

Política de Seguridad de las TIC CCN-STIC 004

Manejo de información con clasificación Difusión Limitada, o equivalente, en nube pública



Febrero 2026

Edita:



© Centro Criptológico Nacional, 2026



CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL,
2.5.4.97=VATES-S2800155J, ou=CENTRO
CRYPTOLOGICO NACIONAL, o=CENTRO
CRYPTOLOGICO NACIONAL, c=ES
2026.02.09 16:58:00 +01'00'

Fecha de Edición: febrero 2026

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN	4
2. OBJETO Y ALCANCE	7
3. CONCEPTOS CLAVE	8
4. ORGANIZACIÓN DE LA SEGURIDAD: ROLES Y RESPONSABILIDADES	11
5. ESTRATEGIA DE ACREDITACIÓN DE SISTEMAS DL EN NUBE PÚBLICA	13
6. MEDIDAS DE SEGURIDAD PARA NUBE DL	15
6.1 SEGURIDAD PERSONAL	15
6.2 SEGURIDAD FÍSICA.....	16
6.3 SEGURIDAD DE LA INFORMACIÓN.....	16
7. DECLARACIÓN DE APLICABILIDAD VINCULADA.....	18
8. DEFINICIONES.....	19
9. REFERENCIAS.....	20
10. ABREVIATURAS	21

1. INTRODUCCIÓN

1. La evolución actual de las Tecnologías de la Información y las Comunicaciones (TIC) demanda cada día más capacidad de computación y almacenamiento, disponibilidad, movilidad o incluso ubicuidad y compartición de información. En un escenario en el que ya casi ningún servicio se encuentra aislado ni anclado a una ubicación física, emerge la necesidad de consumir servicios en la nube. En consecuencia, la adopción de la Computación en la Nube (Cloud Computing, en inglés) es un enfoque cada vez más extendido internacionalmente debido a la eficiencia que proporciona el uso compartido de infraestructuras y recursos de computación.
2. Dicho modelo de uso aporta las siguientes ventajas:
 - a) **Escalabilidad de recursos.** Los servicios que se contratan a un Proveedor de Servicios en la Nube (En inglés, **Cloud Service Provider - CSP**) presentan la ventaja de ser escalables. De hecho, los CSP suelen ofrecer distintas formas de contratación que permiten pago por uso, realizar una reserva de recursos con unas determinadas capacidades, o distintas combinaciones de ambos. En las arquitecturas tradicionales *on premise* existen riesgos de infradimensionar los recursos y tener problemas de caída de servicio por saturación en picos de trabajo; o bien sobredimensionarlos, lo que supondría una infrautilización de la infraestructura y un desperdicio de parte de la inversión realizada. Con la flexibilidad de los servicios en la nube estas decisiones y riesgos asociados desaparecen.
 - b) **Disponibilidad de recursos.** Hoy en día, los servicios en la nube permiten acceder a los recursos desde cualquier ubicación con una disponibilidad casi absoluta. Esto contrasta fuertemente con los servicios *on premise*, que en muchos casos necesitan desplegar costosas infraestructuras para poder ofrecer un nivel de capilaridad aceptable y llegar a todos sus usuarios.
 - c) **Despliegue dinámico de arquitectura.** Dado que es el CSP el que despliega la arquitectura y el cliente de servicios en la nube (En inglés, **Cloud Service Customer - CSC**) solamente paga por su uso, no es necesario realizar grandes inversiones para utilizar una arquitectura determinada y es igualmente sencillo implementar cambios profundos dentro de la arquitectura para adaptarse a las necesidades cambiantes sin que ello suponga un coste inasumible. En los sistemas *on premise* suelen hacerse grandes inversiones a la hora de desplegar un sistema que deben ser rentabilizadas antes de realizar cambios profundos. Esto impide, en ocasiones, realizar adaptaciones dinámicas e incluso obliga a depender de sistemas *legacy* considerados ineficientes o inseguros.
3. No obstante, las organizaciones usuarias de esos servicios en la nube, precisamente por externalizar en terceros su información, deben adoptar una serie de precauciones: en el diseño, la contratación, configuración, uso de la prestación, así como, una vez finalizado el servicio externalizado, en la garantía de devolución y

supresión segura de la información que estaba almacenada en la infraestructura del CSP.

4. Este cambio de paradigma trae asociados cambios en el diseño de las arquitecturas de seguridad que protegen los activos de los usuarios, especialmente si se trata de Información Clasificada. Los cambios estarán basados en:
 - a) **Modificación del perímetro.** Uno de los pilares fundamentales de las arquitecturas de seguridad de sistemas *on premise* es la protección del perímetro y de los flujos de información intercambiados, especialmente en el ámbito de los sistemas clasificados. En este nuevo paradigma, el perímetro se amplía y se desdibuja hasta tal punto que es prácticamente imposible delimitarlo, por lo que la protección debe aplicarse en el propio dato. Esto no quiere decir, ni mucho menos, que el perímetro haya dejado de protegerse o puedan relajarse dichas medidas de protección, únicamente que el perímetro pasará a ser el propio dato cuando no pueda determinarse otro mayor. Es lo que hoy se conoce como el paradigma de Seguridad Centrada en el Dato o *Data Centric Security*, del cual los servicios en la nube son un caso particular.
 - b) **Pérdida de gobierno del dato.** En los sistemas *on premise*, el propietario del Sistema y de la información suele ser el mismo, por lo tanto, es el único responsable de proteger su información. En los servicios en la nube, el acceso y la custodia de dicha información podría delegarse en un tercero. En estos casos, será necesario analizar qué tipo de información y en qué condiciones es posible realizar esta delegación. Este aspecto adquiere especial relevancia en el ámbito de la información clasificada.
 - c) **Aislamiento de datos.** La tenencia múltiple y la compartición de recursos son características frecuentes de la computación en la nube. Esto incrementa el riesgo de divulgación no autorizada de información por fallos de separación en el almacenamiento, la memoria, el enrutamiento, etc.
5. Por otro lado, surge la problemática de que cada CSP tiene unas condiciones propias para dar los servicios en nube lo que afecta en los siguientes ámbitos:
 - a) **Jurídico:** La nacionalidad jurídica y el domicilio social de la entidad corporativa detrás del CSP define la jurisdicción aplicable a dicho CSP, que a su vez conforma el marco u ordenamiento jurídico al que atenerse, llegando incluso a poder ser de aplicación múltiples marcos jurídicos de forma simultánea.
 - b) **Arquitectura TIC:** Cada CSP implementa una arquitectura propia para proporcionar los servicios de nube e incluso el núcleo de dicha arquitectura TIC puede estar basado en tecnología propietaria del CSP y ser de su uso exclusivo. Otra dificultad añadida es que, con frecuencia, el propio perímetro del plano de control / gestión del CSP es global desde el punto de vista geográfico y, en consecuencia, del personal.
 - c) **Personal de administración:** En aquellos CSP con alta dispersión geográfica de sus centros de datos y que ofrecen economías de escala, el personal para

la administración TIC suele estar también distribuido geográficamente y puede tener una alta rotación, es decir, la identidad de los administradores se diluye y trasciende fronteras físicas y jurídicas.

6. Todo esto supone afrontar unos riesgos propios de los sistemas en la nube que son diferentes a los que corresponderían a cualquier sistema TIC en modo local (*on premise*) que será necesario controlar para garantizar la seguridad de los sistemas y de los datos alojados, en todas sus dimensiones.
7. En el caso de los sistemas que manejan información clasificada, se añade la problemática de transponer las medidas o requisitos de seguridad concretos de los sistemas clásicos a un sistema que esté alojado en la nube. Para ello, se hace necesario definir qué medidas de seguridad, organizativas y técnicas, debe implementar el CSP y cuales son responsabilidad del CSC.

2. OBJETO Y ALCANCE

8. Este documento tiene como objetivo definir los requisitos de seguridad que deben cumplir tanto el CSC como el CSP para que el sistema de información en la nube sea acreditable para manejar información clasificada hasta el grado de DIFUSIÓN LIMITADA.
9. Para la definición de estos requisitos de seguridad se han tenido en cuenta los exigidos para sistemas bajo el alcance del ENS de categoría ALTA, además de la de los establecidos en la D32 de la OTAN: *Technical and Implementation Directive for the Protection of NATO Information within Public Cloud-Based Communication and Information Systems*, de 19 de marzo de 2024.
10. La referencia para la implementación de dichos requisitos, tanto del CSC como del CSP, se articulará a través de Normas, Procedimientos, Instrucciones técnicas y cláusulas contractuales.
11. Así mismo, para la elaboración de este documento se han realizado dos asunciones:
 - a) Solamente intervienen dos actores: cliente (CSC) y proveedor (CSP). El primero es el organismo que consume el servicio y el segundo el que lo ofrece, total o parcialmente. En caso de existir más actores deberá analizarse hasta donde alcanzan las responsabilidades en toda la cadena de suministros.
 - b) El CSP y el CSC no pertenecen a la misma organización. Esto implica que el Responsable del Sistema (RSIS) formado por la infraestructura subyacente y el de cada sistema alojado en esa nube son diferentes.

3. CONCEPTOS CLAVE

12. **Responsabilidad compartida en la nube.** Es un principio fundamental que define claramente qué aspectos de la seguridad son gestionados por el CSP y cuáles son responsabilidad del CSC, garantizando así la protección de todos los recursos.
- a) **Seguridad del CSP.** Seguridad de los servicios que el CSP provee al cliente, así como aquellos acuerdos contractuales y de nivel de servicio que establezca con cada CSC. Incluye la seguridad de la infraestructura desde la que se prestan los citados servicios.
 - b) **Seguridad del CSC.** Seguridad de los servicios que el CSC despliega sobre la nube que no son propietarios del CSP, así como las configuraciones que realiza, en base a sus capacidades, dependiendo de las posibilidades del servicio que haya contratado.
13. El modelo de responsabilidad compartida entre CSP y CSC es transversal a todos los modelos de servicio en nube (IaaS, SaaS, PaaS, etc). Para ejemplarizar esta distribución de responsabilidades se detalla el modelo de servicio IaaS, pudiendo establecerse modificaciones para el resto de modelos de servicio.
14. **Responsabilidades del CSP en un modelo de servicio IaaS.** El CSP proporciona los componentes de infraestructura esenciales como servidores, almacenamiento, redes y virtualización. Las responsabilidades principales del CSP incluyen:
- a) **Seguridad Física:** El CSP es responsable de la seguridad física de los centros de datos que albergan la infraestructura, incluyendo el control de acceso a las instalaciones, sistemas de refrigeración, fuentes de energía, etc.
 - b) **Red y Virtualización:** Esto incluye la protección de las capas de red y virtualización que permiten la creación y ejecución de máquinas virtuales, así como de otros recursos de infraestructura. Aunque la configuración es responsabilidad del CSC, el CSP asegura que las conexiones de red y los hipervisores estén debidamente actualizados y protegidos contra vulnerabilidades.
 - c) **Hardware:** El CSP gestiona y asegura el hardware subyacente (servidores, almacenamiento, dispositivos de red, etc.), incluyendo las actualizaciones del hipervisor y del SO del host (no el de la VM), firmware del hardware físico e infraestructura de red física.
 - d) **Monitorización y Respuesta a Incidentes:** El CSP debe implementar herramientas de monitorización para supervisar el rendimiento y la seguridad de los sistemas subyacentes que proporcionan los servicios en la nube, y estar preparado para responder a incidentes de seguridad que afecten a sus sistemas coordinándose principalmente con las autoridades competentes y, si fuese necesario, con los CSC, aunque en la mayor parte de las veces únicamente se requerirá notificar al cliente.
15. **Responsabilidades del CSC en un modelo de servicio IaaS.** El cliente del servicio en la nube, por otro lado, es responsable de la configuración y gestión de los recursos

y aplicaciones que se ejecutan sobre los servicios y la infraestructura proporcionada por el CSP, así como la configuración para la protección de sus datos. Las principales responsabilidades del CSC incluyen:

- a) **Gestión de Sistemas Operativos:** Aunque el CSP proporciona el mecanismo de aprovisionamiento de máquinas virtuales, el CSC es responsable de configurar y mantener el sistema operativo (SO) de esas máquinas virtuales, incluyendo su bastionado. La gestión de parches y actualizaciones de seguridad será compartida.
 - b) **Configuración de Red y Seguridad:** El CSC debe configurar las reglas de firewall, gestionar las subredes y asegurarse de que la configuración de red sea segura y adecuada para sus aplicaciones. Esto también incluye la gestión de VPNs, balanceadores de carga y otros componentes de red según el entorno operativo.
 - c) **Gestión de Aplicaciones y Datos:** Todas las aplicaciones, bases de datos y datos que el CSC despliega sobre la infraestructura como servicio (IaaS) del CSP son de su exclusiva responsabilidad. Esto incluye la configuración, mantenimiento, cifrado y otros aspectos de seguridad, copias de configuraciones, aplicaciones y datos, incluida su posible restauración.
 - d) **Gestión de Identidades y Accesos (IAM):** El CSC debe gestionar las identidades de los usuarios y sus permisos de acceso a los recursos en la nube, utilizando servicios como IAM para definir políticas de acceso y autenticación.
 - e) **Monitorización y Respuesta a Incidentes:** El CSC debe implementar herramientas de monitorización para supervisar el rendimiento y la seguridad de los sistemas bajo su responsabilidad que ejecuta en la nube, y estar preparado para responder a incidentes de seguridad que afecten a sus aplicaciones o datos. Estará asimismo pendiente de la información sobre eventos que le facilite de forma automática el CSP en relación a los elementos de infraestructura subyacente que puedan llegar a afectarle.
16. **Certificación de un sistema de información en la nube.** Es el proceso de auditoría, realizado por una entidad habilitada, mediante el cual se verifica que el sistema de información de la nube cumple con los requisitos de seguridad técnicos, organizativos y procedimentales mínimos establecidos para alojar sistemas de información con garantía.
17. **Productos de seguridad (En inglés, *Security Enforcement Products - SEP*).** Son aquellos productos que forman parte de la arquitectura de seguridad del sistema de información, entendiendo como arquitectura de seguridad aquella cuyo objeto es la protección de la seguridad de los activos del sistema.
18. **Servicios de seguridad (En inglés, *Security Enforcement Services - SES*).** Son aquellos servicios en la nube que forman parte de la arquitectura de seguridad del sistema de información, entendiendo como arquitectura de seguridad aquella cuyo objeto es la protección de la seguridad de los activos del sistema.

19. **Aprobación de SES.** La aprobación de un SES es el proceso mediante el cual se verifica que el servicio de seguridad cumple los requisitos de seguridad necesarios para su uso en sistemas que manejan información clasificada.
20. **Acreditación de un sistema de información en la nube.** Es el proceso de auditoría mediante el cual se verifica que el sistema de información de la nube cumple con los requisitos de seguridad técnicos, organizativos y procedimentales mínimos para alojar sistemas de información que manejan información clasificada. Dichas medidas dependerán, entre otras cosas, del nivel de clasificación de la información que vaya a manejar. La responsabilidad de realizar dichas auditorías recae en la Autoridad de Acreditación Nacional correspondiente.

4. ORGANIZACIÓN DE LA SEGURIDAD: ROLES Y RESPONSABILIDADES

21. Un elemento clave en relación con los sistemas que manejan información clasificada es el conocimiento de las autoridades de acreditación y sus competencias, junto a la propia determinación de los roles y responsabilidades relacionados con la gobernanza de la ciberseguridad de estos sistemas a lo largo de su ciclo de vida (determinación de la necesidad, diseño, desarrollo, implantación, operación, mantenimiento y retirada).
22. Para preservar la ciberseguridad de la información, dichos roles tendrán en cuenta los requisitos de seguridad de las TIC a implementar y supervisar en las diferentes fases del ciclo de vida, debiendo constar y estar presentes en la documentación de seguridad del sistema.
23. Para un mayor detalle, se atenderá especialmente a lo dispuesto en la guía *CCN-STIC 201 ORGANIZACIÓN Y GESTIÓN PARA LA SEGURIDAD DE LAS TIC*, armonizándola con la guía *CCN-STIC 801 ENS Responsabilidades y Funciones*, a efectos de no duplicar roles y/o comités.
24. **Autoridad de Acreditación (AA):** Es la autoridad responsable de conceder la autorización a un determinado sistema para manejar información clasificada hasta un grado determinado o en unas determinadas condiciones de seguridad, con arreglo a su concepto de operación (CO).
25. **Acreditación de un sistema que maneja información clasificada:** La acreditación tiene en cuenta múltiples aspectos, cuya competencia en su evaluación es delegada por el Secretario de Estado Director del Centro Nacional de Inteligencia (CNI) cuyo órgano de trabajo en lo referente a la protección de información clasificada es la Oficina Nacional de Seguridad (ONS), en las siguientes entidades:
 - a) La **ONS** evalúa directamente la seguridad del entorno de operación, con afectación a personas e instalaciones físicas, además de la seguridad documental.
 - b) El **CCN-PYTEC**, adscrito al Centro Criptológico Nacional, evalúa directamente la seguridad de las emanaciones electromagnéticas según normativa TEMPEST en base a la guía *CCN-STIC 210 Norma de Seguridad en las Emanaciones (DL)*.
 - c) El **CCN-PYTEC**, adscrito al Centro Criptológico Nacional, evalúa directamente la seguridad criptológica como Autoridad de Certificación Criptológica (ACC).
 - d) El **CCN**, evalúa directamente la inspección de Seguridad de las TIC, aunque puede delegar su materialización en organizaciones a las que acredite como Entidades Inspectoras STIC (EI-STIC), delegación únicamente posible para sistemas que manejan información clasificada hasta el grado DIFUSIÓN LIMITADA, o equivalente.
26. **Certificación de la Conformidad con el ENS:** La Certificación de la Conformidad con el ENS puede realizarla una Entidad de Certificación (EC) del sector privado, un Órgano de Auditoría Técnica (OAT) del Sector Público, o directamente el CCN en casos especiales. Una EC o un OAT pueden llegar a acreditarse para actuar

simultáneamente como EI-STIC, realizando inspecciones STIC a sistemas que manejan información clasificada del grado DL, o equivalente, a la vez que certificaciones de la conformidad con el ENS.

27. **Gobierno de la ciberseguridad en la organización (Roles y Comités):** La organización que tiene acreditado un sistema de información para manejar información clasificada, o pretende acreditarlo, debe disponer de los siguientes roles y comités:

- a) **Propietario de la Información / Responsable de su custodia / Depositario:** El originador de la información es quién define quien ostenta la propiedad inicial de la información clasificada. El propietario de la información es el que define su clasificación y las reglas por las que se debe regir su manejo. La información clasificada siempre estará asignada a un responsable de su custodia, el cual podrá variar a lo largo del tiempo. Cuando el custodio sea también quién almacena la información podrá designarse como depositario. Puede equipararse con el Responsable de la Información (RINFO) del ENS, el cual en numerosas ocasiones se hace coincidir con el Responsable del Servicio (RSERV) también del ENS.
- b) **Responsable de Seguridad de las TIC (CISO),** equiparable al Responsable de Seguridad del ENS (RSEG). Ambos roles pueden converger en la misma persona física.
- c) **Responsable de Seguridad Física (RSF),** asumiendo este rol la responsabilidad sobre la seguridad física de la organización, pudiendo designarse más de uno en organizaciones con Zonas Administrativas de Protección (ZAP) o Zonas de Acceso Restringido (ZAR) en emplazamientos distribuidos geográficamente; en ese caso, se nombrará un coordinador de entre todos ellos.
- d) **Autoridad de Control del material de Cifra (ACMC),** figura que se encarga del registro, contabilidad y seguimiento de todo el material de cifra cuando se emplea éste para la protección de información clasificada. Se apoya habitualmente en algún órgano de Distribución de Material de Cifra (ODMC) y en un Criptocustodio.
- e) **Responsable del Sistema (RSIS),** figura entre cuyas funciones está la del diseño de la topología del sistema, su desarrollo, operación y mantenimiento durante su ciclo de vida. Es equiparable al rol del mismo nombre en el ENS.
- f) **Comité de Seguridad TIC (CSEGTIC),** constituido como un órgano colegiado, varios de sus miembros ostentarán los roles especializados dentro de la organización de la seguridad que se han definido en este punto de la política. Es equiparable al Comité de Seguridad de la Información (COMSEG) del ENS. Habitualmente sus integrantes son el RSF, el CISO, el RSIS, la ACMC si procede, el representante del propietario o depositario de la información clasificada (jefe de seguridad del órgano de control o responsable de seguridad de la empresa en el registro de difusión limitada), etc. Puede constituirse en base a determinados miembros fijos y otros opcionales, en función de los temas a tratar en sus reuniones.

5. ESTRATEGIA DE ACREDITACIÓN DE SISTEMAS DL EN NUBE PÚBLICA

28. Un sistema de información en la nube acreditado para manejar información DL o equivalente deberá pasar por tres procesos:

- a) **Certificación del CSP:** El sistema de información del CSP sobre el que el CSC desplegará su servicio deberá contar con una Certificación de conformidad con el ENS en categoría ALTA que, además, incluya todos aquellos servicios del CSP que utiliza el CSC.
- b) **Aprobación de SES y SEP:** Los productos y servicios que proporcionan seguridad en el sistema final deberán estar **aprobados para manejar información DIFUSIÓN LIMITADA** o equivalente e incluidos en el listado de productos y servicios aprobados del **CPSTIC** (guía *CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación*). Se prestará especial atención a los medios de cifra y a los elementos de protección de perímetro que garantizan la separación entre dominios de seguridad.

El listado de SES y SEP que deben estar aprobados incluirá, como mínimo, todos aquellos servicios cuya funcionalidad principal es la seguridad, pero no está limitado a ellos. Por ejemplo, en un modelo de nube en el que el CSP y los CSC tienen distintos propietarios y en el que, además, pueden compartir hardware distintos CSC, el hipervisor se convierte en un elemento clave desde el punto de vista de la seguridad, dado que garantiza la separación y el aislamiento entre los sistemas de los CSC alojados en la infraestructura física subyacente del CSP. Por ello deberá ser considerado un SES y superar un proceso de aprobación.

- c) **Acreditación de Seguridad:** El sistema de información compuesto por el CSP+CSC que ofrece el servicio final deberá haber superado un proceso de acreditación de seguridad para DL. Por lo tanto, en este tipo de escenarios se contemplará el cumplimiento de requisitos por parte de la organización responsable de la información clasificada (el CSC), así como la evidencia de que cumple los suyos el proveedor donde se externaliza (el CSP). En el caso concreto de DL, para la acreditación de seguridad se exigirá:
 - a. Certificación de Conformidad con el ENS en categoría ALTA. El propio Real Decreto del ENS, en su artículo 2.2 señala: *“Asimismo, sin perjuicio de la aplicación de la Ley 9/1968, de 5 de abril, de Secretos Oficiales y otra normativa especial, este real decreto será de aplicación a los sistemas que tratan información clasificada, pudiendo resultar necesario adoptar medidas complementarias de seguridad, específicas para dichos sistemas, derivadas de los compromisos internacionales contraídos por España o de su pertenencia a organismos o foros internacionales”*, serán de aplicación a los sistemas que manejan información clasificada las medidas, requisitos y refuerzos de seguridad del Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, para sistemas de categoría ALTA.

El CSP debe considerar el nivel ALTO en las cinco dimensiones de la seguridad que contempla el ENS. Para elaborar la Declaración de Aplicabilidad, se tendrán en cuenta algunas diferencias en función de si la organización es un CSP o un CSC.

- b. Cumplimiento de requisitos específicos necesarios para sistemas que manejan información clasificada del grado DL, o equivalente, que se detallan en otros apartados de este documento. Para la definición de dichos requisitos se han tenido en cuenta los criterios definidos en la normativa OTAN en general y más concretamente los definidos en la norma AC/322-D(2019)0032-REV2 (INV) NATO Cloud Computing Directive, concretada en el documento *Technical and Implementation Directive for the Protection of NATO Information within Public Cloud-Based Communication and Information Systems*, del 19 de marzo de 2024.
29. Por último, en lo relativo a las interconexiones en la nube, es importante tener en cuenta que el CSP proporciona al CSC la infraestructura de red subyacente, así como herramientas y servicios de comunicaciones para que sus usuarios establezcan conexiones seguras. El CSC, por su parte, es responsable de configurar y gestionar de manera segura sus propias redes virtuales y asegurarse de que todas las comunicaciones que involucren sus datos y aplicaciones en la nube estén debidamente protegidas. Ambos deben trabajar en conjunto para garantizar que las comunicaciones en la nube sean seguras y confiables.
30. A efectos de acreditación de interconexiones:
- a) Si los clientes se gestionan y conectan en exclusiva al sistema desplegado por el propio CSC en la nube, se consideran parte del mismo, no existirá una interconexión y, por tanto, su acreditación se acometerá de forma conjunta.
 - b) Si, por el contrario, los usuarios del CSC forman parte de una red o sistema diferenciado, se considerará que existe una interconexión entre ambos sistemas y se tendría que acometer la acreditación de cada sistema de forma separada para, posteriormente, acreditar la interconexión de ambos.

6. MEDIDAS DE SEGURIDAD PARA NUBE DL

31. Con independencia del detalle de las medidas de seguridad, que pueden consultarse en un documento anexo, vinculado a esta política que recoge las directrices para elaborar la Declaración de Aplicabilidad, se concretan en este apartado algunos conceptos relevantes. No obstante, se dispone de la guía *CCN-STIC 001 SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES QUE MANEJAN INFORMACIÓN CLASIFICADA EN LA ADMINISTRACIÓN*, que contiene la política de seguridad para cualquier sistema que maneje información clasificada, con independencia de su grado de clasificación y de su posible externalización en un CSP, o no, incluyendo múltiples consideraciones generales de seguridad.
32. **Medidas y requisitos de seguridad:** Las medidas y requisitos de seguridad que recoge esta política son de aplicación sin perjuicio de las que están recogidas en la guía *CCN-STIC 499 Arquitectura de seguridad para servicios en la nube*, que define el modelo de arquitectura y medidas de seguridad adecuadas para proteger los servicios externalizados en la nube. Debe considerarse que cualquier marco de seguridad, corresponde a los mínimos exigibles, debiendo cada organización potenciarlos en base al riesgo o en base a otra normativa asimismo de obligado cumplimiento.

6.1 SEGURIDAD PERSONAL

33. El personal con rol de administrador de seguridad o del sistema del CSC debe disponer de la Habilitación Personal de Seguridad (**HPS**) de grado de clasificación Reservado o superior.
34. No se requerirá HPS al personal del sistema del CSP siempre y cuando pueda demostrar mediante auditorías de cumplimiento continuas e independientes que cumplen las siguientes medidas:
 - a) Todo individuo que desarrolle funciones de administrador de sistemas como parte del CSP será limitado sistemática y procedimentalmente de tal forma que no podrá impactar en la confidencialidad y la integridad de la información manejada por el sistema TIC. Estas limitaciones incluirán:
 - Acceso físico controlado y limitado a los centros de datos donde se maneja la información DL.
 - Acceso acotado temporalmente a los recursos del sistema TIC que maneja información DL.
 - Acceso acotado en alcance a los recursos del sistema TIC que maneja información DL.
 - Asignación automática controlada por API de tareas administrativas al personal del CSP.

- Imposibilidad o baja probabilidad de localizar física o electrónicamente información DL en la provisión del servicio de nube pública.
 - Segregación de responsabilidades estricta y finamente graduada entre las diferentes funciones asignadas al personal del CSP para reducir el riesgo de colusión.
- b) Cualquier personal contratado por el CSP que pueda ser consciente de la presencia de un sistema TIC que maneja información DL en regiones específicas de su provisión de servicio cloud público deberá ser objeto de un Non-Disclosure Agreements (NDAs) y deberá operar en el contexto de un contrato clasificado con el CSC.
35. Todo el personal del CSP será objeto de una comprobación de antecedentes apoyado por el cuerpo de seguridad pertinente.

6.2 SEGURIDAD FÍSICA

36. Las zonas del CSP que almacenen componentes de red, de sistemas o criptográficos que manejen información DL o equivalente deberán estar controladas y securizadas con medidas equivalentes a una Zona de Acceso Restringido (ZAR). El acceso a esas áreas deberá estar limitado a personal autorizado designado oficialmente para realizar funciones de administración de seguridad o de red/sistema.

6.3 SEGURIDAD DE LA INFORMACIÓN

37. Con la implementación de las medidas descritas anteriormente, el personal del CSP no podrá acceder a los datos del CSC. Por lo tanto, la responsabilidad de clasificar y etiquetar la información clasificada en nube pública para sistemas TIC basados en la nube recae sobre los usuarios autorizados a generar y acceder a dicha información.
38. Con objeto de preservar la soberanía, todos los sistemas que manejen información clasificada nacional deberán cumplir los siguientes requisitos:
- a) Estarán sometidos exclusivamente a la jurisdicción española.
 - b) Estarán localizados en territorio nacional.
 - c) En el caso de sistemas que manejen **exclusivamente** información clasificada de otros ámbitos (OTAN, UE, etc.) deberán cumplirse las restricciones de sometimiento jurisdiccional impuestas por la normativa que sea de aplicación.
39. **Ubicación geográfica:** El CSP debe proporcionar al CSC información relativa a la ubicación geográfica de su información (datos, *logs*, *backups*, etc...), especialmente de la clasificada del grado DIFUSIÓN LIMITADA, o equivalente, que en todo caso deberá estar ubicada en **sistemas acreditados o aprobados por la autoridad correspondiente**.
40. **Gestión y administración de sistemas:** Las medidas de seguridad para la gestión de sistemas serán aplicables tanto al CSP como al CSC:

- a) **El plano de control** de la nube (a nivel de CSP) y del sistema virtualizado alojado en la misma (a nivel de CSC) **no debe trascender a los propios sistemas acreditados**, es decir, no serán accesibles desde otras ubicaciones físicas o por personal ajeno o sin las debidas autorizaciones / habilitaciones de seguridad.
 - b) Los sistemas o equipos desde los que un usuario administrador administra el servicio y/o los sistemas, deberán estar acreditados al mismo nivel de clasificación que el sistema que administran. Estos sistemas deberán estar alojados en **zonas de seguridad (ZAP o ZAR)**
41. **Separación entre diferentes CSC:** Cuando se vaya a manejar información clasificada del grado DIFUSIÓN LIMITADA, o equivalente, en la infraestructura del CSP se admitirá contemplar tanto una separación física como lógica, mientras ésta sea segura. Es decir, se podrá compartir *hardware* en aquellos casos en los que exista una separación virtual que garantice la estanqueidad entre sistemas de los diferentes CSC, y todos los elementos hardware estén en zonas de seguridad (ZAP o ZAR).

7. DECLARACIÓN DE APLICABILIDAD VINCULADA

36. La Declaración de Aplicabilidad asociada a esta política, se ha elaborado como anexo a la misma en la guía *CCN-STIC 004 Anexo I Declaración de Aplicabilidad*.

8. DEFINICIONES

Información Roja	Información clasificada y que, por lo tanto, requiere protección de acuerdo a la Normativa Protección de Información Clasificada generada por la Oficina Nacional de Seguridad (ONS).
Información Negra	Información no clasificada o información clasificada que ha sido cifrada con mecanismos de cifra aprobados por la autoridad competente y que, por lo tanto, puede protegerse con los mismos medios que la información no clasificada.
Información sensible	Información que demanda un alto nivel de seguridad en alguna de sus dimensiones.
Información Clasificada	Asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas puedan dañar o poner en riesgo la seguridad y defensa del Estado.
Ámbito de seguridad	Ámbito de origen al que pertenece la información, es decir, la organización o nación propietaria de la información clasificada a la que puede tener acceso, si es necesario. Por ejemplo: OTAN, UE o NACIONAL.
Nivel de seguridad	Máximo grado de la información clasificada dentro de un mismo ámbito de seguridad.
Dominio de seguridad	Colección de activos, uniformemente protegidos, habitualmente bajo una única autoridad. Suelen corresponder a un mismo ámbito y nivel de seguridad.
Nube privada virtual	Una nube privada virtual (VPC) es una versión virtual de una red física, implementada dentro de la red del CSP.

9. REFERENCIAS

- [1] AC/322(CP/4)WP(2021)0003-REV2 DRAFT Technical and Implementation Directive for the Protection of NATO Information within Public Cloud-Based Communication and Information Systems (CIS).
- [2] CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC).
- [3] CCN-STIC-498 Arquitectura mulidominio de Puesto de Trabajo (Endpoint Seguro).
- [4] CCN-STIC-807 Criptología de empleo en el Esquema Nacional de Seguridad.
- [5] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- [6] CCN-STIC 302 Interconexión de Sistemas TIC que manejan Información nacional clasificada en la administración, Julio 2012.
- [7] CCN-STIC-301 Medidas de Seguridad de las TIC a implementar en Sistemas Clasificados, Mayo 2020 [desplazada por el ENS categoría ALTA (RD 311/2022)]
- [8] CCN-STIC-001 Política de Seguridad de las TIC, Junio 2016.
- [9] CCN-STIC-305 Destrucción y Sanitización de soportes informáticos, Mayo 2017.

10.ABREVIATURAS

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación
CSC	<i>Cloud Service Customer</i>
CSP	<i>Cloud Service Provider</i>
DLP	<i>Data Loss Prevention</i>
ENECSTI	Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información
ENS	Esquema Nacional de Seguridad
HPS	Habilitación Personal de Seguridad
HSM	<i>Hardware Security Modules</i>
HTTPS	<i>Hypertext Transfer Protocol Secure</i>
IaaS	<i>Infrastructure as a Service</i>
KMS	<i>Key Management System</i>
MV	Máquina Virtual
ONS	Oficina Nacional de Seguridad
PaaS	<i>Platform as a Service</i>
PES	Procedimiento de Empleo Seguro
RPO	<i>Recovery Point Objective</i> (Objetivo punto de recuperación)
RSIS	Responsable del Sistema
RTO	<i>Recovery Time Objective</i> (Objetivo tiempo de recuperación)
SaaS	<i>Software as a Service</i>
SDN	<i>Software Defined Network</i>
SLA	Acuerdo de servicio
SO	Sistema Operativo
STIC	Seguridad de las Tecnologías de la Información y la Comunicación
TIC	Tecnologías de la Información y la Comunicación
TLS	<i>Transport Layer Security</i>
VM	<i>Virtual Machine</i>
VPN	<i>Virtual Private Network</i>