procesos candidatos a una ZTA relacionados con activos de alto valor (HVA, por su nombre en

inglés High Value Assets) (M-19-03)[13] que hayan sido identificados como claves para sus tareas. Este trabajo debería realizarse en toda empresa —o agencia— antes de que cualquier proceso empresarial pudiera ser (re)diseñado con un modelo de ZTA. Estos programas deben concebirse de forma que sean extensibles y adaptables a los cambios que se produzcan en la organización, no solo al migrar a una ZTA, sino también al momento de contabilizar nuevos activos, servicios y procesos empresariales que pasen a formar parte de ella.

7.3.3 Identificación de los procesos claves y evaluación de los riesgos asociados a la ejecución del proceso

El tercer inventario que se debe realizar es la identificación y clasificación de los procesos de negocio, los flujos de datos y la relación de todos estos con la misión de la entidad. Las empresas deben informar sobre las circunstancias en las que se conceden y deniegan las solicitudes de acceso a los recursos. Quizás se desee empezar con un emprendimiento de bajo riesgo para la primera transición a la ZTA, ya que es probable que las interrupciones no afecten negativamente a toda la organización. Una vez que se haya adquirido suficiente experiencia, procedimientos empresariales más críticos pueden convertirse en candidatos.

Las organizaciones que utilizan recursos basados en la nube o que cuentan con trabajadores remotos suelen ser buenas candidatas para la ZTA y probablemente notarán mejoras en su disponibilidad y seguridad. En lugar de proyectar el perímetro de la organización dentro de la nube o introducir a los clientes en la red de la empresa a través de una VPN, estos últimos pueden solicitar los servicios en la nube directamente. Los PEP garantizan el cumplimiento de las políticas empresariales antes de conceder el acceso a los recursos a un cliente. Los programadores también deben tener en cuenta las posibles relaciones de costo-beneficio en cuanto al rendimiento, la experiencia del usuario y el posible aumento de la fragilidad del flujo de trabajo que podría producirse al implementar la ZTA en un proceso de negocio determinado.

7.3.4 Formulación de políticas para el candidato a la ZTA

El desarrollo de identificación de un servicio o flujo de trabajo empresarial candidato depende de varios factores: la importancia del proceso para la organización, el grupo de sujetos afectados y el estado actual de los recursos utilizados para la cadena de tareas. El valor del activo o del flujo de trabajo, en función de sus riesgos, se puede estimar utilizando el Marco de Gestión de Riesgos del NIST (SP 800-37).

Una vez identificado el activo o el flujo de trabajo, se deben detectar todos los recursos ascendentes (como los sistemas de gestión de ID, las bases de datos o los microservicios), los descendentes (los registros, la supervisión de la seguridad) y las entidades (por ejemplo, los sujetos y las cuentas de servicio) que se utilizan o se ven afectados. Estos diferentes elementos pueden influir en la elección para la primera migración a la ZTA. De este modo, se preferirá una aplicación o servicio utilizado por un subconjunto identificado de sujetos de la empresa (como

[13] N. del T.: el M-19-03 es el Memorando para los Jefes de los Departamentos y Agencias Ejecutivos, en inglés Memorandum for Heads of Executive Departments and Agencies, que puede encontrarse en «https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf».

un sistema de compras) a uno que sea vital para todos los sujetos de la empresa (por ejemplo, el correo electrónico).

Luego, los administradores deben determinar el conjunto de criterios (si se utiliza un TA basado en criterios) o las ponderaciones del nivel de confianza (si se utiliza un TA basado en la puntuación) para los recursos utilizados en el proceso de negocio candidato (véase la sección 3.3.1). Los administradores quizás necesiten adaptar estos criterios o valores durante la fase de ajuste, lo cual es necesario para garantizar que las políticas sean efectivas y al mismo tiempo no obstaculicen el acceso a los recursos.

7.3.5 Identificación de soluciones candidatas

Una vez elaborada la lista de los procesos de negocio candidatos, los arquitectos de la empresa pueden componer una lista de soluciones potenciales. Algunos modelos de implantación (véase el apartado 3.1) se adaptan mejor a determinados flujos de trabajo y ecosistemas empresariales actuales. Del mismo modo, algunas soluciones de proveedores se adecuan mejor a algunos casos de uso que a otros. A continuación, se exponen ciertos factores para tener en cuenta:

- **¿Requiere la solución que los componentes se instalen en el activo del cliente?** Este requisito puede limitar los procesos empresariales en los que ya se utilicen (o se desee usar) activos que no sean propiedad de la empresa, como el BYOD o las colaboraciones entre organismos.
- **¿Funciona la solución cuando los recursos se encuentran completamente en las instalaciones de la empresa?** Algunas soluciones suponen que los recursos solicitados residirán en la nube (el llamado tráfico norte-sur) y no dentro del perímetro de la empresa (tráfico este-oeste). La ubicación de los recursos del proceso empresarial seleccionado influirá en las soluciones posibles, así como la ZTA en el desarrollo.
- **¿Proporciona la solución un medio para registrar las interacciones a fin de analizarlas?** Un componente clave de la ZT es la recopilación y el uso de datos relacionados con el flujo de los procesos que retroalimentan al PE a la hora de tomar decisiones de acceso.
- **¿Proporciona la solución un amplio soporte para diferentes aplicaciones, servicios y protocolos?** Algunas soluciones pueden admitir una amplia gama de protocolos (web, Secure Shell [SSH], etc.) y de transportes (IPv4 e IPv6), mientras que otras solo pueden funcionar con un enfoque limitado, como la web o el correo electrónico.
- **¿Requiere la solución cambios en el comportamiento del sujeto?** Algunas soluciones pueden requerir pasos adicionales para realizar un determinado flujo de trabajo; así, pueden cambiar la forma en que los sujetos de la empresa realizan los procedimientos laborales**.**

Una solución consiste en remodelar un proceso de negocio ya existente, como un programa piloto —en lugar de una mera sustitución— el cual podría ser general para aplicarse a varios procesos de negocio o específico para un caso de uso en particular. Además, podría utilizarse

como «campo de pruebas» antes de que los sujetos realicen la transición a una implantación de ZTA y se alejen de la infraestructura del proceso heredado.

7.3.6 Implementación inicial y control

Una vez elegidos el flujo de trabajo y los componentes candidatos para la ZTA, la implementación inicial puede comenzar. Los administradores de la empresa deben aplicar las políticas desarrolladas utilizando los componentes seleccionados, pero es posible que al principio deseen operar en modo de observación y supervisión. Son pocas las políticas empresariales que llegan a completarse en sus primeras versiones: puede suceder que a las cuentas de usuario importantes (por ejemplo, las cuentas de administrador) se les niegue el acceso a los recursos que necesitan o, por el contrario, quizás no requieran todos los privilegios de acceso que se les han asignado.

El nuevo flujo de trabajo empresarial ZT podría funcionar en modo solo informe durante algún tiempo, para asegurarse de que las políticas sean eficaces y viables. Además, esta modalidad permite que la empresa comprenda los activos de referencia y las solicitudes de acceso a los recursos, el comportamiento y los patrones de comunicación. El enfoque de solo informe significa que se debe conceder el acceso a la mayoría de las solicitudes, y los registros y rastros de las conexiones deben compararse con la política inicial desarrollada. Deberían aplicarse y registrarse las políticas básicas, como la denegación de solicitudes que no pasen la MFA o que aparezcan desde direcciones IP conocidas, controladas o subvertidas por atacantes; pero tras el despliegue inicial, las políticas de acceso deberían ser más indulgentes para recopilar datos de las interacciones reales del flujo de trabajo de la ZT. Una vez que se hayan establecido los patrones de actividad de referencia para el flujo de trabajo, los comportamientos anómalos podrán identificarse más fácilmente. Si no es posible operar de una manera más flexible, los operadores de redes empresariales deberían supervisar de cerca los registros y estar preparados para modificar las políticas de acceso basándose en la experiencia operativa.

7.3.7 Ampliación de la ZTA

Cuando se adquiere suficiente confianza y se perfecciona el conjunto de políticas de flujo de trabajo, la empresa entra en la fase operativa estable. La red y los activos se siguen supervisando y el tráfico se registra (véase el apartado 2.1); pero las respuestas y las modificaciones de las políticas se realizan a un ritmo más lento, puesto que no deberían ser graves. Los sujetos y las partes interesadas de los recursos y los procesos implicados también tendrían que proporcionar información para mejorar las operaciones. En esta fase, los administradores de la empresa pueden empezar a planificar la siguiente fase de implementación de la ZT. Al igual que en el despliegue anterior, es necesario identificar un flujo de trabajo y un conjunto de soluciones potenciales y desarrollar las políticas iniciales.

Sin embargo, si se produce un cambio en el flujo de trabajo, es necesario reevaluar la arquitectura de ZT operativa. Los cambios significativos en el sistema, como los nuevos dispositivos, las actualizaciones importantes del *software* (especialmente los componentes lógicos de la ZT) y las reformas en la estructura organizativa pueden dar lugar a modificaciones en el flujo de trabajo o en las políticas. En efecto, todo el proceso debe reconsiderarse partiendo

de la base de que parte del trabajo ya se ha realizado. Por ejemplo, se han comprado nuevos dispositivos, pero no se han creado nuevas cuentas de usuario, por lo que solo hay que actualizar el inventario.

Referencias

ACT-IAC American Council for Technology and Industry Advisory Council. (2019). *Zero Trust Cybersecurity Current Trends*. Disponible en https://www.actiac.org/zero-trust-cybersecurity-current-trends

Anderson Anderson B., McGrew D. (2017). Machine Learning for Encrypted Malware Traffic Classification: Accounting for Noisy Labels and Non-Stationarity. *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (ACM, Halifax, Nova Scotia, Canada), pp. 1723-1732. https://doi.org/10.1145/3097983.3098163

BCORE Department of Defense CIO. (2007). Department of Defense Global Information Grid Architecture Vision Version 1.0 June 2007. Disponible en http://www.acqnotes.com/Attachments/DoD%20GIG%20Architectural%20Vision,%20June%2007.pdf

CSA-SDP Cloud Security Alliance. (2015). SDP Specification 1.0. Disponible en https://cloudsecurityalliance.org/artifacts/sdp-specification-v1-0/

FIPS199 National Institute of Standards and Technology. (2004). Standards for Security Categorization of Federal Information and Information Systems. (U. S. Department of Commerce, Washington, DC). Federal Information Processing Standards Publication (FIPS). 199. https://doi.org/10.6028/NIST.FIPS.199

Gilman Gilman E., Barth D. (2017). *Zero Trust Networks: Building Secure Systems in Untrusted Networks* (O'Reilly Media, Inc., Sebastopol, CA). Primera edición.

HWAM Department of Homeland Security. (2015). *Hardware Asset Management (HWAM) Capability Description*. Disponible en https://www.uscert.gov/sites/default/files/cdm_files/HWAM_CapabilityDescription.pdf

IBNVN Cohen R., Barabash K., Rochwerger B., Schour L., Crisan D., Birke R., Minkenberg C., Gusat M., Recio R., Jain V. (2013). An Intent-based Approach for Network Virtualization. *2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013)*. (IEEE, Ghent, Belgium), pp. 42-50. Disponible en https://ieeexplore.ieee.org/document/6572968

JERICHO The Jericho Forum. (2007). *Jericho Forum Commandments*, version 1.2. Disponible en https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf

M-19-03 Office of Management and Budget. (2018). Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program. (The White House, Washington, DC), OMB Memorandum M19-03, 10 de diciembre de 2018. Disponible en https://www.whitehouse.gov/wpcontent/uploads/2018/12/M-19-03.pdf

M-19-17 Office of Management and Budget. (2019). Enabling Mission Delivery through Improved Identity, Credential, and Access Management. (The White House, Washington, DC), OMB Memorandum M-19-17, 21 de mayo de 2019. Disponible en https://www.whitehouse.gov/wpcontent/uploads/2019/05/M-19-17.pdf

M-19-19 Office of Management and Budget. (2019). Update on Data Center Optimization Initiative (DCOI). (The White House, Washington, DC), OMB Memorandum M-19-19, June 25, 2019. Dsiponible en https://datacenters.cio.gov/assets/files/m_19_19.pdf

M-19-26 Office of Management and Budget. (2019). Update to the Trusted Internet Connections (TIC) Initiative. (The White House, Washington, DC), OMB Memorandum M-19-26, September 12, 2019. Disponible en https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf

NISTIR 7987 Ferraiolo D., Gavrila S., Jansen W. (2015). Policy Machine: Features, Architecture, and Specification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7987, Rev. 1. https://doi.org/10.6028/NIST.IR.7987r1

NISTIR 8062 Brooks S. W., Garcia M. E., Lefkovitz N. B., Lightman S., Nadeau E. (2017). An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8062. https://doi.org/10.6028/NIST.IR.8062

NISTPRIV National Institute of Standards and Technology. (2020). Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.01162020

SDNBOOK Nadeau T., Gray K. (2013). *SDN: Software Defined Networks: An Authoritative Review of Network Programmability Technologies*. (O'Reilly), 1era. edición.

SP800-37 Joint Task Force. (2018). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST *Special Publication (SP) 800-37*, Rev. 2.

SP800-63 Grassi P. A., Garcia M. E., Fenton J. L. (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, incluye actualizaciones hasta el 2 de marzo de 2020. https://doi.org/10.6028/NIST.SP.800-63-3

SP800-63A Grassi P. A., Fenton J. L., Lefkovitz N. B., Danker J. M., Choong Y-Y, Greene K. K., Theofanos M. F. (2017) Digital Identity Guidelines: Enrollment and Identity Proofing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63A, incluye actualizaciones hasta el 2 de marzo de 2020. https://doi.org/10.6028/NIST.SP.800-63A

SP800-160v1 Ross R., McEvilley M., Oren J. C. (2016). Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Incluye actualizaciones hasta el 21 de marzo 2018. https://doi.org/10.6028/NIST.SP.800-160v1

SP800-160v2 Ross R., Pillitteri V., Graubart R., Bodeau D., McQuaid R. (2019). Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 2. https://doi.org/10.6028/NIST.SP.800-160v2

SP800-162 Hu V. C., Ferraiolo D. F., Kuhn R., Schnitzer A., Sandlin K., Miller R., Scarfone K. A. (2014). Guide to Attribute Based Access Control (ABAC) Definition and Considerations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-162, incluye actualizaciones hasta el 2 de agosto de 2019. https://doi.org/10.6028/NIST.SP.800-162

SWAM Department of Homeland Security (2015) *Software Asset Management (SWAM) Capability Description*. Disponible en https://www.uscert.gov/sites/default/files/cdm_files/SWAM_CapabilityDescription.pdf

Apéndice A
Siglas

API	Application Programming Interface / Interfaz de programación de aplicaciones
BYOD	Bring Your Own Device / Trae tu propio dispositivo
CDM	Continuous Diagnostics and Mitigation / Diagnóstico y mitigación continuos
DHS	Department of Homeland Security / Departamento de Seguridad Nacional de los Estados Unidos
DoS	Denial of Service / Denegación de servicio
G2B	Government to Business (private industry) / Gobierno a negocio (industria privada)
G2G	Government to Government / Gobierno a Gobierno
NIST	National Institute of Standards and Technology / Instituto Nacional de estándares y tecnología
NPE	Non-Person Entity / Entidad no personal
PA	Policy Administrator / Administrador de políticas
PDP	Policy Decision Point / Punto de decisión de políticas
PE	Policy Engine /Motor de políticas
PEP	Policy Enforcement Point / Punto de aplicación de políticas
PKI	Public Key Infrastructure / Infraestructura de clave pública
RMF	NIST Risk Management Framework / Marco de Gestión de Riesgos
SDN	Software Defined Network / Redes definidas por *software*
SDP	Software Defined Perimeter / Perímetro definido por *software*
SIEM	Security Information and Event Monitoring / Sistema de seguridad de la información y gestión de eventos
TIC	Trusted Internet Connections / Conexión a Internet de confianza
VPN	Virtual Private Network / Red privada virtual

ZT	Zero Trust / Confianza cero
ZTA	Zero Trust Architecture / Arquitectura de confianza cero

Apéndice B
Brechas identificadas en el estado actual de la ZTA

Durante la investigación llevada a cabo para la elaboración de este documento, se estudió la madurez actual de los componentes y soluciones de confianza cero. La conclusión de esta encuesta fue que el estado actual del ecosistema ZTA no es lo suficientemente maduro como para su adopción generalizada. Aunque es posible utilizar estrategias de ZTA para planificar y desplegar un entorno empresarial, no existe una solución única que proporcione todos los componentes necesarios. Además, pocos componentes de ZTA disponibles en la actualidad pueden utilizarse para todos los flujos de trabajo presentes en una empresa.

A continuación se resumen las brechas identificadas en el ecosistema de la ZTA y las áreas que necesitan una mayor investigación. Algunas de estas áreas cuentan con cierta base de trabajo, pero no se conoce bien cómo los principios de ZTA cambian estas áreas, ya que no hay suficiente experiencia con diversos entornos empresariales centrados en ZTA.

B.1 Estudio sobre la tecnología

Se invitó a varios proveedores a presentar sus productos y puntos de vista sobre la confianza cero. El objetivo de esta encuesta fue identificar las piezas que faltan y que impiden a los organismos pasar ahora a una infraestructura empresarial basada en la confianza cero o mantener una implantación de ZTA existente. Estas carencias pueden clasificarse en implantación inmediata (inmediata o a corto plazo), carencias sistémicas que afectan al mantenimiento o a las operaciones (a corto o medio plazo) y falta de conocimientos (áreas para futuras investigaciones). Todas ellas se resumen en la Tabla B-1.

Tabla B-1: resumen de las deficiencias de despliegue identificadas

Categoría	Ejemplos de preguntas	Brechas identificadas
Despliegue inmediato	• ¿Cómo deberían redactarse los requisitos de contratación? • ¿Cómo funciona un plan de ZTA con TIC, FISMA y otros requisitos?	• Falta de un marco y un vocabulario comunes para la ZTA. • Percepción de que la ZTA entra en conflicto con la política vigente.
Sistémico	• ¿Cómo se puede prevenir la dependencia de un proveedor? • ¿Cómo interactúan los distintos entornos de ZTA?	• Demasiada dependencia de las API de los proveedores.

Áreas que necesitan más investigación	• ¿Cómo evolucionarán las amenazas ante la ZTA? • ¿Cómo cambiarán los procesos empresariales ante la ZTA?	• ¿Cómo es un proceso exitoso en una empresa con ZTA? • Experiencia documentada del usuario final en una empresa con una ZTA.

B.2 Brechas que impiden el paso inmediato a la ZTA

A continuación, se presentan los problemas que frenan la adopción de una ZTA en la actualidad. Se clasificaron como problemas inmediatos, y no se pensó en el mantenimiento o la migración futuros para esta categoría. Una empresa con visión de futuro también puede considerar que la categoría de mantenimiento es una preocupación inmediata que impide el despliegue inicial de los componentes de la ZTA. No obstante, para este análisis, estos problemas se consideran una categoría separada.

B.2.1 Falta de términos comunes para el diseño, la planificación y la adquisición de ZTA

La confianza cero como estrategia para el diseño y despliegue de infraestructuras empresariales es todavía un concepto en formación. La industria aún no se ha reunido en torno a un único conjunto de términos o conceptos para describir los componentes y operaciones de la ZTA. Esto hace que resulte difícil para las organizaciones (por ejemplo, las agencias federales) desarrollar requisitos y políticas coherentes para el diseño de infraestructuras empresariales de confianza cero y la adquisición de componentes.

El propósito de las secciones 2.1 y 3.1 es un primer intento de formar una base neutra de términos y conceptos para describir la ZTA. Los componentes abstractos de la ZTA y los modelos de despliegue se desarrollaron para servir como términos básicos y formas de pensar sobre la ZTA. El objetivo es proporcionar una forma común de ver, modelar y discutir soluciones de ZTA el momento de desarrollar requisitos empresariales y realizar estudios de mercado. Las secciones anteriores pueden resultar incompletas a medida que se adquiera más experiencia con la ZTA en los organismos federales, pero actualmente sirven de base para un marco conceptual común.

B.2.2 Percepción de que la ZTA entra en conflicto con las políticas federales de ciberseguridad existentes

Existe la idea errónea de que la ZTA es un marco único con un conjunto de soluciones incompatibles con la visión actual de la ciberseguridad. Por el contrario, la confianza cero debe considerarse una evolución de las estrategias actuales de ciberseguridad, ya que muchos de sus conceptos e ideas están en circulación desde hace tiempo. Se ha animado a las agencias federales a adoptar un enfoque de ciberseguridad más basado en la confianza cero a través de las directrices existentes (véase la Sección 6). Si una agencia dispone de un sistema de gestión de identidad maduro y de herramientas sólidas de CDM, está en el camino hacia una ZTA (véase la Sección 7.3). Entonces, esta percepción se basa en una concepción errónea de la ZTA y de cómo ha evolucionado a partir de anteriores paradigmas de ciberseguridad.

B.3 Brechas sistémicas que afectan a la ZTA

Se trata de las brechas que afectan a la implementación y despliegue iniciales de la ZTA y a la continuidad de su funcionamiento y madurez. Estas podrían ralentizar la adopción de la ZTA en las organizaciones o provocar la fragmentación de la industria de componentes de ZTA. Los estándares abiertos (producidos por organizaciones de desarrollo de estándares [SDO, por su desarrollo en inglés Standards Development Organization] o un consorcio industrial) podrían ayudar en estas brechas sistémicas.

B.3.1 Estandarización de las interfaces entre componentes

Durante la encuesta tecnológica, se hizo evidente que ningún vendedor ofrece una solución única que proporcione confianza cero. Además, no sería conveniente utilizar una solución de un único proveedor para lograr la confianza cero, con el consiguiente riesgo de dependencia. Este aspecto conduce a la interoperabilidad dentro de los componentes no solo en el momento de la compra, sino también con el paso del tiempo.

El espectro de componentes dentro de la empresa en general es muy amplio, y muchos productos se centran en un único campo dentro de la confianza cero y dependen de otros productos para proporcionar datos o algún servicio a otro componente (por ejemplo, la integración de la MFA para el acceso a los recursos). Para lograr esta integración, los vendedores recurren con mucha frecuencia a las API propietarias proporcionadas por empresas asociadas, en lugar de API estandarizadas e independientes de un vendedor. El problema de este enfoque es que estas API son propietarias y están controladas por un único proveedor. El proveedor que las controla puede cambiar el comportamiento de la API, y los integradores de soluciones tecnológicas se ven obligados a actualizar sus productos en respuesta. Esto requiere una estrecha colaboración entre comunidades de vendedores para garantizar la notificación temprana de las modificaciones en las API, que pueden afectar a la compatibilidad entre productos. Por otro lado, se añade una carga adicional a vendedores y consumidores: los vendedores tienen que gastar recursos para cambiar sus productos, y los consumidores tienen que aplicar actualizaciones a múltiples productos cuando un vendedor hace un cambio en su API propietaria. Además, los vendedores tienen que implantar y mantener envoltorios (*wrappers*) para cada componente asociado, a fin de permitir la máxima compatibilidad e interoperabilidad. Por ejemplo, muchos vendedores de productos de MFA están obligados a crear un envoltorio diferente para cada proveedor de nube o sistema de gestión de identidades para que pueda utilizarse en diferentes tipos de combinaciones de clientes.

Por parte del cliente, esto genera problemas adicionales a la hora de desarrollar requisitos para la compra de productos. No existen normas en las que los compradores puedan basarse para identificar la compatibilidad entre productos. Por lo tanto, es muy difícil crear una hoja de ruta plurianual para pasar a la ZTA puesto que es imposible identificar un conjunto mínimo de requisitos de compatibilidad para los componentes.

B.3.2 Nuevas normas para hacer frente a la dependencia excesiva de las API propietarias

Como no existe una única solución para desarrollar una ZTA, tampoco existe un único conjunto de herramientas o servicios para una empresa de confianza cero. Por tanto, es imposible disponer de un protocolo o marco único que permita a una empresa pasar a una ZTA. En la actualidad, existe una gran variedad de modelos y soluciones que tratan de convertirse en la autoridad líder de la ZTA.

Esto indica que existe la oportunidad de desarrollar un conjunto de protocolos o marcos abiertos y estandarizados que ayuden a las organizaciones a migrar a una ZTA. Algunas SDO, como el Grupo de Trabajo de Ingeniería de Internet (IETF, por su nombre en inglés Internet Engineering Task Force) han establecido protocolos que pueden ser útiles en el intercambio de información sobre amenazas (denominado XMPP-Grid [1]). La Cloud Security Alliance (CSA) ha elaborado un marco para el Perímetro Definido por Software (SDP) [2] que también podría ser útil en ZTA. Los esfuerzos deben dirigirse hacia el análisis del estado actual de los marcos relacionados con la ZTA o los protocolos necesarios para una ZTA útil y hacia la identificación de los lugares donde se necesita trabajar para producir o mejorar estas especificaciones.

B.4 Brechas en el conocimiento de la ZTA y futuras áreas de investigación

Las lagunas enumeradas aquí no impiden que una organización adopte una ZTA para su empresa. Se trata de áreas grises en el conocimiento sobre entornos operativos de la ZTA, y la mayoría surgen de la falta de tiempo y experiencia con despliegues maduros de confianza cero. Éstas constituyen áreas de trabajo futuro para los investigadores.

B.4.1 Respuesta de los atacantes a la ZTA

Una ZTA correctamente implementada en una empresa mejorará la postura de ciberseguridad de la empresa con respecto a la seguridad tradicional basada en el perímetro de la red. Los principios de la ZTA tienen como objetivo reducir la exposición de los recursos a los atacantes y minimizar o prevenir el movimiento lateral dentro de una empresa en caso de que un activo *host* se vea comprometido.

Sin embargo, los atacantes decididos no se quedarán sin actuar, sino que cambiarán de comportamiento ante la ZTA. La cuestión pendiente es cómo cambiarán los ataques. Una posibilidad es que los ataques dirigidos al robo de credenciales se amplíen a la MFA (por ejemplo, *phishing*, ingeniería social). Otra posibilidad es que en una empresa híbrida basada en ZTA/perímetro, los atacantes se centren en los procesos empresariales a los que no se hayan aplicado los principios de ZTA (es decir, que sigan la seguridad tradicional basada en el perímetro de la red), en un intento de hacerse un lugar en el proceso de ZTA.

A medida que la ZTA se desarrolla, se realizan más despliegues y se adquiere experiencia, la eficacia de la ZTA se hace evidente a la hora de reducir la superficie de ataque de los recursos. También habrá que desarrollar la métrica del éxito de la ZTA frente a estrategias de ciberseguridad más antiguas.

B.4.2 Experiencia del usuario en un entorno ZTA

No se ha realizado un examen riguroso de cómo actúan los usuarios finales en una empresa que utiliza una ZTA. Esto se debe principalmente a la falta de grandes casos de uso de ZTA disponibles para el análisis. Sin embargo, se han realizado estudios sobre cómo reaccionan los usuarios ante la MFA y otras operaciones de seguridad que forman parte de una ZTA empresarial. Este trabajo podría constituir la base para predecir la experiencia y el comportamiento del usuario final cuando se utilizan flujos de trabajo de ZTA en una empresa.

Los estudios que pueden predecir cómo afecta la ZTA a la experiencia del usuario final podrían ser los trabajos realizados sobre el uso de la MFA en las empresas y la fatiga relacionada con seguridad. La fatiga de seguridad [3] es el fenómeno en el que los usuarios finales se enfrentan a tantas políticas y retos de seguridad que empieza a afectar negativamente a su productividad. Otros estudios muestran que la MFA puede alterar el comportamiento del usuario, pero el cambio general es mixto [4] [5]. Algunos usuarios aceptan con facilidad la MFA si el proceso se agiliza e incluye dispositivos que están acostumbrados a usar o a tener consigo (por ejemplo, aplicaciones en un teléfono inteligente). Sin embargo, a algunos usuarios les molesta tener que utilizar dispositivos de su propiedad para procesos empresariales o sienten que se les vigila constantemente para detectar posibles infracciones de las políticas de TI.

B.4.3 Resiliencia de la ZTA ante las disrupciones de la empresa y la red

El estudio del ecosistema de proveedores de ZTA puso de manifiesto la amplia gama de infraestructuras que una empresa que implemente una ZTA tendría que considerar. Como ya se ha señalado, en la actualidad no existe un único proveedor de una solución completa de confianza cero. Como resultado, las empresas adquirirán varios servicios y productos diferentes, lo que puede dar lugar a una red de dependencias para los componentes. Si un componente vital se interrumpiera o fuera inaccesible, podría producirse una cascada de fallos que afectarían a uno o varios procesos empresariales.

La mayoría de los productos y servicios encuestados se basan en la presencia en la nube para proporcionar robustez, pero incluso los servicios en la nube pueden volverse inaccesibles debido a un ataque o a un simple error. Cuando esto ocurre, los componentes clave utilizados para tomar decisiones de acceso pueden resultar inaccesibles o perder la capacidad de comunicarse con otros componentes. Por ejemplo, durante un ataque de denegación de servicio distribuido (DDoS), los componentes PE y PA ubicados en una nube podrían ser alcanzables, pero quizás no lo sean todos los PEP ubicados junto a los recursos. Es necesario continuar las investigaciones para descubrir los posibles puntos de estrangulamiento de los modelos de despliegue de ZTA y el impacto en las operaciones de red cuando se pierde o se limita la accesibilidad a un componente de ZTA.

Es probable que los planes de continuidad de operaciones (COOP, por su desarrollo en inglés *continuity of operations plan*) de una empresa deban revisarse al adoptar una ZTA. Una ZTA facilita muchos factores de COOP, ya que los trabajadores remotos pueden tener el mismo acceso a los recursos que tenían en las instalaciones. Sin embargo, políticas como la MFA también pueden tener un impacto negativo si los usuarios no están debidamente formados o

carecen de experiencia. Además, durante una emergencia, podrían olvidar o no tener acceso a los *tokens* y dispositivos de la empresa, lo que afectaría a la velocidad y eficacia de los procesos empresariales.

B.5 Referencias

[1] Cam-Winget N. (ed.), Appala S., Pope S., Saint-Andre P. (2019). Using Extensible Messaging and Presence Protocol (XMPP) for Security Information Exchange. (Internet Engineering Task Force (IETF)), IETF Solicitud de observacioines (*Request for Comments* RFC) 8600. https://doi.org/10.17487/RFC8600

[2] Software Defined Perimeter Working Group «SDP Specification 1.0». (2014). Cloud Security Alliance.

[3] Stanton B., Theofanos M. F., Spickard Prettyman S., Furman S. (2016). Security Fatigue. *IT Professional* 18(5): 26-32. https://doi.org/10.1109/MITP.2016.84

[4] Strouble D., Shechtman G. M., Alsop A. S. (2009). Productivity and Usability Effects of Using a Two-Factor Security System. *SAIS 2009 Proceedings* (AIS, Charleston, SC), p. 37. Disponible en http://aisel.aisnet.org/sais2009/37

[5] Weidman J., Grossklags J. (2017). I Like It but I Hate It: Employee Perceptions Towards an Institutional Transition to BYOD Second-Factor Authentication. *Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC 2017)* (ACM, Orlando, FL), pp. 212-224. https://doi.org/10.1145/3134600.3134629