TLP:CLEAR

Modelo de madurez de confianza cero

Abril de 2023

Versión 2.0

Agencia de Ciberseguridad y Seguridad de Infraestructura (Cybersecurity and Infrastructure Security Agency)
División de Ciberseguridad (Cybersecurity Division)

Historial de revisiones

El número de versión se actualizará a medida que se modifique el documento. Este documento se actualizará según sea necesario para reflejar las prácticas y tecnologías de seguridad modernas. La Tabla 1 presenta el historial de revisiones del documento.

Tabla 1: Historial de revisiones

Versión	Fecha	Descripción de la revisión	Secciones o páginas afectadas
1.0	Agosto de 2021	Publicación inicial	Todo
2.0	Marzo de 2022	Respuesta a los comentarios de la petición de comentarios (RFC, por sus siglas en inglés)	Todo

Modelo de madurez de confianza cero

Índice

Lista de figuras

Lista de tablas

1. Introducción

La Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA, por sus siglas en inglés) lidera el esfuerzo nacional para comprender, administrar y reducir el riesgo de ciberseguridad, incluso apoyando a las agencias del Poder Ejecutivo Civil Federal en la evolución y puesta en funcionamiento de programas y capacidades de ciberseguridad. El Modelo de madurez de confianza cero (ZTMM, por sus siglas en inglés) de la CISA brinda un enfoque para lograr esfuerzos continuos de modernización relacionados con la confianza cero dentro de un entorno y un panorama tecnológico que evolucionan rápidamente. Este ZTMM es uno de los muchos caminos que una organización puede tomar para diseñar e implementar su plan de transición a arquitecturas de confianza cero de acuerdo con el párrafo (3)(b)(ii) de la Orden Ejecutiva (EO, por sus siglas en inglés) 14028 "Mejora de la ciberseguridad de la nación",[1] que requiere que las agencias desarrollen un plan para implementar una arquitectura de confianza cero (ZTA, por sus siglas en inglés). Si bien el ZTMM está diseñado específicamente para las agencias federales según lo exige la EO 14028, todas las organizaciones deben revisar los enfoques descritos en este documento y considerar su adopción.

2. Entorno actual

Los incidentes cibernéticos recientes[2, 3] han puesto de relieve los amplios desafíos que supone garantizar una ciberseguridad efectiva en todo el Gobierno federal, como ocurre con muchas grandes empresas, y demuestran que los enfoques de "normalidad" ya no son suficientes para defender a la nación de las amenazas cibernéticas. Al liderar el esfuerzo nacional para comprender, administrar y reducir los riesgos cibernéticos, la CISA debe enfrentar nuevos desafíos para proteger el Poder Ejecutivo Civil Federal utilizando un enfoque claro, viable y basado en los riesgos. Una defensa cibernética adecuada contra las amenazas emergentes requiere una mayor velocidad y agilidad para superar a los adversarios aumentando sustancialmente los costos para los agentes de amenazas y mejorando la durabilidad y la resiliencia para recuperar rápidamente la capacidad operativa total.

La misión de ciberseguridad de la CISA es defender y asegurar el ciberespacio liderando los esfuerzos nacionales para impulsar y permitir una defensa cibernética nacional efectiva, mejorar la resiliencia de las funciones fundamentales nacionales y promover un ecosistema tecnológico sólido. La CISA desempeña una función fundamental en el mantenimiento de la conciencia situacional cibernética en todas las agencias del Poder Ejecutivo Civil Federal (FCEB, por sus siglas en inglés); el aseguramiento del dominio .gov; y la asistencia a las agencias civiles federales, los propietarios y operadores de infraestructura fundamental, así como a los socios de la industria, para administrar los incidentes cibernéticos importantes. Si bien la CISA mantiene capacidades para defenderse de las amenazas cibernéticas conocidas o sospechadas y mitigarlas, un panorama de amenazas en evolución y la adopción de tecnologías nuevas y emergentes plantean desafíos.

La EO 14028 marcó un compromiso renovado con la modernización de la ciberseguridad federal y la priorización de esta. Entre otros mandatos políticos, la EO 14028 adoptó la confianza cero como el modelo de seguridad deseado para el Gobierno federal y solicitó a las agencias del FCEB desarrollar planes para implementar la ZTA. Un plan típico evaluará el estado actual de ciberseguridad de una agencia y planificará la plena implementación de la ZTA. Como agencia líder en la ciberseguridad federal y la reducción de riesgos, el ZTMM de la CISA ayuda a las agencias en el desarrollo de sus estrategias de confianza cero y en la evolución continua de sus planes de implementación, y presenta formas en las que diversos servicios de la CISA pueden apoyar las soluciones de confianza cero en todas las agencias.

---

[1] Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 17, 2021). https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf.

[2] DHS CISA. *Emergency Directive 21-01- Mitigate SolarWinds Orion Code Compromise*. https://www.cisa.gov/emergency-directive-21-01.

[3] DHS CISA. *Emergency Directive 21-02 - Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*. https://www.cisa.gov/emergency-directive-21-02.

El memorando M-22-09 de la Oficina de Administración y Presupuesto (OMB, por sus siglas en inglés), "Llevar al Gobierno de EE. UU. hacia los principios de ciberseguridad de confianza cero",[4] detalló medidas específicas para que adopten las agencias federales en alineación con los pilares descritos en el ZTMM. Este memorando establece una estrategia federal de ZTA, que requiere que las agencias cumplan con los objetivos de ciberseguridad antes del final del año fiscal (FY, por sus siglas en inglés) 2024 para reforzar la defensa del FCEB. La CISA revisó el ZTMM a fin de alinearlo aún más con la dirección del M-22-09 para las agencias. Las agencias del FCEB deben revisar este memorando en paralelo con el desarrollo y la implementación de sus estrategias de confianza cero.

3. ¿Qué es la confianza cero?

La Publicación especial (SP, por sus siglas en inglés) 800-207 del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) proporciona la siguiente definición operativa de "confianza cero" y "ZTA":

> **La confianza cero** proporciona una colección de conceptos e ideas diseñados para minimizar la incertidumbre a la hora de aplicar decisiones de acceso precisas, que cuenta con los mínimos privilegios por solicitud en los servicios y sistemas de información ante una red vista como puesta en riesgo.
> **La ZTA** es un plan de ciberseguridad empresarial que utiliza conceptos de confianza cero y abarca las relaciones de componentes, la planificación del flujo de trabajo y las políticas de acceso.
> Por lo tanto, una empresa de confianza cero es la infraestructura de red (física y virtual) y las políticas operativas que existen para una empresa como producto de un plan de ZTA.[5]

La SP 800-207 enfatiza que el objetivo de la confianza cero (ZT, por sus siglas en inglés) es "evitar el acceso no autorizado a los datos y servicios, además de hacer que la aplicación del control de acceso sea lo más detallada posible". De manera similar, el Comité Asesor de Telecomunicaciones de Seguridad Nacional (NSTAC, por sus siglas en inglés) describe a la confianza cero como una "estrategia de ciberseguridad basada en la idea de que no se debe confiar implícitamente en ningún usuario o activo. Supone que ya se ha producido o se producirá una vulneración y, por lo tanto, no se le debe conceder a un usuario acceso a información confidencial mediante una única verificación realizada en el perímetro de la empresa. En cambio, cada usuario, dispositivo, aplicación y transacción se debe verificar continuamente".[6] La confianza cero presenta un cambio de un modelo centrado en la ubicación a un enfoque centrado en la identidad, el contexto y los datos con controles de seguridad detallados entre usuarios, sistemas, aplicaciones, datos y activos que cambian con el tiempo; por estas razones, adoptar una ZTA no es un esfuerzo trivial. Este cambio proporciona la visibilidad necesaria para apoyar el desarrollo, la implementación, la aplicación y la evolución de las políticas de seguridad. Fundamentalmente, la confianza cero puede requerir un cambio en la filosofía y cultura de ciberseguridad de una organización.

[4] OMB Memo M-22-09. *Moving the U.S. Government Towards Zero Trust Cybersecurity Principles*. January 26, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[5] NIST SP 800-207: Zero Trust Architecture. 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

[6] The President's National Security Telecommunications Advisory Committee. Report to the President on Zero Trust and Identity Management. February 2022. https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management.pdf.

El camino hacia la confianza cero es un proceso incremental que puede tardar años en implementarse.

Inicialmente, la implementación de las capacidades y los servicios requeridos a menudo generará costos adicionales; sin embargo, a largo plazo, la confianza cero permitirá una asignación más prudente de las inversiones en seguridad hacia los datos y servicios más fundamentales, en lugar de inversiones en seguridad "iguales" en toda la empresa.

4. Desafíos en la adopción de la confianza cero

El Gobierno federal, como ocurre con la mayoría de las grandes empresas, enfrenta varios desafíos al implementar la ZTA. Los sistemas heredados suelen basarse en una "confianza implícita", en la que el acceso y la autorización rara vez se evalúan en función de atributos fijos; esto entra en conflicto con el principio básico de la evaluación adaptativa de la confianza dentro de una ZTA. Las infraestructuras existentes basadas en la confianza implícita requerirán inversiones para cambiar los sistemas y alinearlos mejor con los principios de confianza cero. Además, a medida que el panorama tecnológico continúa evolucionando, son primordiales las nuevas soluciones y las conversaciones continuas sobre cómo lograr mejor los objetivos de confianza cero.

La adopción de la confianza cero requiere el compromiso y la cooperación de los altos directivos, el personal informático (IT, por sus siglas en inglés), los propietarios de datos y sistemas, y los usuarios de todo el Gobierno federal para lograr de manera efectiva los objetivos de diseño y mejorar la postura de ciberseguridad. La modernización de la ciberseguridad del Gobierno federal requerirá que las agencias hagan la transición de servicios y personal informáticos restringidos y aislados a componentes coordinados y colaborativos de una estrategia de confianza cero, con la aceptación de toda la agencia para una arquitectura común y políticas de gobernanza. Esto incluye los planes actuales y futuros para adoptar tecnologías de la nube.[7]

Las agencias federales están iniciando su proceso de confianza cero desde diferentes puntos de partida. Algunas agencias pueden estar más avanzadas o mejor posicionadas que otras para lograr estos avances; sin embargo, independientemente del punto de partida, la adopción exitosa de la confianza cero puede producir numerosos beneficios, como productividad mejorada, experiencias mejoradas del usuario final, costos informáticos reducidos, acceso flexible y seguridad reforzada.

5. Modelo de madurez de confianza cero

El ZTMM representa una gradiente de implementación a través de cinco pilares distintos, en los que, con el tiempo, se pueden realizar avances menores hacia la optimización. Los pilares, representados en la Figura 1, incluyen **Identidad**, **Dispositivos**, **Redes**, **Aplicaciones y cargas de trabajo**, y **Datos**. Cada pilar incluye detalles generales sobre las siguientes capacidades interdisciplinarias: *Visibilidad y análisis*, *Automatización y organización*, y *Gobernanza*.

[7] Las agencias deben revisar la Arquitectura de referencia técnica de seguridad en la nube, elaborada en conjunto por la CISA, el Servicio Digital de Estados Unidos (United States Digital Service) y el Programa Federal de Administración de Riesgos y Autorizaciones (FedRAMP, por sus siglas en inglés), a fin de obtener orientación adicional sobre los enfoques recomendados para la migración a la nube y la protección de datos. Arquitectura de referencia técnica de seguridad en la nube v.2 (cisa.gov).

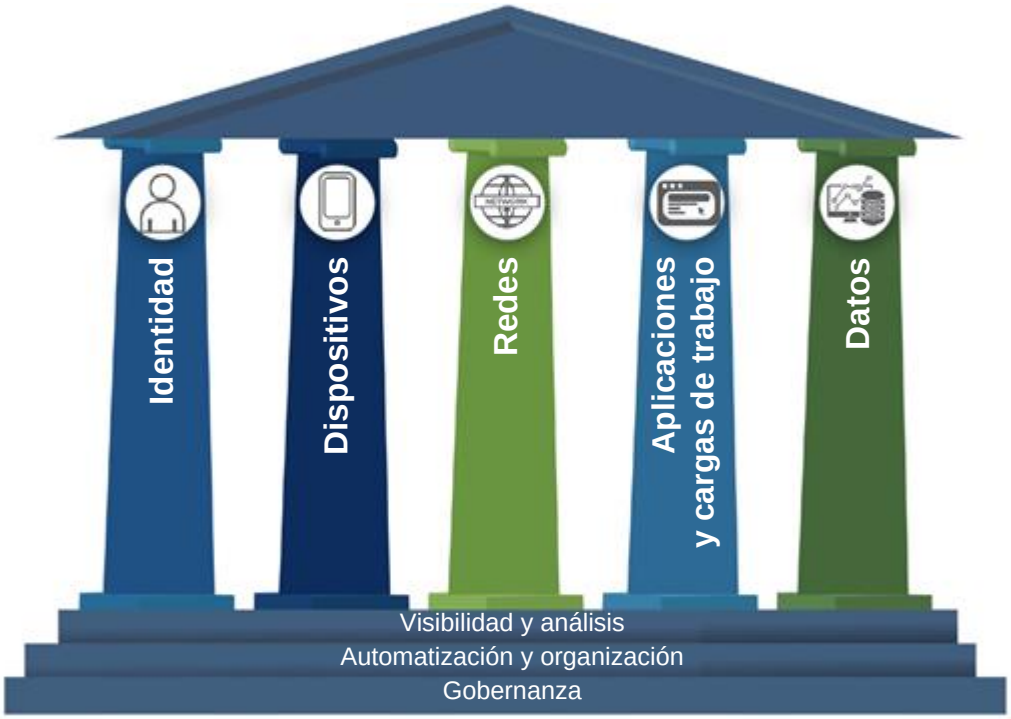

Figura 1: Pilares del Modelo de madurez de confianza cero[8]

El ZTMM de la CISA es uno de los muchos caminos para apoyar la transición hacia la confianza cero.

Varias publicaciones de la ZTA conformaron el desarrollo de este modelo de madurez (consulte la Sección 6 para obtener detalles adicionales). Este modelo refleja los siete principios de confianza cero, tal como se describe en NIST SP 800-207:

1. Todas las fuentes de datos y los servicios informáticos se consideran recursos.
2. Todas las comunicaciones están protegidas, independientemente de la ubicación de la red.
3. El acceso a recursos empresariales individuales se otorga por sesión.
4. El acceso a los recursos se determina con una política dinámica.
5. La empresa supervisa y mide la integridad y la postura de seguridad de todos los activos propios y asociados.
6. Toda la autenticación y autorización de recursos es dinámica, y se aplica estrictamente antes de permitir el acceso.
7. La empresa recopila tanta información como sea posible sobre el estado actual de los activos, la infraestructura de red y las comunicaciones, y la utiliza para mejorar su postura de seguridad.

A medida que las agencias hacen la transición hacia implementaciones óptimas de confianza cero, las soluciones asociadas dependen cada vez más de procesos y sistemas automatizados que se integran de manera más completa entre los pilares y que aplican las decisiones políticas de forma más dinámica. Cada pilar puede avanzar a su propio ritmo y puede progresar de forma más rápida que otros hasta que se requiera coordinación entre pilares. Sin embargo, esta coordinación solo se puede lograr con capacidades y dependencias compatibles

[8] Esta ilustración se inspiró en la Figura 1 del Consejo Estadounidense de Tecnología (ACT, por sus siglas en inglés) y el Consejo Asesor de la Industria (IAC, por sus siglas en inglés), “Tendencias actuales de ciberseguridad de confianza cero” (2019). https://www.actiac.org/system/files/ACTIAC%20Zero%20Trust%20Project%20Report%2004182019.pdf.

entre sí y con el entorno de toda la empresa. Esto permite y define una evolución gradual hacia la confianza cero, distribuyendo los costos a lo largo del tiempo en lugar de hacerlo completamente por adelantado.

En alineación con los pasos del NIST para la transición a la confianza cero, las agencias deben evaluar sus sistemas, sus recursos, su infraestructura, su personal y sus procesos empresariales actuales antes de invertir en capacidades de confianza cero (incluidos los pilares y las funciones que se describen en este modelo).[9] Esta evaluación puede ayudar a las agencias a identificar las capacidades existentes para apoyar una mayor madurez de confianza cero, así como las deficiencias para priorizarlas. Las agencias también pueden planificar oportunidades para coordinar capacidades entre los pilares a fin de permitir controles de acceso detallados y con privilegios mínimos, y mitigar riesgos adicionales. [10]

Las tres etapas del proceso de madurez de confianza cero (ZTM, por sus siglas en inglés) que avanzan desde el punto de partida Tradicional hasta Inicial, Avanzado y Óptimo facilitarán la implementación federal de la ZTA. Cada etapa posterior requiere *mayores* niveles de protección, detalle y complejidad para su adopción.

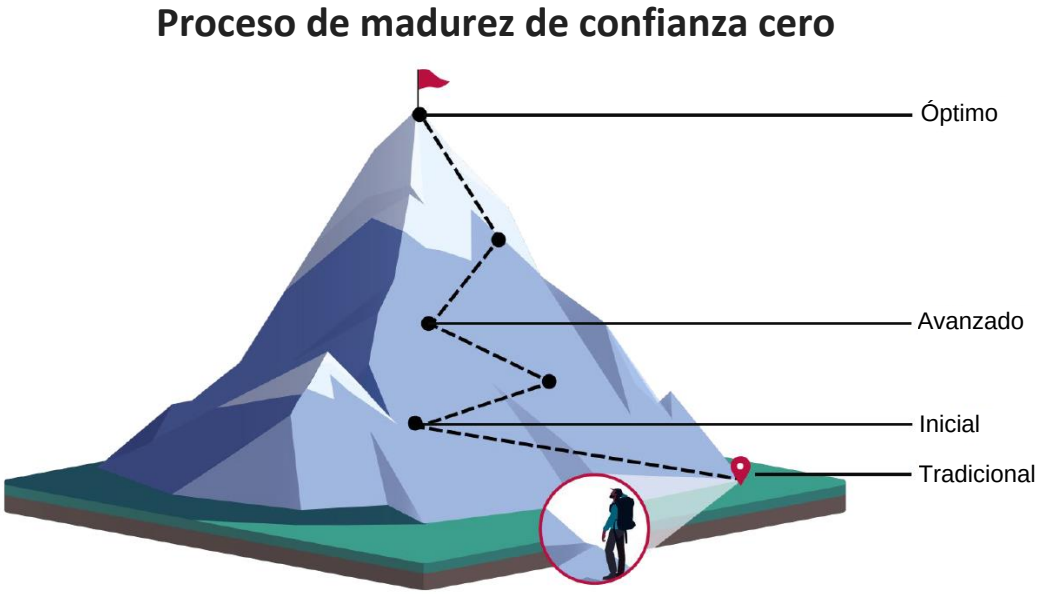

Figura 2: Proceso de madurez de confianza cero

Como se observa en la Figura 2, las agencias deben esperar que los niveles requeridos de esfuerzo y los beneficios obtenidos aumenten de forma significativa a medida que la madurez de confianza cero avanza entre los pilares y dentro de estos. A medida que las agencias trazan su proceso de ZTA, deben explorar oportunidades para promover la madurez de los pilares a fin de alinearse con las necesidades específicas de la misión y apoyar un mayor crecimiento en otros pilares. La Figura 3 destaca la evolución prevista de las agencias con el tiempo desde una empresa tradicional hasta un estado futuro que presenta actualizaciones más dinámicas, procesos automatizados, capacidades integradas y otras características de las etapas de Óptimo (como se describe en el modelo de madurez). Estas etapas son dinámicas y crecen de forma exponencial; el progreso planificado de una etapa de madurez a otra puede cambiar en su alcance e impacto con el tiempo.

[9] NIST White Paper. Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators. https://csrc.nist.gov/publications/detail/white-paper/2022/05/06/planning-for-a-zero-trust-architecture/final.

[10] Consulte la sección AC-6 en NIST SP 800-53, revisión 5. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

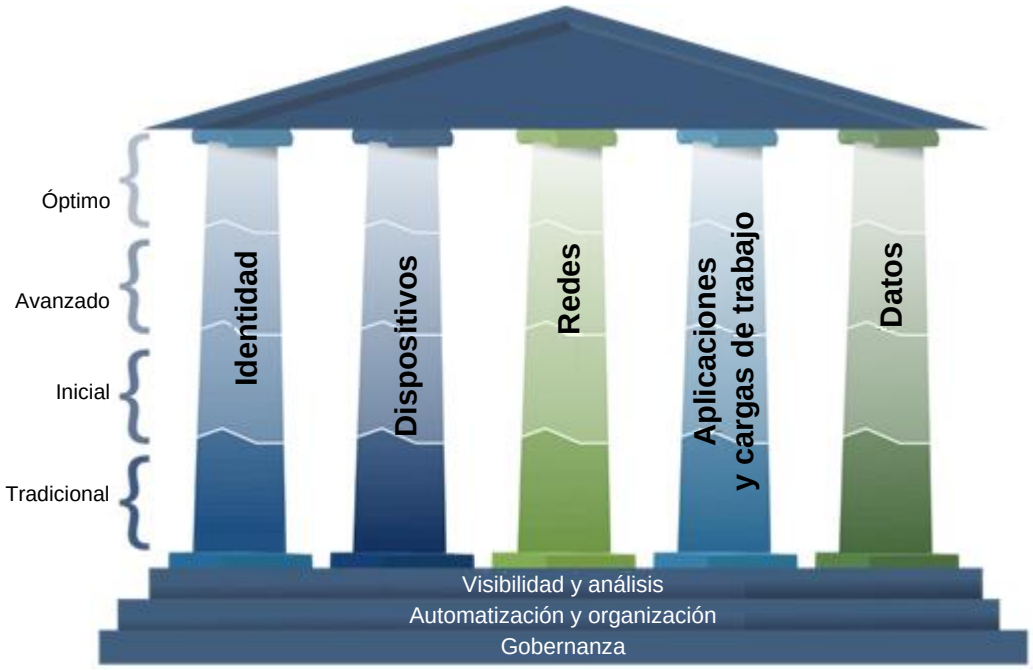

Figura 3: Evolución de la madurez de confianza cero

Las agencias deben utilizar los siguientes criterios rectores de cada etapa para identificar la madurez de cada pilar tecnológico de confianza cero y proporcionar coherencia en todo el modelo de madurez:

- **Tradicional**: ciclos de vida configurados manualmente (p. ej., desde el establecimiento hasta el desmantelamiento) y asignaciones de atributos (seguridad y registro); políticas y soluciones de seguridad estáticas que abordan un pilar a la vez con dependencias discretas de sistemas externos; privilegio mínimo establecido solo en el aprovisionamiento; pilares aislados de aplicación de políticas; implementación manual de respuestas y mitigación; y relación limitada de dependencias, registros y telemetría.
- **Inicial**: inicio de la automatización de asignación de atributos y configuración de ciclos de vida, decisiones y aplicación de políticas, así como soluciones iniciales entre pilares con integración de sistemas externos; algunos cambios de respuesta al privilegio mínimo después del aprovisionamiento; y visibilidad agregada para los sistemas internos.
- **Avanzado**: cuando corresponda, controles automatizados para el ciclo de vida y la asignación de configuraciones y políticas con coordinación entre pilares; visibilidad centralizada y control de identidades; aplicación de políticas integrada en todos los pilares; respuesta a las medidas de mitigación predefinidas; cambios al privilegio mínimo en función de las evaluaciones de riesgo y postura; y generación de conciencia en toda la empresa (incluidos los recursos alojados externamente).
- **Óptimo**: ciclos de vida totalmente automatizados y oportunos, y asignaciones de atributos a activos y recursos que se autoevalúan con políticas dinámicas basadas en desencadenadores automatizados/observados; acceso dinámico de privilegio mínimo (suficiente y dentro de los umbrales) para los activos y sus respectivas dependencias en toda la empresa; interoperabilidad entre pilares con supervisión continua; y visibilidad centralizada con una conciencia situacional integral.

La Figura 4 brinda una descripción general de alto nivel del ZTMM e incluye los aspectos clave de las funciones específicas de cada pilar y en cada etapa de madurez.

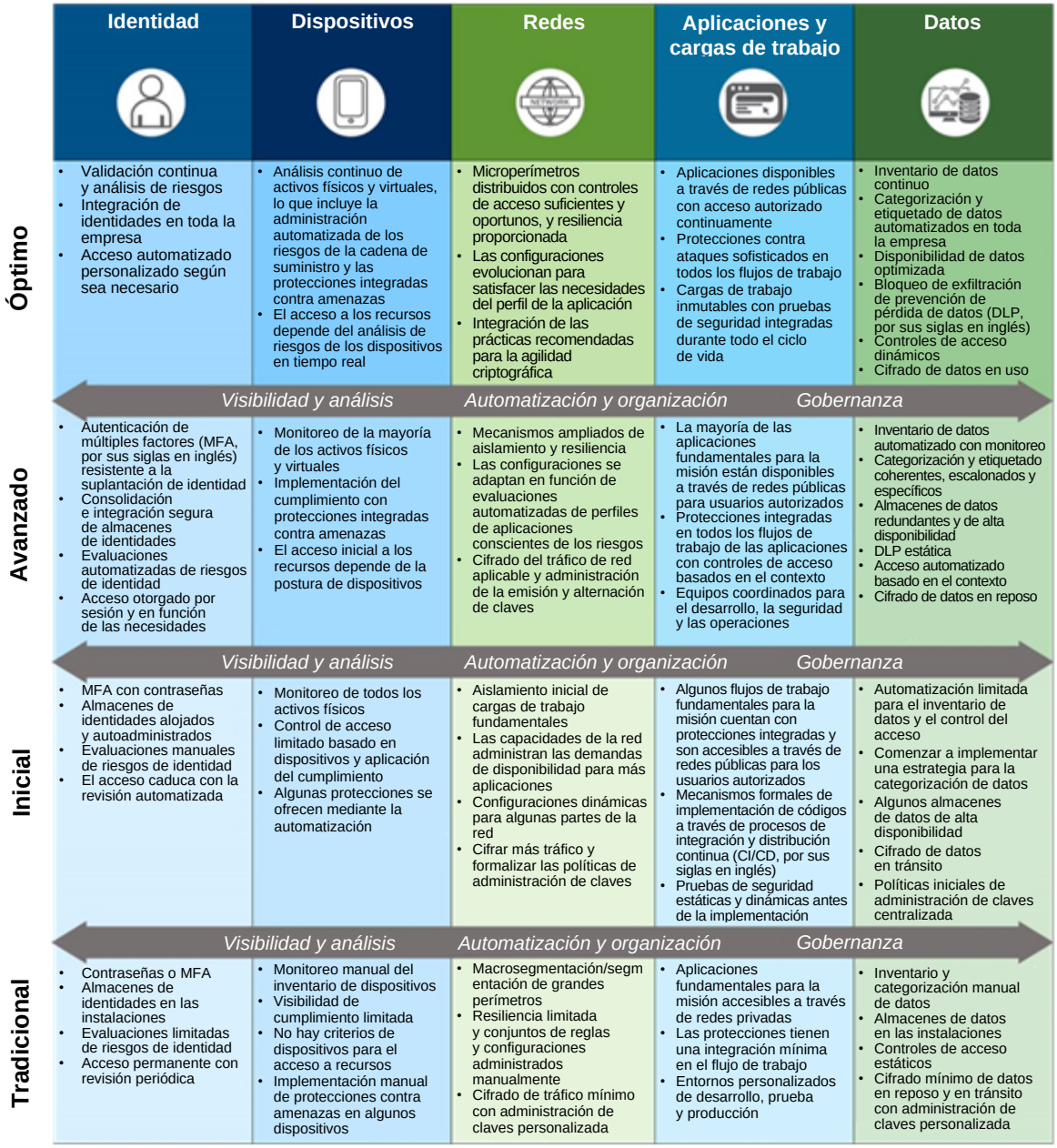

Figura 4: Descripción general de alto nivel del modelo de madurez de confianza cero

Estas etapas de madurez y los detalles asociados con cada pilar permiten a las agencias evaluar, planificar y mantener las inversiones necesarias para avanzar hacia una ZTA. Las subsecciones 0-5.5 brindan información de alto nivel para apoyar a las agencias en la transición hacia la confianza cero en los cinco pilares diferentes: **Identidad**, **Dispositivos**, **Redes**, **Aplicaciones y cargas de trabajo**, y **Datos**. Cada pilar también incluye detalles generales sobre las capacidades *Visibilidad y análisis*, *Automatización y organización*, y *Gobernanza* para apoyar la integración con ese pilar y en todo el modelo.

Estas tres capacidades interdisciplinarias destacan actividades para apoyar la interoperabilidad de funciones entre pilares según las siguientes descripciones:

- **Visibilidad y análisis:** La visibilidad se refiere a los artefactos observables que se generan por las características y los eventos de los entornos de toda la empresa.[11] Centrarse en el análisis de datos relacionados con la cibernética puede ayudar a conformar las decisiones políticas, facilitar las actividades de respuesta y crear un perfil de riesgo para desarrollar medidas de seguridad proactivas antes de que ocurra un incidente.[12]
- **Automatización y organización:** La confianza cero hace pleno uso de las herramientas y los flujos de trabajo automatizados que apoyan las funciones de respuesta de seguridad en todos los productos y servicios, al mismo tiempo que mantiene la supervisión, la seguridad y la interacción del proceso de desarrollo de tales funciones, productos y servicios.
- **Gobernanza:** La gobernanza hace referencia a la definición y a la aplicación asociada de las políticas, los procedimientos y los procesos de ciberseguridad de las agencias, en los pilares y entre estos, para administrar la empresa de una agencia y mitigar los riesgos de seguridad en apoyo de los principios de confianza cero y el cumplimiento de los requisitos federales.[13]

Si bien el ZTMM cubre muchos aspectos de la ciberseguridad fundamentales para las empresas federales, no aborda otros aspectos de la ciberseguridad, como las actividades relacionadas con la respuesta a incidentes o los detalles de los registros, la supervisión, la emisión de alertas, el análisis forense, la aceptación de riesgos y la recuperación.[14] Otros aspectos y las prácticas recomendadas de la administración de la postura de ciberseguridad empresarial no se incluyen de forma explícita dentro de las funciones del modelo de madurez. Aunque el modelo de madurez no pretende ser excluyente, no aborda los desafíos específicos de las tecnologías operativas,[15] ciertas clases de dispositivos de Internet de las cosas (IoT, por sus siglas en inglés)[16] o la incorporación generalizada de tecnologías emergentes, como plataformas de engaño, cortafuegos autenticados de aplicaciones web, análisis del comportamiento, etc. En este modelo, no se incluyen metodologías, como recomendaciones para incorporar mejor las capacidades de aprendizaje automático e inteligencia artificial dentro de las soluciones de confianza cero. Las agencias maduras deben tomar medidas para supervisar y evaluar el desempeño y la integridad de sus capacidades de seguridad, la infraestructura subyacente y las políticas para detectar el acceso no autorizado y los cambios a medida que desarrollan cada pilar. Las agencias deben tener cuidado de no crear nuevas oportunidades de explotación o debilitar los protocolos de seguridad. Se requiere investigación y desarrollo para garantizar efectivamente la integridad de

[11] Consulte la guía del Marco extensible de referencia de la visibilidad (eVRF, por sus siglas en inglés) de la CISA: https://www.cisa.gov/blog/2022/04/19/scuba-it-means-better-visibility-standards-and-security-practices-government-cloud.

[12] Las agencias deben revisar el memorando M-21-31 de la OMB, *Mejora de las capacidades de investigación y corrección del Gobierno federal en relación con los incidentes de ciberseguridad* (27 de agosto de 2021), para obtener más orientación sobre los requisitos de registro a medida que toman decisiones y realizan inversiones para satisfacer las necesidades de visibilidad. https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf.

[13] Con base en la función Gobernanza de la categoría Identificar del Marco de ciberseguridad del NIST, versión 1.1: https://www.nist.gov/cyberframework/framework.

[14] Las copias de seguridad se incluyen en el pilar Datos; sin embargo, para obtener orientación detallada sobre la integridad y la recuperación de los datos, las agencias deben consultar NIST SP 1800-11: https://csrc.nist.gov/News/2020/sp-1800-11-data-integrity-ransomware-recovery.

[15] NIST. Guide to Operational Technology Security: NIST Requests Comments on Draft SP 800-82r3. April 2022. https://csrc.nist.gov/News/2022/guide-to-operational-technology-ot-security.

[16] NIST. Cybersecurity for IoT Program. https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program.

los sistemas de software y hardware a escala en todas las empresas federales.[17,18, 19]
Al planificar la implementación de la ZTA, las agencias deben tomar decisiones basadas en factores que incluyen el riesgo, la misión, los requisitos federales y las limitaciones operativas. Si bien este modelo generalmente está alineado con el dominio administrativo único o el límite de acreditación de una empresa federal, las agencias también deben evaluar de qué manera sus interacciones con los socios externos, las partes interesadas y los proveedores de servicios, así como su dependencia de estos, influyen en su ZTA.[20] Este modelo de madurez no debe verse como un conjunto estricto de requisitos, sino como una guía general para ayudar a que las agencias implementen con éxito su ZTA y adopten una postura general mejorada en materia de ciberseguridad.

[17] NIST NCCOE: Supply Chain Assurance. https://www.nccoe.nist.gov/supply-chain-assurance.

[18] NIST NCCOE: Software Supply Chain and DevOps Security Practices. https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices.

[19] Las agencias deben revisar la información y los recursos disponibles para la lista de materiales de software (SBOM, por sus siglas en inglés) y el intercambio de explotabilidad de vulnerabilidades (VEX, por sus siglas en inglés) a medida que continúan los avances de la comunidad en https://www.cisa.gov/sbom.

[20] Estas consideraciones abarcan ciertos pilares y funciones, como la confianza en las credenciales, la evaluación de las cadenas de suministro, las diferencias en la categorización de datos, las excepciones de políticas, las variaciones en los umbrales de riesgo y más.

5.1 Identidad

Una identidad se refiere a un atributo o a un conjunto de atributos que describe de forma única a un usuario o una entidad de la agencia, lo que incluye las entidades no personales.

Las agencias deben garantizar y aplicar el acceso de los usuarios y las entidades a los recursos correctos en el momento adecuado para el propósito indicado sin otorgar un acceso excesivo. Las agencias deben integrar soluciones de administración de identidades, credenciales y acceso en toda su empresa, siempre que sea posible, a fin de aplicar una autenticación sólida, otorgar autorización personalizada basada en el contexto y evaluar el riesgo de identidad para los usuarios y las entidades de la agencia. Las agencias deben integrar sus almacenes de identidades y sistemas de administración, cuando corresponda, para mejorar la conciencia de las identidades empresariales, así como sus responsabilidades y autoridades asociadas.

La Tabla 2 enumera las funciones de identidad relacionadas con la confianza cero y las consideraciones de Visibilidad y análisis, Automatización y organización, y Gobernanza dentro del contexto de la identidad.

Tabla 2: Pilar Identidad

Función	Tradicional	Inicial	Avanzado	Óptimo
Autenticación	La agencia autentica la identidad utilizando contraseñas o la autenticación de múltiples factores[21] (MFA) con acceso estático para la identidad de la entidad.	La agencia autentica la identidad mediante MFA, que puede incluir contraseñas como un factor y requiere la validación de múltiples atributos de la entidad (p. ej., ubicación o actividad).	La agencia comienza a autenticar todas las identidades mediante atributos y MFA resistente a la suplantación de identidad, lo que incluye la implementación inicial de la MFA	La agencia valida continuamente la identidad con MFA resistente a la suplantación de identidad, no solo cuando se concede el acceso inicialmente.

[21] Los recursos de la CISA para la MFA están disponibles en https://www.cisa.gov/mfa.

Función	Tradicional	Inicial	Avanzado	Óptimo
			sin contraseña mediante FIDO2[22] o la verificación de identidad personal (PIV, por sus siglas en inglés)[23].	
Almacenes de identidades	La agencia solo utiliza almacenes de identidades autoadministrados en las instalaciones (p. ej., planificados, implementados y mantenidos por la agencia).	La agencia tiene una combinación de almacenes de identidades autoadministrados y alojados (p. ej., en la nube u otra agencia) con una integración mínima entre los almacenes (p. ej., inicio de sesión único).	La agencia comienza a consolidar e integrar de forma segura algunos almacenes de identidades alojados y autoadministrados.	La agencia integra de forma segura sus almacenes de identidades en todos los socios y entornos, según corresponda.
Evaluaciones de riesgo	La agencia toma determinaciones limitadas sobre el riesgo de identidad (p. ej., la probabilidad de que una identidad esté en riesgo).	La agencia determina el riesgo de identidad a través de métodos manuales y reglas estáticas para apoyar la visibilidad.	La agencia determina el riesgo de identidad con algunos análisis automatizados y reglas dinámicas para conformar las decisiones de acceso y las actividades de respuesta.	La agencia determina el riesgo de identidad en tiempo real en función de análisis continuos y reglas dinámicas para brindar protección continua.

[22] FIDO2 es un conjunto de protocolos desarrollados en colaboración por Fast IDentity Online (FIDO) Alliance y World Wide Web Consortium (W3C). FIDO2 está diseñado para permitir una autenticación fácil, segura y sin contraseña. Este enfoque aprovecha el protocolo WebAuthn de W3C y el Protocolo de cliente a autenticador (CTAP, por sus siglas en inglés) de FIDO Alliance.

FIDO Alliance. *FIDO Alliance - Open Authentication Standards More Secure than Passwords*. https://fidoalliance.org/.

World Wide Web Consortium. *Web Authentication: An API for accessing Public Key Credentials.* https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.

FIDO Alliance. Client to Authenticator Protocol. Proposed Standard, June 2021. https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-errata-20220621.html.

[23] Verificación de identidad personal. Una credencial PIV es una credencial del Gobierno federal de EE. UU. que se utiliza para acceder a instalaciones y sistemas de información controlados a nivel federal en el nivel de seguridad adecuado. https://playbooks.idmanagement.gov/piv/.

Función	Tradicional	Inicial	Avanzado	Óptimo
Administración de acceso (nueva función)	La agencia autoriza el acceso permanente con revisión periódica tanto para cuentas privilegiadas como no privilegiadas.	La agencia autoriza el acceso, incluso para solicitudes de acceso privilegiado, que caduca con la revisión automatizada.	La agencia autoriza el acceso por sesión y en función de las necesidades, incluso para las solicitudes de acceso privilegiado, que se adapta a las acciones y los recursos.	La agencia utiliza la automatización para autorizar el acceso oportuno y suficiente adaptado a las acciones individuales y las necesidades de recursos individuales.
Capacidad de visibilidad y análisis	La agencia recopila registros de actividad de usuarios y entidades, especialmente para credenciales privilegiadas, y realiza algunos análisis manuales de rutina.	La agencia recopila registros de actividad de usuarios y entidades, y lleva a cabo análisis manuales de rutina y algunos análisis automatizados, con una relación limitada entre los tipos de registros.	La agencia realiza análisis automatizados en algunos tipos de registros de actividad de usuarios y entidades, y aumenta la recopilación para abordar las deficiencias en la visibilidad.	La agencia mantiene una visibilidad integral y una conciencia situacional en toda la empresa a través de la realización de análisis automatizados sobre los tipos de registros de actividades de usuarios, incluidos los análisis basados en el comportamiento.
Capacidad de automatización y organización	La agencia organiza manualmente (incorpora, elimina y deshabilita) identidades autoadministradas (usuarios y entidades), con poca integración, y realiza revisiones periódicas.	La agencia organiza manualmente las identidades privilegiadas y externas, y automatiza la organización de los usuarios no privilegiados y las entidades autoadministradas.	La agencia organiza manualmente las identidades de usuarios privilegiados y automatiza la organización de todas las identidades con integración en todos los entornos.	La agencia automatiza la organización de todas las identidades con una integración total en todos los entornos en función de los comportamientos, las inscripciones y las necesidades de implementación.
Capacidad de gobernanza	La agencia implementa políticas de identidad (autenticación, credenciales, acceso, ciclo de vida, etc.), que se aplican mediante mecanismos técnicos estáticos y revisión manual.	La agencia define y comienza a implementar políticas de identidad para que se apliquen con automatización mínima y actualizaciones manuales en toda la empresa.	La agencia implementa políticas de identidad para que se apliquen con automatización en toda la empresa y actualiza las políticas periódicamente.	La agencia implementa y automatiza completamente las políticas de identidad con aplicación continua y actualizaciones dinámicas en toda la empresa, para todos los usuarios y las entidades, en todos los sistemas.

5.2 Dispositivos

Un dispositivo se refiere a cualquier activo (incluido su hardware, software, firmware, etc.) que pueda conectarse a una red, incluidos servidores, máquinas de escritorio y portátiles, impresoras, teléfonos móviles, dispositivos de IoT, equipos de red y más.

Los dispositivos pueden ser propiedad de la agencia o propiedad personal (traiga su propio dispositivo [BYOD, por sus siglas en inglés]) de los empleados, los socios o los visitantes. Las agencias deben asegurar todos los dispositivos de la agencia, administrar los riesgos de los dispositivos autorizados que no están controlados por la agencia y evitar que los dispositivos no autorizados accedan a los recursos. La administración de dispositivos incluye el mantenimiento de un inventario dinámico de todos los activos, incluido su hardware, software, firmware, etc., junto con sus configuraciones y vulnerabilidades asociadas a medida que se conocen.

Muchos dispositivos presentan desafíos de ZTA específicos y deben evaluarse caso por caso como parte de un proceso basado en riesgos. Por ejemplo, los equipos de red, las impresoras y otros dispositivos pueden ofrecer opciones limitadas de autenticación, visibilidad y seguridad. Las agencias que emplean políticas de BYOD probablemente tendrán menos opciones para mantener la visibilidad y el control de dichos dispositivos. El panorama tecnológico de los dispositivos continúa cambiando y, a medida que las agencias incorporen dispositivos adicionales a sus empresas, deberán seguir administrando los riesgos cambiantes asociados con estos dispositivos.[24] En algunos casos, es posible que las agencias no puedan adoptar las orientaciones para ciertos subconjuntos de sus dispositivos. Las agencias también enfrentarán desafíos para garantizar que los dispositivos confiables y sus servicios no hayan llegado al final de su vida útil y continúen con la cobertura de la asistencia de por vida, ya que los dispositivos heredados suelen tener una mayor cantidad de vulnerabilidades no mitigadas, configuraciones erróneas disponibles y riesgos desconocidos. Sin embargo, a pesar de estos desafíos, las agencias aún deberían poder lograr avances considerables hacia una ZTA.

La administración de activos informáticos en las instalaciones implica documentar y administrar activos físicos (dispositivos). A medida que las agencias se trasladan a entornos en la nube, esto crea nuevas consideraciones y oportunidades para administrar y monitorear los activos virtuales y en la nube de la agencia. Los activos en la nube incluyen recursos informáticos (p. ej., máquinas virtuales, servidores o contenedores), recursos de almacenamiento (p. ej., almacenamiento en bloque o de archivos), activos de plataforma (p. ej., bases de datos, servidores web, colas o buses de mensajes) y recursos de la red (p. ej., redes virtuales, redes privadas virtuales [VPN, por sus siglas en inglés], puertas de enlace, servicios de sistema de nombres de dominio [DNS, por sus siglas en inglés], etc.) y recursos virtuales asociados con otros servicios en la nube administrados (p. ej., modelos de inteligencia artificial).

La Tabla 3 enumera las funciones de dispositivos relacionadas con la confianza cero, así como las consideraciones de *Visibilidad y análisis*, *Automatización y organización*, y *Gobernanza* dentro del contexto de los dispositivos.

[24] Las agencias deben consultar el memorando M-22-01 de la OMB, *Cómo mejorar la detección de vulnerabilidades e incidentes de ciberseguridad en sistemas del Gobierno federal a través de la detección y respuesta de puntos de conexión*. 8 de octubre de 2021. https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf.

Tabla 3: Pilar Dispositivos

Función	Tradicional	Inicial	Avanzado	Óptimo
Aplicación de políticas y supervisión del cumplimiento (nueva función)	La agencia tiene visibilidad limitada, si es que tiene alguna (p. ej., la capacidad para inspeccionar el comportamiento del dispositivo), del cumplimiento del dispositivo con pocos métodos para aplicar políticas o administrar el software, las configuraciones o las vulnerabilidades.	La agencia recibe características del dispositivo autoevaluadas (p. ej., claves, tokens, usuarios, etc., en el dispositivo), pero tiene mecanismos de aplicación limitados. La agencia cuenta con un proceso básico preliminar para aprobar el uso del software e impulsar actualizaciones y cambios de configuración en los dispositivos.	La agencia tiene información verificada (p. ej., un administrador puede inspeccionar y verificar los datos en el dispositivo) sobre el acceso inicial al dispositivo y aplica el cumplimiento para la mayoría de los dispositivos y activos virtuales. La agencia utiliza métodos automatizados para administrar dispositivos y activos virtuales, aprobar software, identificar vulnerabilidades e instalar correcciones.	La agencia verifica continuamente la información y aplica el cumplimiento durante toda la vida útil de los dispositivos y activos virtuales. La agencia integra la administración de los dispositivos, el software, las configuraciones y las vulnerabilidades en todos los entornos de la agencia, incluidos los activos virtuales.
Administración de riesgos de la cadena de suministro y activos (nueva función)	La agencia no monitorea los activos físicos o virtuales en toda la empresa o entre proveedores y administra su propia adquisición de dispositivos y servicios en la cadena de suministro de forma personalizada con una visión limitada de los riesgos empresariales.	La agencia monitorea todos los activos físicos y algunos virtuales, y administra los riesgos de la cadena de suministro a través de políticas y referencias de control de acuerdo con las recomendaciones federales que utilizan un marco sólido (p. ej., Administración de riesgos de la cadena de suministro [SCRM, por sus siglas en inglés] del NIST).[25]	La agencia comienza a desarrollar una visión empresarial integral de los activos físicos y virtuales a través de procesos automatizados que pueden funcionar en múltiples proveedores para verificar adquisiciones, monitorear ciclos de desarrollo y proporcionar evaluaciones de terceros.	La agencia tiene una visión integral, en tiempo real o casi en tiempo real, de todos los activos de los proveedores y proveedores de servicios, automatiza la administración de riesgos de su cadena de suministro según corresponda, desarrolla operaciones que toleran fallas en la cadena de suministro e incorpora prácticas recomendadas.

[25]NIST. NIST Updates Cybersecurity Guidance for Supply Chain Risk Management. May 5, 2022. https://www.nist.gov/news-events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management.

Función	Tradicional	Inicial	Avanzado	Óptimo
Acceso a recursos (anteriormente acceso a datos)	La agencia no requiere visibilidad de los dispositivos o activos virtuales utilizados para acceder a los recursos.	La agencia requiere que algunos dispositivos o activos virtuales informen las características y, luego, se utiliza esta información para aprobar el acceso a los recursos.	El acceso inicial a los recursos de la agencia considera la información verificada de los dispositivos o los activos virtuales.	El acceso a los recursos de la agencia considera análisis de riesgos en tiempo real dentro de dispositivos y activos virtuales.
Protección contra amenazas al dispositivo (nueva función)	La agencia implementa, de forma manual, capacidades de protección contra amenazas en algunos dispositivos.	La agencia tiene algunos procesos automatizados para implementar y actualizar capacidades de protección contra amenazas en dispositivos y activos virtuales con aplicación limitada de políticas e integración de supervisión del cumplimiento.	La agencia comienza a consolidar las capacidades de protección contra amenazas en soluciones centralizadas para dispositivos y activos virtuales, e integra la mayoría de estas capacidades con la aplicación de políticas y la supervisión del cumplimiento.	La agencia tiene soluciones centralizadas de seguridad de protección contra amenazas que se implementaron con capacidades avanzadas para todos los dispositivos y activos virtuales, así como un enfoque unificado para la protección contra amenazas al dispositivo, la aplicación de políticas y la supervisión del cumplimiento.
Capacidad de visibilidad y análisis	La agencia utiliza un inventario etiquetado físicamente y una supervisión de software limitada para revisar los dispositivos de forma periódica con algunos análisis manuales.	La agencia utiliza identificadores digitales (p. ej., direcciones de interfaz, etiquetas digitales) junto con un inventario manual y la supervisión de puntos de conexión de dispositivos cuando están disponibles. Algunos dispositivos y activos virtuales de la agencia se encuentran bajo análisis automatizado (p. ej., análisis basado en software) para detectar anomalías según el riesgo.	La agencia automatiza tanto la recopilación de inventario (incluida la supervisión de puntos de conexión en todos los dispositivos del usuario estándar, como computadoras de escritorio y portátiles, teléfonos móviles, tabletas y sus activos virtuales) como la detección de anomalías para detectar dispositivos no autorizados.	La agencia automatiza la recopilación del estado de todos los dispositivos y activos virtuales conectados a la red mientras se relaciona con identidades, lleva a cabo supervisiones de puntos de conexión y realiza detecciones de anomalías para conformar el acceso a los recursos. La agencia monitorea los patrones de aprovisionamiento o desaprovisionamiento de activos virtuales en busca de anomalías.

Función	Tradicional	Inicial	Avanzado	Óptimo
Capacidad de automatización y organización	La agencia aprovisiona, configura o registra manualmente los dispositivos dentro de la empresa.	La agencia comienza a utilizar herramientas y scripts para automatizar el proceso de aprovisionamiento, configuración, registro o desaprovisionamiento de dispositivos y activos virtuales.	La agencia ha implementado mecanismos de supervisión y aplicación para identificar y desconectar o aislar manualmente dispositivos y activos virtuales que no cumplen con los requisitos (son vulnerables, tienen un certificado no verificado, tienen una dirección mac no registrada).	La agencia cuenta con procesos totalmente automatizados para aprovisionar, registrar, supervisar, aislar, corregir y desaprovisionar dispositivos y activos virtuales.
Capacidad de gobernanza	La agencia establece algunas políticas para el ciclo de vida[26] de sus dispositivos informáticos tradicionales y periféricos, y se basa en procesos manuales para realizar el mantenimiento (p. ej., actualización, corrección, desinfección) de estos dispositivos.	La agencia establece y aplica políticas para la adquisición de nuevos dispositivos, el ciclo de vida de dispositivos informáticos no tradicionales y activos virtuales, y para realizar periódicamente la supervisión y el análisis de dispositivos.	La agencia establece políticas en toda la empresa para el ciclo de vida de los dispositivos y activos virtuales, incluida su enumeración y responsabilidad, con algunos mecanismos de aplicación automatizados.	La agencia automatiza políticas para el ciclo de vida de todos los activos virtuales y dispositivos conectados a la red en toda la empresa.

[26] El ciclo de vida incluye la adquisición, la configuración, el monitoreo, la supervisión, la actualización, el uso, la desinfección, el desaprovisionamiento y la recuperación de dispositivos.

5.3 Redes

Una red se refiere a un medio de comunicación abierto que incluye canales típicos, como redes internas de agencias, redes inalámbricas e Internet, al igual que otros canales potenciales, como canales móviles y de nivel de aplicación utilizados para transportar mensajes.

Las ZTA permiten alejarse de los enfoques tradicionales de seguridad centrados en el perímetro y posibilitan a las agencias administrar los flujos de tráfico internos y externos, aislar hosts, aplicar el cifrado, segmentar la actividad y mejorar la visibilidad de la red en toda la empresa. Las ZTA permiten implementar controles de seguridad más cerca de las aplicaciones, los datos y otros recursos, aumentan las protecciones tradicionales basadas en la red y mejoran la defensa en profundidad. La red puede tratar cada aplicación de forma única según sus demandas de acceso, prioridad, accesibilidad, conexiones a servicios de dependencia y vías de conexión. Estas demandas de aplicaciones de red se pueden reflejar como un perfil de aplicación y, luego, los perfiles repetidos se pueden tratar como una clase de tráfico.

La Tabla 4 enumera las funciones de red relacionadas con la confianza cero y las consideraciones de *Visibilidad y análisis*, *Automatización y organización*, y *Gobernanza* dentro del contexto de las redes.

Tabla 4: Pilar Redes

Función	Tradicional	Inicial	Avanzado	Óptimo
Segmentación de red	La agencia define su arquitectura de red utilizando la macrosegmentación o segmentación de grandes perímetros con restricciones mínimas de accesibilidad dentro de los segmentos de red. La agencia también puede depender de interconexiones de varios servicios (p. ej., túneles de VPN de tráfico masivo).	La agencia comienza a implementar una arquitectura de red con el aislamiento de cargas de trabajo fundamentales, lo que limita la conectividad a los principios de función mínima, así como una transición hacia las interconexiones específicas de servicios.	La agencia amplía la implementación de los mecanismos de aislamiento de perfiles de aplicaciones y puntos de conexión a una mayor parte de su arquitectura de red con microperímetros de ingreso/salida e interconexiones específicas de servicios.	La arquitectura de red de la agencia consiste en microperímetros de ingreso/salida completamente distribuidos y una microsegmentación extensa basada en los perfiles de aplicaciones con conectividad dinámica oportuna y suficiente para las interconexiones específicas de servicios.
Administración del tráfico de red (nueva función)	La agencia implementa, de forma manual, reglas y configuraciones de red estáticas para administrar el tráfico en el aprovisionamiento de servicios, con capacidades	La agencia establece perfiles de aplicaciones con características distintas de administración del tráfico y comienza a asignar todas las aplicaciones a estos perfiles.	La agencia implementa reglas y configuraciones de red dinámicas para la optimización de recursos que se adaptan periódicamente en función de evaluaciones y supervisiones	La agencia implementa reglas y configuraciones de red dinámicas que evolucionan continuamente para satisfacer las necesidades del perfil de aplicaciones y volver a

Función	Tradicional	Inicial	Avanzado	Óptimo
	de supervisión limitadas (p. ej., supervisión del desempeño de las aplicaciones o detección de anomalías), y auditorías y revisiones manuales de cambios de perfil en aplicaciones fundamentales para la misión.	La agencia amplía la aplicación de reglas estáticas a todas las aplicaciones y realiza auditorías manuales periódicas de las evaluaciones del perfil de aplicaciones.	automatizadas de perfiles de aplicaciones conscientes de los riesgos y sensibles a estos.	priorizar las aplicaciones según la importancia de la misión, el riesgo, etc.
Cifrado de tráfico (anteriormente cifrado)	La agencia cifra el tráfico mínimo y se basa en procesos manuales o personalizados para administrar y asegurar las claves de cifrado.	La agencia comienza a cifrar todo el tráfico hacia aplicaciones internas, a preferir el cifrado para el tráfico hacia aplicaciones externas[27], a formalizar políticas de administración de claves y a asegurar las claves de cifrado de servidores o servicios.	La agencia garantiza el cifrado para todos los protocolos de tráfico interno y externo aplicables,[28] administra la emisión y la alternancia de claves y certificados, y comienza a incorporar prácticas recomendadas para la agilidad criptográfica.[29]	La agencia continúa cifrando el tráfico según corresponda, aplica principios de privilegio mínimo para una administración segura de claves en toda la empresa e incorpora las prácticas recomendadas para la agilidad criptográfica lo más ampliamente posible.
Resiliencia de la red (nueva función)	La agencia configura las capacidades de la red caso por caso para satisfacer solo las demandas de disponibilidad de aplicaciones individuales con mecanismos de resiliencia limitados para cargas de trabajo que no se consideran fundamentales para la misión.	La agencia comienza a configurar las capacidades de la red a fin de administrar las demandas de disponibilidad, en el caso de aplicaciones adicionales, y ampliar los mecanismos de resiliencia, en el caso de las cargas de trabajo que no se consideran	La agencia ha configurado capacidades de red para administrar de forma dinámica las demandas de disponibilidad y los mecanismos de resiliencia para la mayoría de sus aplicaciones.	La agencia integra el suministro y la conciencia integrales a fin de adaptarse a los cambios en las demandas de disponibilidad para todas las cargas de trabajo y brinda una resiliencia proporcionada.

[27] Por ejemplo, cuando están disponibles las opciones del protocolo de transferencia de hipertexto (HTTP, por sus siglas en inglés) y del protocolo de transferencia de hipertexto seguro (HTTPS, por sus siglas en inglés), las políticas y las configuraciones prefieren el HTTPS.

[28] Hay una variedad de recursos que las agencias deben revisar con respecto al cifrado y al descifre de tráfico de la red (o no) para las necesidades de inspección y visibilidad como parte de su adopción de la confianza cero: OMB M-15-13, M-19-26, M-22-09; la Directiva Operativa Vinculante 18-01 del Departamento de Seguridad Nacional (DHS, por sus siglas en inglés); NIST SP 800-207; entre otros. Consulte también https://www.cisa.gov/uscert/ncas/alerts/TA17-075A.

[29] DHS. Cryptographic Agility Infographic. May 12, 2022. https://www.dhs.gov/publication/cryptographic-agility-infographic.

Función	Tradicional	Inicial	Avanzado	Óptimo
		fundamentales para la misión.		
Capacidad de visibilidad y análisis	La agencia incorpora capacidades limitadas de supervisión de red centradas en los límites con un análisis mínimo para comenzar a desarrollar una conciencia situacional centralizada.	La agencia emplea capacidades de supervisión de red basadas en los indicadores de riesgo conocidos (incluida la enumeración de redes) para desarrollar conciencia situacional en cada entorno y comienza a relacionar la telemetría entre tipos de tráfico y entornos para actividades de búsqueda de amenazas y análisis.	La agencia implementa capacidades de detección de redes basadas en anomalías con el propósito de desarrollar conciencia situacional en todos los entornos, comienza a relacionar la telemetría de múltiples fuentes para su análisis e incorpora procesos automatizados para actividades sólidas de búsqueda de amenazas.	La agencia mantiene la visibilidad de la comunicación en todas las redes y los entornos de la agencia, al tiempo que permite la conciencia situacional en toda la empresa y capacidades de supervisión avanzadas que automatizan la relación de telemetría en todas las fuentes de detección.
Capacidad de automatización y organización	La agencia utiliza procesos manuales para administrar la configuración y el ciclo de vida de los recursos para las redes y los entornos de la agencia con integración periódica de los requisitos de políticas y la conciencia situacional.	La agencia comienza a utilizar métodos automatizados para administrar la configuración y el ciclo de vida de los recursos para algunas redes o entornos de la agencia, y garantiza que todos los recursos tengan una vida útil definida en función de las políticas y la telemetría.	La agencia utiliza métodos automatizados de administración de cambios (p. ej., CI/CD) para administrar la configuración y el ciclo de vida de los recursos para todas las redes y los entornos de la agencia, respondiendo a los riesgos percibidos y aplicando políticas y protecciones contra estos.	Las redes y los entornos de la agencia se definen utilizando una infraestructura como código administrada mediante métodos automatizados de administración de cambios, lo que incluye el inicio y la caducidad automatizados para alinearse con las necesidades cambiantes.
Capacidad de gobernanza	La agencia implementa políticas de red estáticas (acceso, protocolos, segmentación, alertas y corrección) con un enfoque centrado en las protecciones perimetrales.	La agencia define y comienza a implementar políticas adaptadas a recursos y segmentos de red individuales, y, al mismo tiempo, hereda reglas corporativas según corresponda.	La agencia incorpora la automatización en la implementación de políticas personalizadas y facilita la transición desde protecciones centradas en el perímetro.	La agencia implementa políticas de red en toda la empresa, que permiten controles locales personalizados, actualizaciones dinámicas y conexiones externas seguras basadas en flujos de trabajo de aplicaciones y usuarios.

5.4 Aplicaciones y cargas de trabajo

Las aplicaciones y cargas de trabajo incluyen sistemas, programas informáticos y servicios de la agencia que se ejecutan en las instalaciones, en dispositivos móviles y en entornos en la nube.

Las agencias deben administrar y asegurar sus aplicaciones implementadas, y garantizar el suministro seguro de las aplicaciones. Los controles de acceso detallados y las protecciones integradas contra amenazas pueden ofrecer una mayor conciencia situacional y mitigar las amenazas específicas de aplicaciones. Según OMB M-22-09, las agencias deberían comenzar a explorar oportunidades a fin de que sus aplicaciones estén disponibles a través de redes públicas para usuarios autorizados. En la medida de lo posible, también se deben adoptar las prácticas recomendadas para los procesos de desarrollo, seguridad y operaciones (DevSecOps, por sus siglas en inglés), y CI/CD, lo que incluye el uso de cargas de trabajo inmutables.[30,31] Las agencias deben explorar opciones para alejar sus operaciones del enfoque en los límites de acreditación, actualizar las autorizaciones para operar (ATO, por sus siglas en inglés) de las aplicaciones de apoyo como si estuvieran orientadas hacia el exterior y brindar una seguridad proporcional.

La Tabla 5 enumera las funciones de carga de trabajo relacionadas con la confianza cero, así como las consideraciones de *Visibilidad y análisis*, *Automatización y organización*, y *Gobernanza* dentro del contexto de las aplicaciones y las cargas de trabajo.

Tabla 5: Aplicaciones y cargas de trabajo

Función	Tradicional	Inicial	Avanzado	Óptimo
Acceso a la aplicación (anteriormente autorización de acceso)	La agencia autoriza el acceso a las aplicaciones basándose principalmente en la autorización local y los atributos estáticos.	La agencia comienza a implementar capacidades de autorización de acceso a aplicaciones que incorporan información contextual (p. ej., identidad, cumplimiento del dispositivo u otros atributos) por solicitud con caducidad.	La agencia automatiza las decisiones de acceso a las aplicaciones con información contextual ampliada y condiciones de caducidad aplicadas que se adhieren a los principios de privilegio mínimo.	La agencia autoriza continuamente el acceso a aplicaciones e incorpora análisis de riesgos en tiempo real y ciertos factores, como patrones de uso o comportamientos.
Protecciones contra amenazas a aplicaciones (anteriormente protecciones contra amenazas)	Las protecciones contra amenazas de la agencia tienen una integración mínima con los flujos de trabajo de las aplicaciones y aplican protecciones de propósito	La agencia integra protecciones contra amenazas en los flujos de trabajo de aplicaciones fundamentales para la misión y aplica protecciones contra amenazas	La agencia integra protecciones contra amenazas en todos los flujos de trabajo de las aplicaciones y brinda protección contra algunas amenazas dirigidas y	La agencia integra protecciones avanzadas contra amenazas en todos los flujos de trabajo de las aplicaciones y ofrece visibilidad en tiempo real y protecciones

[30] NIST Projects: DevSecOps. https://csrc.nist.gov/Projects/devsecops#plans.

[31] NIST SP 800-204C: Implementation of DevSecOps for a Microservices-based Application with Service Mesh. March 8, 2022. https://csrc.nist.gov/publications/detail/sp/800-204c/final.

Función	Tradicional	Inicial	Avanzado	Óptimo
	general para amenazas conocidas.	conocidas y algunas amenazas específicas de aplicaciones.	específicas de aplicaciones.	conscientes del contenido contra ataques sofisticados adaptados a las aplicaciones.
Aplicaciones accesibles (anteriormente accesibilidad)	La agencia hace que algunas aplicaciones fundamentales para la misión[32] estén disponibles solo a través de redes privadas y conexiones de redes públicas protegidas (p. ej., VPN) con supervisión.	La agencia pone a disposición de los usuarios autorizados que lo necesiten algunas de sus aplicaciones fundamentales para la misión correspondientes a través de redes públicas abiertas mediante conexiones asincrónicas.	La agencia pone a disposición de los usuarios autorizados la mayoría de sus aplicaciones fundamentales para la misión correspondientes a través de conexiones de redes públicas abiertas, según sea necesario.	La agencia pone a disposición de los usuarios y dispositivos autorizados, cuando corresponda y según sea necesario, todas las aplicaciones correspondientes a través de redes públicas abiertas.
Flujo de trabajo seguro de desarrollo e implementación de aplicaciones (nueva función)	La agencia cuenta con entornos personalizados de desarrollo, pruebas y producción con mecanismos de implementación de código que no son sólidos.	La agencia proporciona infraestructura para los entornos de desarrollo, pruebas y producción (incluida la automatización) con mecanismos formales de implementación de códigos a través de procesos de CI/CD y controles de acceso necesarios en apoyo de los principios de privilegio mínimo.	La agencia utiliza equipos distintos y coordinados para el desarrollo, la seguridad y las operaciones, al tiempo que quita el acceso de los desarrolladores al entorno de producción para la implementación del código.	La agencia aprovecha las cargas de trabajo inmutables cuando es posible y solo permite que los cambios entren en vigencia a través de la reimplementación, como también quita el acceso del administrador a los entornos de implementación a favor de los procesos automatizados para la implementación del código.
Pruebas de seguridad de aplicaciones (anteriormente seguridad de aplicaciones)	La agencia realiza pruebas de seguridad de las aplicaciones antes de su implementación, principalmente mediante métodos de prueba manuales.	La agencia comienza a utilizar métodos de prueba estáticos y dinámicos (p. ej., la aplicación se está ejecutando) para realizar pruebas de seguridad, como el análisis manual de expertos, antes de la implementación de la aplicación.	La agencia integra las pruebas de seguridad de las aplicaciones en el proceso de desarrollo e implementación de aplicaciones, como el uso de métodos de prueba dinámicos periódicos.	La agencia integra las pruebas de seguridad de las aplicaciones a lo largo del ciclo de vida de desarrollo del software en toda la empresa con pruebas automatizadas de rutina de las aplicaciones implementadas.

[32] Esto no incluye los sistemas de Seguridad Nacional. Consulte el Memorando de Seguridad Nacional (NSM, por sus siglas en inglés)-8, "Mejora de la ciberseguridad de los sistemas de Seguridad Nacional, del Departamento de Defensa (Department of Defense) y de Comunidad de Inteligencia (Intelligence Community)". https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-onimproving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/.

Función	Tradicional	Inicial	Avanzado	Óptimo
Capacidad de visibilidad y análisis	La agencia realiza cierta supervisión del desempeño y de la seguridad de las aplicaciones fundamentales para la misión con análisis y agrupación limitados.	La agencia comienza a automatizar el perfil de aplicaciones (p. ej., estado, salud y desempeño) y la supervisión de seguridad para mejorar la recopilación, la agrupación y el análisis de registros.	La agencia automatiza la supervisión de la seguridad y de los perfiles para la mayoría de las aplicaciones con heurística para identificar las tendencias específicas de aplicaciones y de toda la empresa, y perfecciona los procesos con el tiempo para abordar las deficiencias en la visibilidad.	La agencia realiza una supervisión continua y dinámica en todas las aplicaciones para mantener una visibilidad integral en toda la empresa.
Capacidad de automatización y organización	La agencia establece manualmente la ubicación del alojamiento estático de las aplicaciones y el acceso en el aprovisionamiento con mantenimiento y revisión limitados.	La agencia modifica periódicamente las configuraciones de la aplicación (incluida la ubicación y el acceso) para cumplir con los objetivos relevantes de seguridad y desempeño.	La agencia automatiza las configuraciones de la aplicación para responder a los cambios operativos y del entorno.	La agencia automatiza las configuraciones de la aplicación para optimizar continuamente la seguridad y el desempeño.
Capacidad de gobernanza	La agencia se basa principalmente en políticas de aplicación manual para el acceso, el desarrollo, la implementación, la administración de activos de software y las pruebas y evaluaciones de seguridad (ST&E, por sus siglas en inglés) de aplicaciones en la inserción de tecnología, la corrección y el monitoreo de dependencias de software.	La agencia comienza a automatizar la aplicación de políticas para el desarrollo (incluido el acceso a la infraestructura de desarrollo), la implementación, la administración de activos de software y las ST&E de aplicaciones en la inserción de tecnología, la corrección y el monitoreo de dependencias de software según las necesidades de la misión (por ejemplo, con la lista de materiales de software).	La agencia implementa políticas escalonadas y personalizadas en toda la empresa para las aplicaciones y todos los aspectos de los ciclos de vida de desarrollo e implementación de aplicaciones, y aprovecha la automatización, cuando es posible, para apoyar la aplicación.	La agencia automatiza completamente las políticas que rigen el desarrollo y la implementación de aplicaciones, lo que incluye la incorporación de actualizaciones dinámicas para aplicaciones a través de procesos de CI/CD.

5.5 Datos

Los datos incluyen todos los archivos y fragmentos estructurados y no estructurados que residen o han residido en sistemas, dispositivos, redes, aplicaciones, bases de datos, infraestructura y copias de seguridad federales (incluidos los entornos virtuales y en las instalaciones), así como los metadatos asociados.

Los datos de la agencia deben protegerse en dispositivos, aplicaciones y redes de acuerdo con los requisitos federales. Las agencias deben inventariar, categorizar y etiquetar los datos;[33] proteger los datos en reposo y en tránsito; e implementar mecanismos para detectar y detener la exfiltración de datos. Las agencias deben elaborar y revisar cuidadosamente las políticas de gobernanza de datos para garantizar que todos los aspectos de seguridad del ciclo de vida de los datos se apliquen de forma adecuada en toda la empresa.

La Tabla 6 enumera las funciones de datos relacionadas con la confianza cero, así como las consideraciones de *Visibilidad y análisis, Automatización y organización, y Gobernanza* dentro del contexto de los datos.

Tabla 6: Datos

Función	Tradicional	Inicial	Avanzado	Óptimo
Administración del inventario de datos	La agencia identifica y hace inventario de algunos datos de la agencia (p. ej., datos fundamentales para la misión) de forma manual.	La agencia comienza a automatizar los procesos de inventario de datos para los entornos en las instalaciones y en la nube, por lo que cubre la mayoría de los datos de la agencia, y comienza a incorporar protecciones contra la pérdida de datos.	La agencia automatiza el inventario y monitoreo de datos en toda la empresa, cubriendo todos los datos correspondientes de la agencia, con estrategias de prevención de pérdida de datos basadas en las etiquetas o los atributos estáticos.	La agencia realiza un inventario continuo de todos sus datos correspondientes y emplea sólidas estrategias de prevención de pérdida de datos que bloquean dinámicamente la sospecha de exfiltración de datos.
Categorización de datos (nueva función)	La agencia emplea capacidades limitadas y personalizadas de categorización de datos.	La agencia comienza a implementar una estrategia de categorización de datos con etiquetas definidas y mecanismos de aplicación manual.	La agencia automatiza algunos procesos de categorización y etiquetado de datos de manera coherente, escalonada y específica con formatos	La agencia automatiza la categorización y el etiquetado de datos en toda la empresa con técnicas sólidas, formatos detallados y estructurados, y

[33] NIST NCCOE: Data Classification. https://www.nccoe.nist.gov/data-classification.

Función	Tradicional	Inicial	Avanzado	Óptimo
			simples y estructurados, y la revisión periódica.	mecanismos para abordar todos los tipos de datos.
Disponibilidad de datos (nueva función)	La agencia principalmente pone a disposición los datos desde almacenes de datos en las instalaciones con algunas copias de seguridad externas.	La agencia pone a disposición algunos datos desde almacenes de datos redundantes y de alta disponibilidad (p. ej., en la nube), y mantiene copias de seguridad externas de los datos en las instalaciones.	La agencia principalmente pone a disposición datos desde almacenes de datos redundantes y de alta disponibilidad, y garantiza el acceso a datos históricos.	La agencia utiliza métodos dinámicos para optimizar la disponibilidad de datos, incluidos los datos históricos, según las necesidades del usuario y de la entidad.
Acceso a los datos	La agencia rige el acceso de usuarios y entidades (p. ej., permisos para leer, escribir, copiar, otorgar acceso a otros, etc.) a los datos a través de controles de acceso estáticos.	La agencia comienza a implementar controles automatizados de acceso a los datos que incorporan elementos de privilegio mínimo en toda la empresa.	La agencia automatiza controles de acceso a los datos que consideran diversos atributos, como la identidad, el riesgo del dispositivo, la aplicación, la categoría de datos, etc., y tienen un límite de tiempo cuando corresponde.	La agencia automatiza los controles dinámicos de acceso oportuno y suficiente a los datos en toda la empresa con una revisión continua de los permisos.
Cifrado de datos	La agencia cifra sus datos mínimos en reposo y en tránsito, y se basa en procesos manuales o personalizados para administrar y asegurar las claves de cifrado.	La agencia cifra todos los datos en tránsito y, cuando sea posible, los datos en reposo (p. ej., datos fundamentales para la misión y datos almacenados en entornos externos) y comienza a formalizar las políticas de administración de claves y a asegurar las claves de cifrado.[34]	La agencia cifra todos los datos en reposo y en tránsito en toda la empresa en la mayor medida posible, comienza a incorporar la agilidad criptográfica y protege las claves de cifrado (p. ej., los secretos no se codifican de forma rígida y se alternan periódicamente).	La agencia cifra los datos en uso cuando corresponde, aplica los principios de privilegio mínimo para la administración segura de claves en toda la empresa y aplica el cifrado utilizando estándares actualizados y la agilidad criptográfica en la medida de lo posible.[35]

[34] Esto debería incluir los esfuerzos para consolidar los almacenes de claves y reducir la dependencia de almacenes de claves únicos o aislados.

[35] Consulte el NIST para obtener estándares y actualizaciones relevantes, como los siguientes: (1) https://www.nist.gov/itl/fips-general-information, (2) https://www.nist.gov/cryptography y (3) https://csrc.nist.gov/publications/detail/nistir/8413/final

Función	Tradicional	Inicial	Avanzado	Óptimo
Capacidad de visibilidad y análisis	La agencia tiene una visibilidad limitada de los datos, incluida la ubicación, el acceso y el uso, y el análisis consiste principalmente en procesos manuales.	La agencia obtiene visibilidad en función de la administración del inventario de datos, la categorización, el cifrado y los intentos de acceso, con algunos análisis y relaciones automatizados.	La agencia mantiene la visibilidad de los datos de una manera más integral en toda la empresa a través de análisis y relaciones automatizados, y comienza a emplear el análisis predictivo.	La agencia tiene visibilidad en todo el ciclo de vida de los datos con análisis sólidos, incluido el análisis predictivo, que apoyan las vistas integrales de los datos de la agencia y una evaluación continua de la postura de seguridad.
Capacidad de automatización y organización	La agencia implementa políticas de seguridad y ciclo de vida de los datos (p. ej., acceso, uso, almacenamiento, cifrado, configuraciones, protecciones, copias de seguridad, categorización, desinfección) a través de procesos manuales y potencialmente personalizados.	La agencia utiliza algunos procesos automatizados para implementar políticas de seguridad y ciclo de vida de los datos.	La agencia implementa políticas de seguridad y ciclo de vida de los datos principalmente a través de métodos automatizados para la mayoría de los datos de la agencia de manera coherente, escalonada y específica en toda la empresa.	La agencia automatiza, en la mayor medida posible, las políticas de seguridad y los ciclos de vida de los datos para todos los datos de la agencia en toda la empresa.
Capacidad de gobernanza	La agencia se basa en políticas personalizadas de gobernanza de datos (p. ej., para protección, categorización, acceso, inventario, almacenamiento, recuperación, eliminación, etc.) con implementación manual.	La agencia define políticas de gobernanza de datos de alto nivel y se basa, principalmente, en una implementación manual y segmentada.	La agencia comienza a integrar la aplicación de políticas del ciclo de vida de los datos en toda la empresa, lo que permite definiciones más unificadas para las políticas de gobernanza de datos.	Las políticas del ciclo de vida de los datos de la agencia están unificadas en la mayor medida posible y se aplican de forma dinámica en toda la empresa.

5.6 Capacidades interdisciplinarias

Las capacidades interdisciplinarias *Visibilidad y análisis*, *Automatización y organización*, y *Gobernanza* brindan oportunidades para integrar avances en cada uno de los cinco pilares. A medida que las agencias desarrollan estas capacidades con respecto a un pilar determinado, también pueden desarrollar cada capacidad, independientemente de los pilares. La capacidad de *visibilidad y análisis* apoya una visibilidad integral que conforma las decisiones políticas y facilita las actividades de respuesta. Las capacidades de *automatización y organización* aprovechan esta información para apoyar operaciones sólidas y optimizadas a fin de manejar los incidentes de seguridad y responder a los eventos a medida que surgen. La capacidad de *gobernanza* permite a las agencias administrar y supervisar sus requisitos reglamentarios, legales, federales, operativos y del entorno en apoyo de la toma de decisiones basada en riesgos. Estas capacidades también garantizan que se cuente con el personal, los procesos y las tecnologías adecuados para apoyar los objetivos de la misión, los riesgos y el cumplimiento.

La Tabla 7 proporciona una evolución de madurez de alto nivel para cada una de estas capacidades interdisciplinarias.

Tabla 7: Capacidades interdisciplinarias

Función	Tradicional	Inicial	Avanzado	Óptimo
Visibilidad y análisis	La agencia recopila manualmente registros limitados en toda su empresa con baja fidelidad y análisis mínimo.	La agencia comienza a automatizar la recopilación y el análisis de registros y eventos para funciones fundamentales para la misión, y evalúa periódicamente los procesos para detectar deficiencias en la visibilidad.	La agencia amplía la recopilación automatizada de registros y eventos en toda la empresa (incluidos los entornos virtuales) para un análisis centralizado que se relaciona entre múltiples fuentes.	La agencia mantiene una visibilidad integral en toda la empresa a través de la supervisión dinámica centralizada y análisis avanzados de registros y eventos.
Automatización y organización	La agencia se basa en procesos estáticos y manuales para organizar operaciones y actividades de respuesta con automatización limitada.	La agencia comienza a automatizar las actividades de respuesta y organización en apoyo de las funciones fundamentales para la misión.	La agencia automatiza las actividades de respuesta y organización en toda la empresa, y aprovecha la información contextual de múltiples fuentes para fundamentar las decisiones.	Las actividades de respuesta y organización de la agencia responden de forma dinámica a los requisitos cambiantes y a las modificaciones del entorno en toda la empresa.
Gobernanza	La agencia implementa políticas de manera personalizada en toda la empresa, y las políticas se aplican mediante procesos	La agencia define y comienza a implementar políticas para su aplicación en toda la empresa con	La agencia implementa políticas escalonadas y personalizadas en toda la empresa, y aprovecha la automatización cuando es	La agencia implementa y automatiza completamente políticas en toda la empresa, que permiten controles locales personalizados con

Función	Tradicional	Inicial	Avanzado	Óptimo
	manuales o mecanismos técnicos estáticos.	automatización mínima y actualizaciones manuales.	posible para apoyar la aplicación. Las decisiones de políticas de acceso incorporan información contextual de varias fuentes.	aplicación continua y actualizaciones dinámicas.

6. Referencias

La CISA consultó las siguientes publicaciones sobre la ZTA del Gobierno federal mientras desarrollaba y revisaba esta orientación.

M-22-09 de la Oficina de Administración y Presupuesto
Este memorando establece una estrategia federal de arquitectura de confianza cero, que exige que las agencias cumplan con estándares y objetivos de ciberseguridad específicos antes del final del año fiscal (FY) 2024 a fin de reforzar la defensa del Gobierno contra campañas de amenazas cada vez más sofisticadas y persistentes. La estrategia incluye componentes que ponen un énfasis significativo en los controles de identidad y acceso empresariales sólidos (lo que incluye la MFA), requieren cifrar todo el tráfico de la red tan pronto como sea posible, apoyan el desarrollo de una base para automatizar las reglas de acceso de seguridad y tratan cada aplicación como si fuera accesible a través de Internet.

Publicación especial 800-207 del Instituto Nacional de Estándares y Tecnología
El SP 800-207 del NIST describe la confianza cero para los arquitectos de seguridad empresarial a fin de ayudar a comprender la confianza cero para sistemas civiles no clasificados y proporciona una hoja de ruta para migrar los conceptos de seguridad de confianza cero a un entorno empresarial e implementarlos. SP 800-207 es el producto de una colaboración entre múltiples agencias federales, y la supervisión estuvo a cargo del Consejo del Director Federal de Información (CIO, por sus siglas en inglés). El NIST está desarrollando y publicando orientación adicional para la implementación de ZTA.[36]

Arquitectura de referencia de confianza cero del Departamento de Defensa
La Arquitectura de referencia de confianza cero del Departamento de Defensa (DoD, por sus siglas en inglés) describe los estándares y las capacidades empresariales centrados en los datos que se pueden usar para hacer avanzar con éxito la Red de Información del DoD (DoDIN, por sus siglas en inglés) hacia un estado final interoperable de confianza cero. [37]

Adopción del modelo de seguridad de confianza cero de la Agencia de Seguridad Nacional
El documento Adopción del modelo de seguridad de confianza cero de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) explica los beneficios y los desafíos de implementación de un modelo de seguridad de confianza cero. [38] Analiza la importancia de elaborar una estrategia detallada, dedicar los recursos necesarios, desarrollar la implementación y comprometerse plenamente con el modelo de confianza cero para lograr los resultados deseados. Las recomendaciones del documento ayudarán a los líderes de ciberseguridad, a los propietarios de redes empresariales y a los administradores a considerar adoptar este modelo moderno de ciberseguridad.

7. Recursos de la CISA

Los programas de la CISA brindan apoyo y orientación en materia de ciberseguridad, en las áreas de los pilares de confianza cero, lo que incluye la integración de los pilares en una ZTA. Los siguientes documentos son recursos útiles para las agencias que migran a la confianza cero. La CISA continuará revisando y perfeccionando estos recursos a medida que las agencias desarrollen ZTA, y agregará recursos adicionales a la colección con el tiempo.

Diagnóstico y mitigación continuos
La orientación de diagnóstico y mitigación continuos (CDM, por sus siglas en inglés) se puede encontrar en la página de inicio de CDM.

[36] NIST. “Implementing a Zero Trust Architecture Project”. https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture.

[37] DoD. “Zero Trust Reference Architecture”. Version 2.0. July 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf.

[38] NSA. “Embracing a Zero Trust Security Model”. Version 1.0. February 2021. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

Activos de alto valor

La orientación de activos de alto valor (HVA, por sus siglas en inglés) se puede encontrar en la página de inicio de la Oficina de Administración de Programas (PMO, por sus siglas en inglés) de HVA | CISA.

- Superposición de control de activos de alto valor, versión 2.0, enero de 2021
- Preguntas y respuestas (FAQ, por sus siglas en inglés) de la superposición de control de activos de alto valor, versión 1.0, enero de 2018
- Cómo asegurar activos de alto valor, julio de 2018
- CISA Insights: Cómo asegurar activos de alto valor, septiembre de 2019
- Directiva Operativa Vinculante 18-02: Cómo asegurar activos de alto valor, mayo de 2018

Sistema Nacional de Protección de la Ciberseguridad (National Cybersecurity Protection System)
La orientación del Sistema Nacional de Protección de la Ciberseguridad (NCPS, por sus siglas en inglés) se puede encontrar en la página del repositorio de orientación del NCPS.

- Sistema Nacional de Protección de la Ciberseguridad (NCPS), Arquitectura de referencia de la interfaz de la nube, volumen 1: orientación general, versión 1.4, mayo de 2021
- Sistema Nacional de Protección de la Ciberseguridad (NCPS), Arquitectura de referencia de la interfaz de la nube, volumen 2: catálogo de patrones de informe (BORRADOR), versión 1.1, mayo de 2021

Oferta de servicios compartidos de ciberseguridad (anteriormente, Oficina de Administración de Servicios de Calidad [Quality Service Management Office])

- Hoja informativa de la Oficina de Administración de Servicios de Calidad
- Capacidades centralizadas de apoyo a la misión para el Gobierno federal (M-19-16), abril de 2019

Conexiones de Internet Confiables (Trusted Internet Connections)
La orientación de Conexiones de Internet Confiables (TIC, por sus siglas en inglés) se puede encontrar en la página del repositorio de orientación de TIC.

- Guía del programa de Conexiones de Internet Confiables 3.0, versión 1.1, julio de 2021
- Arquitectura de referencia de Conexiones de Internet Confiables 3.0, versión 1.1, julio de 2021
- Catálogo de capacidades de seguridad de Conexiones de Internet Confiables 3.0, versión 2.0, octubre de 2021
- Caso de uso tradicional de TIC de Conexiones de Internet Confiables 3.0, versión 1.0, abril de 2021
- Caso de uso de la sucursal de Conexiones de Internet Confiables 3.0, versión 1.0, abril de 2021
- Caso de uso de usuario remoto de Conexiones de Internet Confiables 3.0, versión 1.0, octubre de 2021
- Caso de uso de la nube de Conexiones de Internet Confiables 3.0, BORRADOR, junio de 2022

Otros recursos de la CISA

- Arquitectura de referencia técnica de seguridad en la nube
- Aplicación de los principios de confianza cero a la movilidad empresarial
- Arquitectura de referencia técnica (TRA, por sus siglas en inglés) de Aplicaciones Empresariales Seguras en la Nube (SCuBA, por sus siglas en inglés) (borrador)
- Guía del Marco extensible de referencia de la visibilidad (eVRF, por sus siglas en inglés) (borrador)
- Autenticación de múltiples factores
- Aplicación de los principios de confianza cero a la movilidad empresarial
- Evaluaciones de revisión de resiliencia cibernética
- Hoja informativa de govCAR
- Día 2 de las sesiones de Cyber Summit 2021: confianza cero