centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 896

Perfil de Cumplimiento Específico para Servicios de Seguridad Gestionados / PCE-SSG

Agosto 2025

Edita:

Firmado digitalmente por CENTRO CRIPTOLOGICO NACIONAL
Fecha: 2025.08.01 11:33:57 +02'00'

Fecha de Edición: agosto de 2025

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

Puede definirse un **servicio de seguridad gestionado (SSG)**[1] como aquel servicio prestado a un tercero que consiste en llevar a cabo o proporcionar asistencia para actividades relacionadas con la gestión de riesgos de ciberseguridad, como, por ejemplo, la gestión de incidentes, las pruebas de penetración, las auditorías de seguridad y la consultoría relacionada con la asistencia técnica, incluidos los conocimientos específicos.

Los servicios de seguridad gestionados son prestados por proveedores de servicios de seguridad gestionados, tal como se definen en el artículo 6, punto 40, de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, prestando asistencia a las entidades en sus esfuerzos de prevención, detección, respuesta y recuperación en relación con los incidentes.

En consecuencia, de una parte, una organización prestadora de SSG debe de poder **evidenciar sus capacidades operativas, así como su competencia técnicas** en relación a los SSG que presta en el ámbito de la ciberseguridad, garantizando que éstos serán de calidad; y de otra, los medios empleados por la organización para poder prestar los SSG deberán cumplir los requisitos necesarios de seguridad que garanticen a su vez que **están protegidos y son confiables para realizar su desempeño de forma segura** para la propia entidad y para aquellas que contraten sus servicios.

Por ello, es preciso abordar ambas aproximaciones, las capacidades operativas y competencias técnicas mínimas obligatorias, así como la protección de los propios recursos, de la información/activos que gestionan. Este enfoque proporciona la validación de la eficiencia de las operaciones de los servicios, así como el hecho de que puedan llevarse a cabo de forma suficientemente segura y acorde a la normativa vigente.

Racionalizando los recursos requeridos, sin menoscabo de la protección perseguida y exigible, los sistemas y demás recursos que soportan los citados servicios deberán disponer de la Certificación de Conformidad con el Esquema Nacional de Seguridad (RD 311/2022, de 3 de mayo) para categoría MEDIA o superior o, en su defecto, evidenciar la adecuada adopción de un conjunto mínimo de 36 medidas de seguridad (recogidas en el apartado 5.1 de este documento) que resulten de aplicación a cada caso concreto, y que incluirán el compromiso formal de alcanzar la ante dicha Conformidad con el ENS en un plazo no superior a 12 meses.

Por tanto, el PCE-SSG incluye los requisitos necesarios para garantizar la confiabilidad y competencia técnica en el despliegue de SSG y acreditar la conformidad con las normativas nacionales o europeas que demanden evidencias de seguridad en los SSG.

Las organizaciones prestadoras de SSG pueden entenderse como un conjunto de personas, procesos y tecnologías que, mediante su interrelación, cooperación y

[1] REGLAMENTO (UE) 2025/37 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 19 de diciembre de 2024 por el que se modifica el Reglamento (UE) 2019/881 en lo que se refiere a los servicios de seguridad gestionados.

coordinación, desarrollan actividades de seguridad gestionado para otras organizaciones, tanto públicas como privadas, con la debida calidad y seguridad.

Con la publicación del presente PCE-SSG el Centro Criptológico Nacional, en el ejercicio de sus competencias, valida y hace públicos los referidos requisitos y su modelo de evaluación y certificación de la conformidad, atendiendo a lo dispuesto en el artículo 30 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS, en adelante), lo que posibilita que las organizaciones prestadoras de SSG puedan alcanzar los adecuados niveles de seguridad y calidad en su prestación, que permitan trasladar la debida confianza a las entidades consumidoras de sus servicios.

2. SOBRE LA CERTIFICACIÓN DE LOS SERVICIOS

El presente documento engloba los requisitos técnicos y procesos operativos para el adecuado despliegue de SSG, así como las medidas de seguridad de conformidad con lo recogido en el Esquema Nacional de Seguridad en materia de protección de sistemas de información. Es por ello que el ENS será de aplicación a los sistemas de información que dan soporte y desde los que se despliegan los SSG, operados por entidades públicas o privadas que, tras el correspondiente proceso de categorización basado en los servicios que prestan y la información que manejan de las organizaciones que puedan ser destinatarias de sus servicios, serán conformes, al menos, con la categoría MEDIA del ENS, sin perjuicio de la aplicación de otras disposiciones normativas que emanen del Esquema Nacional de Seguridad o de cualesquiera otras regulaciones que resulten asimismo de aplicación, tales como la normativa vigente en materia de Protección de Datos.

De conformidad con lo recogido en el ENS, como señala su art. 2, resulta obligatoria su aplicación a los sistemas de información de todas las entidades del sector público y también a los del sector privado cuando presten servicios competenciales a las anteriores -entre los que se encuentran los SSG, toda vez que la seguridad constituye uno de los principios generales del funcionamiento de las entidades públicas, tal y como está regulado en el art. 3 de la Ley 40/2015, de 1 de octubre.

Por todo ello, y de forma sumaria, la conformidad con el presente PCE-SSG servirá para:

- **Evidenciar las capacidades operativas y competencias técnicas mínimas requeridas para la prestación de los SSG,** descritas en el Capítulo Servicios Prestados y Requisitos Operativos, constituyendo un indicador de calidad fundamental para las entidades públicas y privadas que tengan intención de contratar SSG.
- **Garantizar la seguridad de los sistemas de información** que soportan específicamente los SSG prestados**,** lo que supone **dar cumplimiento a los requisitos de seguridad aplicables que emanan del Anexo II del ENS**, descritos en el Capítulo 5 Declaración de Aplicabilidad y que se potenciarán, si es necesario, mediante refuerzos.
- **Definir los mecanismos de evaluación de las capacidades operativas y competencias técnicas para la prestación de los SSG, así como de la seguridad**

de los sistemas implicados. De esta forma se persigue asegurar que dichos SSG que gestionan tal información son prestados con la competencia, capacidad y experiencia necesarias y por personal adecuado. A su vez, garantiza que los SSG evaluados **satisfacen el objetivo de proteger** la disponibilidad, autenticidad, integridad, trazabilidad y confidencialidad de la información consultada, tratada, almacenada o transmitida.

- Dada la naturaleza de los SSG serán de obligado cumplimiento también los **requisitos específicos complementarios a las medidas de seguridad y del entorno** del Anexo II del ENS y que se recogen en la sección 5.2. Asimismo, se debe asegurar que dichos SSG que gestionan tal información son prestados con la competencia, capacidad y experiencia necesarias y por personal adecuado.

El cumplimiento de todos los requisitos organizativos, procedimentales, técnicos y personales que se señalan en el presente PCC-SSG permitirá elevar los niveles de capacidad, competencia y seguridad en la prestación de los SSG y, por tanto, por extensión, de la Red Nacional de SOC (RNS).

Por tanto, la conformidad con este PCE-SSG servirá para evidenciar que los SSG disponen de los recursos necesarios (organizativos, técnicos y humanos) y de los adecuados sistemas de seguridad (físicos y lógicos) para alcanzar la capacidad operativa necesaria, detectando, mitigando y ayudando a contener y remediar, amenazas sobre los datos o sistemas de sus clientes o usuarios, en áreas tan especialmente delicadas como son, por ejemplo, los tratamientos realizados por las entidades del sector público.

Así mismo este perfil garantiza que los clientes que busquen contratar servicios de un Servicio de Seguridad Gestionados (SSG) estén plenamente informados sobre los requisitos esenciales a solicitar, permitiéndoles validar la efectividad y adecuación del servicio contratado.

3. ÁMBITO DE APLICACIÓN

El ámbito de aplicación del presente PCE-SSG se extiende a aquellas organizaciones que presten SSG y que se encuentren comprendidas en el ámbito subjetivo de aplicación del ENS, es decir:

- Todo el sector público español, según lo determina el art. 2 de la Ley 40/2015.
- Las entidades del sector privado, cuando, en virtud de una relación contractual, presten servicios o provean soluciones competenciales a las entidades del sector público (la seguridad, entre ellas), o cuando, formando parte de la cadena de suministro de tales servicios, un análisis de riesgos así lo aconseje.

La verificación del cumplimiento de este Perfil de Cumplimiento Específico aplica a los SSG, independientemente de las competencias[2] que desarrolle mediante los servicios prestados, el volumen de operaciones o el número y tamaño de sus organizaciones cliente.

Aquella entidad u organismo con capacidad y voluntad para abordar este Perfil de Cumplimiento Específico deberá verificar el cumplimiento de al menos uno de los SSG **(prevención, protección, detección, respuesta y/o gestión de la ciberseguridad)** descritos en el apartado Servicios Prestados y Requisitos Operativos, así como, disponer del ENS categoría MEDIA o superior para los sistemas de información que dan soporte a los SSG o por el contrario, de no disponer de certificación ENS categoría MEDIA o superior, cumplir con las 36 medidas de seguridad del ENS descritas en la Declaración de Aplicabilidad de la presente guía.

El CCN considerará para cada Centro de Operaciones de Seguridad o Security Operation Center (SOC) varios niveles de madurez, en función de los SSG certificados bajo el presente Perfil de Cumplimiento Específico que vinculará con la RNS, https://rns.ccn-cert.cni.es/.

Siguiendo este criterio, el CCN a través de la RNS considera los niveles de madurez de un SOC según la siguiente categorización:

- **SOC Básico**: Se requiere presentar la certificación del Servicio de Gestión de la Ciberseguridad y del Servicio de Detección.
- **SOC Avanzado**: Se requiere presentar la certificación del Servicio de Gestión de la Ciberseguridad, Servicio de Prevención, Servicio de Detección y Servicio de Respuesta.
- **SOC Completo**: Se requiere presentar la certificación de todos los servicios. Servicio de Gestión de la Ciberseguridad, Servicio de Prevención, Servicio de Protección, Servicio de Detección y Servicio de Respuesta.

En concreto, la verificación del cumplimiento de este PCE-SSG se aplicará, con **carácter subjetivo**, a los SSG, bajo cualquier modalidad de prestación (SaaS, on-premise, modalidad híbrida, etc.) y, con **carácter material,** en servicios tales como la respuesta a incidentes, las pruebas de penetración, las auditorías de seguridad y la consultoría o la asistencia técnica, prestando asistencia a las entidades en sus esfuerzos de prevención, detección, respuesta y recuperación en relación con los incidentes.

Dado que en un mismo **Centro de Operaciones de Seguridad (SOC)** pueden estar operando **simultáneamente una o varias entidades u organizaciones** que, mediante su cooperación y colaboración implementan conjuntamente los **SSG.** Por tanto, es esencial que para cada **SSG** se verifique que se satisface lo dispuesto en el presente PCE-SSG en todo aquello que le sea particularmente de aplicación, con lo que se garantizará la seguridad global de los SSG que finalmente se proporcionen al cliente final.

[2] Las competencias que puede desarrollar un SOC, mediante su catálogo de servicios, para alcanzar las capacidades deseadas (de prevención, protección, detección, respuesta y gestión de la ciberseguridad) están definidas en la página del CCN-CERT https://rns.ccn-cert.cni.es

Si lo desea el Centro de Operaciones de Seguridad (SOC) solicitará al CCN su inclusión en con el nivel de madurez correspondiente de la RNS.

En el caso de que el **prestador de servicios sea una entidad pública** y vaya a prestar dichos servicios a otras entidades públicas, como primer paso **deberá certificar los SSG** demostrando su responsabilidad, participación en la toma de decisión de las operaciones, supervisión y aprobación de la gestión operativa y documentación correspondiente. En consecuencia, tanto la dirección, coordinación y gestión de los recursos y las operaciones podrían mostrar cumplimiento con los requisitos expuestos en este documento.

De esta forma, **un Centro de Operaciones de Seguridad (SOC)** Básico, Avanzado o Completo **podrá contar con la certificación de los SSG de una o varias entidades u organismos**.

La Auditoría de Seguridad para la Certificación de conformidad con el PCE-SSG será realizada por una Entidad de Certificación del ENS acreditada, o un Órgano de Auditoría Técnica del Sector Público, de los regulados en la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad que disponga de auditores con la capacitación exigida por el CCN.

Una guía determinará la cualificación del personal destinado a la realización de las auditorías de los controles destinados a verificar la capacidad operativa y competencia técnica de los SSG del apartado 4. de esta guía, así como los criterios generales de evaluación y auditoría específicos.

Cuando una parte de la infraestructura de prestación de los servicios de seguridad gestionados estuviera externalizada y dispusiera de una Certificación de Conformidad con el ENS de igual o superior categoría a la que pretende la totalidad de la infraestructura, el equipo auditor, tomando en consideración criterios de responsabilidad compartida de los que se derive la necesidad de una verificación de determinadas medidas (control de accesos, privilegios, etc.), determinará el conjunto de medidas para las que resulta suficiente la exhibición de la Certificación Conformidad previamente obtenida, así como aquellas para las que resulta necesario realizar alguna verificación adicional.

El titular de un certificado informará al CCN de cualquier vulnerabilidad o irregularidad que se detecte posteriormente relativa a los SSG certificados que pueda afectar al cumplimiento de los requisitos de certificación.

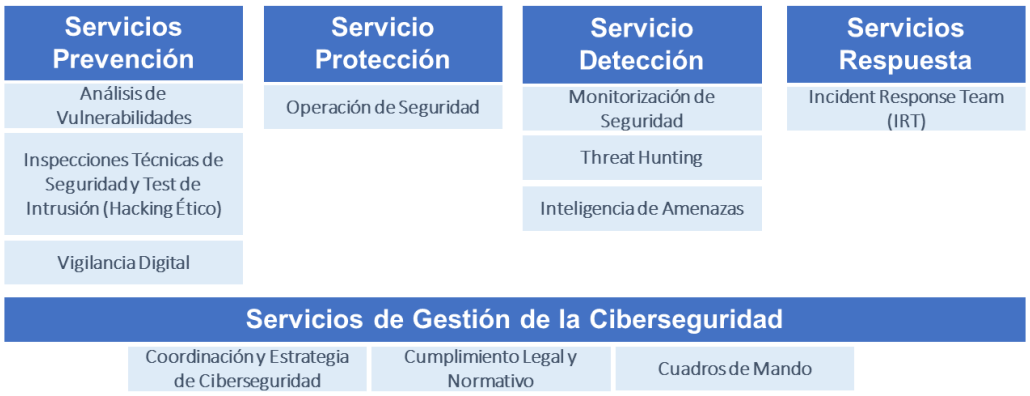
Los SSG deberán poner a disposición del CCN, cuando así le sea solicitado, la documentación técnica o cualquier otra documentación relativa a los servicios prestados y su seguridad, incluyendo los Informes de Auditoría, documentación que el CCN custodiará, preservando la debida confidencialidad.

4. SERVICIOS PRESTADOS Y REQUISITOS OPERATIVOS

Para la redacción del presente PCE-SSG se han identificado los SSG más usados y comúnmente reconocidos. Para garantizar que cada servicio se presta adecuadamente y satisface los requisitos de **capacidad operativas, así como las competencias técnicas mínimas requeridas a su finalidad,** en el capítulo 4.1 **(Requisitos específicos complementarios de los SSG)**, se describen **los requisitos mínimos obligatorios que debe satisfacer cada servicio para obtener su certificación.**

Los SSG gestionados se estructuran y organizan en base al ciclo de vida de la gestión de un incidente de seguridad, tal y como se define en el portal de la Red Nacional de SOC (RNS) del CCN-CERT: https://rns.ccn-cert.cni.es.

Por su parte, los SSG pueden estar compuestos por sub-servicios, tal y como se muestra en la figura siguiente:



El Servicio de Gestión de la Ciberseguridad, a menudo acometido por un área de coordinación a modo de Oficina Técnica u Oficina de Seguridad, es transversal al resto de los SSG, dotando al modelo de una capa estratégica de gestión, coordinación, gobernanza, seguimiento y asesoramiento.

Es importante que los profesionales que prestan SSG, especialmente los operadores y analistas de los primeros niveles, dispongan de procedimientos de operación estandarizados y documentación detallada y actualizada de los diferentes casos de uso o situaciones que se puedan plantear, junto a los protocolos establecidos, de forma que se minimice la improvisación en sus actuaciones.

Igualmente, es importante que los profesionales de ciberseguridad estén especializados, en función de su actividad, estando debidamente capacitados y contando con la competencia, pericia y experiencia necesaria. Para ello, en el Anexo I – Perfiles Asociados a Personal del SOC se describen los perfiles más comúnmente encontrados en los SSG y unos requisitos mínimos orientativos.

4.1 Requisitos específicos complementarios de los servicios de seguridad gestionados

A continuación, se describen en las tablas correspondientes a cada servicio los requisitos mínimos necesarios para su correcta prestación. La tabla de cada SSG muestra:

- Descripción del Servicio en el que se indican el objeto y finalidad de cada sub-servicio.
- Requisitos para garantizar la competencia técnica y la capacidad operativa en la prestación de los servicios que son de obligado cumplimiento.
- Se utiliza el ENS como marco de referencia para identificar la correlación entre los requisitos de los SSG y las medidas de seguridad del Anexo II del ENS.

4.1.1 Servicios de Prevención

ANÁLISIS DE VULNERABILIDADES		
DESCRIPCIÓN DEL SERVICIO	**REQUISITOS PARA LA PRESTACIÓN DE LOS SERVICIOS**	**ARTÍCULOS Y MEDIDAS DE SEGURIDAD DEL ENS COMO FRAMEWORK PARA LA PRESTACIÓN DE LOS SSG**
Servicio enfocado en el escaneado automatizado de activos de la organización, para la identificación de vulnerabilidades existentes en los elementos constituyentes de sus sistemas de información y seguridad.	**SPV.AV.1** Debe mantenerse procedimentada la operativa para la identificación, análisis y reporte de vulnerabilidades, así como para realizar el seguimiento para validar su remediación.	org.3
	SPV.AV.2 Debe mantenerse actualizada la documentación relativa a los procesos de operación y gestión de vulnerabilidades.	org.3, op.exp.3 y op.exp.4
	SPV.AV.3 Debe disponerse un inventario actualizado de los activos, a ser posible una CMDB.	op.exp.1
	SPV.AV.4 Deberá ser llevado a cabo con herramientas específicas (e.g. ANA) u otras herramientas certificadas contenidas en el catálogo CPSTIC (Guía CCN-STIC 105), que incluiría tanto el registro y seguimiento de las	op.exp.4 y op.pl.5

	vulnerabilidades identificadas como el apoyo a la remediación de dichas vulnerabilidades.	
	SPV.AV.5 Debe aplicarse un scoring para las vulnerabilidades identificadas según CVE (Common Vulnerabilities and Exposures) o CVSS 3.1v (Common Vulnerability Scoring System Version), con el fin de establecer una criticidad a cada vulnerabilidad que pueda ser estandarizada y entendible.	op.exp.3 y op.exp.4
	SPV.AV.6 Seguimiento a la publicación de vulnerabilidades tecnológicas que pudieran afectar al Organismo a través de foros internacionales, organizaciones público-privadas u fabricantes de referencia.	
	SPV.AV.7 El servicio debe generar informes y proporcionar cuadros de mando con la información más relevante del servicio de tal forma que favorezcan la toma de decisiones.	Art. 32.3, op.mon.2 y op.ext.2
	SPV.AV.8 El servicio debe hacer uso de una herramienta de gestión de ticket o ITSM para la notificación y seguimiento de alertas de seguridad junto con su correspondiente procedimiento de uso.	op.exp.7 y op.exp.9
	SPV.AV.9 Debe disponerse de un procedimiento para la actuación en horario fuera de oficina que contenga los medios de contacto, personas de contacto y manuales de actuación.	Art. 20, op.exp.7
	SPV.AV.10 Debe disponerse de personal especializado en la gestión de vulnerabilidades, para lo que, preferiblemente, deberá contar con certificaciones reconocidas o, al menos, se encuentre en proceso de obtención.	Art. 16, mp.per.4
INSPECCIONES TÉCNICAS DE SEGURIDAD Y TEST DE INTRUSIÓN (HACKING ÉTICO)		
DESCRIPCIÓN	**REQUISITOS PARA LA PRESTACIÓN DE LOS SERVICIOS**	**ARTÍCULOS Y MEDIDAS DE SEGURIDAD DEL ENS COMO FRAMEWORK PARA LA PRESTACIÓN DE LOS SSG**

Se trata de una auditoría técnica enfocada en identificar fallas de seguridad y vulnerabilidades explotables en los sistemas de información y el ecosistema tecnológico que lo soporta de un organismo. Estas técnicas tienden a simular la actividad de un potencial atacante y cómo este podría terminar comprometiendo al organismo.	**SPV.ITSTI.1** Deberá llevarse a cabo poniendo foco sobre la infraestructura de producción, con especial atención tras la puesta en marcha de nuevas infraestructuras (adquisiciones de activos tecnológicos).	mp.sw.2 y op.nub.1
	SPV.ITSTI.2 Podrá ofrecerse al menos en modalidad "caja negra", "caja blanca" o "caja gris" en función de la información previa que se disponga del entorno.	mp.s.2
	SPV.ITSTI.3 Se emplearán técnicas y metodologías avaladas internacionalmente en función del alcance o activos a tratar, tales como OSSTMM, OWASP, PTES, ISSAF y/o OWISAM.	
	SPV.ITSTI.4 Debe aplicarse un scoring para las vulnerabilidades identificadas según CVE (Common Vulnerabilities and Exposures) o CVSS 3.1v (Common Vulnerability Scoring System Version), con el fin de establecer una criticidad a éstas que pueda ser estandarizada y entendible.	op.exp.3 y op.exp.4
	SPV.ITSTI.5 El servicio debe generar informes con la información más relevante del servicio de tal forma que favorezcan la toma de decisiones	op.ext.2
	SPV.ITSTI.6 Los resultados deben ser centralizados en una herramienta de análisis de vulnerabilidades	op.exp.4 y op.mon.3
	SPV.ITSTI.7 Debe disponerse de un procedimiento para la actuación en horario fuera de oficina que contenga los medios de contacto, personas de contacto y manuales de actuación.	Art. 20, op.exp.7
	SPV.ITSTI.8 Debe disponerse de personal especializado en la gestión de vulnerabilidades. Preferiblemente el personal contará con certificaciones reconocidas en el sector o al menos las estará cursando (e.g. CEH).	Art. 16, mp.per.4
	SPV.ITSTI.9 El servicio debe analizar en totalidad la superficie de exposición de internet de sus clientes tanto a nivel de IPs como de URLs, al menos, una vez cada dos meses, de forma automática.	op.mon.1 y mp.s.2
	SPV.ITSTI.10 El servicio debe alertar al cliente sobre las vulnerabilidades que aparezcan con un valor mayor de 7.0 según CVSS.	Art. 10

	SPV.ITSTI.11 Después de un incidente este servicio realizará un análisis para revisar la integridad del sistema.	op.mon.3
	SPVITSTI.12 Se debe proporcionar un servicio de análisis de código fuente de las aplicaciones de las entidades a las que se da servicio. El SSG gestionados debe revisar las aplicaciones *core* de cada entidad a nivel de código y de las aplicaciones expuestas a internet.	mp.sw.1 y mp.sw.2
VIGILANCIA DIGITAL		
DESCRIPCIÓN	**REQUISITOS PARA LA PRESTACIÓN DE LOS SERVICIOS**	**ARTÍCULOS Y MEDIDAS DE SEGURIDAD DEL ENS COMO FRAMEWORK PARA LA PRESTACIÓN DE LOS SSG**
Servicio enfocado en la detección temprana de amenazas externas en fuente abierta, Internet, Deep y Dark Web. Algunos ejemplos de alcance son: alerta temprana de tendencias y vulnerabilidades, uso ilícito de marca, phishing, suplantación de identidad, fuga o robo de información y/o credenciales, reputación, redes sociales, seguimiento de VIPs, entre otros.	**SPV.VD.1** Debe desarrollarse y mantenerse un procedimiento de notificación, escalado y seguimiento de amenazas y abusos identificados, así como procesos de vigilancia digital.	op.mon.3 y medidas organizativas [org*]
	SPV.VD.2 Debe llevarse a cabo la revisión de cuentas y fuga de información expuesta en repositorios en fuente abierta (Internet, Deep y Dark Web), tanto en lo relativo a la entidad que contrata el servicio como a la que lo presta.	op.mon.3
	SPV.VD.3 Deben generarse procedimientos de comunicación con terceros para la retirada y/o solicitud de baja de contenido malicioso o suplantación de identidad de direcciones IP y/o dominios.	op.exp.7 y op.exp.9
	SPV.VD.4 El servicio debe generar informes y proporcionar cuadros de mando con la información más relevante del servicio de tal forma que favorezcan la toma de decisiones.	Art. 32.3, op.mon.2 y op.ext.2
	SPV.VD.5 El servicio debe hacer uso de una herramienta de gestión de ticket o ITSM para la notificación y seguimiento de alertas de seguridad junto con su correspondiente procedimiento de uso.	op.exp.7 y op.exp.9

	SPV.VD.6 Debe disponerse de un procedimiento para la actuación en horario fuera de oficina que contenga los medios de contacto, personas de contacto y manuales de actuación.	Art. 20, op.exp.7

4.1.2 Servicios de Protección

OPERACIÓN DE CIBERSEGURIDAD		
DESCRIPCIÓN	**REQUISITOS PARA LA PRESTACIÓN DE LOS SERVICIOS**	**ARTÍCULOS Y MEDIDAS DE SEGURIDAD DEL ENS COMO FRAMEWORK PARA LA PRESTACIÓN DE LOS SSG**
Servicio enfocado en el suministro, implantación, administración, operación y/o mantenimiento de los distintos elementos que conforman la infraestructura de seguridad de una organización, cuyo objetivo es la protección de seguridad para redes y endpoints. Algunas de las herramientas o tecnologías que pueden ser objeto del servicio son: EDR, Firewall, IPS/IDS, Proxy, DNS, AV, CASB, DLP, IRM, NAC, WAF, CMDB, etc. El servicio debe velar por el correcto funcionamiento, configuración y disponibilidad de dichas tecnologías.	**SPT.OS.1** Deberán realizarse y comprobarse periódicamente las copias de seguridad de la configuración de los elementos que conforman la infraestructura de seguridad y de las herramientas de protección.	mp.info.6 y op.exp.3
	SPT.OS.2 Debe disponerse de procedimientos para la actualización de las herramientas, así como de los procesos de marcha atrás ante fallos o incidencias.	op.exp.4 y op.exp.5
	SPT.OS.3 Debe disponerse de procedimientos de operación y escalado de incidentes a especialistas y/o fabricantes.	op.ext.2
	SPT.OS.4 Deben aplicarse, siempre que existan para las tecnologías concretas, guías de buenas prácticas publicadas por el CCN-CERT o, en su defecto, de otras organizaciones de prestigio internacional.	Disposición adicional segunda. Desarrollo del Esquema Nacional de Seguridad.

	SPT.OS.5 Debe realizarse una auditoría semestral de la configuración de las tecnologías de protección.	op.exp.3
	SPT.OS.6 Debe mantenerse actualizada la documentación relativa a la operación de las distintas herramientas de seguridad existentes.	org.3 y op.pl.2
	SPT.OS.7 Se emplearán herramientas certificadas contenidas en el catálogo CPSTIC (Guía CCN-STIC 105).	op.pl.5
	SPT.OS.8 Debe permitir la conexión de elementos para la copia de tráfico.	op.ext.4
	SPT.OS.9 Debe poder generar alertas ante conexiones de dentro a fuera de las entidades que estén relacionadas con IPs de listas negras o posibilidad de ser maliciosas.	mp.s.3
	SPT.OS.10 El servicio debe generar informes y proporcionar cuadros de mando con la información más relevante del servicio de tal forma que favorezcan la toma de decisiones.	Art. 32.3, op.mon.2 y op.ext.2
	SPT.OS.11 El servicio debe hacer uso de una herramienta de gestión de ticket o ITSM para la notificación y seguimiento de alertas de seguridad junto con su correspondiente procedimiento de uso	op.exp.7 y op.exp.9
	SPT.OS.12 Se debe disponer de un procedimiento para la actuación en horario fuera de oficina que contenga los medios de contacto, personas de contacto y manuales de actuación. En 24x7 se deberán atender y gestionar las incidencias de severidad a partir de muy altas.	Art. 20, op.exp.7
	SPT.OS.13 Debe disponerse de técnicos especializados en administración, gestión y mantenimiento de herramientas o tecnologías de seguridad. Preferiblemente el personal contará con certificaciones reconocidas en el sector o al menos las estará cursando.	Art. 16, mp.per.4

4.1.3 Servicios de Detección

MONITORIZACIÓN DE SEGURIDAD		
DESCRIPCIÓN	**REQUISITOS PARA LA PRESTACIÓN DE LOS SERVICIOS**	**ARTÍCULOS Y MEDIDAS DE SEGURIDAD DEL ENS COMO FRAMEWORK PARA LA PRESTACIÓN DE LOS SSG**
Servicio enfocado en la identificación, análisis y notificación de forma continua de posibles amenazas de seguridad, velando por la detección proactiva y reactiva ante incidentes de seguridad. Se valorará tener en cuenta las siguientes especificaciones técnicas [3]ETSI GS ISI 007 Information Security Indicators (ISI); Guidelines for building and operating a secured Security Operations Center (SOC).	**SD.MS.01** Debe disponerse de procedimientos operativos para todos los puntos del servicio de monitorización: detección, análisis, escalado, reporte, registro, notificación, soporte, etc.	org.3, op.pl.2, op.exp.7, op.exp.8 y op.mon.1
	SD.MS.02 Se debe instalar un EDR en todos los activos, equipos finales y servidores, relevantes y críticos de una organización	op.exp.6
	SD.MS.03 Debe hacerse uso de herramientas SIEM/XDR o correladores de eventos de seguridad, certificadas en el catálogo CPSTIC (Guía CCN-STIC 105).	op.mon.3 y op.pl.5
	SD.MS.04 Ha de aplicarse inteligencia de amenazas en base a Indicadores de Compromiso (IOC) y/o Indicadores de Ataques (IOA) a la hora de procesar y correlacionar los eventos de ciberseguridad.	op.mon.3, op.mon.1 y op.exp.8
	SD.MS.05 Ha de disponerse de un inventario actualizado de los activos, a ser posible una CMDB.	op.exp.1

[3] «especificación técnica»: un documento que prescribe los requisitos técnicos que debe cumplir un producto, servicio o proceso de TIC, o procedimientos de evaluación de la conformidad relativos a los mismos;

	SD.MS.06 La detección de incidentes y amenazas de seguridad debe hacerse en base a casos de uso. Estos deberán estar basados en estándares y Frameworks de referencia como MITTRE ATT&CK y MaGMa.	mp.s.2 y op.mon.3
	SD.MS.07 Entre los casos de uso propuestos por el prestador del servicio deben encontrarse los suministrados por la RNS.	Art. 29
	SD.MS.08 Debe mantenerse actualizada toda la documentación relativa a los casos de uso.	Art. 12, org.*, op.pl.2 y op.exp.7
	SD.MS.09 Deben integrarse las fuentes de información necesarias a la herramienta SIEM/XDR para garantizar la visibilidad y la recepción de telemetría de los activos de protección y seguridad de la organización. Estas fuentes de información deberán ser, siempre que sea posible o estén implementadas, las siguientes: Directorio Activo, Proxy, EndPoint (EDR/AntiVirus), Firewall, logs de servidores y equipos críticos y balanceadores. Igualmente es deseable disponer de la telemetría del DNS, VPNs o accesos externos, correo electrónico y/o O365.	op.mon.3
	SD.MS.10 La retención y almacenamiento de los logs dentro de la plataforma SIEM/XDR se realizará de acuerdo con las políticas y procedimientos de gestión de incidentes de seguridad definidos, también se tendrán en cuenta otras políticas de retención de datos que pudieran afectar a la resolución de potenciales incidentes de seguridad.	op.exp.8 y op.exp.9
	SD.MS.11 La integración de logs en el SIEM/XDR o correlador de eventos se hará siguiendo un estricto análisis de aquella telemetría y logs que activarán o harán saltar los casos de uso tratando de evitar la ingesta innecesaria de telemetría que no aporta valor.	

	SD.MS.12 Toda la telemetría y logs generados serán propiedad del propietario de la infraestructura origen de los datos de tal forma que se garantice el acceso a la misma en caso de producirse un incidente de seguridad o finalización del servicio	op.exp.1, op.exp.8 y op.exp.9
	SD.MS.13 Se requiere el despliegue y uso de una Malware Information Sharing Platform (MISP) interconectada con la Red Nacional de SOC para la compartición de información con especial atención en aquellas amenazas que se consideren importantes o que pudieran con mayor probabilidad impactar a las organizaciones mejorando así la madurez de la ciberseguridad en el ámbito nacional.	op.ext.4, op.mon.3 y mp.com.1
	SD.MS.14 Las notificaciones de las posibles amenazas reportadas han de contener campos de información que proporcionen la mayor cantidad de datos posible para su tratamiento (tipología de amenazas, peligrosidad, impacto, descripción detallada, activo afectado, etc.).	op.exp.7
	SD.MS.15 En caso de identificación de un incidente de seguridad para un organismo del sector público o infraestructura crítica, se deberá notificar en tiempo y forma al organismo público competente (CCN-CERT o INCIBE-CERT, según corresponda)	Art. 33, op.exp.7
	SD.MS.16 La monitorización y detección de incidentes de seguridad debe realizarse de manera automática y continua 24x7.	op.mon.3
	SD.MS.17 El servicio debe generar informes y proporcionar cuadros de mando con la información más relevante del servicio de tal forma que favorezcan la toma de decisiones.	Art. 32.3, op.mon.2 y op.ext.2
	SD.MS.18 El servicio debe hacer uso de una herramienta de gestión de ticket o ITSM para la notificación y	op.exp.7 y op.exp.9

	seguimiento de alertas de seguridad junto con su correspondiente procedimiento de uso.	
	SD.MS.19 Se debe disponer de un procedimiento para la actuación en horario fuera de oficina que contenga los medios de contacto, personas de contacto y manuales de actuación. En 24x7 debe existir un sistema de aviso y notificación para atender y gestionar las incidencias de severidad a partir de muy altas.	Art. 20, op.exp.7
	SD.MS.20 Se debe disponer de técnicos especializados en capacidades de detección y en la gestión de incidentes de Seguridad. Preferiblemente el personal contará con certificaciones reconocidas en el sector o al menos las estará cursando.	Art. 16, mp.per.4
THREAT HUNTING (CAZA DE AMENAZAS)		
DESCRIPCIÓN	**REQUISITOS PARA LA PRESTACIÓN DE LOS SERVICIOS**	**ARTÍCULOS Y MEDIDAS DE SEGURIDAD DEL ENS COMO FRAMEWORK PARA LA PRESTACIÓN DE LOS SSG**
Servicio enfocado en la caza de amenazas o búsqueda proactiva de amenazas de seguridad, permitiendo la identificación de anomalías y posibles incidentes de seguridad que los procesos tradicionales o pasivos no son capaces de identificar.	**SD.TH.1** Debe disponerse de procedimientos de análisis e investigación sobre las distintas tecnologías de seguridad de la organización para la identificación de anomalías o amenazas avanzadas de seguridad.	op.exp.7 y op.mon.1
	SD.TH.2 Debe elaborarse y ser aplicada una metodología de Threat Hunting basada en playbooks y Técnicas Tácticas y Procedimientos (TTPs), que se ejecuten periódicamente.	op.mon.3 y org.3
	SD.TH.3 Debe mantenerse actualizada la documentación relativa a la creación y validación de hipótesis, la búsqueda de evidencias, el descubrimiento de nuevos patrones de ataque, etc.	op.pl.2 y org.3

	SD.TH.4 Deben generarse y mantener procesos de notificación y seguimiento de amenazas, así como su apoyo para el análisis y tratamiento de posibles incidentes de seguridad.	op.exp.7
	SD.TH.5 Debe integrarse con los servicios de Monitorización de Seguridad e Inteligencia de Amenazas para complementar mutuamente los trabajos realizados por cada uno de esos servicios y favorecer la mejora continua de los mismos.	op.mon.3
	SD.TH.6 El servicio debe generar informes con la información más relevante del servicio de tal forma que favorezcan la toma de decisiones.	op.ext.2
	SD.TH.7 Se debe disponer de técnicos especializados en operación de Threat Hunting. Preferiblemente el personal contará con certificaciones reconocidas en el sector o al menos las estará cursando.	Art. 16, mp.per.4
	SD.TH.8 Se debe realizar una revisión de las conectividades ante la aparición de IOCs revisando con al menos 3 meses de antigüedad, si se ha recibido el ataque.	op.mon.3

INTELIGENCIA DE AMENAZAS		
DESCRIPCIÓN	**REQUISITOS PARA LA PRESTACIÓN DE LOS SERVICIOS**	**ARTÍCULOS Y MEDIDAS DE SEGURIDAD DEL ENS COMO FRAMEWORK PARA LA PRESTACIÓN DE LOS SSG**
Servicio enfocado en la obtención de información para generar inteligencia sobre amenazas avanzadas de tal forma que ayude a la gestión de la ciberseguridad, la mejora continua y la toma de decisiones de las organizaciones.	**SD.IA.01** Debe emplearse una plataforma de centralización de inteligencia MISP para la gestión y compartición de IOCs (Indicadores de Compromiso).	op.mon.3
	SD.IA.02 La MISP debe estar federada con foros y grupos de ciberseguridad, en especial, con la Red Nacional de SOC para contribuir activamente a la compartición de información de amenazas de seguridad.	op.mon.3 y op.pl.5
	SD.IA.03 La MISP debe integrarse con las distintas tecnologías de seguridad perimetral para la compartición de los indicadores de compromiso existentes.	op.mon.3
	SD.IA.04 Debe disponerse de procedimientos operativos para la gestión de la inteligencia de amenazas. Los procedimientos del servicio y documentación relativa deben mantenerse actualizados.	op.pl.2
	SD.IA.05 Debe disponerse de un inventario actualizado de los activos, a ser posible una CMDB.	op.exp.1
	SD.IA.06 Debe disponerse de un procedimiento para la actuación en horario fuera de oficina que contenga los medios de contacto, personas de contacto y manuales de actuación.	Art. 20, op.exp.7
	SD.IA.07 Debe disponerse de técnicos especializados en operación de inteligencia de amenazas.	Art. 16, mp.per.4

4.1.4 Servicios de Respuesta

INCIDENT RESPONSE TEAM (IRT)		
DESCRIPCIÓN	**REQUISITOS PARA LA PRESTACIÓN DE LOS SERVICIOS**	**ARTÍCULOS Y MEDIDAS DE SEGURIDAD DEL ENS COMO FRAMEWORK PARA LA PRESTACIÓN DE LOS SSG**
Consiste en un servicio experto que es activado ante la confirmación de la materialización de un incidente de seguridad, permitiendo su análisis forense, contención, mitigación, recuperación y post-incidente o lecciones aprendidas. Debe disponerse de Procedimientos de Respuesta ante Incidentes y Playbooks de actuación relativos a distintas tipologías de amenazas y personalizados a la entidad u organismo que recibe el servicio. Se valorará tener en cuenta las siguientes normas de la familia de la ISO 27035 (Servicios de respuesta a Incidentes). • ISO/IEC **27035**-1:2023 Information technology — Information security incident management — Part 1: Principles and process • ISO/IEC **27035**-2:2023 Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response.	**SR.IRT.1** Debe mantenerse actualizada la documentación relativa a los procedimientos establecidos de respuesta ante incidentes.	op.pl.2
	SR.IRT.2 Debe apoyar y orientar a la organización en las tareas de contención y remediación del incidente, dando soporte proactivo en las acciones que se requieran para su consecución.	op.exp.7
	SR.IRT.3 Debe liderar el proceso de respuesta ante incidentes y apoyar al comité de crisis en los aspectos que sean necesarios.	
	SR.IRT.4 En caso necesario, previo aviso y notificación de la organización afectada por un incidente, en las labores de respuesta al incidente se dotará de los medios técnicos y humanos para que las posibles evidencias recabadas puedan ser aportadas en un proceso judicial.	op.exp.9
	SR.IRT.5 En caso de que el incidente se materialice en una organización del sector público, o en una infraestructura crítica, debe notificarse tras la identificación del incidente al CERT de referencia (CCN-CERT o INCIBE-CERT, según corresponda), proporcionando el soporte que estos organismos requieran.	Art. 33, op.exp.7

• ISO/IEC **27035**-3:2020 Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations • ISO/IEC **27035**-4:2024 Information technology — Information security incident management — Part 4: Coordination	**SR.IRT.6** El servicio, en el ejercicio de sus funciones, tras el análisis y confirmación de incidentes y vulnerabilidades de seguridad, deberá compartir la información, experiencia y lecciones aprendidas usando REYES y la RNS.	Art. 33
	SR.IRT.7 El servicio debe generar informes con la información más relevante del servicio de tal forma que favorezcan la toma de decisiones.	op.ext.2
	SR.IRT.8 La cobertura de servicio ha de ser 24x7 incluyendo tiempos de respuesta, incluso si fuera necesario acudir in situ a la organización afectada.	Art. 20, op.exp.7
	SR.IRT.9 Debe disponerse de un procedimiento para la actuación en horario fuera de oficina o ausencia de respuesta por la entidad, que contenga los medios de contacto, personas de contacto y manuales de actuación.	
	SR.IRT.10 Debe disponerse de técnicos especializados en Respuesta ante Incidentes. Preferiblemente el personal contará con certificaciones reconocidas en el sector o al menos las estará cursando.	Art. 16, mp.per.4

4.1.5 Servicios de Gestión de la Ciberseguridad

COORDINACIÓN Y ESTRATEGIA DE CIBERSEGURIDAD		
DESCRIPCIÓN	**REQUISITOS PARA LA PRESTACIÓN DE LOS SERVICIOS**	**ARTÍCULOS Y MEDIDAS DE SEGURIDAD DEL ENS COMO FRAMEWORK PARA LA PRESTACIÓN DE LOS SSG**
Consiste en gestionar, hacer seguimiento y asesorar en lo que respecta a diversos aspectos de ciberseguridad, incluyendo estrategia de ciberseguridad a corto, medio y largo plazo, gestión y seguimiento de los servicios provistos o subcontratados, arquitecturas de seguridad e implantación, documentación y procedimientos asociados, mantenimientos, así como la planificación e implementación de la misma.	**SGC.AC.1** Procedimientos donde se defina el alcance del servicio descrito.	op.ext.1
	SGC.AC.2 Gestión contractual de las responsabilidades adquiridas o delegadas.	op.ext.1 y mp.per.2
	SGC.AC.3 Plan de mejora continua	op.ext.1 y op.ext.2
	SGC.AC.4 Plan de continuidad y transiciones relativo a los servicios	op.cont.4
CUMPLIMIENTO LEGAL Y NORMATIVO		
DESCRIPCIÓN	**REQUISITOS PARA LA PRESTACIÓN DE LOS SERVICIOS**	**ARTÍCULOS Y MEDIDAS DE SEGURIDAD DEL ENS COMO FRAMEWORK PARA LA PRESTACIÓN DE LOS SSG**
Consiste en la adaptación a normativa vigente en ciberseguridad.	**SGC.CLN.1** Elaboración de procedimientos y demás documentación necesaria para dar cumplimiento a la normativa.	org.3 y op.pl.2
	SGC.CLN.2 Realización de los análisis de riesgo necesarios.	op.pl.1
	SGC.CLN.3 Listado y repositorio con las certificaciones y acreditaciones legales y normativas que debe cumplir la entidad u organismo al que va dirigido el servicio.	Art. 16

CUADROS DE MANDO		
DESCRIPCIÓN	**REQUISITOS PARA LA PRESTACIÓN DE LOS SERVICIOS**	**ARTÍCULOS Y MEDIDAS DE SEGURIDAD DEL ENS COMO FRAMEWORK PARA LA PRESTACIÓN DE LOS SSG**
Debe existir un cuadro de mando que centralice la información que los SSG generan, para dar una visión completa del estado de la seguridad de cada entidad.	**SGC.CM.1** El cuadro de mandos debe contar al menos con los siguientes apartados: • Incidentes en curso. • Vulnerabilidades de más de 8 que afectan a la entidad, mostrando que equipos están afectados. • Número de vulnerabilidades y corrección de las mismas. • Volumetría de entrada y salida de tráfico. • Top 10 de equipos con más detecciones del EDR/AV. • Tasa de falsos positivos e incidentes con impacto. • Top reglas del EDR y FW que más están bloqueando. • Estado del análisis de riesgo de la entidad. • Número de incidentes bajo investigación. • Top de vulnerabilidades que afectan a la entidad. • Top 10 Departamentos o equipos o aplicación con más vulnerabilidades. • IPs o países más bloqueados.	op.mon.2

4.2 Los artículos y medidas de seguridad del ENS como marco de referencia

La siguiente tabla muestra el resumen de los artículos y medidas de seguridad del ENS que sirven como marco de referencia para la implantación de los requisitos específicos complementarios destinados a la prestación del SSG.

	SERVICIOS DE PREVENCION			SERVICIOS DE PROTECCION	SERVICIOS DE DETECCIÓN			SERVICIOS DE RESPUESTA	SERVICIOS DE GESTIÓN DE LA CIBERSEGURIDAD		
Medida	**ANALISIS DE VULNERABILIDADES**	**INSPECCIONES TÉCNICAS DE SEGURIDAD Y TEST DE INTRUSIÓN (HACKING ÉTICO)**	**VIGILANCIA DIGITAL**	**OPERACIÓN DE CIBERSEGURIDAD**	**MONITORIZACION DE CIBERSEGURIDAD**	**THREAT HUNTING (CAZA DE AMENAZAS)**	**INTELIGENCIA DE AMENAZAS**	**INCIDENT RESPONSE TEAM (IRT)**	**COORDINACIÓN Y ESTRATEGIA DE CIBERSEGURIDAD**	**CUMPLIMIENTO LEGAL Y NORMATIVO**	**CUADROS DE MANDO**
org.3	X		X	X	X	X				X	
op.pl.1										X	
op.pl.2				X	X	X	X	X		X	
op.pl.5	X			X	X		X				
op.exp.1	X				X		X				
op.exp.3	X	X		X							
op.exp.4	X	X		X							
op.exp.5				X							
op.exp.6					X						
op.exp.7	X	X	X	X	X	X	X	X			
op.exp.8					X						
op.exp.9	X		X	X	X			X			
op.ext.1									X		
op.ext.2	X	X	X	X	X	X		X	X		

	SERVICIOS DE PREVENCION			SERVICIOS DE PROTECCION	SERVICIOS DE DETECCIÓN			SERVICIOS DE RESPUESTA	SERVICIOS DE GESTIÓN DE LA CIBERSEGURIDAD		
Medida	**ANALISIS DE VULNERABILIDADES**	**INSPECCIONES TÉCNICAS DE SEGURIDAD Y TEST DE INTRUSIÓN (HACKING ÉTICO)**	**VIGILANCIA DIGITAL**	**OPERACIÓN DE CIBERSEGURIDAD**	**MONITORIZACION DE CIBERSEGURIDAD**	**THREAT HUNTING (CAZA DE AMENAZAS)**	**INTELIGENCIA DE AMENAZAS**	**INCIDENT RESPONSE TEAM (IRT)**	**COORDINACIÓN Y ESTRATEGIA DE CIBERSEGURIDAD**	**CUMPLIMIENTO LEGAL Y NORMATIVO**	**CUADROS DE MANDO**
op.ext.4				X	X						
op.nub.1		X									
op.cont.4									X		
op.mon.1		X			X	X					
op.mon.2	X		X	X	X						X
op.mon.3		X	X		X	X	X				
mp.per.2									X		
mp.per.4	X	X		X	X	X	X	X			
mp.com.1					X						
mp.sw.1		X									
mp.sw.2		X									
mp.info.6				X							
mp.s.2		X			X						
mp.s.3				X							

5. DECLARACIÓN DE APLICABILIDAD

Como es sabido, la declaración de aplicabilidad comprende el conjunto de medidas de seguridad que son de aplicación para el cumplimiento del ENS en un sistema concreto. Tal conjunto de medidas dependerá de la categoría del sistema y de los niveles asociados a las dimensiones de seguridad.

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 en su categoría MEDIA, sino la de posibles refuerzos aplicables a las medidas del ENS de obligado cumplimiento.

Esta guía a su vez, en la sección 5.2, añade requisitos específicos complementarios adicionales de obligado cumplimiento de aplicación a los sistemas de información que soportan los SSG independientemente de su modalidad de despliegue.

Para la prestación del servicio se habilitan tres alternativas con respecto a la Declaración de Aplicabilidad del ENS y, por ende, las medidas que son de aplicación para dar cumplimiento al presente Perfil de Cumplimiento Específico:

a. Aquellos SSG que se presten desde entidades públicas o privados, que dispongan y puedan presentar la **certificación ENS de categoría MEDIA o superior** cuyo alcance cubra el o los sistemas de información que dan soporte a los SSG no tendrán que verificar el cumplimiento de la Declaración de Aplicabilidad descrita anteriormente. Sin embargo, estos SSG deben ser conocedores de los posibles refuerzos contemplados en el ENS indicados en la Declaración de Aplicabilidad y descritos en el capítulo 5.1 Criterios de Aplicación de Medidas para los sistemas de información desde los que se despliegan los SSG, y deben tener la capacidad de evidenciar su cumplimiento, así como de los **requisitos específicos complementarios** al ENS expuestos en la sección 5.2 de este documento.

b. Aquellos SSG que se presten desde entidades públicas o privados cuyos sistemas de información que dan soporte a los SSG **NO dispongan de la certificación ENS categoría MEDIA o superior**, podrán evidenciar inicialmente el cumplimiento de 36 medidas de seguridad y sus posibles refuerzos obligatorios que se muestran en las secciones 5.1 Medidas que son de Aplicación para los sistemas de información desde los que se despliegan los SSG. Estas 36 medidas han sido el resultado de un análisis exhaustivo de los requisitos de seguridad mínimos para proteger los SSG desplegados desde los sistemas de información concernidos. Por tanto, serán de obligado cumplimiento las **medidas y posibles refuerzos que emanan del propio ENS**, definidas en su Anexo II del RD 311/2022, de 3 de mayo, así como de los **requisitos específicos complementarios** al ENS expuestos en la sección 5.2 de este documento, con el **compromiso formal de obtener o haber iniciado el proceso de Certificación en el ENS** para los sistemas de información que dan soporte a los SSG en un **plazo máximo de 12 meses**.

c. Aquellos SSG que se despliegan desde entidades que no tengan por objeto prestar estos servicios a entidades públicas, infraestructuras críticas, infraestructuras esenciales o de cualquier otra naturaleza recogida en la Directiva NIS/2, no se les requerirá la certificación ENS categoría MEDIA o superior. En su defecto, se requerirá cumplimiento de las 36 **medidas de seguridad** citadas anteriormente y recogidas en la sección 5.1, así como dar cumplimiento a los **requisitos específicos complementarios** al ENS expuestos en la sección 5.2 de este documento.

Como material de apoyo para identificar las medidas que son de aplicación del ENS, los SSG podrán hacer uso del propio **ENS, Anexo II del RD 311/2022, de 3 de mayo** y de la **Guía de Seguridad de las TIC CCN-STIC 808 que describe la Verificación del Cumplimiento del ENS**.

Se debe tener en cuenta que los proveedores de SSG deberán tener en consideración los dispuesto en el REGLAMENTO DE EJECUCIÓN (UE) 2024/2690 DE LA COMISIÓN de 17 de octubre de 2024. Estas medidas deberán ser satisfechas en base a la categorización del sistema de la organización a la que se aplique y a su análisis de riesgos, pudiendo requerirse un incremento de las medidas de seguridad necesarias.

Teniendo en cuenta la casuística del modelo propuesto se ha determinado que, para garantizar la seguridad de los sistemas concernidos, la relación de medidas del Anexo II del ENS que resultan de aplicación y exigencia en el nivel de seguridad, son las recogidas en la siguiente tabla. El color azul en la columna “Aplicación” indica aquellas medidas cuya aplicación difiere con respecto a lo definido en el Anexo II del ENS. La numeración de la columna “Requisitos Específicos Complementarios” se corresponde con los requisitos definidos en la sección 5.2, que complementan los requisitos definidos en el ENS.

	Dimensiones					
Medida	Afectadas	CAT B	CAT M	CAT A	Aplicación	Requisitos Específicos Complementarios
org.1	Categoría	aplica	aplica	aplica	MEDIA	5.2.1
org.2	Categoría	aplica	aplica	aplica	MEDIA	
org.3	Categoría	aplica	aplica	aplica	MEDIA (+ R1)	
org.4	Categoría	aplica	aplica	aplica	MEDIA	
op.pl.1	Categoría	aplica	+ R1	+ R2	MEDIA (+ R2)	
op.pl.2	Categoría	aplica	+ R1	+ R1 + R2 + R3	MEDIA (+ R2)	5.2.2
op.pl.3	Categoría	aplica	aplica	aplica	MEDIA	
op.pl.4	D	aplica	+ R1	+ R1	Medio	
op.pl.5	Categoría	n.a.	aplica	aplica	MEDIA	5.2.3
op.acc.1	T A	aplica	+ R1	+ R1	Medio	
op.acc.2	C I T A	aplica	aplica	+ R1	Medio	
op.acc.3	C I T A	n.a.	aplica	+ R1	Medio (+ R1)	

op.acc.4	C I T A	aplica	aplica	aplica	Medio	
op.acc.5	C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5	Medio (obligatorio R4)	
op.acc.6	C I T A	[R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9	Medio (obligatorio R4)	
op.exp.1	Categoría	aplica	aplica	aplica	MEDIA (+ R2 + R3)	5.2.4
op.exp.2	Categoría	aplica	aplica	aplica	MEDIA	
op.exp.3	Categoría	aplica	+ R1	+ R1 + R2 + R3	MEDIA (+R3+R4+R5)	
op.exp.4	Categoría	aplica	+ R1	+ R1 + R2	MEDIA (+ R3 + R4)	
op.exp.5	Categoría	n.a.	aplica	+ R1	MEDIA (+ R1)	
op.exp.6	Categoría	aplica	+ R1+R2	+ R1+R2 + R3 R4	MEDIA (+ R4)	
op.exp.7	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3	MEDIA (+ R4)	5.2.5
op.exp.8	T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5	Medio (+ R5)	5.2.6
op.exp.9	Categoría	aplica	aplica	aplica	MEDIA	
op.exp.10	Categoría	aplica	+ R1	+ R1	MEDIA	
op.ext.1	Categoría	n.a.	aplica	aplica	MEDIA	5.2.7
op.ext.2	Categoría	n.a.	aplica	aplica	MEDIA	
op.ext.3	Categoría	n.a.	n.a.	aplica	ALTA (+ R1)	
op.ext.4	Categoría	n.a.	aplica	+ R1	MEDIA	
op.nub.1	Categoría	aplica	+ R1	+ R1 + R2	MEDIA	5.2.8
op.cont.1	D	n.a.	aplica	aplica	Medio	
op.cont.2	D	n.a.	n.a.	aplica	Alto (+ R1)	
op.cont.3	D	n.a.	n.a.	aplica	n.a.	
op.cont.4	D	n.a.	n.a.	aplica	Alto (+ R1)	
op.mon.1	Categoría	aplica	+ R1	+ R1 + R2	MEDIA (+ R2)	5.2.9
op.mon.2	Categoría	aplica	+ R1 + R2	+ R1 + R2	MEDIA	
op.mon.3	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 +R6	MEDIA	5.2.10
mp.if.1	Categoría	aplica	aplica	aplica	MEDIA	5.2.11
mp.if.2	Categoría	aplica	aplica	aplica	MEDIA	
mp.if.3	Categoría	aplica	aplica	aplica	MEDIA	
mp.if.4	D	aplica	+ R1	+ R1	Medio	
mp.if.5	D	aplica	aplica	aplica	Medio	
mp.if.6	D	n.a.	aplica	aplica	Medio	
mp.if.7	Categoría	aplica	aplica	aplica	MEDIA	
mp.per.1	Categoría	n.a.	aplica	aplica	MEDIA (+ R1 si aplica)	
mp.per.2	Categoría	aplica	+ R1	+ R1	MEDIA	
mp.per.3	Categoría	aplica	aplica	aplica	MEDIA	5.2.12
mp.per.4	Categoría	aplica	aplica	aplica	MEDIA	5.2.13
mp.eq.1	Categoría	aplica	+ R1	+ R1	MEDIA	
mp.eq.2	A	n.a.	aplica	+ R1	Medio	
mp.eq.3	Categoría	aplica	aplica	+ R1 + R2	MEDIA (+ R2)	
mp.eq.4	C	aplica	+ R1	+ R1	Medio	
mp.com.1	Categoría	aplica	aplica	aplica	MEDIA	

mp.com.2	C	aplica	+ R1	+ R1 + R2 + R3	Medio	5.2.14
mp.com.3	I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	Medio	
mp.com.4	Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4	MEDIA	
mp.si.1	C	n.a.	aplica	aplica	Medio	
mp.si.2	C I	n.a.	aplica	+ R1 + R2	Medio (+ R2)	
mp.si.3	Categoría	aplica	aplica	aplica	MEDIA	
mp.si.4	Categoría	aplica	aplica	aplica	MEDIA	
mp.si.5	C	aplica	R1	R1	Medio	
mp.sw.1	Categoría	n.a.	+ R1 + R2 + R3 +R4	+ R1 + R2 + R3 + R4	MEDIA	
mp.sw.2	Categoría	aplica	+ R1	+ R1	MEDIA (+ R2)	
mp.info.1	Categoría	aplica	aplica	aplica	MEDIA	
mp.info.2	C	n.a.	aplica	aplica	Medio	
mp.info.3	IA	aplica	+R1+R2+R3	+ R1+R2+R3+R4	Medio	
mp.info.4	T	n.a.	n.a.	aplica	n.a.	
mp.info.5	C	aplica	aplica	aplica	Medio	
mp.info.6	C	aplica	+ R1	+ R1 + R2	Medio	
mp.s.1	Categoría	aplica	aplica	aplica	MEDIA	
mp.s.2	Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3	MEDIA	
mp.s.3	Categoría	aplica	aplica	+ R1	MEDIA (+ R1 + R2)	
mp.s.4	D	n.a.	aplica	+ R1	Medio (+ R1 + R2)	

5.1 Medidas que son de aplicación para los sistemas de información que soportan y desde donde se despliegan los SSG

Según se describe en el apartado anterior, esta sección de medidas que son de aplicación para los sistemas de información que soportan y desde donde se despliegan los SSG recoge las 36 medidas de seguridad y sus posibles refuerzos que aplican únicamente a aquellos sistemas de información desde los que se despliegan los SSG que en el momento de la verificación del cumplimiento del presente PCE-SSG no dispongan de una certificación de ENS para categoría MEDIA o superior que abarque los SSG prestados o aquellos que no tengan por objeto prestar SSG a entidades públicas, infraestructuras críticas, infraestructuras esenciales o de cualquier otra naturaleza recogida en la Directiva NIS/2.

Para determinar las medidas de seguridad que son de aplicación se ha tenido en cuenta el nivel del riesgo asociado al sistema de información, en términos de probabilidad y repercusiones de un incidente de seguridad que pueda producirse durante la prestación de uno o más SSG.

Siguiendo dicho criterio, se han determinado para el Perfil de Cumplimiento Específico para SSG las medidas que son de aplicación para los sistemas de información que soportan y desde donde se despliegan los SSG, y, en caso de aplicar, la exigencia de los

posibles refuerzos del propio ENS obligatorios. Para este PCE aplica la categoría MEDIA del ENS para todas las medidas de aplicabilidad descritas a continuación.

La siguiente tabla refleja las 36 medidas de aplicación que emanan del Anexo II del ENS del RD 311/2022, de 3 de mayo en su categoría MEDIA y destaca o señala aquellos refuerzos adicionales que amplían o refuerzan lo definido en la categoría MEDIA del Anexo II del ENS.

En la columna de la derecha titulada "Aplicación" se encuentra la categoría del ENS de aplicación junto con, entre paréntesis, el refuerzo adicional requerido para el cumplimiento del presente PCE-SSG.

Las medidas en celdas de color blanco recogen aquellas medidas que son de aplicación y se mantienen estrictamente como se refleja en el Anexo II del ENS en su Categoría MEDIA, sin refuerzos ni ampliaciones.

Las medidas en celdas de color azul son aquellas que han sido ampliadas o reforzadas con respecto a lo definido en el Anexo II del ENS.

Numero	Medida ENS	Control	Aplicación
Marco Organizativo			
1	ORG.1	POLÍTICA DE SEGURIDAD	MEDIA
2	ORG.3	PROCEDIMIENTOS DE SEGURIDAD	MEDIA (+ R1)
Marco Operacional			
3	OP.PL.1	ANÁLISIS DE RIESGOS	MEDIA (+ R2)
4	OP.PL.2	ARQUITECTURA DE SEGURIDAD	MEDIA (+ R2)
5	OP.PL.4	DIMENSIONAMIENTO / GESTIÓN DE LA CAPACIDAD	MEDIA
6	OP.PL.5	COMPONENTES CERTIFICADOS	MEDIA
7	OP.ACC.3	SEGREGACIÓN DE FUNCIONES Y TAREAS	MEDIA (+ R1)
8	OP.ACC.5	MECANISMOS DE AUTENTICACIÓN (USUARIOS EXTERNOS)	MEDIA (obligatorio R4)
9	OP.ACC.6	MECANISMOS DE AUTENTICACIÓN (USUARIOS INTERNOS)	MEDIA (obligatorio R4)
10	OP.EXP.1	INVENTARIO DE ACTIVOS	MEDIA (+ R2 + R3)
11	OP.EXP.3	GESTIÓN DE LA CONFIGURACIÓN DE SEGURIDAD	MEDIA (+R3+R4+R5)
12	OP.EXP.4	MANTENIMIENTO Y ACTUALIZACIONES DE SEGURIDAD	MEDIA (+ R3 + R4)
13	OP.EXP.5	GESTIÓN DE CAMBIOS	MEDIA (+ R1)
14	OP.EXP.6	PROTECCIÓN FRENTE A CÓDIGO DAÑINO	MEDIA (+ R4)
15	OP.EXP.7	GESTIÓN DE INCIDENTES	MEDIA (+ R4)
16	OP.EXP.8	REGISTRO DE LA ACTIVIDAD	MEDIA (+ R5)
17	OP.EXT.1	CONTRATACIÓN Y ACUERDOS DE NIVEL DE SERVICIO	MEDIA
18	OP.EXT.3	PROTECCIÓN DE LA CADENA DE SUMINISTRO	ALTA (+ R1)
19	OP.NUB.1	PROTECCIÓN DE SERVICIOS EN LA NUBE	MEDIA
20	OP.CONT.2	PLAN DE CONTINUIDAD DE NEGOCIO	ALTA (+ R1)
21	OP.CONT.4	MEDIOS ALTERNATIVOS	ALTA (+R1)
22	OP.MON.1	DETECCIÓN DE INTRUSIÓN	MEDIA (+ R2)
23	OP.MON.2	SISTEMA DE MÉTRICAS	MEDIA
24	OP.MON.3	VIGILANCIA	MEDIA

Medidas de Protección			
25	MP.IF.1	ÁREAS SEPARADAS Y CON CONTROL DE ACCESO	MEDIA
26	MP.PER.1	CARACTERIZACIÓN DEL PUESTO DE TRABAJO	MEDIA (+ R1 si aplica)
27	MP.PER.3	CONCIENCIACIÓN	MEDIA
28	MP.PER.4	FORMACIÓN	MEDIA
29	MP.EQ.2	BLOQUEO DEL PUESTO DE TRABAJO	MEDIA
30	MP.EQ.3	PROTECCIÓN DE DISPOSITIVOS PORTÁTILES	MEDIA (+ R2)
31	MP.COM.2	PROTECCIÓN DE LA CONFIDENCIALIDAD	MEDIA
32	MP.SI.2	CRIPTOGRAFÍA	MEDIA (+ R2)
33	MP.SW.2	ACEPTACIÓN Y PUESTA EN SERVICIO	MEDIA (+ R2)
34	MP.INFO.6	COPIAS DE SEGURIDAD	MEDIA
35	MP.S.3	PROTECCIÓN DE LA NAVEGACIÓN WEB	MEDIA (+ R1 + R2)
36	MP.S.4	PROTECCIÓN FRENTE A DENEGACIÓN DE SERVICIO	MEDIA (+ R1 + R2)

Se han incorporado algunas medidas no aplicables en categoría **MEDIA** pero dada la naturaleza de los SSG resulta esencial incorporarlas. Estas medidas son: op.ext.3, op.cont.2 y op.cont.4.

5.2 Requisitos específicos complementarios que son de aplicación para los sistemas de información desde los que se despliegan los SSG

Tal y como se ha expuesto en las consideraciones previas de la Declaración de Aplicabilidad (Capítulo 5) y dada la naturaleza de los SSG se precisa disponer y cumplir a su vez con los **requisitos específicos complementarios que complementan las medidas de seguridad y del entorno del Anexo II del ENS**. Por tanto, toda entidad u organización cuyo objetivo sea certificarse bajo el presente PCE-SSG, debe y deberá verificar el cumplimiento de los requisitos específicos complementarios descritos a continuación.

5.2.1 [ORG.1] Política de Seguridad

En aquellos casos en los que los SSG opten por aplicar los requisitos de una inteligencia artificial en diferentes actividades como la revisión de patrones, alertas o implantación de filtros spam para el correo electrónico deberán tener en cuenta los aspectos derivados del Reglamento europeo de IA de la UE.

5.2.2 [OP.PL.2] Arquitectura de seguridad

La operación de los servicios de ciberseguridad se puede realizar desde una sala física y/o en remoto. Para ello, deben cumplirse los siguientes requisitos de seguridad:

a. Una sala física separada y segregada a nivel físico/lógico del resto de instancias de la organización. Se requerirá de un firewall dedicado, o solución similar, para la segmentación de redes y la interconexión con el resto de los recursos de la organización.

b. Se contempla la operación y el acceso por teletrabajo o en remoto al SOC. Este formato requiere el empleo de procedimientos para el teletrabajo y tecnologías que permitan mantener un elevado nivel de seguridad. Los equipos y usuarios que accedan a recursos del SOC en remoto deben cumplir con los siguientes requisitos:

    - Emplear VPN para garantizar comunicaciones cifradas y seguras.
    - Emplear Multi Factor de Autenticación (MFA) para garantizar un acceso seguro a los recursos e información del SOC.
    - Emplear y tener implementada herramienta Endpoint Detection and Response (EDR).

5.2.3 [OP.PL.5] Componentes certificados

Además de emplear componentes certificados, se verificará que los productos estén configurados tal y como han sido evaluados y han presentado conformidad con lo especificado para las diferentes taxonomías de seguridad del CPSTIC.

5.2.4 [OP.EXP.1] Inventario de activos

Se dispondrá de un inventario de activos (o una CMDB mostrando las dependencias entre los diferentes activos), permanentemente actualizado con verificaciones periódicas, que contenga todos los activos de valor para la operativa del servicio de ciberseguridad: recursos físicos, lógicos, operativos, personas, accesos, roles, configuraciones, procedimientos, etc.

5.2.5 [OP.EXP.7] Gestión de incidentes

Ante la posible materialización de un incidente de ciberseguridad, atendiendo al artículo 23 de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (NIS2), se deberán notificar aquellos incidentes de seguridad de categorías muy alta y crítica al Equipo de Respuesta ante Emergencias Informáticas (CERT) de referencia en materia de seguridad de las redes y sistemas de información, a saber:

- El CCN-CERT, del Centro Criptológico Nacional, al que corresponde la comunidad de referencia constituida por las entidades del ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre (sector público)
- El INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, al que corresponde la comunidad de referencia constituida por aquellas entidades no incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre. El INCIBE-CERT será operado conjuntamente por el INCIBE y el CNPIC en todo lo que se refiera a la gestión de incidentes que afecten a los operadores críticos. El INCIBE-CERT será, así mismo, equipo de respuesta a incidentes de referencia para los ciudadanos, entidades de derecho privado y otras entidades no incluidas anteriormente.

- El ESPDEF-CERT, del Ministerio de Defensa, que cooperará con el CCN-CERT y el INCIBE-CERT en aquellas situaciones que éstos requieran en apoyo de los operadores de servicios esenciales y, necesariamente, en aquellos operadores que tengan incidencia en la Defensa Nacional y que reglamentariamente se determinen.
- Su correspondiente Agencia de Ciber Seguridad para realizar la coordinación.

Se debe disponer de procedimientos de actuación ante un ciber-incidente. El procedimiento contemplará los casos de actuación al no contactar con la entidad a la que se presta el SSG. En estos procedimientos debe quedar reflejado los procesos de peticiones de evidencias, análisis y resultados de toda evidencia solicitada.

Se debe disponer de un servicio de asesoramiento de comunicación al exterior, comunicación dentro de la entidad o comunicación a medios de comunicación del incidente.

5.2.6 [OP.EXP.8] Registro de la actividad

Se deben generar registros de auditoría cuando se produzca alguno de los siguientes eventos:

- Al inicio y finalización de las funciones de auditoría.
- Login y logout de usuarios registrados.
- Cambios en las credenciales de usuarios.
- Cambios en la configuración de la solución [asignación: listado de cambios].
- Eventos relativos a la funcionalidad de la solución [asignación: listado de eventos].
- Si se gestionan claves criptográficas, [selección: generación; importación; cambio; eliminación de claves criptográficas].
- Los registros de auditoría contendrán, al menos, la siguiente información: fecha y hora del evento, tipo de evento identificado, resultado del evento, usuario que produce el evento.
- Creación de usuarios.
- Creación de usuario administrador.
- Instalación de programas.
- Cambios en las tareas programadas o servicios automáticos.
- Borrado de los logs.
- Borrado o desactivación de los elementos de protección como son EDR, AV, FW…

A los registros de auditoría se les aplicará la siguiente política de acceso:

- Lectura: usuarios autorizados.
- Modificación: ningún usuario.
- Borrado: no será posible, salvo que se alcance el período de retención establecido, y en todo caso bajo condiciones de supervisión.

5.2.7 [OP.EXT.1] Contratación y acuerdos de nivel de servicio

Con relación a los proveedores externos que sean contratados por la organización para provisionar recursos humanos, materiales o de servicios para la operativa de los SSG, se deberá:

- Realizar el seguimiento de la ejecución de los contratos con la organización en materia de seguridad de la información (en todas sus dimensiones), con el objetivo de obtener indicadores sobre la seguridad de los servicios ofrecidos por los proveedores.
- Relativo a los recursos humanos, la organización ha de validar que el personal provisionado por el proveedor externo cumple con los requisitos de personal referidos en este documento.
- Relativo a los recursos materiales, la organización ha de validar que lo provisionado por el proveedor externo cumple con los requisitos referidos en este documento.
- Relativo a los servicios, la organización ha de validar que lo provisionado por el proveedor externo cumple con los requisitos de seguridad establecidos en este documento.

De la misma manera, se documentarán los procedimientos de coordinación y gestión de los servicios contratados al proveedor, así como la gestión de los incidentes y eventos de seguridad identificados, con indicación del punto de contacto (POC) para reportarlos.

5.2.8 [OP.NUB.1] Protección de servicios en la nube

En el caso de disponer de entorno Cloud y/o aplicaciones Cloud en modalidad SaaS, se deberán seguir los requerimientos que se indican en siguientes apartados, así como disponer de un tenant Cloud dedicado para la operación de servicios de ciberseguridad.

En la actualidad, los entornos Cloud están siendo más utilizados que los modelos on premise para la operativa de los servicios de ciberseguridad, por lo que se requiere que dichos entornos en la Nube cumplan con unas medidas de seguridad parejas a los modelos en modo local, garantizando un entorno seguro, a saber:

- Seguridad de la información y los servicios: el proveedor de Cloud en el que se alberga parte de la infraestructura de los SSG de ciberseguridad o en el que se apoyan algunos de sus servicios debe disponer de sus Sistemas de Información, que soportan los servicios prestados, certificado del ENS categoría ALTA, certificación que garantiza un cumplimiento adecuado respecto a la seguridad.
- Integridad y protección de los datos: los datos que se alojen en los sistemas provistos por el proveedor Cloud serán de la organización, y en su defecto del cliente de esta. Por ello se debe contar con garantías en la disponibilidad de los datos durante el periodo requerido, asegurando a su vez que sea inalterable e inviolable. En consecuencia, se requerirá:

  - Política de backup y recuperación de los datos, con el testeo periódico de los mecanismos de recuperación.
  - Controles de seguridad de acceso a los datos almacenados y copiados.
  - Controles de monitorización del uso de los datos y flujo de los mismos.
  - Garantías de que los datos están claramente separados y aislados del resto de clientes del proveedor Cloud.
  - Cumplimiento de la normativa vigente de protección de datos, como el RGPD.
- Gestión del cambio y de la configuración: los cambios deben ser gestionados por el proveedor Cloud con un control exhaustivo de las acciones, del impacto que tiene sobre el servicio contratado por la organización y su nivel de intervención. En este sentido, deben existir unos mecanismos claros de comunicación de los cambios desde el proveedor del servicio de Cloud a la organización que presta los servicios gestionados. La documentación generada en este sentido deberá estar disponible para consulta de la organización en caso de necesidad.
- Seguridad: se ha de disponer de información muy detallada de cómo se realiza la gestión de los usuarios del Cloud, control de acceso, política de contraseñas, cifrado, etc. El proveedor debe demostrar que los controles implantados son efectivos y funcionan correctamente, ya sea mediante renovación de certificaciones, auditorías periódicas o informes respecto a los controles aplicados.
- Gestión de incidentes: el proveedor Cloud ha de disponer de un sistema eficaz de registro, clasificación, evaluación y resolución de las incidencias operativas y de los incidentes de seguridad. Los mecanismos de notificación de los incidentes a la organización que presta los servicios gestionados por parte del proveedor Cloud deben estar bien definidos, así como el nivel de intervención en la decisión de las acciones a tomar y las verificaciones de su resolución.
- Plan de continuidad: el proveedor Cloud ha de tener bien definido el plan de continuidad y verificar periódicamente su correcta aplicación, debiendo disponer de la capacidad técnica y de personal suficiente para ejecutar dicho plan en caso de necesidad.

Se tendrán en cuenta los certificados de seguridad de la UE como por ejemplo el esquema EUCS Esquema de Certificación de Ciberseguridad de la UE para Servicios en la Nube una vez que sea publicado.

5.2.9 [OP.MON.1] Detección de intrusión

No basta con implementar un sistema para la detección de intrusión, este debe implementar debidamente capacidades que permitan proteger debidamente los sistemas de información desde los que se despliegan los SSG. Por ello, la capacidad de detección de intrusión propia debe considerar:

- Los servidores y equipos finales deben estar protegidos con soluciones EDR o XDR.
- La definición de patrones de tráfico esperados y aprobados, anomalías, comportamiento, así como la descripción de la actividad de cada anomalía.
- la creación de listas blancas y/o negras de direcciones IP.
- La configuración de las políticas de IPS.
- Las aplicaciones web deben contar con un WAF que a su vez debe estar conectado con un sistema de monitorización.
- El análisis del tráfico de red basado en IP y detección de violaciones de las políticas definidas por el administrador del IPS.
- detección basada en casos de uso actualizados y que protejan de las amenazas más avanzadas y novedosas.
- Analizar, al menos, los siguientes tipos de tráfico: IPv4, IPv6, ICMPv4, ICMPv6, TCP, UDP, inspeccionando el contenido de las cabeceras de paquetes/unidades de datos, para detectar las siguientes firmas basadas en cabeceras:
    - Ataques IP: Solapamiento de fragmentos IP, IP origen y destino iguales.
    - Ataques ICMP: Tráfico ICMP fragmentado.
    - Ataques de 'ping flood' conocidos como ping de la muerte.
    - Ataques TCP: Flags TCP NULL, flags TCP SYN+FIN, flags solo TCP SYN, Flags TCP SYN+RST.
    - Ataques UDP: Ataques bomba UDP, Ataques DoS Chargen.
- Inspeccionar el contenido del payload (carga que se ejecuta aprovechando un exploit) de paquetes/unidades de datos IPv4, IPv6, ICMPv4, ICMPv6, TCP, UDP y detectar las siguientes firmas basadas en patrones de tráfico:
    - Ataques DoS a host: inundación ICMP, inundación TCP.
    - Ataques DoS a red.
    - Escaneo de puertos y protocolos (IP, TCP, UDP, ICMP).
    - Establecimiento umbrales de consultas o de uso de la red.
    - Generación de perfiles de usuarios conforme al uso de los sistemas de la entidad y estableciendo umbrales para detectar movimientos laterales.

5.2.10 [OP.MON.3] Vigilancia

La vigilancia de los sistemas de información debe cubrir al completo el ecosistema tecnológico de los sistemas de información concernidos para identificar posibles agujeros de ciberseguridad en la organización, en base a considerar la seguridad como un proceso integral.

De igual modo, deben considerarse otros aspectos determinados por la normativa en materia de protección de datos (RGPD / LOPDGDD). Esto es especialmente relevante para los SSG que operen con el sector público, considerando que para dicho sector las

medidas de seguridad necesarias para proteger datos de carácter personal, según la Disposición adicional primera de la LO 3/2018 (LOPDGDD), serán las del ENS.

Se realizará con una **periodicidad mínima de seis (6) meses, un test de penetración**, así como, con **periodicidad bimensual o inferior, un proceso de análisis automatizado de vulnerabilidades** de su superficie de exposición a internet de manera que queden cubiertos los requisitos técnicos aplicables a la organización. Para la red interna se deben revisar al menos equipos representativos y de uso diario de cada departamento de la entidad.

Estos análisis de vulnerabilidades y test de penetración seguirán una metodología aprobada por la organización y un procedimiento donde se detalle el alcance y detalle de dicho análisis: por ejemplo, activos y/o procesos a analizar y vulnerabilidades buscadas. Un mínimo de una auditoría de intrusión y mapeo de vulnerabilidades debería ser realizada por una tercera parte independiente reconocida por el CCN-CERT.

En el caso de las aplicaciones, además del requisito de ejecución periódica, será necesario realizar análisis técnicos cada vez que se produzcan cambios relevantes sobre las mismas, que pudieran alterar su seguridad o la del resto del sistema de información con el que interactúan.

El resultado de estos análisis técnicos será un elemento de entrada para la auditoría interna de los SSG y para la externa de certificación con respecto a este PCE-SSG.

Los resultados deben almacenarse en una herramienta de seguimiento de vulnerabilidades.

5.2.11 [MP.IF.1] Áreas separadas y con control de acceso

La sala de control y operación, donde desempeñan su trabajo los diferentes turnos, estará aislada del resto de dependencias, siendo sus paredes opacas, o translúcidas, para impedir que personal no relacionado, o visitas externas, accedan al contenido de las pantallas de visualización, especialmente las generales de la sala que suelen ser de grandes dimensiones.

La sala de control y operación estará asimismo permanentemente cerrada, disponiendo de mecanismos de control de acceso físico y registro de los mismos.

5.2.12 [MP.PER.3] Concienciación

Deben realizarse acciones de concienciación de manera que se cree una cultura de ciberseguridad en la organización y se ponga en valor.

5.2.13 [MP.PER.4] Formación

Deben realizarse acciones de concienciación de manera que se cree una cultura de ciberseguridad en la organización y se ponga en valor.

Asimismo, se tendrán en cuenta las iniciativas de formación continua del personal, como por ejemplo, la Cybersecurity Skills academy Cyber Skills Academy | Digital Skills and Jobs Platform (europa.eu)

5.2.14 [MP.COM.2] Protección de la confidencialidad

Para la protección del tráfico de red entre el servidor y sus clientes:

- Debe documentarse el modo en que está diseñada la red, los componentes de enrutamiento que necesita y la forma en que deben configurarse esos componentes (esta información puede ayudar a mantener la red y a identificar las áreas que puedan necesitar una atención especial o una mejora).
- La conexión VPN deberá ser del tipo IPSec y/o TLS-VPN 1.2 o superior, utilizando multi factor de autenticación (MFA) para establecer la conexión.
- Se limitarán los protocolos, puertos y dispositivos de destino accesibles en función del usuario que accede y del rol de este.

Para el control de los dispositivos cliente que acceden a la VPN, se tendrá en cuenta:

- Todo dispositivo cliente deberá cumplir unos requisitos mínimos previos a la conexión, como son:
  - Una protección EDR/XDR correctamente actualizada en el equipo.
  - Sistema operativo del dispositivo correctamente licenciado (en el caso que corresponda), bajo soporte del fabricante, actualizado y con los parches de seguridad precisos.

ANEXO I – PERFILES PROFESIONALES ASOCIADOS A LOS SSG CERTIFICADOS

A efectos meramente orientativos, la siguiente tabla muestra algunos de los perfiles profesionales más habituales en las entidades de prestación de SSG, indicando la cualificación deseable para cada uno de ellos.

PUESTO	DESCRIPCIÓN Y FUNCIONES	FORMACIÓN
Operadores de seguridad o analistas de seguridad de Niveles 1 y 2	Los operadores de seguridad son habitualmente los primeros en detectar, y en su caso responder, ante eventos detectados que puedan llegar a manifestar posibles incidentes de seguridad. Se organizan en varios turnos para detectar y responder a incidentes que surjan a cualquier hora, estando ubicados en el interior de la sala de control del SOC. Distinguiremos operadores, también designados como analistas, de nivel 1 o 2, aunque en determinados SOC no se realiza dicha distinción. Analistas de nivel 1: Son el punto de entrada y su función es la de monitorización, 'triaje' de eventos de seguridad (asignación nivel de criticidad), identificación de falsos positivos y detección temprana de incidentes de seguridad. Generalmente realizan tareas documentadas basadas en procedimientos operativos, escalando lo que se vislumbra como amenaza a nivel 2. Analistas de nivel 2: en este segundo nivel, los analistas realizarán análisis de incidentes no documentados. Todas las alertas de seguridad son supervisadas por este nivel, con el objetivo de centralizar todo el feedback de incidentes y así poder distribuirlo entre todos los niveles del SOC. Mediante investigaciones básicas,	• Formación técnica específica en seguridad de sistemas y redes. • Cursos sobre herramientas de monitorización o protección relativas a la infraestructura de seguridad de una organización. • Curso de concienciación en ciberseguridad. • Recomendable disponer del Curso del ENS • Concienciación respecto al código ético del SOC. • Curso de legislación básica aplicable. • Deberán contar con al menos 3 años de experiencia.

	darán posibles soluciones de contención del incidente y proporcionarán recomendaciones para realizar cambios en los sistemas de la organización cliente de sus servicios, con el fin de evitar posibles propagaciones en el caso de una infección malware. Su desempeño consiste en investigar amenazas, priorizarlas, comunicarlas y, en su caso, responder a ellas, a modo de contención. Para ello seguirá protocolos y casos de uso establecidos.	
Analistas de seguridad de nivel 3	Es el último nivel de escalado dentro del SOC, tanto para alertas de seguridad como problemas de funcionamiento. Este nivel está formado por grupo de especialistas en distintos ámbitos (seguridad de red, seguridad de EndPoint, seguridad de correo, seguridad en sistemas, Malware, APTs, especialistas en sistemas, almacenamiento, etc). Cuando se determina que un incidente representa un problema de seguridad, deberá deducir, entre otros aspectos, quién es el atacante, qué recursos están afectados o la naturaleza del ataque. Su labor consistirá en: • Análisis exhaustivo de incidentes de seguridad escalados por el nivel 2, recopilando y analizando la información relacionada. • Configuración de las herramientas de seguridad (SIEM, IDS/IPS, EDR, etc.). • Determinar qué anomalías representan una amenaza real. • Diseñar / proponer la respuesta de subsanación a la amenaza. • Determinar activos afectados y clasificar el riesgo. • Investigar problemas de seguridad y proponer soluciones	• Formación en disciplinas de tecnologías de la información, informática o equivalente. • Experiencia mínima de 5 años en niveles 1, 2 y 3. • Formación técnica específica en seguridad y ciberdefensa. • Formación y certificación específica de los servicios a operar. • Comprobación de referencias en los puestos previos. • Curso de concienciación en ciberseguridad. • Recomendable disponer del Curso del ENS. • Concienciación respecto al código ético del SOC. • Curso de legislación básica aplicable.

	• Activación y coordinación de la respuesta ante incidentes.	
Ingenieros de seguridad	Su función es responsabilizarse de mantener las herramientas, recomendar nuevas herramientas y actualizar los sistemas del SOC. Muchos ingenieros de seguridad se especializan, entre otras, en plataformas SIEM. Los ingenieros de seguridad son responsables de la construcción de la arquitectura y los sistemas de seguridad. Habitualmente, según las dimensiones de la organización, trabajan con equipos de operaciones para garantizar que los sistemas estén actualizados. Además, los ingenieros de seguridad documentan los requisitos, procedimientos y protocolos para garantizar que otro personal, como los operadores de seguridad, tengan los recursos adecuados. Asimismo, ayudan a los consultores de seguridad a definir la arquitectura de monitorización necesaria tanto en la propia infraestructura, como en la de los clientes del servicio de SOC, así como las comunicaciones seguras entre ambas.	• Formación en disciplinas de tecnologías de la información, informática o equivalente. • Experiencia mínima de 5 años previos al acceso al puesto en actividades relacionadas. • Formación técnica específica en seguridad de sistemas y redes. • Formación y certificación en tecnologías a operar en el servicio SOC. • Comprobación de referencias en puestos previos. • Curso de concienciación en ciberseguridad. • Recomendable disponer del Curso del ENS. • Concienciación respecto al código ético del SOC. • Curso de legislación básica aplicable.
Consultores de seguridad	Su función es de asesoramiento al cliente respecto a los servicios que le son adecuados, de los que ofrece el SOC, en función de su realidad y riesgos. Definirán las necesidades de arquitectura y equipamiento para poder realizar la monitorización adecuada, en coordinación con el/los Ingenieros de Seguridad.	• Formación en disciplinas de tecnologías de la información, informática o equivalente. • Experiencia mínima de 3 años previos acceso al puesto en actividades relacionadas. • Formación técnica específica en seguridad y ciberdefensa.

		• Formación y certificación específica de los servicios base y avanzados que presta el SOC. • Comprobación de referencias puestos previos. • Curso de concienciación en ciberseguridad. • Recomendable disponer del Curso del ENS. • Concienciación respecto al código ético del SOC. • Curso de legislación básica aplicable.
Responsable de un servicio	Para cada servicio (o agrupación de servicios) prestado por el SOC, de acuerdo con las competencias que cubra, puede definirse un responsable que coordinará sus operaciones y recursos.	• Formación en disciplinas de tecnologías de la información, informática o equivalente. • Experiencia mínima de 5 años previos acceso al puesto en dicho servicio. • Formación técnica específica en seguridad y ciberdefensa. • Formación y certificación específica del servicio del que pretende responsabilizarse en el SOC. • Comprobación de referencias puestos previos. • Curso de concienciación en ciberseguridad. • Recomendable disponer del Curso del ENS.

		• Concienciación respecto al código ético del SOC. • Curso de legislación básica aplicable.
SOC Manager o gerente de seguridad	Su función es gestionar los diferentes equipos multidisciplinares dentro del SOC, habitualmente a través de los responsables de cada servicio ofrecido. Como responsable de todos los servicios y miembros del SOC, realiza tareas que tienden a ser menos técnicas y más relacionadas con la gestión, responsabilizándose de supervisar las operaciones en su conjunto, coordinando los equipos y sus relaciones con los ingenieros de seguridad del SOC. Es asimismo responsable de la elaboración de políticas y protocolos para la gestión del SOC, así como de nuevos procesos. Entre sus funciones destacan: • Cumplir los objetivos establecidos por el órgano de gobierno del SOC. • Alinear los objetivos propuestos de gestión con los técnicos, involucrando a todas las partes interesadas. • Gestionar los diferentes equipos del SOC. • Comunicación del SOC con los clientes de sus servicios a través de los consultores de seguridad. • Gestionar el presupuesto del SOC, aprobando las compras de herramientas y activos necesarios.	• Formación gestión de empresas tecnológicas. • Experiencia mínima 5 años previos al acceso al puesto en funciones relacionadas. • Formación técnica específica en seguridad y ciberdefensa. • Formación y certificaciones en gestión e la seguridad. • Comprobación de referencias en puestos previos • Curso de concienciación en ciberseguridad. • Formación del ENS. • Concienciación respecto al código ético del SOC. • Curso de legislación básica aplicable.

Personal de servicios generales (como es Financiero y RRHH)	Como en cualquier organización, puede haber personal sin una implicación directa en los servicios de SOC prestados que deben estar concienciados en seguridad y conducirse bajo los principios éticos del SOC.	• Comprobación de referencias en puestos previos. • Curso de concienciación en ciberseguridad. • Concienciación respecto al código ético del SOC.
Personal externo	El personal externo subcontratado deberá cumplir con los mismos requisitos que se solicitan para los empleados propios de la organización y, a su vez, la empresa a la que pertenece el subcontratado deberá cumplir con los requisitos identificados orientados a empresas proveedoras, según las disposiciones de esta guía para Centros de Operaciones de Ciberseguridad (SOC), acorde con el ENS.	• Medidas [mp.per] para el personal. • Medidas [op.ext] para la organización a la que pertenecen los externos.