Política de Seguridad de las TIC
CCN-STIC 004

Manejo de información con clasificación Difusión Limitada, o equivalente, en nube pública (Anexo I: Declaración de Aplicabilidad)

Febrero 2026

Edita:

centro criptológico nacional

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2026.02.09 16:58:39 +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

ÍNDICE

1. INTRODUCCIÓN

36. Como es sabido, la Declaración de Aplicabilidad (DA, o SOA en inglés) comprende el conjunto de medidas de seguridad que son de aplicación en un sistema de información concreto. Tal conjunto de medidas dependerá, en el caso del ENS, de la categoría del sistema y de los niveles asociados a las cinco dimensiones de la seguridad.
37. El ENS aplica a todos los sistemas que manejan información clasificada, incluyendo los del grado DIFUSION LIMITADA, o equivalente, según dispone el artículo 2.2 Ámbito de aplicación del RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que 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*".
38. En el **Anexo II del RD 311/2022**, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, se tiene en cuenta para cada medida de seguridad, no únicamente la aplicabilidad de requisitos base, sino la de posibles refuerzos obligatorios.
39. Se ha determinado así, que para externalizar en la nube pública un sistema que maneje información clasificada del grado DIFUSIÓN LIMITADA, o equivalente, tanto el sistema de información del CSC que se externaliza en el CSP, como el del propio CSP necesario para soportar los servicios prestados como proveedor, ambos deben cumplir una serie de medidas y requisitos de seguridad, que se simplifican equiparándolos a los determinados de forma estándar para cumplir con el ENS de categoría ALTA, aunque en función de tratarse del CSP o del CSC habrá algunas medidas que no serán de aplicación considerando estrictamente el ámbito de la nube.
40. Complementariamente, se requieren una serie de requisitos adicionales que se detallan en el apartado 7 REQUISITOS ADICIONALES Y CRITERIOS DE APLICACIÓN, que se deberán aplicar algunos de ellos diferenciando CSP y CSC, de forma que estén armonizados, como ya se ha dicho, con 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*, de 19 de marzo de 2024.
41. Estos requisitos adicionales se contextualizan, junto a su criterio de aplicación, referenciados de color azul para determinadas medidas de seguridad en las tablas de este apartado.

Medidas de Seguridad		Dim. de seguridad afectadas	CSP (Proveedor Nube)	Ref.	CSC (Cliente Nube)	Ref.
org	**Marco organizativo**					
org.1	Política de seguridad	Todas	aplica	2.1	aplica	2.1
org.2	Normativa de seguridad	Todas	aplica	2.2	aplica	2.2
org.3	Procedimientos de seguridad	Todas	aplica		aplica	
org.4	Proceso de autorización	Todas	aplica		aplica	
op	**Marco operacional**					
op.pl	Planificación					
op.pl.1	Análisis de riesgos	Todas	+ R2		+ R2	
op.pl.2	Arquitectura de Seguridad	Todas	+ R1 + R2 + R3	2.3	+ R1 + R2 + R3	2.3
op.pl.3	Adquisición de nuevos componentes	Todas	aplica		aplica	
op.pl.4	Dimensionamiento/gestión de la capacidad	D	+ R1		+ R1	
op.pl.5	Componentes certificados	Todas	aplica	2.4	aplica	2.4
op.acc	Control de acceso					
op.acc.1	Identificación	T A	+ R1		+ R1	
op.acc.2	Requisitos de acceso	C I T A	+ R1		+ R1	
op.acc.3	Segregación de funciones y tareas	C I T A	+ R1		+ R1	
op.acc.4	Proceso de gestión de derechos de acceso	C I T A	aplica		aplica	2.5
op.acc.5	Mecanismo autenticación (usr. externos)	C I T A	+ [R2 o R3 o R4] + R5		+ [R2 o R3 o R4] + R5	
op.acc.6	Mecanismo autenticación (usr. organización)	C I T A	+ [R1oR2oR3oR4] +R5+R6+R7+R8+R9		+ [R1oR2oR3oR4] +R5+R6+R7+R8+R9	2.6
op.exp	Explotación					
op.exp.1	Inventario de activos	Todas	aplica		aplica	2.7
op.exp.2	Configuración de seguridad	Todas	aplica		aplica	
op.exp.3	Gestión de la configuración de seguridad	Todas	+ R1 + R2 + R3		+ R1 + R2 + R3	
op.exp.4	Mantenimiento y actualizaciones de seguridad	Todas	+ R1 + R2		+ R1 + R2	
op.exp.5	Gestión de cambios	Todas	+ R1		+ R1	
op.exp.6	Protección frente a código dañino	Todas	+ R1 + R2 + R3 + R4		+ R1 + R2 + R3 + R4	
op.exp.7	Gestión de incidentes	Todas	+ R1 + R2 + R3	2.8	+ R1 + R2 + R3	2.8
op.exp.8	Registro de la actividad	Todas	+ R1 + R2 + R3 + R4 + R5		+ R1 + R2 + R3 + R4 + R5	
op.exp.9	Registro de la gestión de incidentes	Todas	aplica		aplica	
op.exp.10	Protección de claves criptográficas	Todas	+ R1	2.9	+ R1	2.9
op.ext	Recursos externos					
op.ext.1	Contratación y acuerdos de nivel de servicio	Todas	aplica	2.10	aplica	2.10
op.ext.2	Gestión diaria	Todas	aplica		aplica	
op.ext.3	Protección de la cadena de suministro	Todas	aplica	2.11	aplica	
op.ext.4	Interconexión de sistemas	Todas	+ R1		+ R1	
op.nub	Servicio en la nube					
op.nub.1	Protección de servicios en la nube	Todas	+ R1 + R2	2.12	+ R1 + R2	712

op.cont	Continuidad del servicio					
op.cont.1	Análisis de impacto	D	aplica		aplica	
op.cont.2	Plan de continuidad	D	Aplica + R1		n/a (*)	2.3
op.cont.3	Pruebas periódicas	D	aplica		n/a (*)	2.13
op.cont.4	Medios alternativos	D	aplica		n/a (*)	2.13
op.mon	Monitorización del sistema					
op.mon.1	Detección de intrusión	Todas	+ R1 + R2		+ R1 + R2	
op.mon.2	Sistema de métricas	Todas	+ R1 + R2		+ R1 + R2	
op.mon.3	Vigilancia	Todas	+ R1 + R2 + R3 + R4 + R5 +R6	2.14	+ R1 + R2 + R3 + R4 + R5 +R6	2.14
mp	**Medidas de protección**					
mp.if	Protección de las instalaciones e infraestructuras					
mp.if.1	Áreas separadas y con control de acceso	Todas	aplica	2.15	n/a (*)	2.15
mp.if.2	Identificación de las personas	Todas	aplica	2.15	n/a	2.15
mp.if.3	Acondicionamiento de los locales	Todas	aplica		n/a	
mp.if.4	Energía eléctrica	D	+ R1		n/a	
mp.if.5	Protección frente a incendios	D	aplica		n/a	
mp.if.6	Protección frente a inundaciones	D	aplica		n/a	
mp.if.7	Registro de entrada y salida de equipamiento	Todas	aplica		n/a	
mp.per	Gestión del personal					
mp.per.1	Caracterización del puesto de trabajo	Todas	aplica		aplica	
mp.per.2	Deberes y obligaciones	Todas	+ R1	2.16	+ R1	2.16
mp.per.3	Concienciación	Todas	aplica		aplica	
mp.per.4	Formación	Todas	aplica	2.17	aplica	2.17
mp.eq	Protección de los equipos					
mp.eq.1	Puesto de trabajo despejado	Todas	+ R1		+ R1	
mp.eq.2	Bloqueo de puesto de trabajo	A	+ R1		+ R1	
mp.eq.3	Protección de dispositivos portátiles	Todas	+ R1 + R2	2.18	+ R1 + R2	2.18
mp.eq.4	Otros dispositivos conectados a la red	C	+ R1		+ R1	
mp.com	Protección de las comunicaciones					
mp.com.1	Perímetro seguro	Todas	aplica		aplica	
mp.com.2	Protección de la confidencialidad	C	+ R1 + R2 + R3		+ R1 + R2 + R3 + R5	
mp.com.3	Protección de la integridad y autenticidad	I A	+ R1 + R2 + R3 + R4		+ R1 + R2 + R3 + R4	
mp.com.4	Separación de flujos de información en la red	Todas	+ [R2 o R3] + R4		+ [R2 o R3] + R4	
mp.si.	Protección de los soportes de información					
mp.si.1	Marcado de soportes	C	aplica		n/a	2.19
mp.si.2	Criptografía	C I	+ R1 + R2		n/a	2.19
mp.si.3	Custodia	Todas	aplica		n/a	2.19
mp.si.4	Transporte	Todas	aplica		n/a	2.19
mp.si.5	Borrado y destrucción	C	+ R1		+ R1	
mp.sw	Protección de las aplicaciones informáticas					
mp.sw.1	Desarrollo de aplicaciones	Todas	+ R1 + R2 + R3 + R4 + R5	720	+ R1 + R2 + R3 + R4 + R5	720
mp.sw.2	Aceptación y puesta en servicio	Todas	+ R1		+ R1	

mp.info	Protección de la información					
mp.info.1	Datos personales	Todas	aplica		aplica	
mp.info.2	Calificación de la información	C	aplica		aplica	
mp.info.3	Firma electrónica	I A	+ R1 + R2 + R3 + R4		+ R1 + R2 + R3 + R4	
mp.info.4	Sellos de tiempo	T	aplica		aplica	
mp.info.5	Limpieza de documentos	C	aplica		aplica	
mp.info.6	Copias de seguridad	D	+ R1 + R2	2.21	+ R1 + R2	2.21
mp.s	Protección de los servicios					
mp.s.1	Protección del correo electrónico	Todas	aplica		aplica	
mp.s.2	Protección de servicios y aplicaciones web	Todas	+ R2 + R3		+ R2 + R3	
mp.s.3	Protección de la navegación web	Todas	+ R1		+ R1	
mp.s.4	Protección frente a denegación de servicio	D	+ R1		+ R1	

2.xx	Detalles del criterio de aplicación de la medida en el apartado 7 de este documento.
n/a	Se considera que la medida, salvo excepciones basadas en el riesgo y en el entorno de operación, no será de aplicación.

2. REQUISITOS ADICIONALES Y CRITERIOS DE APLICACIÓN

2.1 [org.1] Política de seguridad

42. En **[SM-GRC-08]** de **CD8 - Gobierno, Riesgo y Cumplimiento (GRC)** del documento referenciado de la OTAN, se determina que debe establecerse y mantenerse contacto con grupos de interés especiales relacionados con la nube y otras entidades relevantes de acuerdo con el contexto de la organización. Estos contactos son útiles, tanto al CSC como al CSP, para estar al día, entre otros, de aspectos de seguridad en la nube, como pueden ser tendencias, tácticas y técnicas de ataque, así como sus defensas especializadas.

43. Asimismo, en **[SM-SEF-08]** de **CD14 - Gestión de incidentes de seguridad, descubrimiento electrónico (e-Discovery) y análisis forense en la nube** del documento referenciado de la OTAN, se determina que deben mantenerse puntos de contacto para los grupos de interés aplicables, autoridades reguladoras, fuerzas de seguridad nacionales y locales y otras autoridades jurisdiccionales legales.

2.2 [org.2] Normativa de seguridad

44. En **[SM-GRC-04]** de **CD8 - Gobierno, Riesgo y Cumplimiento (GRC)** del documento referenciado de la OTAN, se determina que debe establecerse y seguirse un proceso de excepción, aprobado según lo exija el programa de gobernanza de la organización, siempre que se produzca una desviación de una política o norma establecida.

2.3 [op.pl.2] Arquitectura de seguridad

45. En **[SM-DSP-06]** de **CD7 - Gestión del ciclo de vida de la seguridad y privacidad de los datos** del referenciado documento de la OTAN, se determina, especialmente para el CSC, que debe documentarse el flujo de datos para identificar qué datos se procesan, almacenan o transmiten y dónde. Debe revisarse la documentación del flujo de datos a intervalos definidos, al menos una vez al año, y después de cualquier cambio.
46. En **[SM-DSP-19]** de **CD7 - Gestión del ciclo de vida de la seguridad y privacidad de los datos** del referenciado documento de la OTAN, se determina que deben definirse e implementarse procesos, procedimientos y medidas técnicas para especificar y documentar las ubicaciones físicas de los datos, incluidas las ubicaciones en las que se procesan o respaldan los datos.

2.4 [op.pl.5] Componentes certificados

47. Los productos y servicios ofrecidos por el CSP que proporcionan seguridad 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*).
48. Lo mismo ocurre con otros productos de seguridad que pueda emplear el CSC por su cuenta, ya sea en su infraestructura virtual albergada en el CSP o en sus propias instalaciones en modo local.
49. Un aspecto específico para determinados sistemas que manejan información clasificada es el refuerzo opcional R1 – Protección de emisiones electromagnéticas que determina que la información deberá ser protegida frente a las amenazas TEMPEST de acuerdo con la normativa en vigor. Se dispone de la guía guía *CCN-STIC 210 Norma de Seguridad en las Emanaciones (DL)*, siendo la Autoridad de Acreditación correspondiente quién determine su aplicabilidad, aunque especialmente corresponderá a aquellos sistemas que manejen información clasificada de los grados CONFIDENCIAL o superior.

2.5 [op.acc.4] Proceso de gestión de derechos de acceso

50. En **[SM-IAM-10]** de **CD10 - Gestión de Accesos e Identidades** del referenciado documento de la OTAN, se determina que debe definirse e implementarse, especialmente en el CSC, un proceso de acceso para garantizar que los roles y derechos de acceso privilegiado se otorguen por un período de tiempo limitado.
51. En **[SM-IAM-12]** de **CD10 - Gestión de Accesos e Identidades** del referenciado documento de la OTAN, se determina, especialmente para el CSC, que deben definirse, implementarse y evaluarse procesos, procedimientos y medidas técnicas para garantizar que la infraestructura de registro sea de solo lectura para todos aquellos que dispongan de acceso de escritura, incluidos los roles de acceso privilegiado, y que la capacidad de deshabilitarla se controle mediante un

procedimiento que garantice la segregación de funciones y procedimientos de emergencia.

2.6 [op.acc.6] Mecanismos autenticación (usuarios de la organización)

52. En **[SM-DCS-08]** de **CD6 - Seguridad del Centro de Proceso de Datos (CPD)** del referenciado documento de la OTAN, se determina que, especialmente para el CSC, adicionalmente debe utilizarse la identificación del equipo como método para la autenticación de la conexión.

2.7 [op.exp.1] Inventario de activos

53. En **[SM-DSP-03]** de **CD6 - Seguridad del Centro de Proceso de Datos (CPD)** del referenciado documento de la OTAN, especialmente para el CSC, se determina que adicionalmente debe crearse y mantenerse un inventario de datos, al menos para cualquier dato sensible o información personal; es decir, que la información clasificada debe estar inventariada.

2.8 [op.exp.7] Gestión de incidentes

54. Los sistemas que manejan información clasificada, deben ser mucho más estrictos respecto a la notificación de incidentes a la autoridad correspondiente que cualquier otro tipo de sistemas. En el caso de incidentes con peligrosidad ALTA, MUY ALTA y/o CRÍTICA es obligatoria la notificación urgente al CCN-CERT según los plazos establecidos, según se detalla en la guía *CCN-STIC 817 Gestión de Ciberincidentes*.
55. El **CCN-CERT**, como CERT Gubernamental Nacional, tiene responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de las Administraciones Públicas y de empresas y organizaciones de interés estratégico para el país. Por este motivo, proporcionará la respuesta a incidentes de seguridad en un segundo nivel.
56. En **[SM-SEF-06]** de **CD14 - Gestión de incidentes de seguridad, descubrimiento electrónico (e-Discovery) y análisis forense en la nube** del referenciado documento de la OTAN, se determina que deben clasificarse los eventos relacionados con la seguridad, empleando una taxonomía reconocida. En este sentido se propone la que consta en la precitada guía *CCN-STIC 817 ENS. Gestión de Ciberincidentes*.

2.9 [op.exp.10] Protección de claves criptográficas

57. En **[SM-CEK-02]** de **CD5 - Criptografía, cifrado y gestión de claves** del referenciado documento de la OTAN, se determina que deben definirse e implementarse roles y responsabilidades criptográficas, de cifrado y de gestión de claves. Asimismo, en **[SM-IAM-15]** de **CD10 - Gestión de Accesos e Identidades** del mismo documento, se determina que deben definirse, implementarse y evaluarse procesos, procedimientos y medidas técnicas para la gestión segura de contraseñas.

58. En **[SM-CEK-05]** de **CD5 - Criptografía, cifrado y gestión de claves** del referenciado documento de la OTAN, se determina que se empleará el procedimiento estándar de Gestión de Cambios (En el ENS [op.exp.5]) para la revisión, aprobación, implementación y comunicación de cambios en tecnologías criptográficas, de cifrado y de gestión de claves.
59. En **[SM-CEK-09]** de **CD5 - Criptografía, cifrado y gestión de claves** del referenciado documento de la OTAN, se determina que deben auditarse los sistemas, políticas y procesos de encriptación y administración de claves con una frecuencia proporcional a la exposición al riesgo del sistema. La auditoría se realizará preferiblemente de manera continua, pero al menos una vez al año y después de cualquier evento de seguridad.
60. En **[SM-CEK-12]** de **CD5 - Criptografía, cifrado y gestión de claves** del referenciado documento de la OTAN, se determina que deben rotarse las claves criptográficas de acuerdo con el período calculado, que incluye disposiciones para considerar el riesgo de divulgación de información y los requisitos legales y reglamentarios.
61. En **[SM-CEK-18]** de **CD5 - Criptografía, cifrado y gestión de claves** del referenciado documento de la OTAN, se determina que se deben definir, implementar y evaluar procesos, procedimientos y medidas técnicas para gestionar claves archivadas en un repositorio seguro (por ejemplo, un gestor de contraseñas) que requiera acceso con el mínimo privilegio y que incluya disposiciones para requisitos legales y reglamentarios.

2.10 [op.ext.1] Contratación y acuerdos de nivel de servicio

62. En **[SM-STA-10]** de **CD15 - Gestión de la Cadena de Suministro, Transparencia y Rendición de Cuentas** del referenciado documento de la OTAN, se determina que deben revisarse los acuerdos de la cadena de suministro entre los CSP y los CSC al menos una vez al año.
63. En **[SM-CCC-05]** de **CD4 - Control de Cambios y Gestión de la Configuración** del referenciado documento de la OTAN, se determina que deben incluirse cláusulas contractuales que limiten los cambios realizados por el CSP, siempre que impactan directamente en los entornos / 'tenants' propiedad del CSC, a solicitudes explícitamente autorizadas dentro de los acuerdos de nivel de servicio entre el CSP y el CSC.
64. En **[SM-CCC-10]** de **CD4 - Control de Cambios y Gestión de la Configuración** del referenciado documento de la OTAN, se determina que deben incluirse cláusulas contractuales que requieran que el CSP disponga de un programa de formación regular y orientado al público objetivo para capacitar y concienciar a empleados internos y externos sobre los estándares y métodos de desarrollo y provisión de software seguro, así como sobre el uso de las herramientas utilizadas para este fin, debiendo dicho programa revisarse y actualizarse periódicamente.
65. En **[SM-CEK-08]** de **CD5 - Criptografía, cifrado y gestión de claves** del referenciado documento de la OTAN, se determina que deben incluirse cláusulas contractuales que requieran al CSP proporcionar al CSC la capacidad de administrar sus propias claves de cifrado de datos.

66. En **[SM-DCS-01]** de **CD6 - Seguridad del Centro de Proceso de Datos (CPD)** del referenciado documento de la OTAN, se determina que deben incluirse cláusulas contractuales que requieran que deben establecerse, documentarse, aprobarse, comunicarse, aplicarse, evaluarse y mantenerse políticas y procedimientos para la eliminación segura de equipos utilizados cuando abandonen las instalaciones del CSP. Si el equipo no se destruye físicamente, debe aplicarse un procedimiento de borrado seguro de datos que imposibilite la recuperación de la información. Deben revisarse y actualizarse las políticas y procedimientos al menos una vez al año.
67. En **[SM-DCS-02]** de **CD6 - Seguridad del Centro de Proceso de Datos (CPD)** del referenciado documento de la OTAN, se determina que deben incluirse cláusulas contractuales que requieran que se establezca, documente, apruebe, comunique, aplique, se evalúe y se mantengan políticas y procedimientos para la reubicación o transferencia de hardware, software o datos/información por parte del CSP a una ubicación externa o alternativa. La solicitud de reubicación o transferencia debe requerir autorización escrita o criptográficamente verificable por parte del CSC.
68. En **[SM-DSP-18]** de **CD7 - Gestión del ciclo de vida de la seguridad y privacidad de los datos** del referenciado documento de la OTAN, se determina que deben incluirse cláusulas contractuales que requieran que el CSP deba implementar y describir al CSC el procedimiento para gestionar y responder a las solicitudes de divulgación de datos personales por parte de las autoridades encargadas de hacer cumplir la ley, de acuerdo con las leyes y normativas aplicables. El CSP debe prestar especial atención al procedimiento de notificación a los CSC afectados, salvo que exista una prohibición legal, como la prohibición penal de preservar la confidencialidad de una investigación policial/judicial.
69. En **[SM-IPY-04]** de **CD11 - Interoperabilidad y Portabilidad** del referenciado documento de la OTAN, se determina que los acuerdos contractuales entre CSP y CSC deben incluir cláusulas que especifiquen el acceso del CSC a los datos tras la rescisión del contrato, incluyendo:
    a. Formato de los datos.
    b. Definición del plazo en el que el CSP pone los datos a disposición del cliente.
    c. Tipo y alcance de los datos conservados y puestos a disposición del CSC.
    d. Política de eliminación de datos, incluyendo la definición del momento a partir del cual el CSP hace que los datos sean inaccesibles para el CSC.
    e. Responsabilidades y obligaciones del CSC para cooperar en el suministro de los datos.
70. En **[SM-SEF-10]** de **CD14 - Gestión de incidentes de seguridad, descubrimiento electrónico (e-Discovery) y análisis forense en la nube** del referenciado documento de la OTAN, se determina que los acuerdos contractuales entre CSP y CSC deben incluir cláusulas contractuales que requieran al CSP informar a sus empleados y socios comerciales externos sobre sus obligaciones. De ser necesario, se comprometerán o estarán obligados contractualmente a informar con prontitud a una oficina central previamente designada por el CSP sobre cualquier

evento de seguridad que conozcan y que esté directamente relacionado con el servicio en la nube proporcionado por el CSP.

71. En **[SM-TVM-11]** de **CD16 - Gestión de amenazas y vulnerabilidades** del referenciado documento de la OTAN, se determina que deben incluirse cláusulas contractuales que requieran que el CSP informe periódicamente al CSC sobre el estado de los incidentes que le afectan o, cuando corresponda y sea necesario, le involucre en su resolución. Una vez resuelto un incidente desde la perspectiva del CSP, debe informar al CSC sobre las medidas adoptadas, de acuerdo con los acuerdos contractuales.

2.11 [op.ext.3] Protección de la cadena de suministro

72. En **[SM-STA-01]** de **CD15 - Gestión de la Cadena de Suministro, Transparencia y Rendición de Cuentas** del referenciado documento de la OTAN, se determina que se deben establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener políticas y procedimientos para la aplicación del Modelo de Responsabilidad Compartida de Seguridad (SSRM) en la organización.
73. En **[SM-STA-07]** de **CD15 - Gestión de la Cadena de Suministro, Transparencia y Rendición de Cuentas** del referenciado documento de la OTAN, se determina que debe desarrollarse y mantenerse un inventario de todas las relaciones de la cadena de suministro.

2.12 [op.nub.1] Protección de servicios en la nube

74. Para cumplir con esta medida de seguridad del ENS no basta con que el CSC elija un CSP que disponga de la Certificación de Conformidad con el ENS para el sistema de información que sustenta los servicios contratados. Es necesario que el CSC configure esos servicios con las posibilidades de configuración que proporciona el CSP y los asegure, incluyendo las máquinas virtuales que haya podido aprovisionar, siguiendo guías de bastionado reconocidas e instrucciones facilitadas por el CSP. El propio Refuerzo R2-Guías de Configuración de Seguridad Específicas [op.nub.1.r2.1] señala "*La configuración de seguridad de los sistemas que proporcionan estos servicios deberá realizarse según la correspondiente guía CCN-STIC de Configuración de Seguridad Específica, orientadas tanto al usuario como al proveedor*".
75. En relación al CSP, si este subcontrata servicios a otro CSP deberá exigirle los mismos requisitos que el CSC le exige a él, en base a lo dispuesto en esta medida del ENS y en la medida [op.exp.3] Protección de la cadena de suministro.

2.13 [op.cont.2] Plan de continuidad (y demás medidas vinculadas)

76. El CSC debe contratar servicios en la nube a un CSP que cumpla, entre otras disposiciones, las del ENS en categoría ALTA en todas las dimensiones, lo que implica alta disponibilidad de dichos servicios abarcando, al menos, dos centros de datos distintos y lo suficientemente alejados para eludir riesgos comunes. Todo

ello con independencia de la redundancia necesaria en la infraestructura subyacente de los servicios contratados al CSP.

77. Pese a constar en la Declaración de Aplicabilidad del CSC como que no aplica ni el plan de continuidad, ni sus pruebas, ni las redundancias, cada CSC decidirá en base a sus especificidades y análisis de riesgos si establece estrategias complementarias de continuidad como pueden ser, por ejemplo, preacuerdos con otro CSP o copias de seguridad cifradas en local de cierta información crítica.
78. En **[SM-BCR-07]** de **CD3 - Gestión de la continuidad del negocio y resiliencia de las operaciones** del referenciado documento de la OTAN, se determina que debe establecerse comunicación con las partes interesadas y participantes en el transcurso de los procedimientos de continuidad y resiliencia de la organización.

2.14 [op.mon.3] Vigilancia

79. En **[SM-TVM-08]** de **CD16 - Gestión de amenazas y vulnerabilidades** del referenciado documento de la OTAN, se determina que debe emplearse un modelo basado en riesgos para la priorización efectiva de la remediación de vulnerabilidades utilizando un marco reconocido por la industria.

2.15 [mp.if] Protección de las instalaciones e infraestructuras

80. La Autoridad de Acreditación correspondiente será quién determinará, en función de qué parte del sistema está externalizada en un CSP y cual permanece en el CSC o es accesible desde sus instalaciones por los usuarios del sistema, el nivel de protección que debe exigirse a las instalaciones e infraestructuras.
81. Este criterio viene avalado por **[SM-DCS-03]** de **CD6 - Seguridad del Centro de Proceso de Datos (CPD)** del referenciado documento de la OTAN, se determina que deben establecerse, documentarse, aprobarse, comunicarse, aplicarse, evaluarse y mantenerse políticas y procedimientos para mantener un entorno de trabajo seguro también en oficinas, además de en los CPDs y otras salas técnicas.

2.16 [mp.per.2] Deberes y obligaciones

82. El CSC debe disponer de **Habilitación de Seguridad de Empresa (HSEM)**, así como, todo su personal en contacto con el sistema que maneja información clasificada, disponer de la **Habilitación Personal de Seguridad (HPS)**. Adicionalmente, a criterio de la ONS, los CSC deberán disponer de Habilitación de Seguridad de Establecimiento (HSES) en las ubicaciones fijas desde las que exploten sus sistemas clasificados desplegados en un CSP.
83. Por su parte el CSP, considerado el aislamiento y cifrado de la información clasificada albergada por el CSC en el CSP, será a criterio de la ONS que se determine si determinado personal de administración deberá estar asimismo en posesión de la HPS y, en su caso de la HSEM.
84. En **[SM-HRS-05]** de **CD9 – Recursos Humanos (RR.HH.)** del referenciado documento de la OTAN, se determina que deben establecerse y documentarse procedimientos para la devolución de activos propiedad de la organización por

parte de empleados despedidos, como concreción de alguna de las obligaciones en caso de término de la relación laboral.

2.17 [mp.per.4] Formación

85. En **[SM-AIS-08]** de **CD2 - Seguridad de aplicaciones e interfaces** del referenciado documento de la OTAN, se determina que deben implementarse y documentarse capacitaciones sobre desarrollo seguro adecuadas para los empleados a cargo de dicha actividad.

2.18 [mp.eq.3] Protección de dispositivos portátiles

86. En **[SM-UEM-11]** de **CD17 - Gestión final de puestos de usuario (endpoints)** del referenciado documento de la OTAN, se determina que deben configurarse los endpoints administrados con tecnologías y reglas de prevención de pérdida de datos (DLP) de acuerdo con una evaluación de riesgos.
87. En **[SM-UEM-10]** del mismo grupo y documento, se determina que deben configurarse los endpoints administrados por la organización con firewalls por software configurados correctamente.
88. En **[SM-UEM-12]** del mismo grupo y documento, se determina que deben habilitarse las capacidades de geolocalización remota para todos los endpoints móviles administrados por la organización (especialmente aquellos que abandonan las sedes de la organización).
89. En **[SM-UEM-13]** del mismo grupo y documento, se determina que se deben definir, implementar y evaluar procesos, procedimientos y medidas técnicas que permitan la eliminación remota de datos de la organización en los dispositivos endpoints gestionados por la organización.
90. En **[SM-UEM-14]** del mismo grupo y documento, se determina que se deben definir, implementar y evaluar procesos, procedimientos y medidas técnicas y/o contractuales para mantener la seguridad adecuada de los endpoints de terceros con acceso a los activos de la organización.

2.19 [mp.si] Protección de los soportes de información

91. En relación al CSC y su externalización de determinados sistemas, o parte de ellos, en un CSP, los soportes habitualmente quedan fuera del alcance de esta política para el CSC, con independencia de que determinada organización requiera considerarlos. Debido a ello, en la Declaración de Aplicabilidad del apartado anterior se considera que los soportes son de aplicación al CSP, salvo que considere que tampoco le aplican, y se han excluido para el CSC.
92. Es importante aclarar que la medida [mp.si.5] Borrado y destrucción, suele aplicar siempre, ya que cualquier disco duro del equipamiento (servidor, cabina de almacenamiento o endpoint, por ejemplo) al final de su vida útil es considerado un soporte y debe ser borrado de forma segura o destruido.

2.20 [mp.sw.1] Desarrollo de aplicaciones

93. En **[SM-CCC-02]** de **CD4 - Control de Cambios y Gestión de la Configuración** del referenciado documento de la OTAN, se determina que debe seguirse un proceso definido de control de cambios, aprobación y pruebas durante el desarrollo e implementación de software, con líneas base, pruebas y estándares de lanzamiento establecidos (con analogía a la medida [op.exp.5] Gestión de cambios).
94. En **[SM-TVM-05]** de **CD16 - Gestión de amenazas y vulnerabilidades** del referenciado documento de la OTAN, se determina que se deben definir, implementar y evaluar procesos, procedimientos y medidas técnicas para identificar actualizaciones para las aplicaciones que utilizan bibliotecas de terceros o de código abierto de acuerdo con la política de gestión de vulnerabilidades de la organización (en línea con el refuerzo opcional R5 - Lista de componentes software de [mp.sw.1] Desarrollo de aplicaciones).

2.21 [mp.info.6] Copias de seguridad

95. En **[SM-BCR-08]** de **CD3 - Gestión de la continuidad del negocio y resiliencia de las operaciones** del referenciado documento de la OTAN, se determina que para garantizar la integridad y disponibilidad de la copia de seguridad y verificar que el servicio de restauración de datos esté disponible, debe asegurarse que permita la recuperación de datos de acuerdo con el SLA establecido por el CSP o acordado entre CSP y CSC.