V. — OTRAS DISPOSICIONES

NORMAS

Resolución 300/10776/24

Cód. Informático: 2024016069.

Resolución de 28 de junio, de la Secretaria de Estado de Defensa, por la que se establece la Estrategia de implantación del concepto de seguridad Confianza Cero en el Ministerio de Defensa.

La Política de los Sistemas y Tecnologías de la Información y las Comunicaciones (Política CIS/TIC) del Ministerio de Defensa, que fue aprobada mediante la Orden DEF/2639/2015, de 3 de diciembre), estableció en su eje estratégico relativo a seguridad: Consolidar la Seguridad en los CIS/TIC, a través del fortalecimiento de las capacidades de prevención, detección y respuesta a ciberataques, en línea con la Política de Seguridad de la Información del Ministerio de Defensa y con la Estrategia de Ciberseguridad Nacional y de las organizaciones internacionales de las que España forma parte. Serán, por tanto, estas dos fuentes de ámbito nacional e internacional las que deberán regir los principios de actuación que se adopten en materia de ciberseguridad.

En el ámbito nacional, la Política de Seguridad de la Información (Política SEGINFO) del Ministerio de Defensa, aprobada por Orden Ministerial 76/2006, de 19 de mayo, fija como objetivo alcanzar la protección adecuada, proporcionada y razonable de la información del Ministerio de Defensa. Esta Política SEGINFO viene enmarcada por un contexto normativo de distintos niveles en función de su amplitud, aspecto tratado, ámbito de aplicación y obligatoriedad de cumplimiento.

Estos distintos niveles normativos son, precisamente, los que, desde el año de aprobación de la vigente Política SEGINFO, han venido evolucionando y recogen la necesidad de dotar de una mayor protección a los sistemas CIS/TIC del Departamento. Concretamente, este conjunto normativo se encuentra actualmente constituido por la Estrategia Nacional de Ciberseguridad 2019, la Estrategia de Seguridad Nacional 2021, el Plan Nacional de Ciberseguridad 2022 y el Esquema Nacional de Seguridad regulado por el Real Decreto 311/2022, de 3 de mayo.

Derivado del eje estratégico de seguridad de la Política CIS/TIC en vigor, y observando la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional y publicada mediante Orden PCI/487/2019 de 26 de abril, se proponen las directrices en materia de planificación y coordinación de la Política de Seguridad Nacional relacionadas con la ciberseguridad. La aproximación realizada por este documento es que la seguridad en el ciberespacio debe abordarse bajo un enfoque multidisciplinar, abarcando aspectos más allá de los puramente técnicos. Es precisamente este enfoque integral el que introduce un cambio de paradigma en la concepción de la ciberseguridad, confiriendo protagonismo no únicamente a la tecnología, sino también a los procesos y a las personas.

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, establece en su artículo 20 que se debe aplicar el principio de mínimo privilegio, tanto en el diseño como en la configuración de los sistemas de información para su explotación, de manera que no se deposite una confianza permanente en los usuarios y recursos. Por esta razón la confiabilidad debe verificarse de forma explícita y continua, minimizando la exposición a una amenaza que puede cambiar continuamente.

En el ámbito internacional, la OTAN ha aprobado su Política sobre el denominado concepto Zero Trust o Confianza Cero (Zero Trust Policy) como visión de la ciberseguridad; la aplicación de este concepto será de obligado cumplimiento para los sistemas de información y telecomunicaciones, nacionales o aliados, que transmitan, procesen o almacenen información clasificada de la Alianza Atlántica.

En su sentido más global, y tal y como se regula en la Arquitectura Global CIS/TIC del Ministerio, aprobada por la Instrucción 58/2016 de 28 de octubre, del Secretario de Estado de Defensa, la ciberseguridad debe entenderse como la capacidad de proteger adecuadamente la confidencialidad, integridad y disponibilidad de Sistemas (CIS/TIC) y la

CVE: BOD-2024-134-19861
Verificable en https://sede.defensa.gob.es/acceda/bod

información procesada, almacenada o transmitida, mediante la aplicación de las medidas necesarias. La Ciberseguridad no debe centrarse exclusivamente en las medidas de protección técnica, ya que sería incompleta; debe incluir todos los aspectos que determinan la capacidad bajo un enfoque integral.

El enfoque de seguridad basado en el concepto de Confianza Cero representa un cambio fundamental en cómo se concibe y se aborda la seguridad de las tecnologías de los sistemas de información y comunicaciones. El modelo actual está enfocado en la defensa perimetral y en la red; el nuevo modelo de seguridad se centra en la ausencia de una confianza implícita en usuarios y dispositivos, independientemente de su localización física, estado, o medio por el que se conectan.

La Confianza Cero conlleva la transición de un paradigma de seguridad basado en el cumplimiento a otro basado en la gestión dinámica del riesgo, lo que requiere un profundo cambio cultural. Por ello, su implantación debe abordarse incrementando de forma paulatina la capacidad de protección, al tiempo que se va mejorando la experiencia de usuario, mediante una adopción progresiva de nuevas herramientas y procesos de gobernanza que sirvan al propósito del Ministerio de Defensa.

Además, no todos los sistemas e infraestructuras legados requerirán una reconversión completa en materia de seguridad, aunque deberán diseñarse y aplicarse controles de seguridad adecuados para todos ellos, que puedan contrarrestar nuevos vectores de ciberataques y amenazas emergentes hasta la finalización de su ciclo de vida.

Por lo tanto, la implantación del concepto de seguridad Confianza Cero constituye una necesidad real y debe abordarse desde el momento actual, para proteger la información del Ministerio, como recurso estratégico del Departamento, ante los retos de seguridad en los que desarrolla su actividad.

En el ejercicio de la facultad que me confiere el artículo 3 del Real Decreto 205/2024, de 27 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa, y la disposición final primera de la Orden DEF/2639/2015, de 3 de diciembre, por la que se establece la Política CIS/TIC,

DISPONGO:

Artículo único. *Aprobación de la estrategia de implantación del concepto de seguridad Confianza Cero del Ministerio de Defensa.*

Se aprueba la estrategia de implantación del concepto de seguridad Confianza Cero en el Ministerio de Defensa, cuyo texto se inserta a continuación.

Disposición final primera. *Facultades dispositivas.*

Se faculta al Director General del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC) para dictar, en el ámbito de sus competencias, las disposiciones oportunas para la aplicación de esta Resolución.

Disposición final segunda. *Entrada en vigor.*

La presente Resolución entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Ministerio de Defensa».

Madrid, 28 de junio de 2024.—La Secretaria de Estado de Defensa, María Amparo Valcarce García.

CVE: BOD-2024-134-19862
Verificable en https://sede.defensa.gob.es/acceda/bod

ESTRATEGIA DE IMPLANTACIÓN DEL CONCEPTO DE SEGURIDAD CONFIANZA CERO EN EL MINISTERIO DE DEFENSA

CAPÍTULO I

Disposiciones Generales

Primero. *Propósito.*

El propósito de esta estrategia es:

a) Proporcionar un escenario general de la ciberseguridad basada en el concepto de Confianza Cero, y definir la finalidad que se persigue con la implantación de este concepto.
b) Establecer los principios que deben regir y guiar la implantación del concepto de seguridad Confianza Cero.
c) Determinar los objetivos generales que se persiguen con la implantación del concepto de seguridad Confianza Cero en el Ministerio de Defensa.
d) Establecer las líneas de acción estratégicas para conseguir los objetivos generales.
e) Plantear un modelo de referencia y modelos tecnológicos para la implantación del concepto de seguridad Confianza Cero en el Ministerio de Defensa, que tengan en cuenta todos los pilares de este paradigma, en especial la seguridad centrada en el dato.
f) Definir el modelo de desarrollo y la estructura de gobierno para la implantación del concepto de seguridad Confianza Cero en el Ministerio de Defensa.

Segundo. *Ámbito de Aplicación.*

La estrategia de Confianza Cero será de aplicación en el Ministerio de Defensa y sus Organismos Públicos adscritos, y a todos los usuarios de servicios CIS/TIC del Departamento.

CAPÍTULO II

Introducción, escenario, finalidad, principios, objetivos y líneas de acción

Tercero. *Introducción y escenario.*

La implantación del concepto de seguridad Confianza Cero implica que el modelo actual, estático y basado en la seguridad perimetral, se debe redefinir hacia un nuevo modelo centrado en la verificación continua de la identidad y de los privilegios de los usuarios; y de la identidad y seguridad de los dispositivos, creando un perímetro virtual alrededor de cada recurso. Todo ello se hará sin asumir confianza implícita alguna en ningún activo por el mero hecho de su ubicación física o de red. Cada vez que se acceda a un servicio deberán concederse los privilegios oportunos a través de políticas basadas en análisis de riesgos.

Para preservar el acceso a los activos se utiliza un conjunto de funciones de autenticación, autorización y responsabilidad (Authentication, Authorization & Accounting - AAA) en cada usuario y dispositivo.

De este modo, la seguridad se enfoca en cada activo; es dinámica porque se evalúa de manera continua. Al estar segmentado el acceso y evaluarse éste para cada servicio, y de manera periódica para confirmar que las autorizaciones concedidas siguen siendo válidas, se reduce la capacidad de que cualquier amenaza que haya podido penetrar en la red se mueva lateralmente hacia otros recursos y acceda a ellos.

Este nuevo paradigma lleva consigo un cambio significativo en los mecanismos tradicionales de seguridad y de autenticación, puesto que actualmente, los privilegios de acceso a los distintos servicios se heredan de otros concedidos antes al usuario. Requiere también un cambio cultural que afecta a las personas, a los procesos y procedimientos de trabajo. Por ello impacta transversalmente a todo el Departamento.

CVE: BOD-2024-134-19863
Verificable en https://sede.defensa.gob.es/acceda/bod

El escenario al que se enfrenta el Ministerio de Defensa en la adopción del concepto de Confianza Cero, se caracteriza por:

a) *La existencia de amenazas complejas y persistentes.* Para mitigar su impacto y estar en disposición de dar respuesta oportuna, anticipada y efectiva a este escenario incierto de riesgos y amenazas, en un entorno multidominio, el Ministerio ha de acelerar la implantación del concepto Confianza Cero y migrar sus entornos a este nuevo marco de seguridad lo más rápidamente posible.
b) *Una rápida evolución en las necesidades operativas y funcionales del Ministerio y de las posibilidades que ofrecen las tecnologías.* Los conceptos de seguridad y protección de la información deben adaptarse a los nuevos retos que supone el proceso de Transformación Digital de acuerdo con la visión del CIO del Ministerio, la implantación de tecnologías emergentes y disruptivas, el incremento de trabajo remoto e híbrido y la migración paulatina de servicios y aplicaciones a entornos de nube.
c) *Una adaptación que no debe ser únicamente tecnológica, sino que se requiere un cambio cultural.* Los retos actuales y futuros en materia de ciberseguridad no se pueden solucionar exclusivamente mediante la aplicación de la tecnología; llevan consigo un cambio de mentalidad y de cultura de seguridad, que es transversal a todo el Departamento y que afecta a todo su capital humano, como usuarios de servicios y sistemas TIC del Ministerio de Defensa.
d) *El impacto en la compartición de información en el entorno multinacional.* La Confianza Cero mejorará el uso compartido de información en condiciones óptimas de seguridad en el seno de las organizaciones internacionales de seguridad y defensa de las que España forma parte.
e) *La necesidad de una implantación coordinada con un enfoque integral.* La Confianza Cero debe implantarse de forma coordinada en los distintos niveles y ámbitos del Departamento, para evitar silos organizativos, de gobernanza y técnicos.
   En relación con lo anterior, la implantación debe contar con la participación de todos los actores con responsabilidades en materia de seguridad, de forma que se eviten brechas o áreas sin cubrir.
f) La privacidad desde el diseño y por defecto debe formar parte del concepto de Confianza Cero, para proteger el activo más importante del Departamento que son las personas. Cualquier sistema, proceso o infraestructura que vaya a utilizar datos personales debe ser concebida y diseñada identificando los posibles riesgos a los derechos y libertades de los interesados y minimizarlos para que no lleguen a concretarse en daños.

Cuarto. *Finalidad.*

La implantación del concepto Confianza Cero pretende aumentar la seguridad de la información del Ministerio de Defensa desde un enfoque integral, a través de un proceso adaptativo que favorezca el cambio de paradigma.

Para alcanzar esta situación se debe disponer de un entorno escalable, resiliente, auditable y defendible, centrado en proteger todos los activos del Ministerio de Defensa incluyendo datos, infraestructura, sistemas y servicios.

El proceso de adopción del nuevo paradigma de seguridad requiere la combinación de tecnología, políticas y aceptación cultural de la organización, para disponer una seguridad más sólida y adaptativa que haga frente al contexto actual, altamente dinámico e incierto de amenazas y riesgos. Por lo tanto, todas las dimensiones del concepto deben abordarse con un enfoque integral y de manera sinérgica.

La Transformación Digital en el Ministerio de Defensa está orientada a las operaciones multidominio, que requieren hiperconectividad, capacidades de Mando y Control, Interoperabilidad y asumir un cambio cultural. La ciberseguridad está integrada en la visión de la Transformación Digital del Ministerio, la cual adopta el paradigma de Confianza Cero.

CVE: BOD-2024-134-19864
Verificable en https://sede.defensa.gob.es/acceda/bod

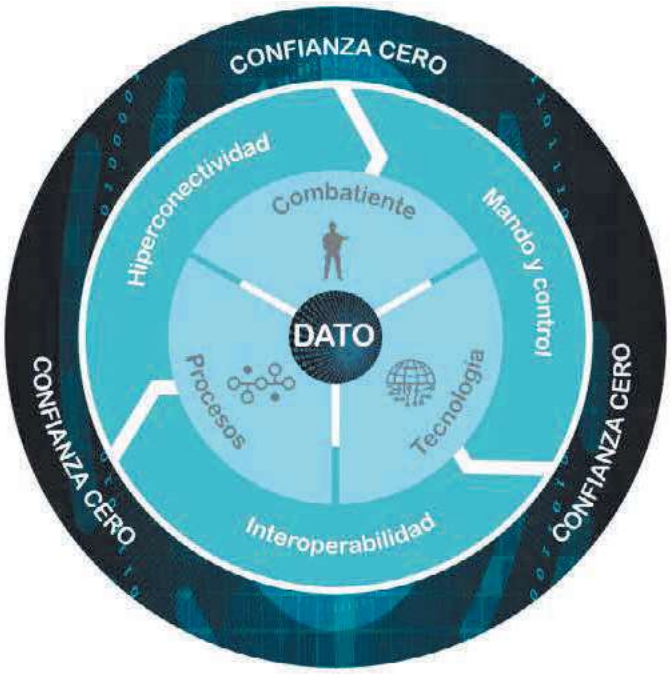

Figura 1 - Ideograma del concepto de seguridad Confianza Cero integrado en la Visión de la Transformación Digital del Ministerio de Defensa.

La consecución de esta finalidad prevé alcanzar, al menos, los siguientes beneficios:

a) Conferir a los usuarios la capacidad de acceder a los recursos y servicios requeridos, independientemente de su ubicación física, mediante cualquier dispositivo adecuadamente autorizado y haciendo uso de la debida autenticación. Este beneficio se potenciará gracias al uso integrado de la Confianza Cero con tecnologías de hiperconectividad, nuevas generaciones de comunicaciones móviles (5G y futuros protocolos inalámbricos), y de computación en el borde (Edge computing).
b) Incrementar la protección de la información procesada, transmitida y almacenada en los sistemas de información y comunicaciones del Ministerio de Defensa, para permitir la evolución del Departamento hacia una organización más ágil y compatible con un modelo de arquitectura basado en la nube.
c) Minimizar la superficie de exposición por medio de medidas de protección preventivas basadas en la microsegmentación.
d) Proporcionar protección a los servicios de interés para el Departamento, por medio de políticas y protocolos de ciberseguridad concretos.
e) Contener y mitigar cualquier daño causado a los activos del Departamento, contando para ello con una infraestructura que evite que ocurran, proactiva y preventivamente.

Quinto. *Principios.*

Los principios que regirán la aplicación de esta estrategia en el Ministerio de Defensa son:

a) *Asumir la brecha.* El diseño, despliegue y operación de los servicios deben llevarse a cabo considerando de antemano que la seguridad puede haber sido comprometida.
b) *Nunca confiar y siempre verificar.* En todas las actuaciones referidas a seguridad de la información debe aplicarse la desconfianza por defecto. Cada usuario, dispositivo o aplicación debe ser tratado, de entrada, como no autorizado ni autenticado.
Se debe garantizar que, una vez autorizados, los usuarios, dispositivos o aplicaciones acceden únicamente a los datos que necesitan y cuando los necesitan.

CVE: BOD-2024-134-19865
Verificable en https://sede.defensa.gob.es/acceda/bod

c) *Verificar de modo explícito y continuo.* El entorno de seguridad debe adaptarse dinámica y permanentemente sobre el usuario, infraestructura, datos y cualquier otro activo asociado con la provisión de servicios. Para ello se verificará la identidad de usuarios, dispositivos o aplicaciones cada vez que requieran acceso a un servicio, información o infraestructura y que, en caso de concederse la autorización, ésta se verifique periódicamente. Se realizará un registro de control de accesos permanente y auditable.
d) *Aplicar el mínimo privilegio.* De manera general, se conferirán a todos los recursos las capacidades mínimas necesarias para el cumplimiento de su función, asegurando un apropiado equilibrio entre la necesidad de conocer y la responsabilidad de compartir.
e) *Tomar decisiones de seguridad basadas en el análisis de conducta y probabilidad.* Todos los eventos relativos a seguridad deben ser monitorizados, almacenados y analizados conforme a métricas precisas que indiquen el nivel de confianza aplicable en cada caso, y teniendo en cuenta la probabilidad de que sucedan esos eventos.
f) *Deslocalizar el puesto de trabajo.* Todos los usuarios deben ser capaces de trabajar y llevar a cabo sus misiones sobre aquellas redes y recursos a los que tienen acceso desde cualquier localización autorizada, por medio de credenciales de seguridad dinámicas.
g) *Asumir el enfoque de Confianza Cero desde el diseño.* Comprende el proceso de definición e implantación de capacidades, servicios, procesos e infraestructuras.
h) *Transparencia.* La efectiva implantación del concepto Confianza Cero exige la provisión de la necesaria información sobre este concepto, sus propósitos y principios, para fomentar su comprensión entre todas las partes interesadas, y en los distintos entornos en que se emplee.

Sexto. *Objetivos generales.*

Los objetivos generales que se establecen con la estrategia de implantación del concepto Confianza Cero en el Ministerio de Defensa son:

a) *Adopción cultural de la Confianza Cero.* Los usuarios deben ser conscientes de las ventajas de la Confianza Cero para el desarrollo de sus cometidos y para la protección de la información; de esta manera, admitirán los cambios sobre los procesos de trabajo en los que participan y facilitarán las actuaciones que son necesarias por su parte para la implantación del nuevo paradigma.
b) *Securización y protección de los servicios basados en tecnologías de la información.* Las políticas y prácticas de ciberseguridad del Departamento y las actuaciones en esta materia deben incorporar y poner en funcionamiento el concepto Confianza Cero, para alcanzar la seguridad requerida en la provisión de los servicios.
c) *Actualización permanente.* El Ministerio de Defensa debe evaluar de forma permanente la evolución en las tecnologías, metodologías y conceptos relacionados con la Confianza Cero, para mantener la posición de ventaja en el entorno dinámico y cambiante de los riesgos y de las amenazas.
d) *Habilitación de la Confianza Cero.* La puesta en funcionamiento del concepto de Confianza Cero en el Ministerio de Defensa se debe integrar con el resto de procesos departamentales dando como resultado una implantación integral, fluida, sinérgica y coordinada.
e) *Alineamiento con Organizaciones Internacionales de Seguridad y Defensa.* Las organizaciones de este ámbito de las que España forma parte, tienen previsto evolucionar hacia una obligatoriedad de cumplimiento del concepto Confianza Cero para todos los sistemas que transmitan, procesen o almacenen información de estas organizaciones.

CVE: BOD-2024-134-19866
Verificable en https://sede.defensa.gob.es/acceda/bod

Séptimo. *Líneas de acción estratégicas.*

Las líneas de acción estratégicas a desarrollar, para alcanzar los objetivos expuestos son:

a) *Evaluar los riesgos y las carencias en relación con los principios del concepto Confianza Cero.* Se impulsará una transición hacia estrategias basadas en la gestión dinámica de riesgos y se llevará a cabo un análisis de riesgos y carencias para determinar la situación actual, como punto de partida del proceso de implantación del concepto Confianza Cero.
b) *Revisar las Arquitecturas de Referencia (ARs).* Se realizará una revisión de las ARs que puedan estar afectadas por este cambio.
c) *Analizar los servicios basados en tecnologías de la información legados.* Los sistemas y servicios legados deberán ser analizados para evaluar su idoneidad, y decidir su sustitución o la aplicación de medidas correctivas, siguiendo criterios de racionalización y optimización.
d) *Establecer los criterios de implantación del concepto Confianza Cero para cada servicio.* Será necesario llevar a cabo un proceso de implantación del concepto Confianza Cero en cada servicio, siendo preciso identificar los parámetros y umbrales de seguridad necesarios en función de los requisitos de seguridad de cada uno de ellos.
e) *Implementar planes de comunicación, concienciación y formación en el concepto Confianza Cero.* Se establecerá un plan de comunicación sobre la Confianza Cero para contribuir a su adopción cultural en el Ministerio. La formación será un elemento clave para que la concienciación y el conocimiento residan en el Departamento y no dependan exclusivamente de proveedores externos.
f) *Desarrollar la normativa asociada al concepto Confianza Cero.* La normativa necesaria para detallar la implantación del concepto de seguridad Confianza Cero en el Ministerio de Defensa será elaborada tras la aprobación de esta estrategia.
g) *Evaluar e implantar modelos tecnológicos de seguridad habilitadores del concepto Confianza Cero.* En el anexo a esta Estrategia se presenta una visión general de estos modelos tecnológicos.

CAPÍTULO III

Modelo de referencia y aplicación en el Ministerio de Defensa

Octavo. *Modelo de referencia.*

Conceptualmente, el modelo de referencia Confianza Cero se basa en unos elementos que sustentan la seguridad (pilares) y unas acciones que constituyen un entorno tecnológico seguro (base).

Los pilares de la Confianza Cero son:

a) *Usuarios:* entidades físicas o lógicas que pueden requerir acceso a los recursos y sobre los que se debe, de forma continuada, autenticar y monitorizar sus patrones de actividad, con el objetivo de delimitar sus privilegios al mínimo y proteger sus interacciones.
b) *Dispositivos:* hardware, software y firmware cuyo estado debe proporcionar información sobre el grado de riesgo implícito que contienen. Su inspección en tiempo real y actualización continua constituye uno de los aspectos determinantes del modelo.
c) *Datos:* elementos en torno a los cuales debe establecerse una seguridad (seguridad centrada en el dato) y que constituyen el pilar central sobre el que se asienta la implantación del concepto Confianza Cero.
d) *Redes:* infraestructura física o lógica que permite la comunicación y que requiere acciones de segmentación, aislamiento y control, basadas en políticas de accesos.
e) *Aplicaciones:* mecanismos basados en software que soportan procesos de trabajo y que deben ser securizadas evitando las configuraciones prestablecidas por defecto.

CVE: BOD-2024-134-19867
Verificable en https://sede.defensa.gob.es/acceda/bod

Los cimientos de la Confianza Cero son:

a) *Monitorización y análisis:* analizar eventos, actividades y comportamientos para que el contexto tecnológico permita tomar decisiones y aplicar, en su caso, medidas de mitigación o correctivas.
b) *Orquestación y automatización:* dar respuestas de seguridad automatizadas y basadas en procesos definidos y políticas de seguridad, soportados mediante mecanismos de inteligencia artificial.
c) *Federación con sistemas externos al MDEF:* permitir el intercambio y tránsito de información entre sistemas y servicios de manera segura, mediante mecanismos de interconexión de igual a igual.

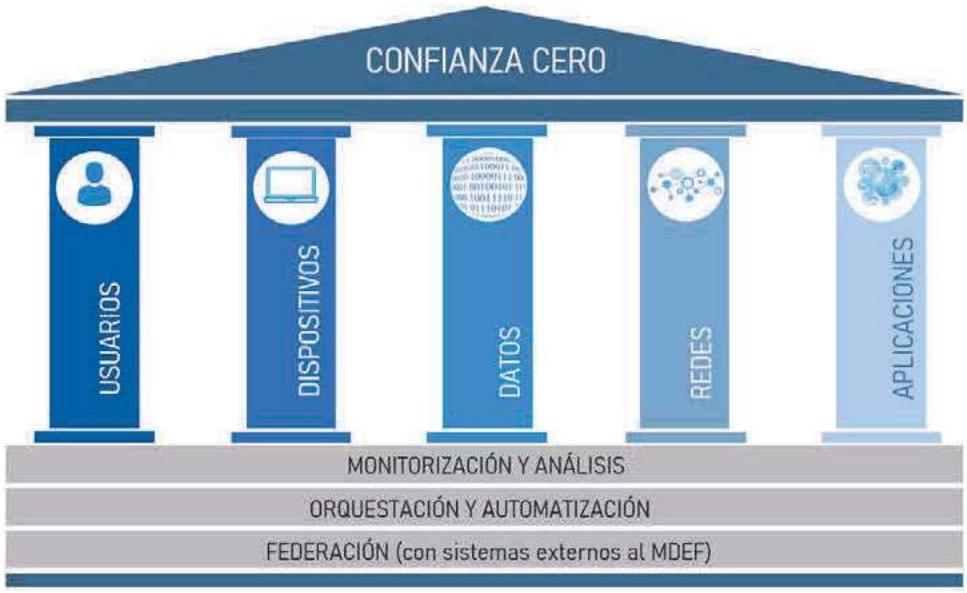

Figura 2 - Modelo de referencia del concepto de seguridad Confianza Cero.

CAPÍTULO IV

Desarrollo e implantación del concepto de seguridad Confianza Cero y estructura de gobierno

Décimo. *Desarrollo e implantación del concepto de seguridad Confianza Cero.*

Para el desarrollo e implementación del concepto de seguridad Confianza Cero, se definirán unos casos de uso y proyectos iniciales, cuya ejecución se adaptará a la evolución del contexto tecnológico y normativo que afecte a dicho concepto, y se desarrollará de acuerdo con las líneas de acción estratégicas definidas en el apartado séptimo. Además, cuando sea necesario se desarrollará la normativa técnica que defina las capacidades de Confianza Cero para cada pilar establecido, junto con los niveles mínimos asociados que permitan establecer la línea base de Confianza Cero para todos los ámbitos del Ministerio.

Los proyectos aprovecharán las iniciativas en curso que desarrollan la Política CIS/TIC, la Política de SEGINFO y el proceso de Transformación Digital del Ministerio de Defensa. La posible aplicación a un ámbito concreto (a modo de experiencia inicial), se concretará y validará por parte de la estructura de gobierno de la estrategia.

Se tomarán como referencia las necesidades y prioridades establecidas en el Proceso de Planeamiento de la Defensa descrito en la Orden Ministerial 60/2015, de 3 de diciembre.

Igualmente, se tendrá en cuenta que, en virtud de las competencias establecidas en el artículo 9, apartado 2, a) del Real Decreto 521/2020, de 19 de mayo, por el que se establece la organización básica de las Fuerzas Armadas, al Estado Mayor de la Defensa le corresponde el desarrollo y detalle de las políticas de Seguridad de la Información en los

CVE: BOD-2024-134-19868
Verificable en https://sede.defensa.gob.es/acceda/bod

Sistemas de Información y Telecomunicaciones en el marco de las políticas establecidas, así como la dirección de la ejecución y el control del cumplimiento de estas políticas en el ámbito de las Fuerzas Armadas y para las operaciones.

En concreto, se presentan a continuación los proyectos iniciales definidos para el desarrollo de la presente Estrategia. Dada su transversalidad, se enfocarán a los pilares del Modelo de Referencia:

- Usuarios:
  - Disponer de un inventario de usuarios, asociado a la definición del puesto de trabajo digital.
  - Identificar los criterios evaluables para la autorización de accesos, incluyendo criterios específicos para las soluciones de trabajo en movilidad del Ministerio.
  - Alinear la evolución del sistema de gestión de identidades y acceso a los requisitos del concepto de seguridad Confianza Cero.
- Dispositivos:
  - Disponer de un inventario de dispositivos.
  - Establecer mecanismos de detección y autorización de dispositivos, incluyendo los Internet of Things (IoT).
- Datos:
  - Disponer de una política de Gobierno Corporativo del Dato.
  - Establecer mecanismos de clasificación y etiquetado de datos asociados a los perfiles de usuarios y dispositivos.
  - Evaluar mecanismos de protección de información centrados en el dato (Data Centric Security).
- Redes:
  - Determinar criterios para la macro y micro segmentación asociada al concepto Confianza Cero, incluyendo la tecnología de nube en la Infraestructura Integral de Información para la Defensa (I3D).
  - Establecer mecanismos de mapeado de los flujos de datos.
- Aplicaciones:
  - Disponer de un inventario de aplicaciones, identificando entre otros factores, sus responsables funcional y técnico y el grado de clasificación de la información manejada.
  - Habilitar mecanismos de monitorización continua de las autorizaciones de acceso a aplicaciones (tanto de usuarios como de dispositivos).

Undécimo. *Estructura de gobierno de la Estrategia de implantación del concepto de seguridad Confianza Cero.*

La responsabilidad del seguimiento de esta estrategia y de la implantación y empleo del concepto de seguridad Confianza Cero corresponde al Comité de Seguridad de la Información en los Sistemas de Información y Telecomunicaciones (SEGINFOSIT) del Ministerio de Defensa que será responsable de la coordinación, seguimiento y control de la presente estrategia, sus líneas de desarrollo y los casos de uso, proyectos y acciones que se propongan y determinen para su consecución.

Con respecto a la presente Estrategia, el Comité tendrá los siguientes cometidos:

a) Realizar el seguimiento de la ejecución de las líneas de acción definidas en el apartado séptimo.
   Los órganos responsables de la ejecución de las líneas de acción y los plazos de consecución en cada caso, se concretarán en los planes de implementación que como desarrollo de esta Estrategia se establezcan.

CVE: BOD-2024-134-19869
Verificable en https://sede.defensa.gob.es/acceda/bod

b) Coordinarse con las estructuras de su nivel responsables de proyectos habilitadores de la confianza cero, en especial con las relativas al gobierno corporativo del dato.
c) Impulsar y promover la revisión del marco normativo actual en materia de Sistemas y Tecnologías de la Información y Comunicaciones, Seguridad de la Información y Gestión de Datos, Información y Conocimiento, para incorporar, en los casos que sea necesario, las consideraciones derivadas de la implantación del concepto Confianza Cero.
d) Proponer la postura del Ministerio de Defensa en relación con la dimensión tecnológica e implicaciones asociadas al concepto de seguridad Confianza Cero, para su presentación en los foros y estructuras en los que participe el Departamento, tanto a nivel nacional, como a nivel internacional.
e) Informar a la comisión Ejecutiva de Seguridad de la Información y a la comisión Ejecutiva CIS/TIC de los resultados de las actividades, riesgos y problemática, así como de cualquier otro aspecto de relevancia en relación con la ejecución de los planes e iniciativas.

El Comité SEGINFOSIT podrá establecer una estructura derivada específica para el desarrollo de estos cometidos.

CVE: BOD-2024-134-19870
Verificable en https://sede.defensa.gob.es/acceda/bod

ANEXO

MODELOS TECNOLÓGICOS DE SEGURIDAD

Para la implantación del concepto de seguridad Confianza Cero en el Ministerio de Defensa, se deben incorporar nuevos modelos tecnológicos de seguridad que proporcionen una respuesta adecuada a las nuevas necesidades de protección. Deben ser complementarios con otras medidas de seguridad que contribuyan a garantizar y reforzar el marco de seguridad y de actuación segura en el ciberespacio utilizado por el Ministerio de Defensa, como los mecanismos de autenticación y de encriptación.

Estos nuevos modelos tecnológicos de seguridad son el Servicio Perimetral de Acceso Seguro (Secure Access Service Edge - SASE), y el Perímetro de Servicio de Seguridad (Security Service Edge - SSE), que ejercen un papel de complementariedad mutua.

El SASE consiste en una arquitectura de seguridad basada en identidad de usuarios y dispositivos que maximiza el valor y la utilidad de las tecnologías de nube.

El SSE está integrado por una serie de servicios de seguridad que sirven de fundamento a la arquitectura de seguridad SASE.

Estos nuevos modelos tecnológicos de seguridad incluyen, entre otras, soluciones de Acceso a Red con Confianza Cero (Zero Trust Network Access - ZTNA). Se trata de un modelo de acceso que aplica el concepto de Confianza Cero a las redes; asume que ningún usuario, dispositivo o aplicación es confiable por defecto, por lo que verifica su identidad y autorización antes de permitir su acceso a los recursos.

El empleo del SASE y el SSE permitirá ofrecer un acceso coherente y contextualizado a los servicios para todos los usuarios autorizados, independientemente de su ubicación. De este modo:

- *SASE* quedará referido a un conjunto de soluciones y herramientas de seguridad basadas en la nube con capacidad de ofrecer soluciones integrales para las necesidades dinámicas de acceso seguro por parte de los usuarios autorizados, incluidas las redes definidas por Software.
- *SSE* quedará definido como un subconjunto de SASE que se centre únicamente en los servicios de seguridad necesarios de una plataforma en la nube de tipo SASE.

Para alcanzar el óptimo despliegue de estos modelos de seguridad, se integrarán soluciones que ofrezcan acceso seguro a los recursos de una forma dinámica y adaptable al riesgo asociado. Entre otras, se habilitarán el Agente de Seguridad de Acceso a la Nube (Cloud Access Security Broker – CASB), la capacidad de Inspección Basada en Riesgos (Risk-Based Inspection - RBI), la capacidad de Prevención de filtración y Pérdida de Datos (Data Loss Prevention - DLP), y la Analítica de Comportamiento de Usuario y Entidad (User and Entity Behaviour Analytics - UEBA).

CVE: BOD-2024-134-19871
Verificable en https://sede.defensa.gob.es/acceda/bod