Guía de Seguridad de las TIC
CCN-STIC 8001

EL ESQUEMA NACIONAL DE SEGURIDAD DE ESPAÑA

Un modelo integral de ciberseguridad, confianza y conformidad para Europa y para el mundo

ENS 360



Documento de síntesis para interlocución institucional y proyección internacional

Noviembre 2026

Edita:

centro criptológico nacional

© Centro Criptológico Nacional, 2026

Firmado digitalmente por CCN
Fecha: 2026.11.23 11:39:39 +01'00'

Fecha de Edición: noviembre de 2026

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

ÍNDICE

0. RESUMEN EJECUTIVO 7
0.1. QUÉ ES EL ENS 7
0.2. QUÉ APORTA EL MODELO ESPAÑOL 8
0.3. A QUIÉN SE APLICA 9
0.4. QUÉ ELEMENTOS LO INTEGRAN 9
0.5. POR QUÉ PUEDE SERVIR COMO REFERENCIA NACIONAL E INTERNACIONAL 10
1. NATURALEZA Y FUNCIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD 11
1.1. EL ENS COMO MARCO JURÍDICO-TÉCNICO DE SEGURIDAD DE LA INFORMACIÓN 12
1.2. EL ENS COMO INSTRUMENTO DE CONFIANZA EN LA ADMINISTRACIÓN DIGITAL 14
1.3. EL ENS COMO MODELO DE GOBERNANZA, CUMPLIMIENTO Y MEJORA CONTINUA 15
1.4. EL ENS COMO SISTEMA VERIFICABLE DE CONFORMIDAD, AUDITORÍA Y CERTIFICACIÓN 16
1.5. VALOR ESTRATÉGICO DEL ENS PARA ESPAÑA Y PARA TERCEROS PAÍSES 18
1.6. LOS PERFILES DE CUMPLIMIENTO ESPECÍFICO COMO RESPUESTA A NECESIDADES SECTORIALES 19
1.7. RESUMIENDO… 20
2. MARCO JURÍDICO Y ÁMBITO DE APLICACIÓN 20
2.1. EL REAL DECRETO 311/2022, DE 3 DE MAYO 22
2.2. RELACIÓN CON LA ADMINISTRACIÓN DIGITAL Y LOS SERVICIOS PÚBLICOS ELECTRÓNICOS 24
2.3. RELACIÓN CON LA CIBERSEGURIDAD NACIONAL 24
2.4. RELACIÓN CON LA PROTECCIÓN DE DATOS PERSONALES 25
2.5. RELACIÓN CON EL DERECHO EUROPEO DE LA CIBERSEGURIDAD 27
2.6. ENTIDADES DEL SECTOR PÚBLICO OBLIGADAS 27
2.7. APLICACIÓN A ENTIDADES PRIVADAS PROVEEDORAS DEL SECTOR PÚBLICO 28
2.8. APLICACIÓN EN CONTRATACIÓN PÚBLICA, SERVICIOS EXTERNALIZADOS, CLOUD Y CADENA DE SUMINISTRO 29
2.9. RESUMIENDO… 30
3. CONTENIDO ESENCIAL DEL ENS (REAL DECRETO 311/2022, DE 3 DE MAYO) 30
3.1. OBJETO, FINALIDAD Y ESTRUCTURA DEL ENS 31
3.2. PRINCIPIOS BÁSICOS DE SEGURIDAD 32
3.3. REQUISITOS MÍNIMOS DE SEGURIDAD 33
3.4. ORGANIZACIÓN DE LA SEGURIDAD Y ROLES ESENCIALES 34
3.5. POLÍTICA DE SEGURIDAD 35
3.6. CATEGORIZACIÓN DE LOS SISTEMAS DE INFORMACIÓN 36
3.7. MEDIDAS DE SEGURIDAD DEL ANEXO II 37
3.8. AUDITORÍA DE LA SEGURIDAD 39
3.9. INFORME DEL ESTADO DE LA SEGURIDAD 40
3.10. GESTIÓN Y NOTIFICACIÓN DE INCIDENTES 40
3.11. DECLARACIÓN Y CERTIFICACIÓN DE CONFORMIDAD 41
3.12. MEJORA CONTINUA Y REEVALUACIÓN PERIÓDICA 42
3.13 RESUMIENDO… 44
4. CATEGORIZACIÓN, MEDIDAS DE SEGURIDAD Y CICLO DE CUMPLIMIENTO 45
4.1. CATEGORIZACIÓN DE LOS SISTEMAS: FINALIDAD Y METODOLOGÍA 46
4.2. DIMENSIONES DE SEGURIDAD: CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD, AUTENTICIDAD Y TRAZABILIDAD 48
4.3. CATEGORÍAS BÁSICA, MEDIA Y ALTA 49
4.4. SELECCIÓN DE MEDIDAS DE SEGURIDAD 51
4.5. MARCO ORGANIZATIVO, MARCO OPERACIONAL Y MEDIDAS DE PROTECCIÓN 52
4.6. DECLARACIÓN DE APLICABILIDAD 53

4.7. DIAGNÓSTICO, ADECUACIÓN, AUDITORÍA Y MANTENIMIENTO DE LA CONFORMIDAD 54
4.8. EL ENS COMO CICLO DE GESTIÓN DE RIESGOS Y MEJORA CONTINUA.....56
4.9. RESUMIENDO… 59
5. LAS INSTRUCCIONES TÉCNICAS DE SEGURIDAD DEL ENS.....59
5.1. NATURALEZA, FUNCIÓN Y VALOR DE LAS ITS 60
5.2. ITS DE CONFORMIDAD CON EL ENS.....62
5.3. ITS DE AUDITORÍA DE LA SEGURIDAD.....63
5.4. ITS DE NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD.....65
5.5. ITS DE INFORME DEL ESTADO DE LA SEGURIDAD.....66
5.6. PAPEL DE LAS ITS EN LA HOMOGENEIZACIÓN DE CRITERIOS.....67
5.7. RELACIÓN ENTRE LAS ITS, EL REAL DECRETO 311/2022 Y LAS GUÍAS CCN-STIC.....69
5.8. VALOR PRÁCTICO DE LAS ITS PARA ENTIDADES OBLIGADAS, AUDITORES Y CERTIFICADORES70
5.9. RESUMIENDO… 72
6. LAS GUÍAS CCN-STIC DE LA SERIE 800 Y LAS HERRAMIENTAS DE APOYO DEL CCN.....73
6.1. NATURALEZA Y FUNCIÓN DE LAS GUÍAS CCN-STIC.....74
6.2. LA SERIE 800 COMO CUERPO DOCTRINAL DE IMPLANTACIÓN DEL ENS 75
6.3. CLASIFICACIÓN FUNCIONAL DE LAS GUÍAS DE LA SERIE 800.....76
6.4. GUÍAS SOBRE ADECUACIÓN Y CUMPLIMIENTO.....78
6.5. GUÍAS SOBRE AUDITORÍA Y CERTIFICACIÓN.....79
6.6. GUÍAS SOBRE ANÁLISIS Y GESTIÓN DE RIESGOS.....80
6.7. GUÍAS SOBRE GOBERNANZA, ROLES Y ORGANIZACIÓN DE LA SEGURIDAD 80
6.8. GUÍAS SOBRE MEDIDAS DE PROTECCIÓN, SERVICIOS CLOUD, CONTRATACIÓN Y EXTERNALIZACIÓN 82
6.9. GUÍAS RELEVANTES PARA ENTIDADES CON REQUISITOS ESPECÍFICOS O DE MENOR DIMENSIÓN: LOS PERFILES DE CUMPLIMIENTO ESPECÍFICO. 83
6.10. HERRAMIENTAS DE APOYO DEL CCN: INES, AMPARO Y OTRAS SOLUCIONES ORIENTADAS AL CUMPLIMIENTO. 84
6.11. VALOR DE LAS GUÍAS Y HERRAMIENTAS PARA LA HOMOGENEIZACIÓN, ESCALABILIDAD Y SOSTENIBILIDAD DEL ENS 86
6.12 RESUMIENDO.....90
7. AUDITORÍA, CERTIFICACIÓN Y ACREDITACIÓN: EL SISTEMA DE CONFIANZA DEL ENS.....91
7.1. DECLARACIÓN DE CONFORMIDAD Y CERTIFICACIÓN DE CONFORMIDAD 92
7.2. SISTEMAS DE CATEGORÍA BÁSICA, MEDIA Y ALTA.....93
7.3. PROCEDIMIENTO DE AUDITORÍA.....94
7.4. PROCEDIMIENTO DE CERTIFICACIÓN 96
7.5. VIGENCIA, SEGUIMIENTO, RENOVACIÓN, SUSPENSIÓN Y RETIRADA DE CERTIFICADOS 97
7.6. ENTIDADES DE CERTIFICACIÓN DEL ENS.....98
7.7. FUNCIÓN DE ENAC EN LA ACREDITACIÓN DE ENTIDADES DE CERTIFICACIÓN.....99
7.8. USO DE UNE-EN ISO/IEC 17065 COMO NORMA DE REFERENCIA PARA LA ACREDITACIÓN DE ENTIDADES CERTIFICADORAS 100
7.9. NORMATIVA INTERNA DE ENAC APLICABLE A ENTIDADES ACREDITADAS O EN PROCESO DE ACREDITACIÓN.....101
7.10. IMPARCIALIDAD, COMPETENCIA TÉCNICA, TRAZABILIDAD Y SUPERVISIÓN 102
7.11. VALOR DE LA ACREDITACIÓN PARA LA CONFIANZA NACIONAL E INTERNACIONAL DEL ENS104
7.12 RESUMIENDO… 107
8. EL ENS COMO MODELO DE CONFIANZA PARA LA CONTRATACIÓN PÚBLICA Y LA COLABORACIÓN PÚBLICO-PRIVADA 108
8.1. INCORPORACIÓN DEL ENS EN PLIEGOS, CONTRATOS Y ENCARGOS PÚBLICOS.....109
8.2. PROVEEDORES TECNOLÓGICOS Y PRESTADORES DE SERVICIOS EXTERNALIZADOS 110

8.3. SERVICIOS CLOUD Y SERVICIOS GESTIONADOS DE SEGURIDAD 111
8.4. CONTROL DE LA CADENA DE SUMINISTRO 112
8.5. BENEFICIOS PARA ENTIDADES PÚBLICAS 113
8.6. BENEFICIOS PARA EMPRESAS PRIVADAS PROVEEDORAS DEL SECTOR PÚBLICO 114
8.7. RIESGOS DE CUMPLIMIENTO MERAMENTE FORMAL 116
8.8. BUENAS PRÁCTICAS CONTRACTUALES 117
8.9. RESUMIENDO… 121
9. ALINEAMIENTO EUROPEO E INTERNACIONAL DEL ENS 121
9.1. ENS Y DIRECTIVA NIS2 122
9.2. ENS Y REGLAMENTO DE CIBERSEGURIDAD DE LA UNIÓN EUROPEA 124
9.3. ENS Y ESQUEMAS EUROPEOS DE CERTIFICACIÓN DE CIBERSEGURIDAD 125
9.4. ENS E ISO/IEC 27001 E ISO/IEC 27002 126
9.5. ENS, ISO/IEC 17065 Y ACREDITACIÓN DE CERTIFICADORES 127
9.6. ENS Y REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS 128
9.7. EL ENS COMO MODELO NACIONAL COMPLEMENTARIO A MARCOS EUROPEOS E INTERNACIONALES 129
9.8. POSIBLES VÍAS DE RECONOCIMIENTO, EQUIVALENCIA O INTEROPERABILIDAD INTERNACIONAL 130
9.9. RESUMIENDO… 133
10. VALOR DIFERENCIAL DEL ENS Y RAZONES PARA SU PROYECCIÓN INTERNACIONAL 134
10.1. EL ENS COMO SISTEMA COMPLETO, NO COMO MERO ESTÁNDAR TÉCNICO 134
10.2. OBLIGATORIEDAD JURÍDICA Y APLICABILIDAD AL SECTOR PÚBLICO 135
10.3. EXTENSIÓN A PROVEEDORES PRIVADOS DEL SECTOR PÚBLICO 136
10.4. CATEGORIZACIÓN PROPORCIONAL BASADA EN IMPACTO 137
10.5. AUDITORÍA Y CERTIFICACIÓN VERIFICABLES 138
10.6. ACREDITACIÓN DE ENTIDADES CERTIFICADORAS 138
10.7. PAPEL DEL CCN COMO AUTORIDAD TÉCNICA DE REFERENCIA 139
10.8. GUÍAS, HERRAMIENTAS Y ACOMPAÑAMIENTO TÉCNICO 140
10.9. MADUREZ, TRAZABILIDAD Y MEJORA CONTINUA 141
10.10. ELEMENTOS EXPORTABLES DEL MODELO ESPAÑOL 141
10.11. RESUMIENDO… 144
11. CONCLUSIONES 145
11.1. EL ENS COMO INFRAESTRUCTURA NACIONAL DE CONFIANZA DIGITAL 145
11.2. EL ENS COMO ACTIVO ESTRATÉGICO DEL ESTADO ESPAÑOL 146
11.3. EL ENS COMO MODELO DE GOBERNANZA, CUMPLIMIENTO Y CERTIFICACIÓN 147
11.4. EL ENS COMO REFERENCIA ÚTIL PARA OTROS PAÍSES 147
11.5. NECESIDAD DE PRESERVAR, REFORZAR Y PROYECTAR INTERNACIONALMENTE EL MODELO ENS 148
ANEXO I. CUADRO RESUMEN DEL REAL DECRETO 311/2022 150
PARTE I: ESTRUCTURA DE CAPÍTULOS Y ARTÍCULOS (DEL 1 AL 41) 150
PARTE II: DISPOSICIONES ADICIONALES, TRANSITORIAS Y FINALES 155
PARTE III: LOS CUATRO ANEXOS TÉCNICOS DEL REAL DECRETO 156
ANEXO II. CUADRO RESUMEN DE LAS CUATRO ITS 161
ANEXO III. RELACIÓN DE GUÍAS CCN-STIC DE LA SERIE 800 164
ANEXO IV. RESUMEN SINTÉTICO DE LAS GUÍAS CCN-STIC DE LA SERIE 800 DE ESPECIAL RELEVANCIA PRÁCTICA 176
CCN-STIC 801: RESPONSABILIDADES Y FUNCIONES EN EL ENS 176
CCN-STIC 802: GUÍA DE AUDITORÍA DEL ENS 176
CCN-STIC 803: VALORACIÓN DE SISTEMAS EN EL ENS 177
CCN-STIC 804: MEDIDAS DE IMPLANTACIÓN DEL ENS 177

CCN-STIC 805: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 178
CCN-STIC 806: PLAN DE ADECUACIÓN AL ENS 178
CCN-STIC 808: VERIFICACIÓN DEL CUMPLIMIENTO DEL ENS 178
CCN-STIC 809: DECLARACIÓN DE CONFORMIDAD CON EL ENS 179
CCN-STIC 831: REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS 179
CCN-STIC 817: GESTIÓN DE CIBERINCIDENTES 179
CCN-STIC 823: SEGURIDAD EN ENTORNOS CLOUD 180
CCN-STIC 830: ÁMBITO DE APLICACIÓN DEL ENS 180
CCN-STIC 827: GESTIÓN Y USO DE DISPOSITIVOS MÓVILES 180
CCN-STIC 824: INFORMACIÓN DEL ESTADO DE SEGURIDAD 181
CCN-STIC 807: CRIPTOLOGÍA DE EMPLEO EN EL ENS 181
CCN-STIC 812: SEGURIDAD EN ENTORNOS Y APLICACIONES WEB 181
CCN-STIC 883: GUÍA DE IMPLANTACIÓN DEL ENS PARA ENTIDADES LOCALES 182
CCN-STIC 823 — ANEXO: CLAUSULADO Y ACUERDOS DE NIVEL DE SERVICIO 182
CCN-STIC 890: ADECUACIÓN AL ENS CONFORME AL PERFIL DE CUMPLIMIENTO ESPECÍFICO DE REQUISITOS FUNDAMENTALES DE SEGURIDAD 183
CCN-STIC 891: PERFIL DE CUMPLIMIENTO ESPECÍFICO PARA SALUD 183
CCN-STIC 896: PERFIL DE CUMPLIMIENTO ESPECÍFICO PARA SERVICIOS DE SEGURIDAD GESTIONADOS / PCE-SSG 183
CCN-STIC 897: PERFIL DE CUMPLIMIENTO ESPECÍFICO PARA LA ADMINISTRACIÓN DE JUSTICIA 184

ANEXO V. HERRAMIENTAS DE APOYO DEL CCN PARA LA IMPLANTACIÓN Y SEGUIMIENTO DEL ENS Y SUS FUNCIONES. 185

ANEXO VI. ESQUEMA GRÁFICO DEL CICLO DE CUMPLIMIENTO DEL ENS. 191

ANEXO VII. ESQUEMA GRÁFICO DEL SISTEMA DE AUDITORÍA, CERTIFICACIÓN Y ACREDITACIÓN 192

ANEXO IX. GLOSARIO DE TÉRMINOS BÁSICOS DEL ENS 198

MARCO GENERAL Y ÁMBITO 198
PRINCIPIOS BÁSICOS 198
ROLES DE RESPONSABILIDAD 199
POLÍTICA DE SEGURIDAD Y REQUISITOS MÍNIMOS 199
CATEGORIZACIÓN DE SISTEMAS Y DIMENSIONES DE SEGURIDAD (ANEXO I ENS) 200
MEDIDAS DE SEGURIDAD (ANEXO II ENS) 200
AUDITORÍA, INFORME Y CONFORMIDAD (CAPÍTULOS IV Y V; ANEXO III ENS) 201
INCIDENTES Y RESPUESTA 201
GLOSARIO OFICIAL — ANEXO IV DEL RD 311/2022 202

0. RESUMEN EJECUTIVO

El **Esquema Nacional de Seguridad** es el marco jurídico-técnico español que ordena la seguridad de los sistemas de información que soportan la actuación del sector público, la prestación de servicios públicos digitales y, cuando proceda, la intervención de proveedores privados vinculados a dichos servicios. Su valor no reside sólo en imponer medidas de seguridad, sino en configurar un modelo integral de confianza digital: obligatorio, proporcionado, verificable, certificable y orientado a la mejora continua.

Desde una **perspectiva institucional**, **el ENS debe entenderse como una infraestructura regulatoria de confianza. Permite conectar norma jurídica, gobernanza, gestión de riesgos, medidas técnicas y organizativas, guías de apoyo, herramientas públicas, auditoría, certificación, acreditación y seguimiento**. Esta combinación convierte al modelo español en una referencia singular dentro del ecosistema europeo de ciberseguridad pública.

El mensaje ejecutivo es claro: **España no dispone únicamente de una norma de ciberseguridad para el sector público; dispone de un sistema nacional para generar, demostrar y proyectar confianza en los servicios públicos digitales y en el mercado tecnológico que los sostiene**.



Figura 0.1 El ENS como cadena de confianza digital.

0.1. QUÉ ES EL ENS

El ENS es el **conjunto de principios básicos, requisitos mínimos, medidas de seguridad y mecanismos de verificación que deben aplicarse para proteger la información tratada y los servicios prestados por medios electrónicos por las entidades incluidas en su ámbito de aplicación.** Su finalidad es asegurar aquellos componentes esenciales del desenvolvimiento electrónico, tales como la disponibilidad de los servicios o la confidencialidad, la integridad, la autenticidad, la trazabilidad, el acceso o la conservación de la información.

Su fundamento normativo se encuentra en el régimen jurídico de la Administración digital y se concreta en el Real Decreto 311/2022, de 3 de mayo. No se trata de una recomendación voluntaria ni de una guía de buenas prácticas, sino de **un marco de obligado cumplimiento en su ámbito de aplicación, con capacidad para ordenar la seguridad de los sistemas públicos y de los sistemas privados que soportan servicios o soluciones para el sector público.**

La seguridad que exige el ENS no es uniforme ni abstracta. Se articula mediante la **categorización de los sistemas, la valoración del impacto en las distintas dimensiones de seguridad, la selección de medidas proporcionadas, la elaboración de la Declaración de Aplicabilidad, la implantación de controles y la verificación de la conformidad.** De este modo, el ENS transforma la seguridad en un proceso gestionable y auditable.

0.2. QUÉ APORTA EL MODELO ESPAÑOL

El modelo español aporta una arquitectura completa. En primer lugar, proporciona **seguridad jurídica**, porque fija obligaciones exigibles para las entidades públicas y para determinados proveedores privados. En segundo lugar, aporta **gobernanza**, porque obliga a definir responsabilidades, políticas de seguridad, procedimientos, órganos de coordinación y mecanismos de supervisión. En tercer lugar, aporta **proporcionalidad**, porque ajusta la exigencia al impacto de la información y de los servicios afectados.

En cuarto lugar, el ENS aporta **operatividad técnica**, mediante un catálogo de medidas estructurado en marco organizativo, marco operacional y medidas de protección. En quinto lugar, ofrece **acompañamiento**, a través de las Instrucciones Técnicas de Seguridad, las Guías CCN-STIC de la serie 800 y las herramientas del CCN. En sexto lugar, genera **confianza verificable**, mediante autoevaluación, auditoría, Declaración de Conformidad, Certificación de Conformidad, acreditación de entidades certificadoras y mantenimiento de evidencias.

Su singularidad está en la integración de todos estos elementos. Muchos marcos ofrecen controles, guías o certificaciones parciales. El ENS los articula en un sistema público de cumplimiento, evaluación y mejora. Por eso debe presentarse como un ecosistema, no como una simple norma técnica.

Dimensión	Aportación del ENS	Mensaje ejecutivo
Jurídica	Marco obligatorio para entidades públicas y determinados proveedores privados.	La seguridad deja de ser voluntaria y se convierte en exigencia institucional.
Organizativa	Roles, política de seguridad, responsabilidades, procedimientos y gestión de riesgos.	La seguridad se gobierna, no se improvisa.
Técnica	Medidas del Anexo II, categorización, Declaración de Aplicabilidad y controles proporcionales.	La seguridad se adapta al impacto real de los sistemas.

Dimensión	Aportación del ENS	Mensaje ejecutivo
Operativa	ITS, Guías CCN-STIC, herramientas del CCN y criterios de implantación.	El modelo no sólo exige: acompaña el cumplimiento.
Confianza	Auditoría, declaración, certificación, acreditación y seguimiento.	El cumplimiento puede demostrarse frente a terceros.
Mercado	Proyección contractual sobre proveedores, cloud, servicios gestionados y cadena de suministro.	La contratación pública se convierte en palanca de ciberseguridad.

Figura 0.2. Propuesta de valor del ENS para una lectura ejecutiva.

0.3. A QUIÉN SE APLICA

El ENS se aplica al conjunto del **sector público** en los términos previstos por la normativa vigente. Esto incluye: **la Administración General del Estado, las Administraciones de las comunidades autónomas, las entidades que integran la Administración local, el sector público institucional y otras entidades que gestionen sistemas de información vinculados al ejercicio de potestades públicas, a la prestación de servicios públicos o al tratamiento de información pública.**

Además, el ENS **se proyecta también sobre entidades privadas** cuando, en virtud de una relación contractual, presten servicios o provean soluciones a entidades del sector público para el ejercicio de sus competencias y potestades administrativas. Esta extensión funcional es decisiva: en una Administración digital dependiente de proveedores, plataformas cloud, servicios gestionados, desarrolladores, integradores y cadenas de suministro complejas, la seguridad no puede quedar encerrada dentro del perímetro interno de la entidad pública.

Por ello, los pliegos, contratos, encargos, acuerdos de nivel de servicio y mecanismos de supervisión deben incorporar los requisitos necesarios para asegurar la conformidad ENS de los sistemas que sustentan los servicios contratados. La contratación pública se convierte así en una palanca de ciberseguridad y en un mecanismo de profesionalización del mercado tecnológico.

0.4. QUÉ ELEMENTOS LO INTEGRAN

El ENS se compone de varias piezas interrelacionadas. En la base se sitúa **el Real Decreto 311/2022**, que define el objeto, ámbito, principios, requisitos mínimos, organización de la seguridad, categorización, medidas, auditoría, conformidad e incidentes. Sobre esa base operan las **Instrucciones Técnicas de Seguridad**, que concretan materias esenciales como conformidad, auditoría, notificación de incidentes e informe del estado de la seguridad.

Las **Guías CCN-STIC de la serie 800** constituyen el cuerpo doctrinal de implantación del ENS. Su función es orientar la adecuación, la gestión de riesgos, la organización de roles, la aplicación de medidas, la auditoría, la certificación, la contratación, los

servicios externalizados, los entornos cloud y el apoyo a entidades de menor dimensión. A su vez, **herramientas del CCN** como INES, AMPARO, PILAR, LUCIA y otras soluciones del CCN facilitan la gestión operativa, la medición, el seguimiento y la generación de evidencias.

El sistema se completa con la **auditoría, la Declaración de Conformidad** para sistemas de categoría Básica, la **Certificación de Conformidad** para sistemas de categoría Media o Alta, la **acreditación** de entidades certificadoras por ENAC conforme a UNE-EN ISO/IEC 17065, la **gestión de incidentes** y la **mejora continua**. La fuerza del ENS está en que ninguna de estas piezas actúa aisladamente: todas forman una cadena de confianza.

0.5. POR QUÉ PUEDE SERVIR COMO REFERENCIA NACIONAL E INTERNACIONAL

El ENS puede servir como referencia porque responde a una necesidad común a muchos Estados: proteger los servicios públicos digitales de forma proporcional, verificable y sostenible. Su estructura permite convertir una política pública de ciberseguridad en obligaciones concretas, medidas aplicables, evidencias auditables y certificados reconocibles. Esta capacidad de pasar de la estrategia a la práctica es uno de sus principales valores exportables.

El modelo español está alineado con las tendencias europeas e internacionales: gestión de riesgos, responsabilidad organizativa, continuidad, notificación de incidentes, seguridad de la cadena de suministro, certificación, acreditación, resiliencia y mejora continua. No sustituye automáticamente a marcos como NIS2, el Reglamento de Ciberseguridad, el RGPD o las normas ISO, pero dialoga con ellos y puede operar como plataforma nacional de cumplimiento y de generación de evidencias.

Para España, el ENS es un activo estratégico. Para las Administraciones Públicas, es un instrumento de gobernanza y confianza. Para las empresas proveedoras, es una vía de diferenciación en el mercado público digital. Para auditores, certificadores y organismos de acreditación, es un esquema estructurado de evaluación de la conformidad. Para otros países, es una experiencia nacional madura que puede inspirar marcos de ciberseguridad pública adaptados a sus propios contextos.

El ENS convierte la ciberseguridad pública en una cadena verificable de confianza digital: obligación, gobernanza, medidas, apoyo técnico, auditoría, certificación, acreditación y mejora continua.

Elemento del modelo	Función dentro del ENS
Real Decreto 311/2022	Define el marco jurídico, principios, requisitos mínimos, categorización, medidas, auditoría y conformidad.
Instrucciones Técnicas de Seguridad	Concretan procedimientos críticos de conformidad, auditoría, incidentes e informe del estado de seguridad.
Guías CCN-STIC serie 800	Constituyen el cuerpo doctrinal de implantación, interpretación, auditoría y maduración del ENS.

Herramientas del CCN	Facilitan la adecuación, la medición, la gestión de riesgos, el seguimiento y la generación de evidencias.
Auditoría y certificación	Transforman el cumplimiento interno en conformidad verificable y comunicable.
Acreditación ENAC	Garantiza competencia técnica, imparcialidad y confianza en las entidades certificadoras.

Figura 0.3 Elementos que integran el ecosistema ENS.

1. NATURALEZA Y FUNCIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, simplemente, Esquema Nacional de Seguridad o ENS) constituye el principal activo institucional de España en materia de **ciberseguridad pública, confianza digital y prestación segura de servicios electrónicos**. Su relevancia no deriva únicamente de su carácter normativo, ni de la existencia de un conjunto estructurado de medidas de seguridad, sino de haber configurado un **modelo integral capaz de conectar regulación, gobernanza, gestión de riesgos, implantación técnica, auditoría, certificación, acreditación y mejora continua**. Esta combinación convierte al ENS en una pieza singular dentro del ecosistema europeo de ciberseguridad y en una referencia especialmente valiosa para el Sector Público y las Administraciones Públicas, incluyendo sus proveedores tecnológicos, entidades certificadoras, organismos de acreditación, instituciones internacionales y terceros Estados interesados en desarrollar marcos nacionales de confianza digital.

Así pues, el ENS no es una mera obligación administrativa ni un catálogo técnico de controles. Su verdadera naturaleza es más amplia: **es un sistema de confianza**. Permite ordenar la seguridad de los sistemas de información que soportan servicios públicos, establecer un lenguaje común entre entidades públicas y privadas, facilitar la verificación externa del cumplimiento y generar evidencias objetivas sobre el nivel de seguridad alcanzado. Desde esta perspectiva, **el ENS opera como una infraestructura regulatoria al servicio de la transformación digital segura, la resiliencia institucional y la credibilidad de los servicios públicos digitales.**

Esta dimensión resulta especialmente importante en un contexto europeo e internacional en el que la ciberseguridad ya no puede concebirse como una cuestión puramente técnica. La digitalización de los servicios públicos, la dependencia de proveedores tecnológicos, la expansión de los servicios *cloud*, la interconexión de sistemas, la intensificación de las amenazas híbridas, la profesionalización del cibercrimen, la presión regulatoria europea y la necesidad de demostrar diligencia convierten la seguridad de la información en un requisito esencial de gobernanza pública.

El ENS ofrece una respuesta madura a ese desafío: no se limita a exigir seguridad, sino que proporciona una arquitectura completa para organizarla, implantarla, verificarla, certificarla y mejorarla.

En este sentido, el ENS debe entenderse también como **una propuesta de valor**. Para las **entidades públicas**, proporciona un marco común de actuación que facilita la gestión de riesgos y refuerza la calidad de los servicios digitales. Para las **empresas proveedoras**, ofrece un sistema reconocible de cumplimiento que permite acreditar solvencia y confianza en el mercado público. Para los **organismos de certificación y acreditación**, constituye un modelo estructurado de evaluación de la conformidad. Para **otros países**, representa una experiencia nacional consolidada que puede servir de inspiración en el diseño de políticas públicas de ciberseguridad.

Para España y para Europa, finalmente, el ENS es un instrumento de soberanía normativa, madurez institucional y proyección internacional.

Para comprender el alcance integral del ENS, resulta útil contemplar sus **capas conceptuales** como un sistema piramidal y estructurado que conecta la base regulatoria con la generación de evidencia y confianza externa:



Figura 1.1 Arquitectura conceptual del ENS como sistema de confianza digital

1.1. EL ENS COMO MARCO JURÍDICO-TÉCNICO DE SEGURIDAD DE LA INFORMACIÓN

El ENS tiene una **naturaleza jurídico-técnica** especialmente relevante:

- Es **jurídico** porque se encuentra regulado mediante una norma de obligado cumplimiento, el Real Decreto 311/2022, de 3 de mayo, cuya fundamentación legal se encuentra en el artículo 156.2 de la **Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público**. Este precepto señala al ENS como el instrumento fundamental para asegurar la seguridad de los sistemas y soluciones adoptadas por las administraciones públicas en sus relaciones por medios electrónicos, garantizando, además, así la protección de los datos personales y el ejercicio de los derechos de los ciudadanos.

- Y es **técnico** porque traduce esa obligación normativa en principios, requisitos, medidas, procedimientos, guías, herramientas y mecanismos de verificación aplicables a sistemas de información concretos. Esta doble naturaleza es uno de sus principales elementos diferenciales: **el ENS no es únicamente una recomendación de buenas prácticas ni una certificación voluntaria de mercado, sino un marco normativo público con capacidad para ordenar la seguridad de la información en el conjunto del sector público y en sus relaciones con proveedores privados.**

El ENS no solo vincula a las entidades públicas, sino que es de aplicación obligatoria a las entidades del sector privado que le presten servicios o provean soluciones a las anteriores en virtud de una relación contractual.

Así pues, por imperativo legal, los pliegos de prescripciones administrativas o técnicas de los contratos deben incluir de forma expresa los requisitos necesarios para asegurar la conformidad con el ENS, tales como la exigencia de presentar las correspondientes Declaraciones o Certificaciones de Conformidad. Esta cautela y responsabilidad se extiende, además, a la cadena de suministro de dichos contratistas, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos, garantizando así un nivel de protección homogéneo en todo el ecosistema digital que soporta el servicio público.

El ENS parte de una **concepción integral de la seguridad**. Su finalidad es proteger la información y los servicios frente a riesgos que puedan afectar a **dimensiones esenciales de la seguridad, tales como la confidencialidad, la integridad, la disponibilidad, la autenticidad y la trazabilidad**. Estas dimensiones no son meramente técnicas: afectan directamente a la continuidad de los servicios públicos, a la garantía de derechos, a la confianza de ciudadanos y empresas, a la responsabilidad de las Administraciones y a la solidez de la Administración digital.

El ENS se sitúa en la intersección entre ciberseguridad, Derecho público, transformación digital, contratación tecnológica, protección de datos y seguridad nacional.

El modelo del ENS se articula mediante una **lógica de proporcionalidad y proactividad**. No todos los sistemas tienen la misma criticidad, ni todos los servicios presentan el mismo impacto potencial. Por ello, el ENS exige **categorizar los sistemas de información, analizar los riesgos y aplicar medidas de seguridad adecuadas a la categoría correspondiente**. Este enfoque permite evitar dos riesgos opuestos: por un lado, una seguridad insuficiente para sistemas que soportan servicios relevantes; por otro, una imposición desproporcionada de cargas técnicas u organizativas a sistemas de menor criticidad.

Desde el punto de vista de su **posicionamiento institucional**, esta estructura convierte al ENS en un modelo especialmente sólido. No se limita a decir que las entidades deben ser seguras, sino que **define cómo deben organizar su seguridad, cómo deben justificar sus decisiones, cómo deben implantar las medidas, cómo deben documentar su cumplimiento y cómo deben someterse a verificación**. Esta capacidad para transformar exigencias generales de seguridad en obligaciones

concretas, auditables y certificables es una de las razones que explican el valor del ENS como modelo nacional exportable.

1.2. EL ENS COMO INSTRUMENTO DE CONFIANZA EN LA ADMINISTRACIÓN DIGITAL

La confianza es el presupuesto de la Administración digital. Ciudadanos, empresas y otras Administraciones sólo pueden relacionarse de forma plenamente electrónica con el sector público si los sistemas que soportan esa relación son seguros, disponibles, íntegros, trazables y resistentes frente a incidentes. En ausencia de seguridad, la digitalización administrativa puede convertirse en una fuente de vulnerabilidad institucional, pérdida de confianza, interrupción de servicios, exposición de datos, responsabilidad jurídica y deterioro reputacional. El ENS responde precisamente a esa necesidad: dotar a la Administración digital de una base común y verificable de seguridad.

El ENS permite afirmar que la digitalización de los servicios públicos españoles no descansa únicamente en criterios de eficiencia, simplificación administrativa o modernización tecnológica, sino también en una exigencia estructural de seguridad.

Esta idea es clave para su desarrollo dentro y fuera de España. El modelo español no concibe la ciberseguridad como un añadido posterior al despliegue de servicios digitales, sino como una condición de diseño, funcionamiento y continuidad de dichos servicios. En términos de mensaje institucional, el ENS permite vincular digitalización y confianza: no hay Administración digital madura sin seguridad verificable.

- Para las **entidades públicas**, el ENS proporciona un marco homogéneo que evita la dispersión de criterios.
- Para los **ciudadanos**, constituye una garantía indirecta de que los servicios públicos electrónicos han sido diseñados y gestionados conforme a exigencias comunes de protección.
- Para las **empresas** que se relacionan con la Administración, aporta previsibilidad y seguridad jurídica.
- Para los **proveedores tecnológicos**, establece un lenguaje común de cumplimiento, y
- Para **otros países**, muestra que es posible construir una Administración digital apoyada en un modelo sistemático de seguridad, certificación y mejora continua.

Esta función de confianza tiene, además, una **dimensión reputacional**.

Un país que dispone de un marco nacional de seguridad como el ENS puede presentar su Administración digital como un entorno regulado, exigente y verificable. Esta característica es especialmente valiosa en el ámbito europeo, donde la confianza en los servicios digitales, la resiliencia de las entidades públicas, la seguridad de las cadenas de suministro y la protección de infraestructuras críticas ocupan un lugar creciente en la agenda regulatoria.

El ENS permite a España mostrar una experiencia consolidada en todos esos ámbitos.

Desde una **perspectiva institucional**, el ENS constituye una garantía. No es sólo una obligación que las entidades deben cumplir; es una marca de confianza del modelo español de Administración digital. Expresa que **los servicios públicos digitales no se apoyan en decisiones aisladas o voluntarias de seguridad, sino en un sistema común, normativo, verificable y sometido a evolución permanente.**

1.3. EL ENS COMO MODELO DE GOBERNANZA, CUMPLIMIENTO Y MEJORA CONTINUA

Uno de los principales valores del ENS es que introduce una verdadera **cultura de gobernanza de la seguridad.** La seguridad no se concibe como responsabilidad exclusiva de los equipos técnicos, sino como una función organizativa que exige dirección, política de seguridad, asignación de responsabilidades, gestión de riesgos, control interno, documentación, supervisión y revisión periódica. Esta aproximación es esencial para que la seguridad deje de ser una cuestión reactiva y se convierta en una capacidad institucional.

El ENS obliga a las entidades a estructurar su seguridad de forma ordenada. Deben identificar **qué sistemas** quedan dentro de su ámbito, qué información y servicios soportan, **qué riesgos** les afectan, **qué medidas** resultan aplicables, **quién asume cada responsabilidad**, **cómo se documenta** la seguridad, **cómo se supervisa** el cumplimiento y **cómo se corrigen las deficiencias**. Esta lógica facilita la profesionalización de la seguridad en el sector público y permite que las decisiones no dependan exclusivamente de criterios informales o de la disponibilidad coyuntural de recursos técnicos.

Para materializar esta estructura operativa, el ENS impone el principio de **diferenciación de responsabilidades**, que obliga a distinguir formalmente cuatro figuras clave en todo sistema:

- El **Responsable de la Información,** que determina los requisitos de seguridad de los datos tratados,
- El **Responsable de los Servicios**, que define los requisitos de su prestación,
- El **Responsable de la Seguridad**, que determina las decisiones para satisfacer dichos requisitos, y
- El **Responsable del Sistema,** encargado de la implementación y operación diaria del sistema de información concernido.

Un requisito estructural e irrenunciable de este modelo es que el responsable de la seguridad debe ser distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos. Esta separación garantiza que la supervisión de la seguridad sea independiente de la explotación técnica, actuando como un control interno que evita conflictos de interés. Solo en situaciones excepcionales por falta de

recursos se permite la coincidencia de funciones, siempre que se apliquen medidas compensatorias documentadas.

La **mejora continua** es otro componente esencial. La seguridad no es un estado que se alcanza de una vez para siempre. Las amenazas evolucionan, los servicios se transforman, los sistemas se actualizan, las organizaciones cambian, aparecen nuevos proveedores, se externalizan funciones, se incorporan tecnologías emergentes y se modifican los marcos regulatorios.

El ENS incorpora esta realidad al exigir reevaluación, auditoría, seguimiento, revisión de medidas y corrección de no conformidades. Esta dinámica permite que el modelo se mantenga vivo y no quede reducido a una fotografía estática del cumplimiento.

Este punto es especialmente importante para evitar una visión formalista del ENS. El valor del modelo no reside únicamente en disponer de documentación, superar una auditoría u obtener un certificado, sino en **asegurar que la entidad mantiene una capacidad real y demostrable de proteger sus sistemas.** La documentación, la auditoría y la certificación son instrumentos necesarios, pero deben estar conectados con una seguridad efectiva. El ENS alcanza su máxima utilidad cuando se convierte en una forma de gestionar, no sólo en una forma de acreditar.

Desde el punto de vista de la **proyección exterior**, esta combinación de gobernanza, cumplimiento y mejora continua permite presentar **el ENS como un modelo de madurez**. Muchos marcos internacionales ofrecen controles o buenas prácticas; el ENS, además, los inserta en una arquitectura pública de responsabilidad, verificación y seguimiento. Esa diferencia es esencial para explicar su valor a instituciones europeas y a otros países: **el ENS no es sólo un estándar de seguridad, sino un sistema público de gestión de la confianza.**

1.4. EL ENS COMO SISTEMA VERIFICABLE DE CONFORMIDAD, AUDITORÍA Y CERTIFICACIÓN

La confianza requiere evidencias. Por ello, uno de los elementos más relevantes del ENS es su **capacidad para transformar el cumplimiento en conformidad verificable**. El modelo no descansa únicamente en declaraciones internas de seguridad, sino que articula procedimientos de autoevaluación, auditoría, Declaración de Conformidad y Certificación de Conformidad, en función de la categoría del sistema. Esta estructura permite diferenciar niveles de exigencia y asociar la verificación externa a los sistemas de mayor impacto.

La **Declaración de Conformidad** y la **Certificación de Conformidad** cumplen funciones distintas, pero complementarias:

- En los sistemas con menores exigencias de seguridad (categoría Básica), la **Declaración de Conformidad** permite acreditar el cumplimiento mediante mecanismos de autoevaluación y responsabilidad interna.
- En sistemas de categoría Media o Alta, la **Certificación de Conformidad** introduce una verificación externa más intensa, apoyada en auditorías y en la

intervención de entidades de certificación u órganos de auditoría técnica del sector público.

De este modo, el ENS equilibra proporcionalidad, exigencia y confianza.

La **auditoría** es el elemento que conecta el cumplimiento documental con la realidad del sistema. Permite comprobar si la categorización es correcta, si el análisis de riesgos resulta adecuado, si las medidas aplicables se han implantado, si existen evidencias suficientes, si la política de seguridad y los procedimientos son operativos y si las no conformidades han sido identificadas y tratadas. La **certificación**, por su parte, convierte ese proceso de verificación en una evidencia formal que puede ser utilizada frente a terceros.

Esta dimensión es especialmente valiosa en el mercado público digital:

- Una entidad proveedora que dispone de certificación ENS puede acreditar ante una Administración que determinados sistemas cumplen las exigencias aplicables.
- Una Administración que exige conformidad ENS en sus pliegos puede elevar el nivel de seguridad de los servicios contratados.
- Un órgano de contratación puede disponer de una evidencia más objetiva para valorar la adecuación de los sistemas que soportarán un servicio público, y
- Una entidad pública puede demostrar que ha sometido sus sistemas a una evaluación estructurada y reconocible.

El sistema se refuerza mediante la **acreditación de las entidades de certificación** y la intervención de la **Entidad Nacional de Acreditación (ENAC)**, así como mediante la utilización de normas internacionales de evaluación de la conformidad, en particular la UNE-EN ISO/IEC 17065. Esta conexión con estándares internacionales incrementa la credibilidad del modelo, facilita su comprensión internacional y permite explicar que la certificación ENS no es un mecanismo aislado, sino parte de un ecosistema de evaluación de la conformidad apoyado en criterios de competencia técnica, imparcialidad, trazabilidad y supervisión.

También debe destacarse la función del **Consejo de Certificación del ENS**, entre cuyos miembros figuran el Centro Criptológico Nacional (CCN), la Agencia Estatal de Administración Digital (AEAD), la Entidad Nacional de Acreditación (ENAC) y un representante de cada Entidad de Certificación y Órgano de Auditoría Técnica del sector Público, presidido por la Agencia Española de Administración Digital y el Centro Criptológico Nacional, como espacio de coordinación, debate y puesta en común de las decisiones que afectan al modelo de certificación. Su existencia refuerza la coherencia del sistema y muestra que el ENS dispone de mecanismos institucionales para evolucionar, resolver dudas, homogeneizar criterios y preservar la confianza en el modelo. Desde una perspectiva estratégica, este punto es importante: **el ENS no sólo certifica; se gobierna, se coordina y se mejora**.

1.5. VALOR ESTRATÉGICO DEL ENS PARA ESPAÑA Y PARA TERCEROS PAÍSES

El ENS tiene valor estratégico para España porque proporciona una base común para proteger la Administración digital y los servicios públicos electrónicos. En un escenario de creciente dependencia tecnológica, disponer de un marco nacional de seguridad obligatorio, verificable y apoyado por una autoridad técnica de referencia constituye una ventaja institucional.

El ENS permite ordenar la seguridad del sector público, proyectar exigencias sobre proveedores, generar un mercado especializado de servicios de adecuación y certificación, y fortalecer la resiliencia del conjunto del ecosistema público digital.

Desde la perspectiva del Estado, **el ENS es también una herramienta de soberanía regulatoria.** Permite definir un nivel nacional de exigencia en materia de seguridad de la información, establecer criterios comunes para las entidades públicas, condicionar la contratación tecnológica y preservar un modelo propio de confianza digital. En un contexto europeo en el que se multiplican las iniciativas sobre ciberseguridad, certificación, resiliencia, identidad digital, datos, inteligencia artificial y servicios críticos, el ENS ofrece a España una posición de partida sólida: no se trata de construir desde cero, sino de poner en valor un modelo ya existente, operativo y reconocido.

Para el sector privado, el ENS crea un entorno de certidumbre. Las empresas proveedoras del sector público pueden conocer qué se les exige, cómo deben prepararse, qué evidencias deben aportar y cómo pueden diferenciarse en el mercado mediante la conformidad o certificación ENS. Esto convierte el modelo en un factor de profesionalización del mercado tecnológico. La seguridad deja de ser un elemento accesorio y se transforma en un criterio de confianza, solvencia y competitividad.

El ENS tiene también un claro potencial internacional. Muchos Estados están buscando modelos que les permitan elevar la seguridad de sus servicios públicos digitales, gestionar riesgos, controlar proveedores, verificar cumplimiento y generar confianza en la ciudadanía. El ENS ofrece una **experiencia práctica acumulada y una arquitectura suficientemente madura como para servir de referencia**. Su valor no reside en que pueda copiarse mecánicamente, sino en que proporciona principios de diseño exportables: obligatoriedad pública, categorización por impacto, gestión de riesgos, medidas proporcionadas, guías técnicas, herramientas de apoyo, certificación, acreditación y mejora continua.

En el ámbito europeo, **el ENS constituye un modelo nacional alineado con las grandes tendencias regulatorias de la Unión**: enfoque basado en riesgos, responsabilidad de las entidades, supervisión, notificación de incidentes, seguridad de proveedores, certificación, resiliencia y confianza digital. **Este alineamiento permite defender el ENS no como una peculiaridad nacional, sino como una experiencia avanzada que puede complementar, inspirar o dialogar con los desarrollos europeos en materia de ciberseguridad**.

La proyección del ENS se apoya, por tanto, en un mensaje claro:

España dispone de un modelo integral, verificable y operativo de ciberseguridad

pública. Un modelo que combina Derecho, técnica, organización, certificación y confianza. Un modelo que protege servicios públicos, disciplina cadenas de suministro, fortalece el mercado de ciberseguridad y ofrece una referencia útil para terceros países.

1.6. LOS PERFILES DE CUMPLIMIENTO ESPECÍFICO COMO RESPUESTA A NECESIDADES SECTORIALES

La **capacidad de adaptación** es una de las condiciones necesarias para que un marco de seguridad pueda consolidarse en entornos complejos y diversos. El ENS se aplica a entidades muy distintas entre sí: grandes organismos públicos, entidades locales de pequeño tamaño, universidades, organismos autónomos, sociedades públicas, proveedores tecnológicos, servicios *cloud*, plataformas digitales, sistemas críticos y servicios externalizados. Pretender aplicar a todos ellos una aproximación indiferenciada podría generar rigidez, inseguridad interpretativa o costes innecesarios. Los Perfiles de Cumplimiento Específico responden precisamente a esta necesidad.

Estos perfiles permiten concretar la aplicación del ENS en determinados sectores, tipos de entidades, servicios o escenarios de riesgo. Su finalidad es facilitar una aplicación más homogénea, proporcionada y operativa del marco general, identificando conjuntos de medidas, criterios o expectativas de cumplimiento especialmente adecuados para una realidad concreta. **No suponen una excepción al ENS ni una rebaja de sus exigencias, sino una forma de hacer más practicable, comprensible y verificable su cumplimiento.**

Desde una **perspectiva técnica y organizativa**, l**os Perfiles de Cumplimiento Específico ayudan a reducir incertidumbres**. Permiten que entidades similares trabajen con criterios comunes, que los auditores dispongan de referencias más homogéneas, que las entidades de certificación puedan evaluar con mayor consistencia y que los responsables de seguridad orienten sus esfuerzos hacia medidas realmente relevantes. En términos de eficiencia, los perfiles pueden facilitar la implantación del ENS en colectivos con características comunes, evitando interpretaciones excesivamente dispares y reduciendo cargas innecesarias.

Desde una **perspectiva estratégica**, **los perfiles refuerzan la capacidad del ENS para crecer y adaptarse**. Un modelo nacional de seguridad sólo puede consolidarse si combina exigencia y flexibilidad. La exigencia garantiza que la seguridad sea real y verificable. La flexibilidad permite que esa seguridad pueda implantarse en contextos diversos. Los Perfiles de Cumplimiento Específico expresan esa madurez: muestran que el ENS no es un marco rígido, sino una arquitectura capaz de responder a necesidades sectoriales sin perder coherencia general.

Para la **proyección nacional e internacional del ENS**, este elemento tiene un valor particular. Muchos países y organizaciones se enfrentan a la dificultad de aplicar marcos generales de ciberseguridad a sectores muy distintos. La experiencia de los Perfiles de Cumplimiento Específico permite presentar el modelo español como **un sistema capaz de combinar una base común de seguridad con adaptaciones sectoriales controladas**. Este equilibrio entre unidad y especialización es una de las

características que puede hacer especialmente atractivo el ENS para otros Estados, instituciones y operadores.

Desde el punto de vista de la certificación, **los Perfiles de Cumplimiento Específico pueden contribuir a mejorar la previsibilidad y la calidad del proceso**. Cuando las expectativas están mejor definidas para un determinado tipo de entidad o servicio, resulta más sencillo preparar la adecuación, recopilar evidencias, orientar la auditoría, valorar no conformidades y sostener la certificación en el tiempo. De este modo, los Perfiles de Cumplimiento Específico no sólo facilitan la implantación, sino que fortalecen el propio sistema de certificación, al hacer más previsible la preparación de evidencias, la valoración de no conformidades y el mantenimiento de la conformidad en el tiempo.

1.7. RESUMIENDO…

En definitiva, la naturaleza y función del ENS sólo pueden entenderse plenamente si se contempla su dimensión completa. **El ENS es una norma jurídica, pero también un marco técnico; es una obligación de seguridad, pero también una garantía de confianza; es un sistema de cumplimiento, pero también una arquitectura de certificación; es un modelo nacional, pero con vocación europea e internacional; es un marco general, pero capaz de adaptarse a necesidades sectoriales mediante Perfiles de Cumplimiento Específico**. Esta combinación explica su valor como infraestructura española de confianza digital y como referencia avanzada para la gobernanza pública de la ciberseguridad.

Destinatario	Valor que aporta el ENS
Administraciones Públicas	Marco común para proteger servicios públicos digitales
Ciudadanos y empresas	Mayor confianza en la Administración digital
Proveedores tecnológicos	Reglas claras de acceso y permanencia en el mercado público
Órganos de contratación	Evidencias objetivas de cumplimiento y control de proveedores
Entidades certificadoras y auditores	Modelo estructurado de evaluación de la conformidad
Otros países e instituciones	Referencia madura para diseñar marcos nacionales de ciberseguridad

Figura 1.2 Los destinatarios del valor del ENS

2. MARCO JURÍDICO Y ÁMBITO DE APLICACIÓN

El ENS se apoya en una arquitectura jurídica singular dentro del **Derecho Público**: nace del régimen jurídico de la Administración electrónica, se proyecta sobre todo el sector público, se extiende funcionalmente a los proveedores privados que sostienen

servicios públicos digitales y se conecta con los principales marcos europeos de ciberseguridad, protección de datos, resiliencia y certificación, sin olvidar su conexión con otros estándares internacionales de seguridad de la información, con los que comparte principios, objetivos y controles. Esta combinación explica y potencia su valor: **el ENS no es una obligación técnica aislada, sino una pieza estructural del modelo español de Administración digital segura en la que se combinan principios comunes relacionados con la seguridad de la información; normas de carácter general y un catálogo de controles y medidas de seguridad adaptables a los cambios tecnológicos**.

El marco jurídico del ENS permite transformar un principio general —la seguridad de la información tratada y de los servicios prestados por medios electrónicos— en un **sistema completo de obligaciones, medidas, evidencias y mecanismos de conformidad.** Su ámbito de aplicación no se define sólo por la naturaleza del sujeto que presta el servicio, sino también por la función que cumple el sistema de información, por la información que trata, por los servicios que soporta y por la relación que pueda existir entre una entidad pública y sus contratistas o proveedores tecnológicos.

Desde una **perspectiva institucional**, es necesario afirmar que **España dispone de un marco jurídico maduro, coherente y exigible, capaz de ordenar la seguridad de los servicios públicos digitales y de irradiar confianza hacia el mercado tecnológico**.

Para los destinatarios europeos e internacionales, el ENS se presenta como un ejemplo avanzado de cómo un Estado articula seguridad jurídica, gobernanza técnica, control de proveedores, protección de datos, certificación y mejora continua en un único modelo nacional, contando con el respaldo y la legitimación establecido en su sistema de fuentes de derecho, dotándolo de un carácter vinculante frente a otros modelos voluntarios.

El **marco legal** en el que se inserta el ENS no opera en el vacío, sino en constante interacción con el Derecho Administrativo, la protección de datos y las directivas europeas. La siguiente tabla sintetiza este mapa normativo:

Bloque normativo	Función dentro del modelo ENS	Mensaje de valor
Ley 40/2015, art. 156.2	Establece el fundamento legal del ENS como política de seguridad en la utilización de medios electrónicos.	Seguridad como pieza estructural del régimen jurídico del sector público.
Real Decreto 311/2022	Regula el ENS vigente: objeto, ámbito, principios, requisitos, medidas, auditoría y conformidad.	Marco nacional completo, exigible y verificable.
Ley 39/2015	Vincula la Administración digital con derechos de los ciudadanos y relaciones electrónicas con las Administraciones.	No hay Administración digital madura sin confianza y seguridad.
RGPD y LOPDGDD	Conectan el ENS con la protección de datos, la seguridad del tratamiento y la	Seguridad y privacidad como garantías

Bloque normativo	Función dentro del modelo ENS	Mensaje de valor
	responsabilidad proactiva.	convergentes.
Contratación pública	Permite trasladar requisitos ENS a pliegos y contratos de servicios públicos digitales.	Control de proveedores y cadena de suministro.
Derecho europeo de ciberseguridad	Sitúa el ENS en diálogo con NIS2, Cybersecurity Act y esquemas europeos de certificación.	Modelo nacional alineado con la agenda europea de resiliencia y certificación.

Figura 2.1 Mapa jurídico-funcional del ENS y convergencia normativa

El Esquema Nacional de Seguridad no se limita al sector público, sino que se extiende al sector privado (y a su cadena de suministro) a través de la contratación administrativa. La Figura 2.2 ilustra este proceso de irradiación, mostrando cómo la obligación legal de las Administraciones Públicas se traslada a sus proveedores de servicios para garantizar la seguridad de la cadena de suministro y generar confianza en el mercado:



Figura 2.2. Ámbito de aplicación del ENS: de la obligación pública a la confianza de mercado.

2.1. EL REAL DECRETO 311/2022, DE 3 DE MAYO

El **Real Decreto 311/2022, de 3 de mayo**, por el que se regula el Esquema Nacional de Seguridad, constituye la norma central del modelo vigente de la seguridad de la información en la Administración Pública. Su relevancia no reside únicamente en actualizar el anterior Real Decreto 3/2010, sino en **consolidar el ENS como una herramienta jurídica adaptada a una Administración plenamente digitalizada, a un entorno de amenazas más complejo y a un mercado tecnológico en el que la**

prestación de servicios públicos depende cada vez más de proveedores, plataformas, servicios cloud, integradores y soluciones gestionadas.

El Real Decreto 311/2022 desarrolla el mandato del artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, según el cual el ENS tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos y se compone de los **principios básicos** y **requisitos mínimos** que garanticen adecuadamente la seguridad de la información tratada. Esta conexión con la Ley 40/2015 sitúa al ENS dentro del núcleo del régimen jurídico del sector público, no como una guía técnica periférica o una norma de rango reglamentario, sino como una pieza normativa esencial de la Administración digital española.

Efectivamente, el artículo 1 del Real Decreto 311/2022 define el ENS como el **conjunto de principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y de los servicios prestados por las entidades de su ámbito de aplicación.** La norma persigue asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos.

Esta formulación convierte al ENS en un instrumento jurídico de seguridad integral: protege datos, servicios, sistemas, derechos, continuidad administrativa y confianza pública.

Por consiguiente, se observa cómo **el ENS se alinea con los postulados tradicionales en cuanto a seguridad de la información y los estándares internacionales sobre la materia** al adoptar un conjunto de requisitos mínimos y obligatorios de la seguridad, además de hacer propias las dimensiones de seguridad clásicas (disponibilidad, confidencialidad e integridad), a las que se añaden la trazabilidad y la autenticidad como notas fundamentales para un sector como el público, que necesita de certidumbre y seguridad jurídica en sus actuaciones frente a terceros.

Desde una **perspectiva institucional**, el Real Decreto 311/2022 permite presentar el ENS como un modelo nacional completo:

Responde a una realidad concreta que analiza las amenazas y el mercado tecnológico presente, y, además, no se limita a formular objetivos generales de seguridad, sino que ofrece una arquitectura operativa para lograrlos. Define principios, requisitos, responsabilidades, medidas, auditorías, informes, incidentes, mecanismos de conformidad, perfiles específicos, instrucciones técnicas y guías.

Su **valor exportable** reside precisamente en **su capacidad de convertir la ciberseguridad pública en un sistema normativo aplicable, auditable y certificable, además de un instrumento adaptable a los distintos escenarios, amenazas y riesgos tecnológicos, y la diversidad de entidades existentes en el ámbito de una Administración Pública con distintos niveles.**

2.2. RELACIÓN CON LA ADMINISTRACIÓN DIGITAL Y LOS SERVICIOS PÚBLICOS ELECTRÓNICOS

El ENS se entiende adecuadamente sólo si se vincula con la transformación digital de la Administración. La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, consolidó la **tramitación electrónica** como forma ordinaria de actuación administrativa y reconoció a las personas, en sus relaciones con las Administraciones, derechos vinculados al uso de medios electrónicos, incluida la protección de datos personales y la seguridad y confidencialidad de los datos que figuren en ficheros, sistemas y aplicaciones administrativas.

La Ley 40/2015 completa esta perspectiva al regular las relaciones electrónicas entre Administraciones y exigir que dichas relaciones **aseguren la interoperabilidad y la seguridad de los sistemas y soluciones adoptadas, así como la protección de los datos personales**. El ENS aparece, por tanto, como el instrumento que permite consolidar los derechos de la ciudadanía en sus relaciones electrónicas con la administración, además de hacer operativa esa exigencia de seguridad en un entorno administrativo en el que expedientes, registros, notificaciones, sedes electrónicas, plataformas de intermediación, archivos, aplicaciones y servicios compartidos dependen de sistemas de información.

Asimismo, el ENS está presente en la producción normativa posterior, como en el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, convirtiéndose como una herramienta indispensable para garantizar la implementación de sistemas de confianza.

La consecuencia es clara: **la seguridad no es un elemento accesorio de la Administración digital, sino una condición de validez práctica, continuidad y confianza**. Un servicio público electrónico no puede considerarse maduro si no garantiza disponibilidad, autenticidad, integridad, trazabilidad y protección de la información. El ENS proporciona el marco común y las herramientas que permiten que esa garantía no dependa de decisiones aisladas de cada entidad, sino de un estándar nacional de cumplimiento medible y certificable.

Este es uno de los mensajes más potentes para la difusión del modelo español en Europa y en el resto del mundo: **España no ha construido una Administración digital basada únicamente en plataformas, portales o procedimientos electrónicos, sino también en un marco de seguridad común que establece una base metodológica de gestión que permite confiar en ellos**. La Administración digital española se apoya en una infraestructura jurídica de confianza, y el ENS es su pieza central en materia de seguridad.

2.3. RELACIÓN CON LA CIBERSEGURIDAD NACIONAL

El ENS tiene una dimensión que trasciende la mera organización interna de las Administraciones Públicas. **La protección de los sistemas de información que**

soportan servicios públicos digitales incide directamente en la resiliencia institucional, la continuidad administrativa, la prestación de servicios esenciales y la seguridad nacional. Cuando un sistema público es interrumpido, manipulado o comprometido, no sólo se produce un problema tecnológico: pueden verse afectados derechos y libertades colectivas e individuales, servicios críticos, obligaciones legales, confianza ciudadana y capacidad operativa del Estado.

El Real Decreto 311/2022 refleja esta dimensión al conectar el ENS con la prestación segura de servicios públicos y con la **capacidad de respuesta a incidentes**. En particular, reconoce el papel del **CCN-CERT** en el soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que afecten a entidades incluidas en su ámbito de aplicación. Esta función refuerza la idea de que **el ENS no es sólo un esquema de cumplimiento, sino también un instrumento de prevención, detección, respuesta y aprendizaje institucional.**

La ciberseguridad nacional exige marcos comunes. En un Estado descentralizado, con múltiples Administraciones, entidades públicas, organismos dependientes, universidades, sociedades públicas, proveedores tecnológicos y servicios externalizados, la seguridad no puede depender exclusivamente de criterios heterogéneos. Por ello, hay una conexión directa con las normativas sobre seguridad nacional (Ley 36/2015) en la que ENS aporta una base de recursos compartidos para elevar el nivel de seguridad del conjunto del sector público y para reducir la exposición sistémica derivada de la fragmentación tecnológica y organizativa, alineándose a su vez con las sucesivas Estrategias Nacionales de Ciberseguridad. El ENS por tanto se constituye como una prioridad estatal para garantizar la resiliencia del ecosistema público.

En términos de **proyección internacional**, este elemento resulta especialmente valioso. **El ENS muestra cómo un Estado puede traducir la ciberseguridad nacional en obligaciones concretas para los sistemas de información públicos y sus proveedores, sin limitarse a declaraciones estratégicas**. Por ello, el modelo español puede presentarse como una forma avanzada de territorializar la resiliencia digital: la estrategia se convierte en norma, la norma en medidas, las medidas en evidencias y las evidencias en confianza.

2.4. RELACIÓN CON LA PROTECCIÓN DE DATOS PERSONALES

La relación entre ENS y protección de datos personales es estructural. Buena parte de los sistemas de información del sector público tratan datos personales de diversa índole y alcance: expedientes administrativos, registros, notificaciones, servicios sociales, sanidad, educación, tributos, empleo público, contratación, subvenciones o seguridad. Considerando el derecho a la protección de datos como un derecho fundamental, todos esos ámbitos de actuación pública requieren de una protección jurídica que, además de apuntar a los principios que contempla la normativa, prevea medidas técnicas y organizativas adecuadas, y es donde el ENS proporciona un marco especialmente relevante para dar certeza y concretarlas.

La normativa de protección de datos refuerza la utilidad práctica del ENS. El Reglamento (UE) 2016/679 (en adelante, RGPD) se basa en la responsabilidad proactiva, en la protección de datos desde el diseño y por defecto, en la seguridad del tratamiento y en la capacidad de demostrar cumplimiento. Estos principios encuentran en el ENS un instrumento operativo especialmente útil cuando el tratamiento se realiza en sistemas de información del sector público o en sistemas de proveedores que prestan servicios a dicho sector.

Por otra parte, el RGPD, exige en su artículo 32 que el responsable y el encargado del tratamiento apliquen medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, incluyendo, entre otras, la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento, así como procesos de verificación, evaluación y valoración regulares de la eficacia de las medidas. Aquí nos encontramos con la primera conexión con la lógica del ENS, que coincide de forma natural con este enfoque: gestión de riesgos, medidas proporcionadas, seguridad integral, auditoría y mejora continua.

Además, el artículo 3 del Real Decreto 311/2022 se refiere expresamente a los sistemas de información que traten datos personales, conectando su tratamiento con el marco de protección de datos. La consecuencia práctica es que **el ENS ayuda a las entidades públicas y a sus proveedores a demostrar diligencia en materia de seguridad del tratamiento**. No sustituye al RGPD ni a la Ley Orgánica 3/2018, pero actúa como una herramienta fundamental para organizar, documentar y verificar medidas de seguridad en entornos públicos.

En este sentido se ha reforzado el papel del ENS como herramienta y catálogo cierto de medidas de seguridad aplicables a la protección de los datos personales objeto de tratamiento a través de su inclusión en la Ley Orgánica 3/2018, en cuya disposición adicional primera, obliga a implantar las medidas del ENS para evitar la pérdida o acceso no autorizado a datos personales.

Esta obligación se extiende tanto a entidades del sector público como a empresas privadas que colaboren en la prestación de servicios que involucren dichos datos

Desde el **punto de vista estratégico**, **la convergencia ENS-RGPD es una fortaleza clara del modelo español.** Permite presentar el ENS como una respuesta no sólo a los riesgos de ciberseguridad, sino también a la necesidad europea de garantizar confianza, protección de derechos y responsabilidad demostrable. Para entidades públicas y proveedores, esto significa que la conformidad ENS no es una carga añadida, sino una inversión en seguridad, cumplimiento, reputación y reducción de riesgo jurídico.

Desde el punto de vista del **mensaje institucional**, **esta conexión permite presentar el ENS como un puente entre ciberseguridad y privacidad**. La seguridad de los sistemas públicos no es sólo protección frente a ataques; también es garantía de derechos fundamentales, confidencialidad administrativa, control de accesos, trazabilidad, conservación y resiliencia de los servicios que tratan datos personales.

Esta convergencia entre ENS y protección de datos refuerza la credibilidad del modelo español ante instituciones europeas y autoridades de control de datos personales.

2.5. RELACIÓN CON EL DERECHO EUROPEO DE LA CIBERSEGURIDAD

El ENS debe situarse dentro de una evolución europea más amplia hacia modelos de ciberseguridad basados en riesgo, gobernanza, supervisión, notificación de incidentes, seguridad de la cadena de suministro y certificación. La Directiva (UE) 2022/2555, conocida como Directiva NIS2, refuerza esta tendencia al exigir a los Estados miembros que garanticen medidas de gestión de riesgos de ciberseguridad para entidades esenciales e importantes, incluyendo medidas relativas a gestión de incidentes, continuidad, seguridad de la cadena de suministro, políticas de seguridad, criptografía, control de acceso, autenticación y formación.

El ENS no es una transposición de NIS2 ni se identifica plenamente con su ámbito subjetivo. Sin embargo, anticipa y materializa muchas de sus lógicas regulatorias: gestión del riesgo, responsabilidad organizativa, medidas proporcionadas, evidencia de cumplimiento, auditoría, seguridad de proveedores, notificación de incidentes y mejora continua. Esta convergencia permite presentarlo como un modelo nacional ya maduro que dialoga de forma natural con las exigencias europeas de resiliencia y gobernanza de la ciberseguridad, contando además con un conjunto de herramientas técnicas y procedimentales avanzadas que permiten el despliegue práctico de estas exigencias de la normativa en cada entidad obligada (Guías CCN-STIC, Catálogo de Productos Certificados, etc.).

También existe una relación relevante con el Reglamento (UE) 2019/881, conocido como Reglamento de Ciberseguridad, que establece el marco europeo para la creación de esquemas europeos de certificación de la ciberseguridad de productos, servicios y procesos TIC. Aunque el ENS opera en un plano propio, centrado en la seguridad de los sistemas de información de las entidades de su ámbito de aplicación y en su conformidad, comparte con el Derecho europeo una idea esencial: **la confianza digital requiere mecanismos de evaluación de la conformidad, certificación, acreditación y reconocimiento de garantías**.

Desde la óptica de posicionamiento europeo, el ENS constituye una experiencia nacional compatible con la agenda de la Unión. Su existencia demuestra que los Estados miembros pueden construir marcos nacionales robustos, orientados a la protección del sector público y de sus proveedores, sin entrar en contradicción con los esquemas europeos.

El planteamiento, por tanto, es claro: **el ENS como un activo complementario**; un modelo que eleva el nivel nacional de ciberseguridad y que puede contribuir al debate europeo sobre certificación, equivalencia, interoperabilidad y confianza.

2.6. ENTIDADES DEL SECTOR PÚBLICO OBLIGADAS

El **ámbito subjetivo de aplicación** del ENS se determina por referencia al artículo 2 de la Ley 40/2015. En consecuencia, el Real Decreto 311/2022 se aplica a **todo el**

sector público, lo que incluye la Administración General del Estado, las Administraciones de las Comunidades Autónomas, las entidades que integran la Administración Local y el sector público institucional. Este último comprende organismos públicos y entidades de derecho público vinculados o dependientes de las Administraciones Públicas, entidades de derecho privado vinculadas o dependientes y universidades públicas, en los términos previstos por la propia Ley 40/2015.

Esta amplitud es una de las fortalezas del modelo español. **El ENS no se limita a la Administración General del Estado ni a determinados órganos centrales. Su vocación es configurar una base común de seguridad para el conjunto del sector público, en un Estado compuesto y descentralizado**. Ello permite proyectar una política de seguridad homogénea sobre Administraciones autonómicas, locales, organismos dependientes, entidades institucionales, universidades públicas y, en determinados supuestos, entidades de derecho privado vinculadas o dependientes de las Administraciones.

Desde el **punto de vista operativo**, **esta amplitud exige adaptar la implantación del ENS a organizaciones muy diversas.** No es lo mismo aplicar el ENS en un ministerio, en una gran comunidad autónoma, en una diputación, en un ayuntamiento pequeño, en una universidad pública o en una sociedad mercantil pública. Sin embargo, la existencia de un marco común permite ordenar la seguridad con criterios compartidos potenciando además las interrelaciones entre organismos y entidades pública y la construcción de sistemas interconectados, aunque la implantación concreta deba ajustarse a la categoría del sistema, al riesgo y a la capacidad organizativa.

Desde una **perspectiva institucional**, **esta cobertura amplia permite presentar el ENS como una infraestructura nacional y no como una política sectorial limitada**. La amplitud de su ámbito de aplicación demuestra que España ha optado por una aproximación transversal: la seguridad de los servicios públicos digitales debe estar presente en todo el sector público, cualquiera que sea su nivel territorial, forma jurídica o dimensión organizativa.

2.7. APLICACIÓN A ENTIDADES PRIVADAS PROVEEDORAS DEL SECTOR PÚBLICO

Una de las características más relevantes del ENS es su **proyección sobre entidades privadas que prestan servicios, suministran soluciones o gestionan sistemas vinculados al sector público.** Esta extensión funcional es esencial en un contexto en el que la Administración digital depende de contratistas, desarrolladores, integradores, operadores cloud, empresas de mantenimiento, proveedores de comunicaciones, servicios gestionados de seguridad y subcontratistas.

> **La seguridad pública ya no puede garantizarse sólo dentro del perímetro formal de la Administración: debe extenderse a la cadena de suministro o de prestación del servicio.**

El Real Decreto 311/2022 refleja esta idea desde su concepción al exigir que los pliegos de prescripciones administrativas o técnicas de los contratos celebrados por entidades del sector público contemplen los requisitos necesarios para asegurar la conformidad con el ENS de los sistemas de información en los que se sustenten los

servicios prestados por los contratistas, incluyendo la presentación de las correspondientes declaraciones o certificaciones de conformidad con el ENS cuando proceda. Esta previsión otorga al ENS una doble faceta: lo convierte en una **herramienta de disciplina contractual y de control del mercado proveedor**, y se constituye como **elemento de diferenciación y de garantía entre las empresas concurrentes que se benefician de la adopción de un estándar de seguridad flexible y adecuado al alcance de sus servicios.**

La aplicación del ENS a proveedores privados no significa que toda empresa contratista quede sometida al ENS en bloque y con independencia del servicio prestado. La clave está en determinar si los sistemas de información del proveedor sostienen servicios públicos, tratan información pública, prestan servicios a entidades del sector público o forman parte del sistema que debe ser protegido. Esta aproximación funcional permite evitar interpretaciones excesivamente expansivas que puedan afectar a la libre concurrencia, pero también impide que la externalización se utilice para desplazar fuera del control público obligaciones esenciales de seguridad o dar cabida a proveedores que no cuenten con una madurez necesaria o requerida.

Para las empresas, la conformidad o certificación ENS puede convertirse en un activo competitivo o valor diferencial. Les permite acreditar madurez, confianza y capacidad para operar en el mercado público digital. Para las Administraciones, permite seleccionar proveedores con mayores garantías. Para el conjunto del ecosistema, eleva el nivel de seguridad de la cadena de suministro. Este es uno de los mensajes más eficaces para vender el ENS en España y en Europa: el modelo no sólo regula a la Administración, sino que crea un mercado de confianza en torno a la prestación segura de servicios públicos digitales.

2.8. APLICACIÓN EN CONTRATACIÓN PÚBLICA, SERVICIOS EXTERNALIZADOS, CLOUD Y CADENA DE SUMINISTRO

La contratación pública es uno de los principales canales de efectividad del ENS. Cuando una Administración contrata servicios tecnológicos, soluciones cloud, desarrollo de aplicaciones, mantenimiento, soporte, ciberseguridad gestionada, alojamiento, comunicaciones o explotación de plataformas, los sistemas del adjudicatario pueden convertirse en parte esencial del servicio público digital. Por ello, **la conformidad con el ENS debe incorporarse correctamente a los pliegos, al objeto del contrato, a las condiciones técnicas, a los acuerdos de nivel de servicio, a las obligaciones de seguridad, a las evidencias exigibles y a los mecanismos de supervisión durante la ejecución.**

Esta incorporación debe realizarse con precisión. No basta con incluir una cláusula genérica de cumplimiento del ENS. El órgano de contratación debe identificar qué sistemas, servicios, datos, interconexiones, ubicaciones, subcontrataciones y responsabilidades quedan afectados; qué categoría de sistema resulta aplicable; qué declaración o certificación debe exigirse; qué evidencias deben aportarse; qué obligaciones de notificación de incidentes corresponden; qué controles se aplican a la

subcontratación; y cómo se verificará el mantenimiento de la conformidad durante toda la vida del contrato.

Los **servicios externalizados y cloud** requieren especial atención. La externalización puede mejorar eficiencia, escalabilidad y especialización, pero también introduce dependencias tecnológicas, concentración de riesgo, problemas de trazabilidad, incertidumbre sobre subcontratistas, ubicación de datos, continuidad de servicio y capacidad de auditoría. El ENS ofrece un marco para gestionar estos riesgos, siempre que se aplique desde el diseño contractual y no como un requisito añadido al final del proceso de contratación.

La **cadena de suministro** es hoy uno de los grandes vectores de riesgo en ciberseguridad. El ENS permite abordarla desde una perspectiva jurídica y técnica: exige seguridad en los sistemas que soportan servicios públicos, permite trasladar obligaciones a proveedores, facilita la exigencia de certificaciones y crea un lenguaje común para auditores, responsables de seguridad, órganos de contratación y empresas. En términos de proyección exterior, este es un argumento central: el ENS permite convertir la contratación pública en palanca de mejora del mercado de ciberseguridad y de reducción del riesgo sistémico.

2.9. RESUMIENDO…

El marco jurídico y el ámbito de aplicación del ENS muestran que el modelo español tiene una arquitectura particularmente robusta. Su fundamento en la Ley 40/2015, su desarrollo mediante el Real Decreto 311/2022, su conexión con la Administración digital, la protección de datos, la contratación pública, la ciberseguridad nacional y el Derecho europeo, así como su extensión funcional a proveedores privados, configuran un sistema con capacidad real para generar confianza.

Este es el mensaje que preside la presentación del ENS dentro y fuera de España: **se trata de un marco jurídico-técnico completo, exigible, transversal y verificable, capaz de proteger los servicios públicos digitales y de disciplinar el ecosistema de proveedores que los hace posibles. El ENS no sólo regula la seguridad; la convierte en un elemento de gobernanza pública, en un criterio de contratación, en una evidencia de confianza y en una propuesta de valor internacional.**

3. CONTENIDO ESENCIAL DEL ENS (REAL DECRETO 311/2022, DE 3 DE MAYO)

El Real Decreto 311/2022, de 3 de mayo, constituye la pieza normativa central del Esquema Nacional de Seguridad vigente. Su importancia no reside únicamente en actualizar el marco aprobado inicialmente por el Real Decreto 3/2010, de 8 de enero, sino en consolidar un modelo completo de seguridad de la información para el sector público español y para las entidades privadas que participan en la prestación de servicios o en la provisión de soluciones al sector público. **El Real Decreto no se limita**

a establecer obligaciones abstractas de protección, sino que configura una arquitectura completa de gobernanza, gestión de riesgos, categorización de sistemas, implantación de medidas, auditoría, conformidad, certificación, respuesta ante incidentes y mejora continua.

Desde una **perspectiva técnico-jurídica**, **el Real Decreto 311/2022 ofrece el núcleo obligatorio del modelo ENS.** Desde una **perspectiva organizativa**, proporciona una **metodología para ordenar la seguridad dentro de las entidades obligadas, asignar responsabilidades y asegurar que la protección de la información y de los servicios se integre en la gestión ordinaria de la organización**. Por otra parte, desde la **perspectiva estratégica y de posicionamiento institucional**, permite presentar el ENS como un **modelo nacional maduro, verificable y exportable,** capaz de generar confianza dentro y fuera de España.

El valor del Real Decreto radica en que convierte la seguridad de los sistemas de información en una obligación que se articula en torno a un **proceso regulado, documentado, proporcional y verificable**. La entidad no sólo debe "ser segura", sino demostrar cómo ha identificado sus sistemas, cómo los ha categorizado, qué riesgos ha considerado, qué medidas ha implantado, quién responde de cada decisión, cómo verifica el cumplimiento, cómo notifica incidentes y cómo mantiene actualizada su seguridad. Esta lógica traslada el clásico ciclo de mejora continua en los sistemas de gestión al ámbito de la seguridad de la información y la ciberseguridad traduciéndolo en una **función de gobernanza pública** y en un **elemento de confianza para ciudadanos, empresas, proveedores, auditores, certificadores e instituciones internacionales.**

3.1. OBJETO, FINALIDAD Y ESTRUCTURA DEL ENS

El artículo 1 del Real Decreto 311/2022 define el objeto del ENS como el establecimiento de los **principios básicos y requisitos mínimos** necesarios para una protección adecuada de la información tratada y de los servicios prestados por las entidades incluidas en su ámbito de aplicación. La norma persigue asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos. Esta formulación es relevante porque muestra que **el ENS no se limita a la seguridad informática en sentido estricto ni a las dimensiones clásicas de la seguridad de la información, sino que protege el conjunto de condiciones que permiten que los servicios públicos digitales funcionen de forma fiable.**

La finalidad última del ENS es **generar confianza frente a terceros**. Confianza en que los sistemas de información utilizados por las entidades públicas y por sus proveedores prestan sus servicios de forma adecuada, custodian la información sin alteraciones no autorizadas, mantienen la disponibilidad de los servicios y garantizan que la información no llegue a personas no autorizadas. Esa confianza no se apoya sólo en declaraciones internas, sino en un modelo estructurado de cumplimiento, auditoría y certificación.

La estructura del Real Decreto responde a una lógica progresiva comparable con otros estándares de seguridad de la información:

- Delimita su **objeto, ámbito de aplicación y definiciones**,
- Establece los **principios básicos** del ENS,
- Regula la **política de seguridad** y los **requisitos mínimos,**
- Desarrolla la **categorización de los sistemas**, las **medidas de seguridad**, la **auditoría**, el **informe del estado de seguridad**, la **respuesta ante incidentes** y la **conformidad,**
- Finalmente, incorpora anexos esenciales, entre ellos el Anexo I, relativo a la **categorización de los sistemas**; el Anexo II, que contiene las **medidas de seguridad**; el Anexo III sobre la **Auditoría de cumplimiento** y el Anexo IV, que incluye el **glosario** de términos.

Esta estructura permite explicar el ENS como el ciclo de mejora continua mencionado anteriormente: identificar el sistema, determinar su categoría, analizar sus riesgos, organizar la seguridad, aplicar medidas, verificar el cumplimiento, declarar o certificar la conformidad, gestionar incidentes, informar del estado de seguridad y mejorar de forma continua. Esa lectura cíclica es especialmente útil para presentar el ENS a públicos no especializados, porque permite comprender que no se trata de una norma estática, sino de **un sistema operativo de gestión de la seguridad**.

Desde la óptica de **posicionamiento institucional**, este es uno de los mensajes más relevantes:

> **España no dispone únicamente de una norma de ciberseguridad, sino de un modelo público completo para convertir la seguridad en una capacidad verificable**.

El ENS regula qué debe protegerse, cómo debe protegerse, quién debe responsabilizarse, cómo debe comprobarse y cómo debe mantenerse en el tiempo.

3.2. PRINCIPIOS BÁSICOS DE SEGURIDAD

Los **principios básicos** del ENS constituyen la base conceptual del modelo. No son meras declaraciones programáticas, sino criterios rectores que informan la totalidad de la implantación, operación, auditoría y mejora del sistema de seguridad. El Real Decreto 311/2022 identifica como principios básicos la seguridad como proceso integral, la gestión de la seguridad basada en los riesgos, la prevención, detección, respuesta y conservación, la existencia de líneas de defensa, la vigilancia continua y reevaluación periódica, y la diferenciación de responsabilidades.

La **seguridad como proceso integral** implica que la protección no puede fragmentarse ni reducirse a medidas técnicas aisladas. Debe abarcar personas, procesos, tecnología, información, servicios, contratos, proveedores, instalaciones, continuidad y gobierno interno. Este principio permite presentar el ENS como un modelo de seguridad total del sistema, no como una suma de controles desconectados.

La **gestión de la seguridad basada en los riesgos** es otro elemento nuclear. El ENS no impone una seguridad uniforme para todos los sistemas, sino una seguridad proporcionada a la naturaleza de la información, a la criticidad del servicio, a las amenazas existentes y al impacto de los incidentes. Esto refuerza su legitimidad y su viabilidad práctica: el modelo es exigente, pero no ciego a la realidad de cada entidad.

El principio de **prevención, detección, respuesta y conservación** sitúa el ENS en una lógica de resiliencia. La seguridad no consiste sólo en prevenir ataques o incidentes, sino también en detectarlos, responder de forma ordenada, conservar evidencias, recuperar servicios y aprender de lo ocurrido. Esta visión es especialmente valiosa en el entorno actual, en el que la exposición a amenazas es permanente y en el que ninguna organización puede basar su estrategia en la expectativa de riesgo cero.

La existencia de **líneas de defensa y la vigilancia continua** refuerzan la idea de seguridad permanente. El ENS exige que la protección se mantenga activa, se supervise y se revise de forma periódica. No basta con implantar medidas en un momento inicial; es necesario verificar que siguen siendo eficaces frente a cambios tecnológicos, organizativos, contractuales y de amenaza.

La **diferenciación de responsabilidades** cierra el conjunto de principios básicos. En los sistemas de información debe distinguirse entre el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema. Esta separación evita concentraciones indebidas de responsabilidad, facilita la rendición de cuentas y permite resolver conflictos entre las necesidades funcionales, técnicas y de seguridad.

En términos de **comunicación institucional**, los principios básicos permiten formular una idea clara: **el ENS es un marco moderno porque asume que la seguridad no es un producto, sino un proceso; no es sólo tecnología, sino gobernanza; no es sólo prevención, sino resiliencia; y no es sólo cumplimiento, sino confianza demostrable.**

3.3. REQUISITOS MÍNIMOS DE SEGURIDAD

Los **requisitos mínimos** de seguridad son el puente entre los principios generales del ENS y la implantación efectiva de la seguridad. El artículo 12 del Real Decreto 311/2022 enumera estos requisitos, que deben desarrollarse a través de la política de seguridad y aplicarse de forma proporcionada a los riesgos identificados en cada sistema. Su función es asegurar que todas las entidades incluidas en el ámbito del ENS aborden, al menos, los aspectos esenciales de una gestión madura de la seguridad.

Entre los requisitos mínimos se incluyen la **organización e implantación del proceso de seguridad, el análisis y gestión de los riesgos, la gestión de personal, la profesionalidad, la autorización y control de accesos, la protección de las instalaciones, la adquisición de productos de seguridad y contratación de servicios de seguridad, el mínimo privilegio, la integridad y actualización del sistema, la protección de la información almacenada y en tránsito, la prevención ante otros sistemas interconectados, el registro de actividad y detección de código dañino, la gestión de incidentes, la continuidad de la actividad y la mejora continua del proceso de seguridad.**

La amplitud de estos requisitos revela la vocación integral del ENS. La seguridad no se agota en controles de acceso, cortafuegos, cifrado o monitorización. Incluye también gobierno, personas, contratación, mantenimiento, interconexiones, continuidad, evidencias, trazabilidad y mejora. Esta visión es especialmente adecuada para entornos públicos, donde la seguridad de los sistemas puede afectar a derechos, servicios esenciales, continuidad administrativa y confianza institucional.

Los requisitos mínimos tienen, además, una **función de homogeneización**. Permiten que entidades muy distintas —ministerios, comunidades autónomas, entidades locales, universidades públicas, organismos autónomos, sociedades públicas o proveedores privados— trabajen sobre **una base común**. Esa base común no impide la adaptación al riesgo ni a la categoría del sistema, pero evita que cada organización construya su seguridad desde cero o con criterios incompatibles.

Desde el punto de vista de la certificación, **los requisitos mínimos son esenciales porque permiten transformar el cumplimiento en evidencia evaluable**. Un auditor o una entidad de certificación no evalúa una intuición general de seguridad, sino la existencia, adecuación y eficacia de requisitos concretos. Esto dota al modelo ENS de objetividad, trazabilidad y capacidad de comparación.

Como **mensaje de valor**, **los requisitos mínimos permiten presentar el ENS como un marco que profesionaliza la seguridad.** Obliga a las entidades a mirar más allá de la tecnología, incorporar la seguridad en la gestión interna y demostrar que los aspectos esenciales están cubiertos de forma proporcionada y verificable.

3.4. ORGANIZACIÓN DE LA SEGURIDAD Y ROLES ESENCIALES

El ENS dedica una atención especial a la organización de la seguridad. Esta es una de sus grandes fortalezas. Muchos marcos de seguridad fracasan cuando se aplican como listas de controles técnicos sin una estructura clara de gobierno, responsabilidad y decisión. El ENS evita ese riesgo al exigir que la seguridad comprometa a todos los miembros de la organización y al diferenciar los roles esenciales que intervienen en la protección de la información y de los servicios.

El artículo 11 del Real Decreto 311/2022 establece la diferenciación entre diferentes **tipos de responsabilidad**. Esta separación permite distribuir correctamente las decisiones. El **Responsable de la Información** determina los requisitos de seguridad la información tratada; el **Responsable del Servicio** determina los requisitos de seguridad de los servicios prestados; el **Responsable de la Seguridad** adopta decisiones para satisfacer los requisitos de seguridad de la información y de los servicios y supervisa la implantación de las medidas necesarias; y el **Responsable del Sistema** se ocupa de desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.

Un requisito estructural del modelo de gobernanza es la independencia jerárquica. El Real Decreto establece de forma taxativa que el responsable de la seguridad debe ser distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos. Esta separación garantiza que la supervisión de la seguridad sea independiente de la explotación técnica, actuando como un control interno para evitar conflictos de interés. Solo en situaciones excepcionales se permitirá modular esta

exigencia, siempre que se apliquen medidas compensatorias documentadas, de manera que no suponga un obstáculo para entidades que por recursos, tamaño o funciones no puedan adoptar esta estructura o principio de jerarquía.

La **diferenciación de responsabilidades** tiene una **finalidad jurídica y organizativa evidente**. Evita que las decisiones de seguridad queden absorbidas exclusivamente por la explotación técnica de los sistemas. También permite que quienes conocen el valor de la información y de los servicios participen en la determinación de los requisitos de seguridad. De este modo, el ENS introduce un modelo equilibrado entre necesidades funcionales, obligaciones jurídicas, criterios técnicos y gestión de riesgos.

La política de seguridad debe detallar las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos. Este punto es especialmente relevante porque los conflictos son frecuentes: entre disponibilidad y confidencialidad, entre facilidad de uso y control de accesos, entre continuidad del servicio y actualización de sistemas, entre externalización y capacidad de auditoría, o entre agilidad contractual y exigencias de seguridad. El ENS obliga a anticipar estos conflictos y a establecer mecanismos de gobierno.

Desde una **perspectiva institucional**, la organización de roles permite presentar **el ENS como un modelo de responsabilidad**. No se limita a exigir medidas, sino que **obliga a saber quién decide, quién valida, quién opera, quién supervisa y quién responde**. En una época en la que las instituciones europeas y nacionales reclaman responsabilidad de los órganos de dirección y diligencia demostrable en materia de ciberseguridad, esta estructura constituye un argumento de especial fuerza.

3.5. POLÍTICA DE SEGURIDAD

La política de seguridad es el instrumento de gobierno que ordena la forma en que una organización gestiona y protege la información que trata y los servicios que presta. El artículo 12 del Real Decreto 311/2022 exige que cada Administración Pública cuente con una política de seguridad formalmente aprobada por el órgano competente y que cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 disponga igualmente de una política formalmente aprobada, sin perjuicio de determinadas posibilidades de políticas comunes o integradas en el sector público institucional.

La política de seguridad **debe incluir, como mínimo, los objetivos o misión de la organización, el marco regulatorio aplicable, los roles o funciones de seguridad, los deberes y responsabilidades asociados, el procedimiento de designación y renovación, la estructura y composición de los comités de gestión y coordinación de la seguridad, las directrices sobre la documentación de seguridad y los riesgos derivados del tratamiento de datos personales**.

Su importancia radica en que **convierte la seguridad en una decisión formal de la organización**. La política de seguridad no debe ser un documento decorativo, sino la norma interna que fija el marco de gestión, responsabilidad y coordinación. A partir de ella se ordena el resto de la documentación, se articulan procedimientos, se asignan responsabilidades y se vincula la seguridad con la misión de la entidad.

La política de seguridad cumple también una **función de legitimación interna**. En organizaciones complejas, la seguridad puede percibirse como un obstáculo operativo o como una responsabilidad exclusiva del área tecnológica. La aprobación formal de una política de seguridad por el órgano competente eleva la seguridad al nivel de decisión organizativa. Esto favorece la asignación de recursos, la coordinación transversal y la integración de la seguridad en la toma de decisiones.

Desde una **perspectiva de proyección del ENS**, la política de seguridad muestra que **el modelo español no se conforma con exigir controles técnicos, sino que sitúa la seguridad en el gobierno de la organización o lo que tradicionalmente se ha interpretado como implicación de la Dirección,** que con los recientes cambios normativos cobra una especial relevancia y significado. Esta es una idea especialmente importante para interlocutores internacionales:

> **El ENS no es sólo un estándar técnico, sino un marco de gobernanza pública de la seguridad a través del cual se asumen responsabilidades relacionadas con la seguridad y el cumplimiento normativo.**

3.6. CATEGORIZACIÓN DE LOS SISTEMAS DE INFORMACIÓN

La categorización de los sistemas de información es una de las piezas clave del ENS. **Permite determinar el nivel de exigencia aplicable a cada sistema en función del impacto que tendría un incidente sobre determinadas dimensiones de seguridad**. El Anexo I del Real Decreto 311/2022 regula esta categorización atendiendo a las dimensiones de seguridad: confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad.

La categorización permite clasificar los sistemas en **categoría Básica, categoría Media o categoría Alta**. Esta clasificación no es meramente nominal, sino que **condiciona la selección de medidas, la intensidad de los controles, la necesidad de auditoría y el régimen de declaración o certificación de conformidad.**

> **De este modo, el ENS introduce una lógica de proporcionalidad: los sistemas con mayor impacto potencial deben someterse a mayores exigencias de protección y verificación.**

El proceso de categorización obliga a la organización a reflexionar sobre qué información trata, qué servicios presta, qué dependencias existen, qué consecuencias tendría la pérdida de disponibilidad, la alteración de datos, la falta de trazabilidad o el acceso no autorizado, y qué nivel de protección resulta necesario. Esta reflexión es esencial para evitar una seguridad puramente formal. La categoría del sistema debe responder a la realidad del servicio y de la información, no a una preferencia organizativa o a una estrategia de reducción artificial de obligaciones.

La categorización tiene una función práctica inmediata: **permite seleccionar las medidas de seguridad adecuadas**. Pero tiene también una función estratégica: **obliga a la organización a conocer sus sistemas y a priorizar recursos**. En términos de gestión pública, esto es fundamental.

> **El ENS permite ordenar la inversión en seguridad en función del impacto, evitando**

tanto la infra protección de sistemas críticos como la sobredimensión de sistemas menos relevantes.

Desde el **punto de vista de la comunicación internacional del modelo ENS**, la categorización es uno de sus elementos más atractivos. Permite explicar que **el modelo español no aplica el mismo nivel de exigencia a todos los sistemas, sino que introduce una aproximación graduada, razonable y basada en impacto**. Esta combinación de rigor y proporcionalidad refuerza la credibilidad del ENS ante entidades públicas, proveedores y observadores internacionales.

Para objetivar la eficacia de los procesos, el ENS adopta el **Modelo de Madurez de Capacidad (CMM)**, que permite medir el grado de profesionalización e institucionalización de las medidas desde el nivel L0 (Inexistente) hasta el L5 (Optimizado). El Real Decreto exige niveles mínimos de madurez según la criticidad:

Nivel	Denominación	Descripción	Categoría ENS Exigible
L0	Inexistente	No existe un proceso que soporte el servicio requerido.	-
L1	Inicial / Ad hoc	Ambiente inestable. El éxito se basa en el esfuerzo personal; soluciones reactivas a incidentes y procedimientos informales o incompletas.	-
L2	Reproducible, pero intuitivo	Prácticas de gestión institucionalizadas con métricas básicas y seguimiento de calidad. Procedimientos existentes pero no siempre documentados.	BÁSICA
L3	Proceso definido	Gestión sólida con normativa y procedimientos detallados, documentados y coordinados entre grupos. Formación específica del personal.	MEDIA
L4	Gestionado y medible	Uso sistemático de métricas de efectividad y eficiencia para la toma de decisiones y gestión de riesgos. Servicio de alta calidad.	ALTA
L5	Optimizado	Organización volcada en la mejora continua. Uso intensivo de métricas y gestión activa del proceso de innovación.	(Nivel de excelencia)

Figura 3.1 Niveles de madurez (CMMI) exigibles según la categoría del sistema de información

Este modelo transforma la mejora continua en una métrica auditable que garantiza que la seguridad no sea solo documental, sino un proceso gestionado y medible.

3.7. MEDIDAS DE SEGURIDAD DEL ANEXO II

El Anexo II del Real Decreto 311/2022 contiene el catálogo de medidas de seguridad del ENS. **Estas medidas son el instrumento técnico mediante el cual los principios básicos y requisitos mínimos se traducen en controles concretos.**

La norma estructura las medidas en tres grandes bloques: marco organizativo, marco operacional y medidas de protección.

El **marco organizativo** contiene las **medidas relacionadas con la organización global de la seguridad.** Incluye aspectos como la política de seguridad, la normativa interna, los procedimientos, la autorización de procesos y otros elementos que permiten ordenar la seguridad desde la dirección y la gestión interna. Su función es asegurar que la seguridad tiene una base organizativa clara.

El **marco operacional** agrupa **medidas destinadas a proteger la operación del sistema como conjunto integral de componentes orientados a una finalidad**. Incluye, entre otras cuestiones, planificación, control de acceso, explotación, monitorización, gestión de cambios, continuidad, protección frente a código dañino, gestión de incidentes y otros aspectos vinculados al funcionamiento ordinario de los sistemas. Su función es asegurar que la seguridad se integra en la operación diaria.

Las **medidas de protección** **se centran en activos concretos, atendiendo a su naturaleza y al nivel de seguridad exigido por las dimensiones afectadas**. Pueden referirse a instalaciones, personal, equipos, comunicaciones, soportes, aplicaciones, información, servicios externos y otros elementos del sistema. Su función es proteger los componentes materiales, lógicos y funcionales que hacen posible la prestación segura de los servicios.

El marco jurídico introduce una flexibilidad técnica esencial: las medidas de seguridad del Anexo II pueden ser reemplazadas por **medidas compensatorias**. Para ello, la entidad debe justificar documentalmente en la **Declaración de Aplicabilidad** que la medida alternativa protege el activo de forma equivalente o superior, satisfaciendo siempre los principios básicos y requisitos mínimos.

Además, para dotar al sistema de flexibilidad y adecuación al entorno, se ha introducido un **sistema de refuerzos** que vienen a incrementar el nivel de seguridad para cada dimensión y control seleccionado y que pasan por un esquema que contempla:

- Controles o refuerzos **obligatorios**, inherentes al control o medida de seguridad, que podrán ser incrementales en función el control o medida a aplicar.
- Refuerzos **alternativos**, que permiten seleccionar distintas vías para cumplir con el control seleccionado.
- Refuerzos **voluntarios**, que permiten ampliar las capacidades técnicas y organizativas en entidades o sistemas de información con un alto grado de madurez.

La selección de medidas debe realizarse atendiendo a los tipos de activos presentes, las dimensiones de seguridad relevantes, el nivel correspondiente a cada dimensión, la categoría del sistema y los refuerzos aplicables. Esta metodología permite que las medidas no se apliquen de forma mecánica, sino conforme a una lógica de adecuación al sistema y al riesgo.

El Anexo II es uno de los elementos que permite exhibir el ENS como modelo maduro. No se limita a proclamar objetivos, sino que ofrece un catálogo operativo de medidas organizado y vinculable a la categoría de los sistemas. Esta concreción facilita la implantación, la auditoría y la certificación, y permite a las entidades saber qué se espera de ellas.

3.8. AUDITORÍA DE LA SEGURIDAD

La auditoría es el mecanismo que permite verificar si el sistema de información se ha adecuado efectivamente al ENS. Su importancia es central, porque transforma el cumplimiento en evidencia y permite detectar deficiencias, desviaciones o no conformidades. Sin auditoría, el ENS correría el riesgo de convertirse en un modelo de cumplimiento meramente declarativo. Con auditoría, se configura como un sistema de confianza verificable.

El Real Decreto 311/2022 exige la realización de auditorías en los términos previstos para los sistemas que correspondan, especialmente en sistemas de categoría Media y Alta. **La auditoría debe valorar la adecuación de la política de seguridad, la correcta categorización del sistema, el análisis y gestión de riesgos, la implantación de medidas, la documentación de seguridad, la organización de roles, la gestión de incidentes, la continuidad, la existencia de evidencias y el grado de cumplimiento general del ENS.**

La auditoría no debe concebirse como un trámite final, sino como una **herramienta de mejora**. Permite identificar debilidades antes de que se materialicen incidentes graves, priorizar acciones correctoras, reforzar la trazabilidad de las decisiones y preparar a la organización para la certificación o para el mantenimiento de la conformidad. En este sentido**, la auditoría es tanto un mecanismo de control como un instrumento de madurez.**

Desde el punto de vista de la **contratación pública** y de la **relación con proveedores**, la auditoría adquiere una dimensión adicional. **Permite verificar que los sistemas que soportan servicios públicos o tratan información pública cumplen las exigencias aplicables**. En entornos externalizados o cloud, la capacidad de auditar o de recibir evidencias auditables es esencial para evitar dependencias opacas y para mantener el control sobre la seguridad del servicio.

En términos de **proyección internacional**, **la auditoría refuerza el valor del ENS como modelo de confianza**. Muchos marcos nacionales o sectoriales establecen obligaciones de seguridad, pero no todos articulan un sistema tan claro de verificación. **La auditoría ENS muestra que España ha construido un modelo que exige seguridad y, además, exige demostrarla.** Además, su alineamiento con estándares internacionales de seguridad permitan aplicar al ENS los elementos tradicionales de la auditoría sobre sistemas de gestión, integrándose dentro de planes y programas de auditoría comunes.

3.9. INFORME DEL ESTADO DE LA SEGURIDAD

El informe del estado de la seguridad es otro componente relevante del ENS, porque **permite obtener una visión agregada y periódica de la situación de seguridad de las entidades incluidas en su ámbito, además de convertirse en una herramienta de medición en tiempo real del estado de la seguridad nacional.** Su función no es sólo documental, sino también estratégica: medir, comparar, detectar tendencias, identificar áreas de mejora y alimentar la toma de decisiones en materia de ciberseguridad pública.

Este informe permite pasar de la gestión aislada de cada sistema a una visión de conjunto.

En un Estado complejo y descentralizado, con múltiples Administraciones, organismos, entidades públicas y proveedores, disponer de información sobre el estado de la seguridad resulta esencial para planificar políticas públicas, priorizar recursos, orientar guías, reforzar capacidades y conocer el grado real de madurez del ecosistema.

La elaboración del informe exige que las entidades dispongan de información ordenada sobre su seguridad: sistemas, categorías, medidas, auditorías, incidentes, nivel de adecuación, evolución y deficiencias. Por ello, el informe no es sólo una obligación de reporte; incentiva la disciplina interna de gestión y documentación.

Una entidad que no conoce su estado de seguridad difícilmente puede mejorarlo.

El informe del estado de la seguridad conecta también con las **herramientas de apoyo del CCN**, en particular con aquellas destinadas a facilitar la medición y seguimiento de la adecuación al ENS. Esta dimensión instrumental es importante porque muestra que el ENS no sólo impone obligaciones, sino que proporciona medios para hacerlas practicables.

Desde una **perspectiva institucional**, el informe del estado de seguridad permite presentar **el ENS como un modelo de inteligencia regulatoria**. No se trata sólo de regular, sino de medir el cumplimiento, conocer la realidad, identificar debilidades y actuar sobre ellas. Esta capacidad de medición es uno de los atributos que refuerzan la madurez del modelo español.

3.10. GESTIÓN Y NOTIFICACIÓN DE INCIDENTES

La gestión y notificación de incidentes constituye una pieza esencial del ENS. La seguridad moderna no puede basarse en la idea de que los incidentes nunca se producirán. Al contrario, debe asumir que los incidentes son posibles y que la diferencia entre una organización madura y una organización vulnerable reside en su capacidad para prevenirlos, detectarlos, responder a ellos, contenerlos, recuperarse y aprender.

El ENS incorpora la gestión de incidentes dentro de los requisitos mínimos de seguridad y la conecta con las obligaciones de notificación y con la capacidad de respuesta del ecosistema público. La notificación permite que los incidentes relevantes no queden encerrados en la organización afectada, sino que puedan ser

conocidos, gestionados y, en su caso, coordinados por los órganos competentes. Esto resulta especialmente importante cuando los incidentes pueden afectar a servicios públicos, datos personales, cadenas de suministro o sistemas interconectados.

La gestión de incidentes exige procedimientos claros: detección, clasificación, escalado, comunicación interna, comunicación externa, preservación de evidencias, análisis forense cuando proceda, medidas de contención, recuperación, cierre y lecciones aprendidas. Estos procedimientos deben integrarse en la organización y ensayarse, porque improvisar durante un incidente aumenta el riesgo de daño técnico, jurídico y reputacional.

La notificación de incidentes tiene también una función colectiva: **permite mejorar el conocimiento de las amenazas, detectar patrones, emitir alertas, coordinar respuestas y elevar el nivel de ciberseguridad del conjunto del sector público**. En este sentido, el ENS no sólo protege a cada entidad individualmente considerada, sino que contribuye a la resiliencia del ecosistema público digital.

Desde el punto de vista de la propuesta de valor, **este elemento permite presentar el ENS como un modelo de resiliencia y como un modelo maduro, adelantado a las actuales exigencias normativas, el cual cuenta con una experiencia más que contrastada en la adopción de mecanismos de gestión de incidentes que han sido escalados a través de todo el sector público español**. No promete invulnerabilidad; ofrece capacidad organizada de respuesta. Este mensaje resulta creíble y estratégico: en el contexto actual, la confianza no deriva de afirmar que no habrá incidentes, sino de demostrar que existen mecanismos para gestionarlos con eficacia, transparencia y coordinación.

3.11. DECLARACIÓN Y CERTIFICACIÓN DE CONFORMIDAD

El régimen de Declaración y Certificación de Conformidad es uno de los rasgos más relevantes del ENS como sistema de confianza. **Permite convertir el cumplimiento en una evidencia formal frente a terceros**. La Declaración de Conformidad y la Certificación de Conformidad son instrumentos distintos, adecuados a diferentes niveles de exigencia, pero ambos cumplen una función común: hacer visible y verificable la adecuación al ENS.

La **Declaración de Conformidad** vincula a los sistemas en los que el modelo permite acreditar la adecuación mediante autoevaluación y responsabilidad interna, únicamente aplicable a sistemas de categoría **Básica**. La **Certificación de Conformidad**, en cambio, incorpora una evaluación externa más intensa, especialmente relevante para sistemas de categoría **Media** y **Alta**. Esta diferenciación responde a la lógica de proporcionalidad del ENS: a mayor criticidad del sistema, mayor necesidad de verificación externa.

La Certificación de Conformidad tiene un valor jurídico, técnico y de mercado:

- **Jurídico**, porque permite acreditar cumplimiento de una norma obligatoria.
- **Técnico**, porque presupone una evaluación del sistema conforme a criterios estructurados.

- **De mercado**, porque ofrece a proveedores y entidades públicas una evidencia reconocible de confianza.

En la contratación pública, la certificación ENS puede convertirse en una herramienta para evaluar la solvencia técnica, reducir riesgos y asegurar que los servicios contratados se prestan sobre sistemas adecuados.

La certificación no debe entenderse, sin embargo, como un fin en sí mismo. Su valor depende de la calidad del proceso de adecuación, de la correcta categorización del sistema, de la implantación real de medidas, de la independencia y competencia de quienes evalúan y de la capacidad de mantener la conformidad en el tiempo. Una certificación desvinculada de la seguridad efectiva perdería valor. Por ello, **el ENS combina certificación, auditoría, seguimiento y mejora continua**.

Desde la **perspectiva institucional**, la Declaración y la Certificación de Conformidad son esenciales para presentar **el ENS como un modelo de confianza demostrable.** No se trata sólo de afirmar que España tiene un marco de seguridad; se puede mostrar que ese marco permite verificar, certificar y acreditar el cumplimiento. Esta capacidad de demostración es especialmente atractiva para instituciones europeas, Estados terceros y operadores económicos.

3.12. MEJORA CONTINUA Y REEVALUACIÓN PERIÓDICA

La mejora continua es el principio que asegura la vigencia del ENS en el tiempo. Los sistemas de información evolucionan, las amenazas cambian, los servicios se transforman, los proveedores se sustituyen, la tecnología avanza y el marco normativo europeo se intensifica. Un modelo de seguridad que no incorpore revisión periódica está condenado a quedar obsoleto. El ENS evita ese riesgo al integrar la reevaluación como parte del propio proceso de seguridad.

La mejora continua exige revisar el análisis de riesgos, actualizar medidas, corregir no conformidades, incorporar lecciones aprendidas de incidentes, adaptar la política de seguridad, reforzar procedimientos, mejorar la documentación y revisar la adecuación de los sistemas. También exige que la organización no entienda la certificación como un punto final, sino como una evidencia temporal que debe sostenerse mediante seguimiento, mantenimiento y evolución.

Este enfoque es **especialmente importante en ámbitos como servicios cloud, inteligencia artificial, automatización, tecnologías cuánticas, interoperabilidad, cadena de suministro y servicios gestionados**. La transformación tecnológica puede alterar los riesgos de forma muy rápida. Por ello, la seguridad debe formar parte del ciclo de vida de los sistemas y no limitarse al momento inicial de diseño o contratación.

La mejora continua tiene también una **dimensión cultural:** obliga a las entidades a asumir que la seguridad no es un proyecto puntual, sino una función permanente. Esto implica formar al personal, mantener capacidades, revisar procedimientos, invertir en tecnologías adecuadas, coordinar áreas jurídicas y técnicas, y fortalecer la responsabilidad directiva. El ENS, en este sentido, promueve una cultura de seguridad institucional.

Desde el **punto de vista de la proyección exterior**, **la mejora continua permite presentar el ENS como un modelo vivo. No es un marco cerrado, sino una arquitectura capaz de adaptarse al cambio**. Esta característica resulta fundamental para su venta institucional.

El ENS combina estabilidad normativa, coherencia técnica y capacidad evolutiva. Esa combinación es precisamente la que necesitan los Estados y organizaciones que buscan modelos de ciberseguridad sostenibles.

Fase del ciclo ENS	Elemento regulado	Función dentro del modelo	Mensaje de valor
Identificación	Determinación del sistema, servicios e información afectados	Delimitar qué debe protegerse	Seguridad basada en conocimiento real del sistema
Gobierno	Política de seguridad, roles y responsabilidades	Ordenar la toma de decisiones y la rendición de cuentas	La seguridad se gestiona desde la organización
Evaluación	Categorización y análisis de riesgos	Determinar impacto, criticidad y nivel de exigencia	Modelo proporcional y basado en riesgos
Implantación	Requisitos mínimos y medidas del Anexo II	Traducir obligaciones en controles concretos	Seguridad operativa, no meramente declarativa
Verificación	Auditoría, declaración y certificación de conformidad	Comprobar y evidenciar el cumplimiento	Confianza verificable ante terceros
Respuesta	Gestión y notificación de incidentes	Detectar, contener, comunicar y recuperar	Resiliencia y coordinación institucional
Medición	Informe del estado de la seguridad	Conocer el grado de madurez y evolución	Inteligencia regulatoria y mejora del ecosistema
Evolución	Reevaluación periódica y mejora continua	Mantener la adecuación frente al cambio	Modelo vivo, adaptable y sostenible

Figura 3.1 Ciclo de gestión de la seguridad conforme al Real Decreto 311/2022

El Real Decreto 311/2022 actúa como el núcleo operativo del Esquema Nacional de Seguridad, articulando de forma dinámica sus principios, requisitos y medidas dentro de una lógica de mejora continua. La siguiente ilustración sintetiza el funcionamiento de esta norma como motor del sistema, mostrando cómo se conectan las distintas etapas del ciclo de vida de la seguridad digital: desde la gobernanza y el análisis de riesgos iniciales hasta la verificación y auditoría periódica.



Figura 3.3 El Real Decreto 311/2022, de 3 de mayo, como motor del ENS

3.13 RESUMIENDO…

El contenido esencial del Real Decreto 311/2022 permite comprender por qué **el ENS es mucho más que una obligación normativa**.

La norma articula un modelo completo que parte de principios básicos, exige requisitos mínimos, ordena responsabilidades, impone una política de seguridad, categoriza sistemas, selecciona medidas, verifica el cumplimiento, gestiona incidentes, mide el estado de seguridad y exige mejora continua. Todo ello configura una arquitectura de confianza digital especialmente sólida.

El valor del Real Decreto reside en su **capacidad para convertir la seguridad en un proceso jurídico, técnico, organizativo y estratégico**.

- **Jurídico**, porque establece obligaciones exigibles.
- **Técnico**, porque concreta medidas y criterios de protección.
- **Organizativo**, porque distribuye responsabilidades y exige políticas, procedimientos y gobierno interno.
- **Estratégico**, porque permite presentar el ENS como un modelo español de ciberseguridad pública, verificable, proporcional, maduro y alineado con las tendencias europeas e internacionales.

El Real Decreto 311/2022, de 3 de mayo, no solo regula la seguridad; estructura un sistema nacional para generar confianza, demostrar cumplimiento, elevar la madurez del sector público, disciplinar la cadena de suministro y proyectar internacionalmente un modelo español de gobernanza de la ciberseguridad.

4. CATEGORIZACIÓN, MEDIDAS DE SEGURIDAD Y CICLO DE CUMPLIMIENTO

El Esquema Nacional de Seguridad no impone una seguridad abstracta, uniforme o indiferenciada. Su valor reside precisamente en lo contrario: **traduce principios generales de seguridad en un sistema graduado, proporcional y verificable**, capaz de adaptarse a la naturaleza de cada sistema de información, al valor de la información tratada, a la criticidad de los servicios prestados y al impacto que podría producir un incidente de seguridad. **La categorización de los sistemas, la selección de medidas de seguridad y el ciclo de cumplimiento constituyen, por ello, el núcleo operativo del ENS.**

Este epígrafe permite comprender cómo funciona el ENS en la práctica. Si los capítulos anteriores explican qué es el ENS, cuál es su fundamento jurídico y cuáles son los principales elementos del Real Decreto 311/2022, este capítulo muestra:

- Cómo se pasa **de la norma al cumplimiento efectivo,**
- Cómo se **identifica el sistema,**
- Cómo se valora su **impacto,**
- Cómo se determina su **categoría de seguridad,**
- Cómo se seleccionan las **medidas del Anexo II,**
- Cómo se documenta la **Declaración de Aplicabilidad,**
- Cómo se realiza el **diagnóstico y la adecuación,**
- Cómo se verifica el **cumplimiento,** y
- Cómo se mantiene la **conformidad en el tiempo.**

Desde una **perspectiva técnica,** este ciclo permite **ordenar la seguridad de la información con criterios objetivos**. Desde una **perspectiva organizativa**, permite **asignar responsabilidades, priorizar recursos y hacer gestionable el cumplimiento**. Desde una **perspectiva de certificación o auditoría**, permite **convertir la seguridad en evidencia auditable**. Y desde una **perspectiva institucional**, permite presentar **el ENS como un modelo de madurez**: un sistema que no se limita a exigir seguridad, sino que ofrece una metodología clara para alcanzarla, demostrarla y mantenerla.

El modelo español no se apoya en una exigencia genérica de diligencia, ni en una recomendación voluntaria de buenas prácticas, sino en una arquitectura que vincula la categoría del sistema, las dimensiones de seguridad, el riesgo, las medidas exigibles, la documentación, la auditoría y la conformidad. Esa arquitectura convierte el ENS en un marco operativo de confianza digital.



Figura 4.1 Arquitectura del modelo ENS

4.1. CATEGORIZACIÓN DE LOS SISTEMAS: FINALIDAD Y METODOLOGÍA

La **categorización** de los sistemas de información es el punto de partida para determinar el nivel de exigencia aplicable a cada sistema sujeto al ENS. Su finalidad es **modular el esfuerzo de seguridad en función de la importancia de la información tratada, la relevancia de los servicios prestados y los riesgos a los que el sistema está expuesto.** El artículo 40.1 del Real Decreto 311/2022 expresa esta lógica al señalar que la categoría de seguridad de un sistema debe modular el equilibrio entre la importancia de la información y los servicios, por un lado, y el esfuerzo de seguridad requerido, por otro, **bajo el principio de proporcionalidad**.

Esta formulación es decisiva:

> **El ENS no pretende que todos los sistemas reciban el mismo tratamiento, sino que cada sistema reciba el tratamiento adecuado. La categorización es, por tanto, una herramienta de racionalidad jurídica, técnica y económica**

Con ello **se evita tanto la infraprotección de sistemas relevantes como la sobredimensión de sistemas de menor impacto**. Permite justificar por qué un sistema debe ser objeto de medidas reforzadas, auditoría y certificación, y por qué otro puede operar con un nivel de exigencia inferior, siempre que ello sea coherente con la información y los servicios que soporta.

> **La metodología de categorización parte de la valoración del impacto que tendría un incidente que afectase a la seguridad de la información tratada o de los servicios prestados**.

No se trata, por tanto, de una clasificación basada en la mera complejidad tecnológica del sistema, ni en el tamaño de la entidad, ni en el número de usuarios, aunque todos esos elementos puedan ser relevantes en la práctica. Lo determinante es el impacto que tendría una pérdida o degradación de las dimensiones de seguridad

sobre la organización, los servicios, los activos, los derechos de los ciudadanos, el cumplimiento normativo y la continuidad de la actividad.

La categorización obliga a la entidad a formular **preguntas básicas pero esenciales: qué información se trata, qué servicios se prestan, qué procesos dependen del sistema, qué consecuencias tendría una interrupción, qué efectos tendría una alteración de los datos, qué daño provocaría un acceso no autorizado, qué impacto tendría la imposibilidad de acreditar una actuación, qué obligaciones legales podrían incumplirse y qué perjuicios podrían ocasionarse a ciudadanos, empresas u otras Administraciones.**

El resultado de esa valoración no es meramente documental, sino que condiciona todo el ciclo posterior: **la selección de medidas de seguridad, los refuerzos aplicables, la Declaración de Aplicabilidad, la intensidad de las evidencias, la necesidad de auditoría, la declaración o certificación de conformidad y el mantenimiento del sistema.** Por ello, una categorización incorrecta puede distorsionar todo el modelo de cumplimiento. Si se categoriza a la baja un sistema relevante, se reducirá indebidamente el nivel de protección. Si se categoriza al alza sin justificación, se impondrán costes y cargas desproporcionadas.

Desde el **punto de vista de la gobernanza**, la categorización no debería abordarse como un ejercicio exclusivamente técnico. **Deben participar quienes conocen el valor de la información, la criticidad de los servicios, los riesgos jurídicos, las dependencias tecnológicas, los compromisos contractuales y las consecuencias organizativas de un incidente**.

> **La categorización exige la intervención coordinada de responsables de la información, responsables del servicio, responsables de seguridad, responsables del sistema y, cuando proceda, áreas jurídicas, unidades de contratación, responsables de protección de datos y responsables de continuidad.**

Esto implica que cada entidad lleve u organización lleve a cabo un análisis crítico en cuanto a la asignación de las responsabilidades previstas en la norma, considerando el impacto que va a tener en la toma de decisiones y en la valoración de los servicios e información objeto de tratamiento.

Esta característica constituye uno de los elementos de madurez del ENS.

> **El modelo español obliga a que la seguridad se piense desde el impacto real del servicio y no sólo desde la tecnología, conectando la capa de responsabilidades, competencia y en definitiva "negocio" con la capa de gestión de la seguridad.**

Esto permite explicar internacionalmente el ENS como un marco que conecta la gestión de riesgos con la prestación efectiva de servicios públicos digitales y cuestiones derivadas como la dotación de recursos, contratación, seguimiento de la cadena de suministro, continuidad de los servicios, etc.

4.2. DIMENSIONES DE SEGURIDAD: CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD, AUTENTICIDAD Y TRAZABILIDAD

El ENS determina la categoría de los sistemas mediante la valoración de cinco **dimensiones de seguridad**: **confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad**. Como se puede observar, el ENS introduce o valora las dimensiones de trazabilidad y autenticidad dada la importancia de estas dimensiones en el contexto de lo público, en el que la trascendencia jurídica de las actuaciones electrónicas y su impacto en los derechos de los interesados requiere de mecanismos de protección específicos. Estas dimensiones permiten analizar el impacto de un incidente desde distintas perspectivas y evitar una visión reduccionista de la seguridad. El Anexo I del Real Decreto 311/2022 identifica expresamente estas dimensiones como criterios para valorar el impacto sobre la información tratada y los servicios prestados.

La **confidencialidad** se refiere a la **protección frente al acceso, conocimiento o divulgación no autorizada de la información**. En el sector público, esta dimensión es especialmente relevante cuando el sistema trata datos personales, información tributaria, sanitaria, social, policial, contractual, estratégica, presupuestaria, sancionadora o cualquier otra información sometida a deberes de reserva. La pérdida de confidencialidad puede generar daños jurídicos, reputacionales, económicos e institucionales.

La **integridad** se refiere a la **garantía de que la información y los servicios no han sido alterados de forma no autorizada o indebida**. En un expediente administrativo, en un registro, en una plataforma de contratación, en una base de datos tributaria o en un sistema de gestión sanitaria, la alteración de datos puede tener consecuencias graves: decisiones administrativas incorrectas, perjuicios a ciudadanos, fraudes, invalidez de actuaciones o pérdida de confianza en el servicio.

La **disponibilidad** expresa la **capacidad de acceder a la información y utilizar los servicios cuando resulten necesarios**. En la Administración digital, la disponibilidad no es una cuestión meramente técnica. Puede afectar al ejercicio de derechos, al cumplimiento de plazos, a la continuidad de servicios públicos, a la gestión de emergencias, a la atención ciudadana, a la recaudación tributaria, a la tramitación de ayudas o al funcionamiento ordinario de una entidad pública. Por ello, la indisponibilidad de determinados sistemas puede tener un impacto institucional elevado.

La **autenticidad** permite **garantizar la identidad de quienes intervienen y la legitimidad de las actuaciones realizadas en el sistema**. Es una dimensión particularmente importante en entornos de identificación electrónica, firma electrónica, intercambio de datos, acceso a expedientes, notificaciones, presentación de solicitudes y prestación de servicios públicos por medios electrónicos. Sin autenticidad, la Administración digital pierde fiabilidad jurídica.

La **trazabilidad** permite **conocer y reconstruir las actuaciones realizadas en un sistema: quién hizo qué, cuándo, desde dónde, con qué permisos, sobre qué información y con qué resultado**. Esta dimensión es esencial para la auditoría, la

investigación de incidentes, la rendición de cuentas, la conservación de evidencias y la depuración de responsabilidades. En términos de confianza, la trazabilidad es una de las dimensiones más importantes, porque permite demostrar lo ocurrido.

Estas cinco dimensiones hacen del ENS un modelo especialmente sólido. Frente a enfoques que identifican la seguridad casi exclusivamente con la confidencialidad o con la disponibilidad, **el ENS ofrece una visión completa de la seguridad de la información y de los servicios**. Esta amplitud resulta muy valiosa para la proyección europea e internacional del modelo, porque permite explicar que la seguridad pública digital requiere proteger simultáneamente datos, servicios, identidades, actuaciones y evidencias.

La valoración de cada dimensión debe realizarse respecto de las informaciones tratadas y los servicios prestados. Cuando un sistema trate diferentes informaciones o preste distintos servicios, debe atenderse al mayor nivel exigible en cada dimensión. Esta regla evita que sistemas complejos queden infra protegidos por una valoración agregada o superficial. En la práctica, obliga a analizar con precisión los componentes funcionales del sistema y las consecuencias de los incidentes sobre cada dimensión.

4.3. CATEGORÍAS BÁSICA, MEDIA Y ALTA

El ENS clasifica los sistemas de información en **tres categorías**: **Básica, Media y Alta.** Esta clasificación, regulada en el Anexo I del Real Decreto 311/2022, **permite traducir la valoración de impacto en un nivel concreto de exigencia**. Un sistema será de categoría Alta si alguna de sus dimensiones de seguridad alcanza nivel alto; será de categoría Media si alguna dimensión alcanza nivel medio y ninguna alcanza nivel superior; y será de categoría Básica si alguna dimensión alcanza nivel bajo y ninguna alcanza nivel superior.

Esta regla tiene una lógica prudente: basta con que una dimensión alcance un nivel superior para que el sistema quede situado en la categoría correspondiente. Ello evita que una dimensión crítica quede diluida por otras menos relevantes. Por ejemplo, un sistema puede no requerir una disponibilidad especialmente elevada, pero tratar información cuya confidencialidad o integridad sea crítica. En ese caso, la categoría debe reflejar la dimensión más exigente.

La categoría **Básica** no debe interpretarse como ausencia de seguridad. Todo sistema sometido al ENS requiere medidas de seguridad, documentación, responsabilidad y seguimiento. La categoría Básica indica que **el impacto de los incidentes, en las dimensiones consideradas, no alcanza niveles superiores, pero no exime del cumplimiento del marco ENS**. De hecho, los sistemas de categoría básica también deben ser objeto de autoevaluación y declaración de conformidad cuando proceda.

La categoría **Media** representa un nivel de exigencia superior y suele asociarse a **sistemas cuya afectación puede producir perjuicios relevantes para la organización, los servicios, los derechos de las personas o el cumplimiento normativo**. En estos sistemas, el modelo exige una mayor intensidad en la implantación de medidas, en la obtención de evidencias y en la verificación de la conformidad.

La categoría **Alta** se reserva para **sistemas cuya afectación puede producir impactos especialmente graves.** Estos sistemas requieren el máximo nivel de atención, tanto en la implantación de medidas como en la auditoría, gestión de riesgos, continuidad, seguimiento y eventual certificación. En términos de gobernanza pública, la categoría alta obliga a tratar la seguridad como un asunto estratégico de la entidad.

La clasificación en tres categorías tiene una ventaja comunicativa evidente puesto que permite explicar el ENS de forma sencilla: **cuanto mayor sea el impacto potencial, mayor será el nivel de exigencia**. Esta proporcionalidad es esencial para defender el modelo ante entidades españolas y ante terceros países.

El ENS no impone un marco uniforme ni arbitrario; establece una escala comprensible y vinculada a la criticidad real del sistema.

Desde el punto de vista de la **certificación**, **la categoría condiciona la forma de acreditar la conformidad.**

1 Sistemas de categoría **Media** o **Alta** → precisan **Auditoría** (externa, de tercera parte) para la Certificación de su conformidad.

2 Sistemas de categoría **Básica** → requieren A**utoevaluación** (auditoría de primera parte) para la declaración de conformidad, sin perjuicio de que también puedan someterse a auditoría de certificación.



Figura 4.2 Marco de cumplimiento ENS

Esta conexión entre categoría y conformidad refuerza la lógica del sistema: **la intensidad de la verificación aumenta con la criticidad del sistema.**

Para que la mejora continua no sea un concepto abstracto, el ENS adopta el **Modelo de Madurez de Capacidad (CMMI)**, que permite medir el grado de profesionalización e institucionalización de cada medida desde el nivel L0 (Inexistente) hasta el L5 (Optimizado). El cumplimiento legal exige alcanzar un **nivel mínimo de madurez** según la categoría del sistema: **L2 (Reproducible) para categoría Básica, L3 (Proceso**

definido) para Media y L4 (Gestionado y medible) para Alta. Sin alcanzar estos umbrales de madurez, el sistema no se considera plenamente conforme, con independencia de la implantación técnica de los controles.

4.4. SELECCIÓN DE MEDIDAS DE SEGURIDAD

Una vez determinada la categoría del sistema, debe seleccionarse el conjunto de medidas de seguridad aplicables. **El Anexo II del Real Decreto 311/2022 establece que las medidas deben ser proporcionales a las dimensiones de seguridad relevantes y a la categoría del sistema**. La selección no es un ejercicio automático, sino un proceso ordenado que exige identificar activos, determinar dimensiones relevantes, asignar niveles de seguridad, establecer la categoría del sistema y seleccionar las medidas y refuerzos correspondientes.

Esta lógica convierte al ENS en un modelo técnico operativo. Las medidas no se eligen por intuición ni por mera disponibilidad tecnológica, sino en función de un proceso estructurado. **Ello permite justificar por qué determinadas medidas son aplicables y otras no, qué refuerzos son necesarios y qué evidencias deberán conservarse**. La selección de medidas es, por tanto, una decisión técnica con relevancia jurídica y organizativa.

El artículo 28 del Real Decreto 311/2022 establece que, para cumplir los requisitos mínimos, las entidades comprendidas en su ámbito de aplicación adoptarán las medidas y refuerzos de seguridad correspondientes del Anexo II, teniendo en cuenta los activos que constituyen los sistemas de información, la categoría del sistema y las decisiones adoptadas para gestionar los riesgos identificados. Esta previsión confirma que el ENS combina categorización, análisis de riesgos y selección de medidas.

El modelo admite **medidas compensatorias**, siempre que se justifique documentalmente que protegen igual o mejor frente al riesgo sobre los activos y que satisfacen los principios básicos y requisitos mínimos del ENS. **Esta posibilidad es importante porque evita que el ENS se convierta en un marco rígido incapaz de adaptarse a tecnologías, arquitecturas o soluciones alternativas**. Sin embargo, también exige rigor: la compensación debe estar documentada, aprobada y reflejada en la Declaración de Aplicabilidad.

La selección de medidas debe entenderse como una actividad de diseño de seguridad. No basta con marcar medidas como aplicables o no aplicables. **Es necesario determinar cómo se implantan, quién las gestiona, qué procedimientos las sostienen, qué evidencias generan, cómo se verifican, qué dependencias existen y cómo se mantienen**. En sistemas externalizados o cloud, esta tarea exige además identificar qué medidas corresponden a la entidad titular, cuáles al proveedor, cuáles son compartidas y cómo se acreditará su cumplimiento.

Desde una **perspectiva de mercado**, **la selección de medidas aporta previsibilidad**. Los proveedores tecnológicos pueden conocer qué exigencias deberán cumplir según el tipo de sistema y servicio. Las Administraciones pueden exigir evidencias concretas. Los auditores pueden verificar con criterios homogéneos. Las entidades certificadoras

pueden evaluar de forma trazable. Esta previsibilidad convierte al ENS en un instrumento de profesionalización del mercado público digital.

4.5. MARCO ORGANIZATIVO, MARCO OPERACIONAL Y MEDIDAS DE PROTECCIÓN

El Anexo II estructura las medidas de seguridad en **tres grandes grupos: marco organizativo, marco operacional y medidas de protección.** Esta división es uno de los elementos que mejor expresa la madurez del modelo ENS, porque evita reducir la seguridad a herramientas tecnológicas y la concibe como un conjunto integrado de gobierno, operación y protección de activos.

El **marco organizativo** está constituido por las **medidas relacionadas con la organización global de la seguridad. Incluye la política de seguridad, la normativa de seguridad interna, los procedimientos y los mecanismos que permiten integrar la seguridad en la estructura de la entidad.** Su función es asegurar que existe un gobierno formal de la seguridad, un marco de gestión formal con reglas, responsabilidades y criterios aprobados. Sin marco organizativo, las medidas técnicas tienden a ser fragmentarias, dependientes de equipos concretos y difíciles de sostener en el tiempo.

El **marco operacional** agrupa las **medidas destinadas a proteger la operación del sistema como conjunto integral de componentes orientados a una finalidad**. Definen el modelo de gestión de la seguridad de la información en su actividad normal. Abarca aspectos relacionados con la planificación, el control de accesos, la explotación, la monitorización, la gestión de cambios, la continuidad, la protección frente a código dañino, la gestión de incidentes y otras actividades necesarias para que el sistema funcione de forma segura. Su finalidad es incorporar la seguridad a la operación diaria.

Las **medidas de protección se centran en activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas**. Pueden referirse a instalaciones, personal, equipos, comunicaciones, soportes de información, aplicaciones, servicios externos, información o elementos criptográficos. Su función es proteger los activos sobre los que descansan la información y los servicios, de manera que, partiendo de los servicios e información como activos esenciales, obtengamos una cobertura integral de los elementos básicos de un sistema de información.

Esta triple estructura permite explicar el ENS de manera clara a públicos no especializados. **La seguridad requiere organización, operación y protección**.

1. La **organización** define el **gobierno, la dirección, políticas y objetivos.**
2. La **operación** asegura que **el sistema funcione de forma controlada**.
3. La **protección actúa sobre activos concretos**.

Esta división ayuda a transmitir que **el ENS es un modelo integral y no un inventario de controles inconexos o aleatorios.**



Figura 4.3 Estructura de responsabilidad ENS

También tiene valor desde el punto de vista de la auditoría y certificación. Al igual que ocurre con otros estándares de seguridad de la información, permite ordenar las evidencias, clasificar hallazgos, identificar debilidades y analizar si las deficiencias son de gobierno, de operación o de protección técnica. Una entidad puede tener buenas medidas técnicas pero una gobernanza deficiente; o una política de seguridad correcta pero una operación mal controlada. La estructura del Anexo II permite detectar esas diferencias y tratarlas adecuadamente.

El ENS ofrece una visión completa de la seguridad pública digital: gobierno de la seguridad, operación segura y protección efectiva de activos. Esta combinación lo hace comprensible, evaluable y replicable.

4.6. DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad es una pieza documental central del ciclo de cumplimiento del ENS. El artículo 28 del Real Decreto 311/2022 establece que la **relación de medidas de seguridad seleccionadas** debe formalizarse en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad. Este documento permite dejar constancia de qué medidas son aplicables, qué refuerzos proceden, qué medidas compensatorias se han adoptado y cómo se justifica la correspondencia entre los riesgos identificados y los controles implantados.

Su función no es meramente administrativa. **La Declaración de Aplicabilidad es el puente entre la categorización, el análisis de riesgos, la selección de medidas y la auditoría. Permite demostrar que la entidad ha seguido un proceso razonado para determinar qué medidas debe aplicar**. Sin una Declaración de Aplicabilidad clara y bien fundamentada, resulta difícil verificar la coherencia del sistema de seguridad.

La Declaración de Aplicabilidad debe ser específica del sistema. No debería limitarse a reproducir el Anexo II ni a marcar casillas de cumplimiento de forma genérica. Debe reflejar la realidad del sistema, sus activos, dimensiones relevantes, categoría, medidas seleccionadas, refuerzos aplicables, medidas no aplicables, justificaciones, medidas compensatorias y evidencias. En este sentido, es uno de los documentos que mejor permite distinguir entre cumplimiento formal y cumplimiento efectivo.

En entornos externalizados, la Declaración de Aplicabilidad adquiere una relevancia adicional. Cuando un servicio depende de proveedores, subcontratistas, infraestructuras cloud o servicios gestionados, debe quedar claro qué medidas son responsabilidad de la entidad titular, cuáles corresponden al proveedor, cuáles son compartidas y qué evidencias permiten demostrar su cumplimiento. La Declaración de Aplicabilidad puede convertirse, así, en una **herramienta de gobierno de la cadena de suministro**. En la gestión de servicios externalizados, el control de la cadena de suministro se instrumentaliza mediante dos figuras operativas: el **Punto de Contacto (POC)** de seguridad del proveedor, encargado de canalizar incidentes y evidencias, y la exigencia de que los subcontratistas críticos también acrediten su conformidad. La Declaración de Aplicabilidad debe delimitar con precisión qué medidas son responsabilidad de la entidad pública cliente, cuáles del proveedor privado y cuáles son compartidas, sirviendo así como una **herramienta de gobierno de la cadena de suministro.**

Desde la **perspectiva de certificación**, la Declaración de Aplicabilidad es esencial. **El auditor necesita conocer el alcance del sistema, las medidas aplicables y la justificación de las decisiones adoptadas**. La entidad certificadora debe poder evaluar si la selección es coherente y si las evidencias sostienen el grado de cumplimiento declarado. Por ello, la Declaración de Aplicabilidad es una pieza clave para transformar la seguridad en confianza verificable.

Desde la **perspectiva institucional,** este instrumento permite presentar el ENS como un marco serio y trazable. **No basta con afirmar que se cumplen medidas; hay que documentar cuáles, por qué, con qué alcance, con qué refuerzos, con qué compensaciones y bajo qué responsabilidad**. Esta trazabilidad es uno de los elementos que aportan credibilidad al modelo español.

4.7. DIAGNÓSTICO, ADECUACIÓN, AUDITORÍA Y MANTENIMIENTO DE LA CONFORMIDAD

El cumplimiento del ENS debe entenderse como un **ciclo**: comienza con un **diagnóstico inicial**, continúa con la **planificación** y **ejecución** de la adecuación, se **verifica** mediante autoevaluación o auditoría, se **formaliza** mediante la Declaración o la Certificación de Conformidad y se **mantiene** mediante seguimiento, revisión y mejora continua. Esta secuencia permite que la seguridad no sea un acto puntual, sino una función permanente.

El **diagnóstico inicial** permite conocer la situación de partida. Debe **identificar sistemas, servicios, información tratada, activos, responsables, dependencias, proveedores, documentación existente, medidas implantadas, carencias, riesgos y**

nivel de madurez. Sin diagnóstico, la adecuación corre el riesgo de convertirse en una acumulación desordenada de actuaciones. Con diagnóstico, la entidad puede priorizar, planificar y asignar recursos.

La **adecuación** consiste en **implantar las medidas necesarias para alcanzar el nivel de cumplimiento exigible**. Incluye actuaciones jurídicas, organizativas, técnicas y documentales: aprobar o actualizar la política de seguridad, asignar roles, categorizar sistemas, realizar análisis de riesgos, seleccionar medidas, elaborar procedimientos, implantar controles, formar al personal, gestionar contratos, establecer mecanismos de monitorización, preparar evidencias y documentar decisiones.

La **auditoría** permite **verificar el grado de cumplimiento y detectar no conformidades.** El artículo 31 del Real Decreto 311/2022 prevé una auditoría regular ordinaria al menos cada dos años para verificar el cumplimiento de los requerimientos del ENS, así como auditoría extraordinaria cuando se produzcan modificaciones sustanciales que puedan repercutir en las medidas de seguridad requeridas. La auditoría se realiza en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico aplicable.

El **mantenimiento** de la conformidad no solo implica una revisión cada dos años. El marco jurídico impone la realización de una **auditoría extraordinaria** siempre que se produzcan **modificaciones sustanciales** en los sistemas de información que puedan repercutir en las medidas de seguridad requeridas. Este mecanismo asegura que el ENS sea un sistema dinámico que reacciona ante cambios en la arquitectura tecnológica o en el modelo de prestación de servicios, evitando la obsolescencia de la seguridad en entornos de cambio constante.

La **conformidad** puede formalizarse mediante **Declaración o Certificación**, según la categoría del sistema. Los sistemas de categoría Básica requieren autoevaluación para su Declaración de Conformidad, mientras que los sistemas de categoría Media o Alta precisan auditoría para la Certificación de Conformidad. Esta diferenciación conecta nuevamente proporcionalidad y confianza: a mayor impacto, mayor intensidad de verificación.

El **mantenimiento de la conformidad** es tan importante como la obtención inicial. Los sistemas cambian, los riesgos evolucionan y las medidas pueden perder eficacia. Por ello, la entidad debe **mantener controles, revisar documentación, gestionar cambios, tratar no conformidades, actualizar evidencias, formar al personal y reevaluar el sistema cuando proceda**. La conformidad ENS no debe entenderse como un certificado colgado en una web, sino como una disciplina sostenida de gestión.

La culminación del ciclo de cumplimiento es la obtención y exhibición del **Distintivo de Conformidad con el ENS** (ya sea mediante Declaración para sistemas de categoría Básica o Certificación para sistemas de categoría Media o Alta). Este distintivo es un documento electrónico firmado que debe ser **publicado obligatoriamente en la sede electrónica o portal de internet** de la entidad responsable. Esta visibilidad pública transforma el cumplimiento interno en un activo de confianza ciudadana, permitiendo verificar la solvencia de seguridad del sistema de forma inmediata.

El modelo español ofrece una ruta clara desde la situación inicial hasta la confianza verificable.

Diagnosticar → Categorizar → Adecuar → Auditar → Certificar → Mantener.



Figura 4.4 Ciclo de adecuación al ENS

4.8. EL ENS COMO CICLO DE GESTIÓN DE RIESGOS Y MEJORA CONTINUA

El ENS se basa en una idea fundamental: **la seguridad debe gestionarse como un proceso continuo de reducción del riesgo.** No se trata de eliminar todo riesgo, lo que resultaría imposible, sino de identificarlo, valorarlo, tratarlo, reducirlo a niveles aceptables, monitorizarlo y revisarlo periódicamente. **Esta lógica conecta el ENS con los marcos internacionales de gestión de riesgos y con la evolución del Derecho europeo de la ciberseguridad**, cada vez más orientado a la diligencia demostrable, la resiliencia y la responsabilidad de las entidades.

El ciclo de gestión de riesgos comienza con el conocimiento del sistema. La entidad debe saber qué servicios presta, qué información trata, qué activos utiliza, qué dependencias existen, qué proveedores intervienen y qué impacto tendría un incidente. **Sobre esa base se categorizan los sistemas, se identifican amenazas y vulnerabilidades, se valoran impactos y se seleccionan medidas.**

La mejora continua implica que este proceso no finaliza con la implantación inicial. La aparición de nuevas amenazas, la modificación de servicios, la incorporación de nuevas tecnologías, la externalización de funciones, la migración a la nube, la adopción de inteligencia artificial, la dependencia de terceros o la aparición de vulnerabilidades críticas pueden alterar sustancialmente el riesgo. El ENS debe ser capaz de absorber esos cambios y ajustar el modelo de seguridad a dichos cambios y ante nuevos escenarios o requisitos normativos.

Asimismo, en un escenario de amenazas cambiantes, la gestión del riesgo obligará a una revisión cuasi permanente, de manera que se adecúen las medidas de seguridad implementadas a la mitigación o tratamiento de dichos riesgos o bien a establecer los canales y medios necesarios para un adecuado tratamiento, conectándolo con la planificación económica y presupuestaria del organismo y al tiempo, a la toma de decisiones por parte de los órganos de gobierno.

La auditoría, la gestión de incidentes, el informe del estado de seguridad y la certificación son mecanismos que alimentan la mejora continua. Cada auditoría identifica hallazgos; cada incidente aporta lecciones; cada informe permite medir evolución; cada renovación de conformidad obliga a comprobar si el sistema sigue siendo adecuado. Por ello, el ENS no debe interpretarse como un conjunto de requisitos estáticos, sino como un ciclo de aprendizaje institucional.

Esta característica refuerza la posición del ENS como **modelo exportable**. Los Estados y organizaciones no necesitan únicamente catálogos de controles; necesitan sistemas que permitan gestionar la seguridad en el tiempo. El ENS aporta ese enfoque: **una estructura que combina categorización, medidas, evidencias, auditoría, certificación y revisión permanente**. Su valor no está sólo en definir qué controles aplicar, sino en ordenar el proceso por el que una entidad mantiene su seguridad de forma verificable.

Desde el punto de vista del **mensaje estratégico**, el ENS permite afirmar que:

> **España dispone de un modelo que convierte la ciberseguridad pública en gestión de riesgos, cumplimiento verificable y mejora continua.**

Esa combinación es especialmente atractiva para el entorno europeo, donde la confianza digital exige cada vez más capacidad de demostrar diligencia, madurez y resiliencia.

La implantación del ENS responde a un itinerario metodológico en el que cada fase exige dar respuesta a preguntas clave y genera un entregable o instrumento específico (véase la Figura 4.5):

Fase	Pregunta que debe responder la entidad	Instrumento ENS	Resultado esperado	Valor estratégico
Identificación del sistema	¿Qué información y servicios deben protegerse?	Inventario, delimitación de alcance, identificación de activos	Conocimiento del perímetro real	Evita seguridad fragmentada o incompleta
Valoración de impacto	¿Qué ocurriría si se afectara cada dimensión de seguridad?	Dimensiones C, I, D, A y T del Anexo I	Nivel de impacto por dimensión	Conecta seguridad con servicios, derechos y continuidad
Determinación de categoría	¿El sistema es básico, medio o alto?	Artículo 40 y Anexo I	Categoría de seguridad	Proporcionalidad y asignación racional de recursos

Fase	Pregunta que debe responder la entidad	Instrumento ENS	Resultado esperado	Valor estratégico
Selección de medidas	¿Qué controles deben implantarse?	Anexo II y artículo 28	Medidas y refuerzos aplicables	Seguridad concreta y operativa
Declaración de Aplicabilidad	¿Cómo se documenta lo aplicable y lo justificado?	Declaración de Aplicabilidad	Trazabilidad de decisiones	Base de auditoría y certificación
Adecuación	¿Qué debe implantarse o corregirse?	Plan de adecuación y tratamiento de riesgos	Cumplimiento efectivo	Paso de la norma a la realidad operativa
Verificación	¿Puede demostrarse el cumplimiento?	Autoevaluación, auditoría, declaración o certificación	Evidencia de conformidad	Confianza verificable ante terceros
Mantenimiento	¿Sigue siendo válido el nivel de seguridad?	Seguimiento, revisión, auditoría periódica y mejora continua	Conformidad sostenida	Modelo vivo y resiliente

Figura 4.5 Fases operativas del ciclo de cumplimiento y su instrumento correspondiente

La **verificación independiente** constituye la última etapa del ciclo de cumplimiento y el elemento que aporta validez pública al sistema. La siguiente ilustración sintetiza el proceso final de auditoría y certificación conforme al Real Decreto 311/2022, detallando los hitos necesarios para transformar las evidencias de seguridad en una Declaración o Certificación de Conformidad reconocible por el mercado y las Administraciones Públicas.



Figura 4.6. El ciclo del ENS de cumplimiento verificable

4.9. RESUMIENDO…

La categorización, las medidas de seguridad y el ciclo de cumplimiento constituyen el corazón operativo del ENS. La categorización permite graduar la exigencia según el impacto; las dimensiones de seguridad aseguran una valoración completa de la información y de los servicios; las categorías Básica, Media y Alta permiten ordenar la proporcionalidad; el Anexo II traduce esa valoración en medidas concretas; la Declaración de Aplicabilidad documenta las decisiones adoptadas; y el ciclo de diagnóstico, adecuación, auditoría y mantenimiento convierte el cumplimiento en una disciplina permanente.

El ENS no se limita a imponer obligaciones ni a recomendar buenas prácticas. Proporciona una metodología completa para identificar lo que debe protegerse, determinar cuánto debe protegerse, seleccionar cómo debe protegerse, demostrar que se protege y mantener esa protección en el tiempo.

Esa combinación de rigor jurídico, operatividad técnica, gobernanza organizativa y confianza verificable es lo que permite presentar el ENS como una referencia avanzada de ciberseguridad pública en España y en Europa.

5. LAS INSTRUCCIONES TÉCNICAS DE SEGURIDAD DEL ENS

Las **Instrucciones Técnicas de Seguridad** (en adelante, **ITS**) constituyen una pieza esencial del Esquema Nacional de Seguridad. **Su función es desarrollar, concretar y hacer operativos determinados aspectos del ENS que resultan especialmente relevantes para garantizar una aplicación homogénea, verificable y jurídicamente segura del modelo**. Si el Real Decreto 311/2022, de 3 de mayo, proporciona la arquitectura normativa principal, **las ITS actúan como normas técnicas de desarrollo que permiten convertir esa arquitectura en procedimientos, criterios, obligaciones documentales, mecanismos de evidencia y pautas de actuación común.** Se trata, en términos generales, de herramientas de trabajo que desarrollan, de una manera pormenorizada, aspectos contemplados en el ENS.

Su importancia práctica es considerable. El ENS no puede funcionar adecuadamente si cada entidad interpreta de forma aislada cómo debe declarar la conformidad, cómo debe someterse a auditoría, cómo debe notificar incidentes o cómo debe informar sobre su estado de seguridad**.**

> **Las ITS reducen esa dispersión interpretativa, facilitan la comparabilidad, orientan a las entidades obligadas, proporcionan criterios a auditores y entidades de certificación, y permiten que el modelo ENS opere como un sistema común de confianza y no como una suma de prácticas heterogéneas**

Además, se caracterizan por una mayor flexibilidad en cuanto a su producción, de manera que se dota a todo el marco impulsado por el ENS de una mayor eficacia y capacidad de respuesta al cambio, así como a la incorporación de criterios prácticos.

Desde el **punto de vista jurídico**, **las ITS refuerzan la seguridad normativa del ENS**. No sustituyen al Real Decreto 311/2022, ni pueden alterar su contenido, pero sí **concretan aspectos necesarios para su aplicación efectiva**. Esta función de desarrollo resulta especialmente importante en un marco como el ENS, que combina obligaciones jurídicas, medidas técnicas, criterios organizativos, procedimientos de evaluación, gestión de riesgos, auditoría, certificación y mejora continua. Las ITS permiten que esa combinación sea aplicable en la práctica con criterios comunes.

Desde el **punto de vista organizativo**, **las ITS ayudan a las entidades a transformar obligaciones generales en actuaciones concretas**. Una entidad puede conocer, mediante las ITS, cómo debe publicar su conformidad, qué condiciones debe cumplir una auditoría, cuándo y cómo debe notificar determinados incidentes, o qué información debe recopilar y comunicar para contribuir al conocimiento del estado de la seguridad. De este modo, **las ITS conectan la gobernanza interna de la seguridad con las exigencias externas de transparencia, verificación, coordinación y medición.**

Desde una **perspectiva institucional**, **las ITS son uno de los elementos que permiten presentar el ENS como un modelo maduro**. Muchos marcos de ciberseguridad contienen principios, controles o recomendaciones; el ENS, además, dispone de instrucciones técnicas obligatorias que ordenan cuestiones críticas para su funcionamiento. Esa existencia de un segundo nivel normativo-operativo aumenta la credibilidad del modelo español y facilita su explicación a otros países: el ENS no sólo define lo que debe cumplirse, sino también cómo se debe evidenciar, auditar, comunicar y medir.

5.1. NATURALEZA, FUNCIÓN Y VALOR DE LAS ITS

Las Instrucciones Técnicas de Seguridad son instrumentos de desarrollo del ENS destinados a regular materias concretas en las que resulta necesaria una aplicación común. Su naturaleza debe entenderse en relación directa con el Real Decreto 311/2022. La disposición adicional segunda de dicho Real Decreto prevé que, en desarrollo del ENS, se aprueben instrucciones técnicas de seguridad de obligado cumplimiento mediante resolución de la Secretaría de Estado competente, a propuesta de la Comisión Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional. Además, la misma disposición prevé que el CCN elabore y difunda las guías CCN-STIC, particularmente las correspondientes a la serie 800, para facilitar el mejor cumplimiento del Real Decreto.

Esta previsión normativa confirma que **el ENS está diseñado como un sistema articulado por niveles.**

- En el **primer nivel** se sitúa el **Real Decreto 311/2022**, que establece el marco general.
- En un **segundo nivel se encuentran las ITS**, que concretan aspectos específicos de aplicación obligatoria.
- En un **tercer nivel** se sitúan las **guías CCN-STIC**, que orientan la implantación, interpretación, auditoría y maduración práctica del modelo. Esta estructura

dota al ENS de una combinación especialmente valiosa de estabilidad normativa y flexibilidad técnica, incorporando los elementos técnicos necesarios para alinear la realidad de los sistemas de información con los requisitos normativos.

Las ITS tienen, por tanto, una función de homogeneización.

En un Estado compuesto y descentralizado, con múltiples Administraciones Públicas, entidades del sector público, organismos, universidades, sociedades públicas, fundaciones, proveedores privados, auditores y entidades certificadoras, resulta imprescindible que determinadas cuestiones críticas se apliquen con criterios comunes.

La conformidad, la auditoría, la notificación de incidentes y el informe del estado de seguridad no pueden depender de interpretaciones locales o prácticas informales. Requieren procedimientos comunes que permitan comparar, verificar y confiar.

Las ITS tienen también una función de trazabilidad. Permiten documentar actuaciones, fijar evidencias, identificar responsabilidades y justificar decisiones. Esto resulta esencial para la auditoría y certificación de conformidad, pero también para la rendición de cuentas, la supervisión, la contratación pública y la gestión de incidentes. En términos prácticos, las ITS convierten el cumplimiento ENS en un conjunto de actuaciones demostrables.

Desde la **perspectiva institucional, las ITS son una prueba de madurez regulatoria**. Un modelo de ciberseguridad pública resulta más creíble cuando no se limita a formular exigencias generales, sino que dispone de instrumentos técnicos obligatorios para concretar cómo se acredita la conformidad, cómo se audita, cómo se notifican incidentes y cómo se mide el estado de seguridad. Este es uno de los mensajes que destacan la proyección internacional del ENS:

España ha construido un modelo que no sólo exige seguridad, sino que proporciona reglas para verificarla, coordinarla y medirla.

Debe tenerse presente que las ITS actualmente vigentes fueron aprobadas bajo el marco del anterior Real Decreto 3/2010, de 8 de enero. Sin embargo, siguen desempeñando una función práctica relevante en el ecosistema ENS y deben interpretarse hoy de forma coherente con el Real Decreto 311/2022. Esta precisión es importante para evitar confusiones: las ITS forman parte del cuerpo operativo del ENS, pero su lectura debe actualizarse sistemáticamente conforme al marco vigente y a las guías, criterios y prácticas que hayan ido consolidándose bajo el Real Decreto 311/2022.

Conviene señalar que **el ecosistema de las ITS es dinámico y está llamado a completarse bajo el marco del Real Decreto 311/2022**. El propio texto prevé o presupone el desarrollo de instrucciones técnicas específicas para materias de alta sensibilidad operativa: la ITS de Interconexión de Sistemas de Información, llamada a regular los requisitos de seguridad en los puntos de unión entre dominios; la ITS del Esquema de Certificación de Responsables de Seguridad, vinculada a las condiciones de profesionalidad y requisitos exigibles para esta figura clave; y la ITS de Criptología de Empleo en el ENS, que deberá concretar los aspectos necesarios para el uso de

mecanismos criptográficos, incluyendo la transición hacia capacidades postcuánticas cuando proceda. Estas adiciones reforzarán el ciclo de confianza y reducirán el riesgo de interpretaciones heterogéneas.

5.2. ITS DE CONFORMIDAD CON EL ENS

La Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad fue aprobada por Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas. **Su objeto es establecer los procedimientos para dar publicidad a la conformidad con el ENS, así como los requisitos exigibles a las entidades certificadoras**. Esta ITS es una de las piezas más importantes del modelo, porque conecta el cumplimiento interno de una entidad con su reconocimiento externo.

Su finalidad principal es **ordenar cómo se acredita y publica la conformidad con el ENS**. Esta cuestión es esencial para un modelo que pretende generar confianza. No basta con que una entidad afirme que cumple el ENS; debe existir un procedimiento reconocible, unos documentos mínimos, unos distintivos de conformidad y unas reglas sobre quién puede declarar o certificar el cumplimiento. La ITS de Conformidad cumple precisamente esa función: convertir la adecuación al ENS en una evidencia formalmente comunicable.

La ITS distingue entre la **Declaración de Conformidad** y la **Certificación de Conformidad**. La Declaración de Conformidad se aplica a sistemas de categoría Básica y es expedida por la propia entidad bajo cuya responsabilidad se encuentren dichos sistemas. La Certificación de Conformidad se aplica a sistemas de categoría Media o Alta y debe ser expedida por una entidad certificadora. Esta diferenciación refleja la lógica general del ENS: a mayor categoría del sistema, mayor exigencia de verificación externa.

La **Declaración de Conformidad** cumple una función relevante **en sistemas de menor impacto**. Permite que la entidad asuma formalmente la responsabilidad de su adecuación al ENS, previa autoevaluación, y publique dicha conformidad mediante el correspondiente distintivo. Aunque no incorpora la misma intensidad de verificación que la certificación, sí introduce un mecanismo de transparencia y responsabilidad. **La entidad no se limita a cumplir internamente, sino que hace pública su conformidad y se compromete frente a terceros** en cuanto al mantenimiento y gestión de las medidas de seguridad indicadas**.**

La **Certificación de Conformidad**, por su parte, tiene una especial relevancia para sistemas de categoría Media y Alta**. Su expedición por una entidad certificadora introduce una capa de confianza externa**.

> **La Certificación de Conformidad con el ENS acredita que un sistema ha sido auditado y encontrado conforme con las exigencias del ENS aplicables a su categoría**.
> Este elemento es crucial para la contratación pública, para la relación con proveedores, para la rendición de cuentas interna y para la proyección internacional del modelo.

La ITS de Conformidad regula también los Distintivos de Conformidad y su publicidad. Estos distintivos tienen una función comunicativa muy importante. Permiten identificar visualmente que una entidad, sistema o servicio ha alcanzado determinado nivel de conformidad con el ENS. En términos de marketing institucional, el distintivo es una pieza de marca pública: transmite confianza, madurez y sujeción a un marco común de seguridad.

La ITS establece, además, requisitos para las entidades certificadoras. Entre ellos destaca la **exigencia de acreditación por la Entidad Nacional de Acreditación (ENAC)** conforme a la norma UNE-EN ISO/IEC 17065, relativa a organismos que certifican productos, procesos y servicios. Esta conexión con normas internacionales de evaluación de la conformidad refuerza la credibilidad del sistema ENS y permite explicarlo mejor ante interlocutores europeos e internacionales. La certificación ENS no se presenta como una mera declaración administrativa, sino como una certificación inserta en una arquitectura de acreditación, competencia técnica e imparcialidad con un nivel de exigencia comparable al utilizado en otros ámbitos internacionales de certificación y acreditación.

Especial importancia tiene también la **aplicación de esta ITS a soluciones y servicios prestados por operadores privados**. Cuando los operadores del sector privado prestan servicios o proveen soluciones a entidades públicas y resulte exigible el cumplimiento del ENS, deben estar en condiciones de exhibir la correspondiente Declaración o Certificación de Conformidad, según la categoría del sistema. Esta previsión proyecta el ENS sobre la cadena de suministro y lo convierte en un instrumento de disciplina del mercado público digital.

Desde una perspectiva estratégica, la ITS de Conformidad muestra que el modelo español no se queda en la imposición de obligaciones, sino que permite acreditar cumplimiento mediante mecanismos visibles, verificables y respaldados por entidades certificadoras acreditadas. En un entorno europeo en el que la certificación de ciberseguridad adquiere una importancia creciente, esta característica del modelo español es especialmente valiosa y aporta una experiencia acreditada y probada a través de la cantidad de entidades tanto públicas como privadas que han accedido a la certificación de conformidad.

5.3. ITS DE AUDITORÍA DE LA SEGURIDAD

La Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información fue aprobada por Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública. Su objeto es establecer las condiciones para la realización de las auditorías ordinarias o extraordinarias previstas en el ENS. Esta ITS constituye una pieza esencial del sistema de verificación, porque define cómo debe comprobarse el cumplimiento de los requisitos y medidas de seguridad.

La auditoría es el mecanismo que permite pasar del cumplimiento declarado al cumplimiento comprobado. En el ENS, la seguridad no puede quedar reducida a una documentación interna, a una autoevaluación superficial o a una implantación técnica no contrastada. **La auditoría permite evaluar si la categorización del sistema es**

correcta, si el análisis de riesgos se ha realizado adecuadamente, si las medidas de seguridad aplicables se han implantado, si existen evidencias suficientes, si la política de seguridad y los procedimientos son operativos y si el sistema mantiene un grado de cumplimiento coherente con su categoría.

La ITS de Auditoría regula aspectos esenciales como el propósito de la auditoría, su obligatoriedad, la definición de alcance y objetivos, la ejecución de los trabajos, el contenido del informe de auditoría y la intervención de entidades auditoras. **Su utilidad práctica consiste en proporcionar un marco común para que las auditorías se realicen con criterios homogéneos, evitando que cada auditor o entidad interprete de manera diferente el alcance del examen, la naturaleza de las evidencias o la forma de documentar los resultados.**

La **definición del alcance** es uno de los aspectos más relevantes. Una auditoría ENS debe referirse a sistemas de información determinados, con una categoría concreta, unos servicios identificados, unas medidas aplicables y un conjunto de evidencias asociado. Si el alcance no está bien definido, la auditoría pierde valor. Puede generar una apariencia de conformidad sin que quede claro qué sistema ha sido evaluado, qué servicios cubre, qué medidas se han comprobado y qué riesgos quedan fuera.

El **informe de auditoría** es otro elemento central. Debe recoger de manera ordenada los trabajos realizados, los hallazgos identificados, las no conformidades detectadas, las evidencias examinadas y las conclusiones alcanzadas. Su importancia va más allá del procedimiento de certificación. El informe de auditoría es una herramienta de dirección y mejora. Permite a la entidad conocer sus debilidades, priorizar correcciones, justificar inversiones, reforzar controles y mantener la conformidad en el tiempo.

Desde el **punto de vista organizativo**, **la auditoría ENS favorece la rendición de cuentas.** Obliga a que las decisiones de seguridad se documenten y puedan ser revisadas por terceros. También incentiva la coordinación entre áreas técnicas, jurídicas, responsables de servicio, responsables de información, responsables de seguridad, responsables del sistema y órganos de dirección. La auditoría no evalúa sólo tecnología; evalúa también gobernanza, procesos, responsabilidades, evidencias y continuidad.

La ITS de Auditoría tiene un valor especialmente importante para el modelo de certificación. La certificación de conformidad de sistemas de categoría Media o Alta se apoya necesariamente en una auditoría que permita comprobar el cumplimiento. Por tanto, esta ITS es una de las bases sobre las que descansa la confianza en los certificados ENS. Sin una auditoría rigurosa, homogénea y documentada, la certificación perdería credibilidad.

Desde la **perspectiva de proyección exterior**, **la ITS de Auditoría demuestra que el ENS dispone de un mecanismo formal de control**. Este aspecto diferencia al modelo español de marcos que se limitan a establecer buenas prácticas o controles recomendados. El ENS no sólo exige medidas; exige verificar su implantación y conservar evidencias. Este elemento refuerza su valor como modelo nacional de confianza digital susceptible de ser explicado y defendido en Europa y ante terceros

países. En este proceso de verificación, la ITS de Auditoría adquiere una dimensión métrica fundamental al conectarse con el **Modelo de Madurez de Capacidad (CMMI)**. El dictamen del auditor no debe limitarse a validar la existencia técnica de una medida, sino que debe certificar que esta alcanza el **nivel de madurez mínimo exigido** por el Real Decreto según la categoría del sistema: **L2 para categoría Básica, L3 para Media y L4 para Alta**. Esta exigencia transforma la auditoría en una prueba de institucionalización y eficacia real de los procesos, impidiendo que una implantación puramente nominal o documental sea suficiente para obtener la certificación.

5.4. ITS DE NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD

La Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad fue aprobada por Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública. Su objeto es regular la notificación y gestión de incidentes de seguridad en los sistemas de información de las entidades del sector público comprendidas en el ámbito del ENS, cuando dichos incidentes tengan un impacto significativo en la seguridad de la información que manejan o en los servicios que prestan.

Esta ITS responde a una realidad básica de la ciberseguridad contemporánea: **los incidentes son inevitables. Un modelo maduro no puede limitarse a prevenir, sino que debe establecer procedimientos de detección, clasificación, comunicación, gestión, conservación de evidencias, coordinación y aprendizaje**. La notificación de incidentes no debe percibirse como una carga formal, sino como una herramienta de resiliencia institucional.

La ITS regula criterios de determinación del nivel de impacto, notificación obligatoria de incidentes con determinados niveles de impacto, evidencias a entregar, remisión de estadísticas, notificación de impactos recibidos, desarrollo de herramientas automatizadas y régimen legal de las comunicaciones. Esta estructura muestra que la gestión de incidentes en el ENS tiene una dimensión individual y una dimensión colectiva. Individual, porque cada entidad debe gestionar adecuadamente sus propios incidentes. Colectiva, porque la notificación permite generar conocimiento agregado, coordinar respuestas y mejorar el nivel de seguridad del conjunto del sector público.

La clasificación del impacto es esencial. No todos los incidentes tienen la misma gravedad ni exigen la misma respuesta. La ITS permite ordenar la reacción según el nivel de impacto, evitando tanto la banalización de incidentes graves como la saturación del sistema con comunicaciones irrelevantes. Esta proporcionalidad resulta coherente con la lógica general del ENS: las obligaciones deben ajustarse a la importancia del sistema, de la información y del servicio afectado.

La **obligación de aportar evidencias en incidentes de mayor impacto** tiene un valor técnico y jurídico significativo. Las evidencias permiten reconstruir lo ocurrido, identificar causas, valorar daños, determinar responsabilidades, activar medidas de contención, informar adecuadamente a los órganos competentes y aprender para el futuro. Sin evidencias, la gestión del incidente se debilita y se reduce la capacidad de respuesta institucional.

La **remisión de estadísticas de incidentes** también tiene una finalidad estratégica. Permite conocer tendencias, tipologías de ataque, vulnerabilidades recurrentes, sectores más afectados, niveles de exposición y evolución de la amenaza. Esta información es esencial para orientar políticas públicas de ciberseguridad, actualizar guías, priorizar recursos y reforzar capacidades. En este sentido, la ITS convierte la notificación de incidentes en un mecanismo de inteligencia colectiva.

Desde el punto de vista organizativo, la ITS de Notificación obliga a las entidades a disponer de procedimientos internos claros. Deben saber quién detecta, quién clasifica, quién comunica, quién conserva evidencias, quién coordina la respuesta, quién toma decisiones y quién informa a los órganos competentes. La improvisación durante un incidente es una fuente adicional de riesgo. Por ello, la notificación ENS debe integrarse en los planes de gestión de incidentes, continuidad, comunicación, protección de datos y relación con proveedores.

Esta ITS tiene una **importancia especial en entornos externalizados y de cadena de suministro.** Cuando un proveedor presta servicios a una entidad pública o gestiona sistemas vinculados al ENS, la detección y comunicación de incidentes no puede depender de cláusulas genéricas o de la buena voluntad contractual. Deben existir obligaciones claras de comunicación, tiempos de respuesta, conservación de evidencias, cooperación y escalado. La ITS de Notificación permite reforzar esa dimensión contractual y operativa.

Desde la **perspectiva institucional**, **la ITS de Notificación permite presentar el ENS como un modelo de resiliencia, no de mera prevención**. Esta es una idea especialmente atractiva y realista: ningún sistema puede garantizar la ausencia absoluta de incidentes, pero un marco maduro puede exigir que los incidentes se detecten, se comuniquen, se gestionen y se utilicen para mejorar. El ENS aporta esa lógica de resiliencia coordinada.

Por otra parte, el modelo del ENS integra ya una dilatada experiencia en la gestión de incidentes de seguridad y en el establecimiento de un modelo de notificación y seguimiento, de modo que se adelanta a los modelos propuestos por las recientes novedades legislativas como la Directiva NIS 2, estableciendo un mecanismo fácilmente asimilable a dicha normativa.

5.5. ITS DE INFORME DEL ESTADO DE LA SEGURIDAD

La Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad fue aprobada por Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas. Su objeto es establecer las condiciones relativas a la recopilación y comunicación de datos que permitan conocer las principales variables de la seguridad de la información de los sistemas comprendidos en el ámbito del ENS y confeccionar un perfil general del estado de la ciberseguridad en las Administraciones Públicas.

Esta ITS es especialmente relevante porque introduce una dimensión de medición y conocimiento agregado. La seguridad pública no puede gestionarse adecuadamente si no se conoce su estado real. Las entidades pueden implantar

medidas, realizar auditorías y declarar o certificar conformidad, pero el conjunto del sistema requiere información agregada para valorar madurez, detectar carencias, orientar recursos, identificar tendencias y formular políticas públicas. El Informe del Estado de la Seguridad cumple esa función.

La ITS exige la recopilación y comunicación de datos sobre variables de seguridad. Entre los ámbitos de información que se relacionan con este proceso se encuentran la identificación de la entidad, datos generales, organización de la seguridad, procesos críticos, concienciación y formación, gestión de incidentes, recursos y presupuestos, auditoría, indicadores críticos de riesgo y medidas de seguridad. Este conjunto de variables permite obtener una imagen más completa de la seguridad que la mera existencia de certificados o declaraciones.

La herramienta INES, del Centro Criptológico Nacional, desempeña un papel central en este ámbito. Permite canalizar la comunicación de información por parte de las entidades y facilita la elaboración de una visión agregada del estado de seguridad. Desde el punto de vista práctico, esta herramienta reduce cargas, homogeneiza la información y permite que los datos comunicados puedan tratarse de forma sistemática.

La utilidad del Informe del Estado de la Seguridad no debe valorarse únicamente desde la perspectiva de control. También tiene una función de mejora. Al recopilar información de forma periódica, las entidades se ven obligadas a conocer su propio estado de seguridad, identificar debilidades, comparar evolución y preparar acciones de mejora. El reporte externo incentiva la disciplina interna.

Desde la **perspectiva de política pública**, **esta ITS permite avanzar hacia una ciberseguridad basada en datos**.

> **Un Estado no puede mejorar lo que no mide.**

El ENS incorpora, mediante esta ITS, una herramienta para conocer el grado de implantación, madurez y evolución de la seguridad en el sector público. Esta capacidad es especialmente relevante para orientar programas de apoyo, formación, guías, inversión, supervisión y actualización normativa.

Desde la **perspectiva de proyección internacional**, el Informe del Estado de la Seguridad es uno de los elementos más interesantes del ENS. **Muchos modelos de seguridad se centran en controles, pero pocos integran de forma tan clara una lógica de medición agregada del estado de seguridad**. Esta dimensión permite presentar el ENS como un sistema no sólo normativo y certificable, sino también medible. La combinación de regulación, conformidad, auditoría, incidentes e indicadores refuerza la imagen del ENS como modelo avanzado de gobernanza de la ciberseguridad.

5.6. PAPEL DE LAS ITS EN LA HOMOGENEIZACIÓN DE CRITERIOS

La homogeneización de criterios es una de las principales funciones de las ITS. El ENS se aplica a un conjunto muy amplio de entidades, sistemas, servicios y proveedores. Sin instrucciones técnicas comunes, existiría un riesgo elevado de fragmentación interpretativa: distintas entidades podrían publicar conformidades con

formatos diversos, realizar auditorías con criterios heterogéneos, notificar incidentes de forma desigual o comunicar información de seguridad con variables incompatibles. Las ITS reducen ese riesgo.

La homogeneización es especialmente importante para la confianza. La confianza exige comparabilidad. Una declaración de conformidad, una certificación, una auditoría, una notificación de incidente o un informe de seguridad sólo tienen valor si quienes los reciben pueden entender qué significan, cómo se han elaborado y qué garantías ofrecen. Las ITS aportan ese lenguaje común.

> **ANEXO A.** En materia de **conformidad**, la ITS correspondiente define modelos, distintivos, publicidad y requisitos de entidades certificadoras.
>
> **ANEXO B.** En materia de **auditoría**, la ITS establece condiciones para realizar auditorías ordinarias y extraordinarias.
>
> **ANEXO C.** En materia de **incidentes**, fija criterios de impacto y obligaciones de notificación.
>
> **ANEXO D.** En materia de **informe del estado de seguridad**, ordena la recopilación y comunicación de variables.
>
> Cada una actúa sobre un aspecto distinto, pero todas comparten una misma función: convertir el ENS en un sistema coherente.

Desde el punto de vista de auditores y certificadores, las ITS proporcionan criterios de referencia. Esto no elimina la necesidad de juicio profesional, pero reduce la discrecionalidad injustificada. Facilita que las auditorías sean más consistentes, que las certificaciones tengan mayor credibilidad y que las entidades puedan prepararse con mayor previsibilidad.

Desde el punto de vista de las entidades obligadas, la homogeneización reduce incertidumbre. Una entidad que desea adecuarse al ENS necesita saber qué se espera de ella, qué documentos debe generar, qué evidencias debe conservar, cómo debe publicar su conformidad, cómo debe notificar incidentes y qué información debe comunicar sobre su estado de seguridad. Las ITS proporcionan ese marco operativo.

Desde una perspectiva de mercado, la homogeneización es también una ventaja competitiva. Los proveedores privados pueden comprender las exigencias ENS y adaptar sus servicios. Las entidades públicas pueden incorporar requisitos en pliegos y contratos con mayor claridad. Las entidades certificadoras pueden ofrecer servicios evaluables conforme a criterios comunes. Esta previsibilidad favorece el desarrollo de un ecosistema profesional de ciberseguridad y certificación.

En términos de presencia institucional, la homogeneización permite presentar el ENS como un modelo escalable. Un marco nacional sólo es verdaderamente útil si puede aplicarse de manera coherente en entidades muy diversas. Las ITS ayudan a conseguirlo y permiten que el ENS no dependa únicamente de la interpretación local, sino de criterios comunes definidos en normas técnicas obligatorias.

Junto a ello, conviene distinguir la arquitectura técnica de las ITS de la previsión específica de la disposición adicional tercera del Real Decreto 311/2022. El principio de "no causar un perjuicio significativo" al medioambiente (DNSH) opera respecto de las

actuaciones ejecutadas en el marco del Plan de Recuperación, Transformación y Resiliencia, no como requisito técnico general de las ITS. Por tanto, debe tratarse como una cautela transversal aplicable cuando la actuación de adecuación, implantación o adquisición vinculada al ENS esté financiada o conectada con el PRTR.

5.7. RELACIÓN ENTRE LAS ITS, EL REAL DECRETO 311/2022 Y LAS GUÍAS CCN-STIC

El ENS funciona como un ecosistema documental articulado.

> 2.1 El **Real Decreto 311/2022** establece el marco jurídico general, define el ámbito de aplicación, principios básicos, requisitos mínimos, categorización, medidas de seguridad, auditoría, conformidad y obligaciones esenciales.
>
> 2.2 Las **ITS** desarrollan aspectos concretos de ese marco con carácter obligatorio.
>
> 2.3 Las **guías CCN-STIC**, particularmente las de la serie 800, proporcionan orientación técnica, metodológica y práctica para facilitar la implantación y auditoría del ENS.

Esta relación entre Real Decreto, ITS y guías es una de las fortalezas del modelo. Permite combinar tres necesidades que, en ocasiones, resultan difíciles de equilibrar: **seguridad jurídica, concreción operativa y adaptabilidad técnica**. El Real Decreto ofrece estabilidad normativa. Las ITS proporcionan reglas obligatorias sobre materias críticas. Las guías permiten actualizar criterios, orientar prácticas y acompañar a las entidades en la implantación.

Debe evitarse, sin embargo, una confusión entre estos niveles. El Real Decreto tiene rango reglamentario y constituye la norma principal del ENS. Las ITS son instrucciones técnicas de obligado cumplimiento aprobadas mediante resolución. Las guías CCN-STIC son documentos de apoyo técnico elaborados y difundidos por el CCN, que adquieren una importancia práctica notable, especialmente en procesos de implantación, auditoría y certificación. Esta distinción es relevante para ordenar correctamente el sistema de fuentes y para explicar el modelo a interlocutores jurídicos y técnicos.

La disposición adicional segunda del Real Decreto 311/2022 confirma esta arquitectura. Prevé la aprobación de ITS de obligado cumplimiento y encarga al CCN la elaboración y difusión de guías de seguridad de las tecnologías de la información y la comunicación, particularmente de la serie 800, que se incorporan al conjunto documental utilizado para la realización de auditorías de seguridad. Este último inciso es especialmente relevante: las guías no son meras recomendaciones externas al modelo, sino instrumentos que forman parte del ecosistema práctico de auditoría y cumplimiento.

La relación entre ITS y guías puede explicarse de forma funcional:

- Las ITS determinan ***QUÉ*** debe hacerse en aspectos concretos de aplicación obligatoria.
- Las guías ayudan a entender ***CÓMO*** hacerlo correctamente.

Por ejemplo, la ITS de Conformidad regula procedimientos y distintivos, mientras las guías CCN-STIC pueden ofrecer modelos, criterios y orientaciones para la declaración y certificación. La ITS de Informe del Estado de la Seguridad regula la comunicación de variables, mientras las guías asociadas ayudan a estructurar la información. La ITS de Auditoría fija condiciones de auditoría, mientras las guías facilitan criterios de evaluación. La ITS de Incidentes regula notificación y gestión, mientras las guías orientan la respuesta técnica.

Desde la **perspectiva de posicionamiento internacional**, esta arquitectura documental es un elemento especialmente vendible.

El ENS no se limita a aprobar una norma y dejar a las entidades solas ante su cumplimiento. Proporciona un sistema escalonado de apoyo: norma, instrucciones, guías, herramientas, auditoría y certificación. Esta combinación convierte al modelo español en una referencia práctica, no sólo conceptual.

5.8. VALOR PRÁCTICO DE LAS ITS PARA ENTIDADES OBLIGADAS, AUDITORES Y CERTIFICADORES

Las ITS tienen un valor práctico directo para todos los actores del ecosistema ENS. Para las **entidades obligadas**, proporcionan seguridad sobre cómo cumplir determinadas obligaciones. Para los **auditores**, ofrecen criterios para evaluar. Para las **entidades certificadoras**, permiten construir procesos de certificación coherentes. Para los **órganos de contratación**, facilitan la exigencia de conformidad. Para el **CCN** y el **conjunto del sector público**, permiten recopilar información, coordinar respuestas, homogeneizar prácticas y reforzar la confianza en el modelo.

Para **las entidades públicas**, **las ITS reducen incertidumbres**. Una Administración que debe adecuarse al ENS necesita saber cómo declarar o certificar conformidad, cómo preparar una auditoría, cómo notificar incidentes y cómo informar sobre su estado de seguridad. Las ITS convierten esas obligaciones en procedimientos más concretos y permiten que la entidad planifique recursos, responsabilidades y documentación.

Para las **entidades privadas proveedoras del sector público**, la utilidad es igualmente clara. La ITS de Conformidad permite conocer **cómo deben acreditar su adecuación cuando prestan servicios o proveen soluciones sometidas al ENS**. La ITS de Auditoría condiciona las evidencias que deberán preparar. La ITS de Notificación de Incidentes incide en sus obligaciones contractuales y operativas cuando gestionan servicios o sistemas vinculados a entidades públicas. El resultado es un mercado más transparente: los proveedores conocen las reglas y pueden diferenciarse mediante conformidad verificable.

Para **auditores y entidades certificadoras**, las ITS son instrumentos de consistencia. **Ayudan a fijar alcance, criterios, evidencias, informes, procedimientos y condiciones de certificación**. Esto es esencial para evitar que el valor de la certificación dependa en exceso de prácticas particulares. Un certificado ENS debe significar lo mismo con

independencia de la entidad que lo haya expedido, dentro del marco de acreditación correspondiente. Las ITS contribuyen a preservar esa equivalencia funcional.

Para los **órganos de contratación**, **las ITS aportan seguridad jurídica**. Cuando un pliego exige conformidad ENS, debe poder apoyarse en un sistema claro de declaración, certificación y publicidad. Cuando el contrato incluye obligaciones de notificación de incidentes, debe existir un marco que permita determinar cuándo, cómo y con qué evidencias se comunica. Cuando un servicio afecta a sistemas de categoría media o alta, la auditoría y certificación deben estar conectadas con criterios reconocibles. Las ITS facilitan esta integración del ENS en la contratación pública.

Para el conjunto del modelo, las ITS aportan escalabilidad. El ENS sólo puede proyectarse eficazmente en España y fuera de España si sus procedimientos son comprensibles, repetibles y verificables. Las ITS permiten pasar de la norma general a la práctica institucional. Refuerzan la coherencia, reducen la discrecionalidad, mejoran la calidad de las evidencias y consolidan la confianza.

Desde una **perspectiva estratégica**, el mensaje es claro: **el ENS no se limita a formular obligaciones de seguridad, sino que dispone de un segundo nivel normativo que permite operativizarlas**. Las ITS son una prueba de que el modelo español ha alcanzado un grado de madurez suficiente para regular no sólo la seguridad que debe alcanzarse, sino también la forma en que dicha seguridad debe declararse, certificarse, auditarse, notificarse y medirse.



Figura 5.1 Las cuatro ITS como piezas operativas del modelo ENS

Para comprender la aplicación práctica del ENS es necesario analizar el papel articulador que desempeñan las ITS. Estas disposiciones actúan como un nexo operativo fundamental entre el mandato regulatorio de nivel superior (establecido por el Real Decreto 311/2022) y los resultados tangibles que se ejecutan en el nivel base del sistema.

Como se refleja en la Figura 5.2, las cuatro ITS clave (Conformidad, Auditoría, Incidentes e Informe del Estado de la Seguridad) transforman la obligación normativa general en un modelo de confianza verificable. Este nivel intermedio traslada las exigencias legales hacia la operativa diaria mediante la publicidad de la conformidad, la verificación auditada, la respuesta coordinada ante incidentes, la medición objetiva del estado de seguridad y la mejora continua de la organización.



Figura 5.2 Las ITS como puente entre norma, operación y confianza

5.9. RESUMIENDO…

Las Instrucciones Técnicas de Seguridad son una pieza indispensable para comprender el funcionamiento real del ENS. **Mientras que el Real Decreto 311/2022 establece el marco general; las ITS concretan aspectos críticos de su aplicación; las guías CCN-STIC y las herramientas del CCN facilitan la implantación y auditoría**. Esta arquitectura escalonada permite que el ENS sea un sistema jurídicamente exigible, técnicamente operativo y organizativamente viable.

La ITS de Conformidad permite hacer visible y publicable el cumplimiento. La ITS de Auditoría permite verificarlo. La ITS de Notificación de Incidentes permite responder y coordinar. La ITS de Informe del Estado de la Seguridad permite medir y mejorar. En conjunto, las cuatro ITS convierten el ENS en un modelo de confianza demostrable.

Corolario: **el ENS no es sólo una norma de ciberseguridad, sino un ecosistema regulatorio capaz de convertir la seguridad en evidencia, la evidencia en confianza y la confianza en un activo institucional**. Las ITS son uno de los instrumentos que hacen posible esa transformación.

6. LAS GUÍAS CCN-STIC DE LA SERIE 800 Y LAS HERRAMIENTAS DE APOYO DEL CCN

El Esquema Nacional de Seguridad no puede entenderse únicamente a partir del Real Decreto 311/2022 y de las Instrucciones Técnicas de Seguridad que desarrollan aspectos concretos del modelo. Su aplicación efectiva exige también un conjunto de instrumentos técnicos, metodológicos y operativos que permitan a las entidades comprender, implantar, documentar, auditar y mantener el cumplimiento. En este punto adquieren una importancia central las guías CCN-STIC de la serie 800 y las herramientas de apoyo puestas a disposición por el Centro Criptológico Nacional.

La serie de Guías CCN-STIC 800 constituye uno de los elementos más valiosos del modelo español. Su función no es sustituir al Real Decreto ni alterar el contenido de las obligaciones normativas, sino **facilitar su interpretación y aplicación práctica con independencia del tipo de entidad u organización**.

Las guías permiten transformar un marco jurídico-técnico complejo en criterios comprensibles, procedimientos operativos, orientaciones de implantación, modelos documentales, pautas de auditoría y referencias metodológicas. Por ello, constituyen una pieza esencial del ecosistema ENS.

Desde una **perspectiva técnico-jurídica**, las guías CCN-STIC de la serie 800 **ayudan a concretar cómo se aplican los principios básicos, requisitos mínimos y medidas de seguridad del ENS**. Desde una **perspectiva organizativa**, **facilitan que las entidades estructuren su política de seguridad, asignen responsabilidades, documenten decisiones, realicen análisis de riesgos, seleccionen medidas, preparen auditorías y mantengan la conformidad**. Desde una **perspectiva institucional**, son una **prueba de madurez del modelo español.**

El ENS no se limita a imponer obligaciones, sino que acompaña a las entidades en su cumplimiento a través de guías metodológicas y prácticas vinculadas a aspectos concretos de la norma.

Esta dimensión es especialmente relevante para la **proyección europea e internacional** del ENS. Muchos marcos normativos de ciberseguridad establecen obligaciones generales, pero no siempre ofrecen a las entidades un cuerpo doctrinal amplio y especializado para hacerlas operativas. **El valor diferencial del modelo español reside, precisamente, en que combina norma jurídica, instrucciones técnicas, guías especializadas, herramientas de gobernanza, auditoría, certificación y acreditación**. Esta combinación permite presentar el ENS como un sistema completo y no como un estándar aislado. De esta forma se facilita la inmersión de las organizaciones a la hora de implementar la norma y en su desarrollo posterior, ofreciendo soluciones prácticas y estableciendo orientaciones que permiten adecuar la norma a la realidad de un sistema de información u organización.

Las herramientas de apoyo del CCN completan esta función. Soluciones como INES, AMPARO, PILAR y otras herramientas relacionadas con la gobernanza de la ciberseguridad **permiten facilitar la adecuación, medición, implantación, gestión de riesgos, auditoría y certificación**. Su valor es doble. Por un lado, **reducen la carga**

operativa que supone implantar el ENS, especialmente para entidades con menor capacidad técnica. Por otro, **contribuyen a homogeneizar los procesos, mejorar la calidad de la información y aumentar la trazabilidad de las evidencias.**

Su proceso de desarrollo y validación se somete a los más altos estándares del mercado y ofrece una garantía de cumplimiento a las organizaciones que las implantan. Por tanto, nos encontramos con una situación de ventaja frente a otros estándares o normas que requieren de un análisis de cumplimiento previo para adecuarlo a los requisitos de la norma. En el modelo del ENS, la dinámica se produce a la inversa. El desarrollo se orienta a aspectos concretos de la norma, ofreciendo soluciones prácticas a problemas de operativa concretos, con la ventaja añadida de disponer de la conformidad de la autoridad de control.

El conjunto formado por guías y herramientas constituye una de las principales ventajas competitivas del ENS. Permite pasar del cumplimiento normativo al cumplimiento asistido; de la obligación abstracta a la metodología concreta; de la interpretación dispersa a la homogeneización técnica; y de la seguridad meramente documental a una seguridad medible, auditable y sostenible.

6.1. NATURALEZA Y FUNCIÓN DE LAS GUÍAS CCN-STIC

Las guías CCN-STIC son documentos técnicos elaborados y difundidos por el **Centro Criptológico Nacional (CCN)** para facilitar la seguridad de las tecnologías de la información y la comunicación en el ámbito de sus competencias. En el contexto del ENS, **las guías de la serie 800 cumplen una función específica: orientar la aplicación práctica del Esquema Nacional de Seguridad y ayudar a las entidades a implantar, mantener, auditar y evidenciar su cumplimiento**.

Su naturaleza debe explicarse con precisión. Las guías no tienen el mismo rango normativo que el Real Decreto 311/2022, ni sustituyen a las Instrucciones Técnicas de Seguridad aprobadas mediante resolución. Sin embargo, su relevancia práctica es muy alta. El propio Real Decreto 311/2022 reconoce expresamente la función del CCN en la elaboración y difusión de guías CCN-STIC, particularmente de la serie 800 (vinculadas al cumplimiento del ENS), y prevé su incorporación al conjunto documental utilizado para las auditorías de seguridad. Esta previsión sitúa a las guías en una posición singular dentro del ecosistema ENS: no son una fuente normativa primaria, pero sí un instrumento técnico de referencia para aplicar y evaluar el cumplimiento.

Las guías cumplen varias funciones:

- En primer lugar, una **función interpretativa**: **ayudan a comprender conceptos, requisitos, medidas, roles y procedimientos del ENS**.
- En segundo lugar, una **función metodológica**: **ofrecen pautas para abordar actividades como la categorización, el análisis de riesgos, la elaboración de la política de seguridad, la Declaración de Aplicabilidad, la auditoría o la verificación de cumplimiento**.
- En tercer lugar, una **función operativa**: **proporcionan criterios, modelos, ejemplos y orientaciones que facilitan la implantación práctica.**

- En cuarto lugar, una **función de homogeneización**: **permiten que entidades, auditores, certificadores y proveedores trabajen sobre referencias comunes**.

Esta función de homogeneización es especialmente importante en un Estado descentralizado y en un mercado tecnológico complejo. El ENS se aplica a ministerios, organismos públicos, comunidades autónomas, entidades locales, universidades, sociedades públicas, fundaciones públicas y proveedores privados que prestan servicios o suministran soluciones al sector público. Sin guías comunes, el riesgo de interpretaciones divergentes sería elevado. Las guías CCN-STIC contribuyen a que el ENS se aplique con criterios más previsibles y comparables.

Desde el punto de vista del cumplimiento, las guías reducen incertidumbre. Una entidad que debe adecuarse al ENS necesita saber cómo comenzar, cómo organizar el proyecto, qué documentación debe elaborar, cómo debe categorizar sus sistemas, cómo debe seleccionar medidas, cómo debe preparar la auditoría y cómo debe mantener la conformidad. Las guías proporcionan un camino ordenado para abordar esas tareas.

Desde el punto de vista de la certificación, las guías refuerzan la calidad del modelo. Permiten que auditores y entidades de certificación dispongan de referencias técnicas comunes, reduciendo el riesgo de criterios dispares. Esto favorece la coherencia del mercado de certificación, mejora la calidad de las evaluaciones y aumenta la confianza de terceros en los certificados ENS.

Desde una perspectiva estratégica, las guías CCN-STIC permiten presentar el ENS como un modelo acompañado. Esta idea tiene fuerza comunicativa:

> **España no exige a sus entidades cumplir un marco de seguridad complejo sin apoyo, sino que pone a su disposición un cuerpo técnico de orientación elaborado por la autoridad nacional de referencia. Esta capacidad de acompañamiento es una de las razones por las que el ENS puede ser presentado como modelo de buenas prácticas ante otros países y, especialmente, en Europa.**

6.2. LA SERIE 800 COMO CUERPO DOCTRINAL DE IMPLANTACIÓN DEL ENS

La serie CCN-STIC 800 puede definirse como el cuerpo doctrinal específico del ENS. Agrupa guías destinadas a facilitar la **implantación, interpretación, auditoría, certificación, mantenimiento y mejora del Esquema Nacional de Seguridad**. Su utilidad no reside únicamente en el número de guías disponibles, sino en la función sistemática que desempeñan: acompañar a las entidades a lo largo de todo el ciclo de cumplimiento.

Este ciclo comienza con la comprensión del ENS y la delimitación del sistema; continúa con la categorización, análisis de riesgos, política de seguridad, asignación de roles, selección de medidas, elaboración documental y Declaración de Aplicabilidad; avanza hacia la implantación efectiva de controles; se verifica mediante autoevaluación, auditoría o certificación; y se mantiene mediante seguimiento,

revisión, informe del estado de seguridad y mejora continua. Las guías de la serie 800 ofrecen apoyo para cada una de estas fases.

La existencia de este cuerpo doctrinal es uno de los rasgos más característicos del modelo español.

El ENS no se limita a establecer una obligación general de aplicar medidas técnicas y organizativas adecuadas. Proporciona una metodología pública para hacerlo.

Esto es especialmente importante en entidades que carecen de grandes equipos especializados o que necesitan referencias estables para orientar sus procesos de adecuación.

La serie 800 cumple también una **función pedagógica**. **Permite que los responsables jurídicos, responsables de seguridad, responsables de sistemas, responsables de contratación, auditores, certificadores, consultores y directivos compartan un lenguaje común.** La ciberseguridad pública requiere coordinación entre perfiles muy distintos. Las guías facilitan esa coordinación porque convierten conceptos técnicos y jurídicos en procedimientos comprensibles y aplicables.

Esta función doctrinal no debe confundirse con rigidez. El ENS es un modelo basado en riesgos y proporcionalidad. Las guías ayudan a aplicar esa lógica, pero no eliminan la necesidad de analizar cada sistema, su categoría, su contexto, sus activos, sus proveedores y sus riesgos. La serie 800 proporciona orientación común, no automatismo acrítico. Su buena utilización exige criterio profesional.

Desde la perspectiva del **posicionamiento internacional, la serie 800 es uno de los activos más exportables del ENS**. Permite explicar que España no sólo ha regulado un marco nacional de seguridad, sino que ha creado una doctrina técnica de implantación. Esto resulta especialmente atractivo para terceros países que quieran desarrollar marcos nacionales de ciberseguridad: el valor no está sólo en la norma, sino en todo el material que hace viable su cumplimiento.

La serie de Guías 800 es, por tanto, una infraestructura de conocimiento. No es un mero repositorio de documentos. Es el conjunto de referencias técnicas que permite escalar el ENS, homogeneizar criterios, reducir incertidumbre, mejorar auditorías y sostener la conformidad en el tiempo.

6.3. CLASIFICACIÓN FUNCIONAL DE LAS GUÍAS DE LA SERIE 800

Para facilitar su comprensión, conviene presentar las guías de la serie 800 mediante una clasificación funcional. Esta clasificación no pretende sustituir al listado oficial, que se incluye en el Anexo III de este documento, sino ayudar al lector a comprender qué papel desempeñan las guías dentro del ecosistema ENS. La clasificación funcional permite evitar una lectura fragmentada y mostrar que la serie 800 acompaña todo el ciclo de cumplimiento.

Un primer bloque estaría integrado por **guías de carácter general, conceptual o terminológico**, destinadas a facilitar la comprensión del ENS, sus términos, estructura, principios y lógica de aplicación. Estas guías son especialmente útiles para entidades

que se aproximan por primera vez al modelo y para interlocutores internacionales que necesitan comprender su arquitectura.

Conceptos como la **gestión de incidentes de seguridad**, su taxonomía y clasificación; el **empleo de mecanismos criptográficos y de cifrado**, o el establecimiento de **métricas e indicadores** para la evolución y mejora continua de los sistemas, ayudan a las entidades a traducir conceptos desde una perspectiva meramente técnica al ámbito operacional de la organización.

Un segundo bloque estaría formado por **guías de adecuación y cumplimiento**. Estas guías ayudan a las entidades a **organizar el proceso de implantación, preparar planes de adecuación, identificar requisitos, seleccionar medidas y documentar el cumplimiento**. Son guías orientadas a pasar de la norma a la acción.

Un tercer bloque comprendería **guías de auditoría, verificación y certificación**. Su finalidad es **orientar los procesos mediante los cuales se comprueba el cumplimiento y se generan evidencias.** Son especialmente relevantes para auditores, entidades de certificación, órganos de auditoría técnica y entidades que se preparan para obtener o mantener la conformidad.

Una de las ventajas que introducen estas guías es la disposición de criterios de auditoría claros que permiten analizar supuestos concretos en los que las entidades y organizaciones han implementado medidas y herramientas compensatorias o complementarias, validando la eficacia y la alineación de las mismas con la norma.

Un cuarto bloque estaría integrado por **guías de análisis y gestión de riesgos**. Su función es **apoyar la categorización, valoración de sistemas, análisis de amenazas, determinación de impactos y selección de medidas proporcionadas**. Este bloque conecta directamente con uno de los principios básicos del ENS: la seguridad basada en riesgos.

En relación a esta gestión de riesgos surge una de las grandes bazas del modelo español, y es la adopción de una metodología homogénea para la gestión de riesgos de seguridad de la información, como es **MAGERIT**, acompañada a la vez de una herramienta propia, que facilita la operativa diaria en cuanto a riesgos de manera escalable y adecuada a la complejidad del sistema de información y los activos que lo componen.

Un quinto bloque agruparía **guías de gobernanza, roles y organización de la seguridad**. En ellas se abordan **responsabilidades, funciones, política de seguridad, comités, estructura organizativa y gobierno interno del cumplimiento**. Son esenciales para evitar que el ENS se perciba como una cuestión meramente tecnológica.

Un sexto bloque estaría formado por **guías relativas a medidas de protección, configuración segura, servicios tecnológicos, externalización, cloud, contratación y cadena de suministro**. Este grupo adquiere cada vez mayor relevancia por la creciente dependencia del sector público respecto de **proveedores, plataformas, servicios gestionados e infraestructuras externas**.

Desde un punto de vista práctico, estas guías facilitan la operativa diaria de la seguridad en las entidades, estableciendo pautas comunes para la implementación de soluciones y procedimientos con la garantía de contar con una validación previa.

Un séptimo bloque estaría integrado por **guías dirigidas a colectivos específicos o entidades de menor dimensión, como entidades locales, universidades u organizaciones con capacidades limitadas.** Su importancia radica en facilitar la escalabilidad del ENS y evitar que el cumplimiento quede reservado a entidades con grandes recursos.

En este sentido, destacar la labor y la aproximación prácticas que incorporan las guías relacionadas con **perfiles de cumplimiento específico**, que constituyen una herramienta de trabajo directa al ofrecer valoraciones y mecanismos de cumplimiento preconfigurados, como la valoración de servicios e información, declaraciones de aplicabilidad, etc.

6.4. GUÍAS SOBRE ADECUACIÓN Y CUMPLIMIENTO

Las guías sobre adecuación y cumplimiento ocupan una posición central dentro de la serie 800. Su finalidad es **ayudar a las entidades a recorrer el proceso de adaptación al ENS de forma ordenada.** La adecuación no consiste en una actuación aislada, sino en un proyecto organizativo, técnico y documental que afecta a políticas, procedimientos, sistemas, contratos, personas, proveedores y evidencias.

Estas guías permiten **orientar las fases esenciales del proceso: identificación del ámbito, determinación de sistemas afectados, categorización, análisis de riesgos, selección de medidas, elaboración de la Declaración de Aplicabilidad, planificación de acciones, implantación de controles, generación de evidencias, autoevaluación, auditoría y mantenimiento**. Sin una metodología de adecuación, las entidades pueden caer en dos errores frecuentes: abordar el ENS como una acumulación de documentos desconectados o intentar implantar medidas técnicas sin una visión de gobierno.

La utilidad de estas guías es especialmente clara para entidades que inician por primera vez su adecuación al ENS. Les proporcionan una ruta de trabajo y les ayudan a evitar improvisaciones. También son útiles para entidades ya certificadas, porque permiten revisar el grado de madurez del sistema, identificar carencias, actualizar documentación y preparar renovaciones o auditorías periódicas.

Desde el **punto de vista jurídico**, **las guías de adecuación ayudan a traducir obligaciones normativas en actuaciones verificables**. Una entidad no sólo debe cumplir, sino poder demostrar cómo ha cumplido. Las guías orientan esa demostración: qué documentos deben existir, qué decisiones deben quedar justificadas, qué evidencias deben conservarse y qué coherencia debe existir entre categoría, riesgos, medidas y procedimientos.

Desde una **perspectiva organizativa**, estas guías **favorecen la gestión de proyectos ENS**. Permiten asignar tareas, ordenar responsabilidades, establecer calendarios, priorizar acciones y coordinar perfiles jurídicos, técnicos, directivos y contractuales.

Esto es especialmente importante porque el ENS no puede implantarse eficazmente desde un único departamento. Requiere colaboración transversal.

Desde el **punto de vista institucional,** las guías de adecuación **permiten presentar el ENS como un marco exigente pero practicable**. La existencia de metodología pública reduce la percepción de complejidad y transmite un mensaje relevante: el modelo español no sólo exige seguridad, sino que ayuda a alcanzarla. Esta idea resulta particularmente útil para entidades pequeñas, proveedores privados y terceros países interesados en adoptar modelos similares.

6.5. GUÍAS SOBRE AUDITORÍA Y CERTIFICACIÓN

Las guías sobre auditoría y certificación son esenciales para el funcionamiento del ENS como sistema de confianza verificable. La auditoría y la certificación no pueden depender exclusivamente de criterios individuales de cada auditor o entidad certificadora. Requieren **referencias comunes que permitan delimitar el alcance, evaluar evidencias, identificar no conformidades, documentar resultados y mantener la coherencia del proceso.**

Estas guías complementan el régimen establecido por el Real Decreto 311/2022 y por la Instrucción Técnica de Seguridad de Auditoría de la Seguridad. Su función es facilitar la preparación, ejecución y revisión de auditorías ENS, así como orientar la verificación del cumplimiento y la obtención o mantenimiento de la certificación de conformidad. Son especialmente importantes para sistemas de categoría Media y Alta, donde la certificación se convierte en un elemento de confianza frente a terceros.

La auditoría ENS exige evaluar múltiples dimensiones: política de seguridad, roles, categorización, análisis de riesgos, Declaración de Aplicabilidad, medidas del Anexo II, evidencias, gestión de incidentes, continuidad, proveedores, documentación y mejora continua. Las guías ayudan a ordenar esa evaluación. Sin ellas, el proceso podría volverse heterogéneo, dificultando la comparabilidad entre auditorías y reduciendo la credibilidad del sistema.

Para las entidades auditadas, estas guías proporcionan previsibilidad. Permiten saber qué se va a revisar, cómo debe prepararse la documentación, qué evidencias conviene conservar, qué errores son habituales y cómo debe gestionarse un plan de acciones correctoras. Esto facilita la preparación de auditorías y reduce el riesgo de que la certificación se perciba como un procedimiento opaco.

Para los auditores y entidades certificadoras, las guías favorecen la consistencia técnica. Ayudan a evitar desviaciones injustificadas, criterios excesivamente laxos o exigencias no homogéneas. La confianza en el certificado ENS depende en gran medida de que el mercado de auditoría y certificación actúe con criterios rigurosos y comparables. Las guías contribuyen a ese objetivo.

Desde el punto de vista estratégico, las guías de auditoría y certificación refuerzan el carácter diferencial del ENS. El modelo español no sólo contempla certificados; proporciona doctrina para auditar y verificar el cumplimiento. Esta característica permite posicionar el ENS como un sistema de conformidad robusto, especialmente

relevante en contextos europeos donde la certificación y evaluación de la conformidad tienen un papel creciente.

6.6. GUÍAS SOBRE ANÁLISIS Y GESTIÓN DE RIESGOS

La gestión de riesgos es uno de los principios estructurales del ENS. La seguridad debe ser proporcional al valor de la información, a la criticidad de los servicios, a las amenazas existentes, a las vulnerabilidades identificadas y al impacto potencial de los incidentes. Las guías sobre análisis y gestión de riesgos son, por ello, fundamentales para aplicar correctamente el modelo.

Estas guías ayudan a las entidades a identificar activos, valorar dimensiones de seguridad, estimar impactos, identificar amenazas, reconocer vulnerabilidades, valorar riesgos, seleccionar medidas y justificar decisiones. Su función es evitar que la implantación del ENS se convierta en una aplicación mecánica de controles sin conexión con el contexto real del sistema.

El análisis de riesgos es esencial para la categorización, la Declaración de Aplicabilidad y la selección de medidas. Si el análisis de riesgos es débil, todo el modelo posterior queda comprometido. Una categorización incorrecta puede conducir a medidas insuficientes o desproporcionadas. Una selección de medidas sin justificación puede dificultar la auditoría. Una Declaración de Aplicabilidad sin trazabilidad puede convertirse en un documento formal sin valor real.

Las guías de riesgos permiten introducir disciplina metodológica. **Ayudan a que la entidad documente sus decisiones y pueda explicar por qué se han adoptado determinadas medidas**. Esta documentación resulta relevante para responsables internos, auditores, entidades de certificación, órganos de contratación, responsables de protección de datos y órganos directivos.

Desde el punto de vista organizativo, estas guías ayudan a integrar la gestión de riesgos en la gestión ordinaria de la entidad. La seguridad no debe analizarse sólo al inicio del proyecto de adecuación. Debe revisarse cuando cambian los sistemas, se incorporan proveedores, se externalizan servicios, se migran plataformas a la nube, se introducen nuevas tecnologías o se producen incidentes relevantes.

Desde la perspectiva del posicionamiento internacional, la existencia de guías específicas sobre riesgos permite presentar el ENS como un modelo alineado con las mejores prácticas europeas e internacionales.

> **El ENS no se basa en cumplimiento ciego, sino en seguridad proporcionada y justificada. Esta lógica de riesgo es especialmente relevante para la aplicación del modelo español ante interlocutores europeos o internacionales.**

6.7. GUÍAS SOBRE GOBERNANZA, ROLES Y ORGANIZACIÓN DE LA SEGURIDAD

El ENS es un modelo de seguridad, pero también de gobernanza. La asignación de responsabilidades, la política de seguridad, los comités de seguridad de la información,

los procedimientos, la segregación de funciones y la toma de decisiones son elementos tan relevantes como las medidas técnicas. Por ello, las guías de gobernanza, roles y organización de la seguridad cumplen una función crítica.

Estas guías ayudan a **definir y aplicar correctamente los roles esenciales del ENS: responsable de la información, responsable del servicio, responsable de la seguridad y responsable del sistema.** También orientan la elaboración de **políticas de seguridad**, la constitución de **comités**, la aprobación de **normativa interna**, la **coordinación entre áreas** y la **resolución de conflictos** entre necesidades funcionales, técnicas y de seguridad.



Figura 6.1 Valor estratégico de la gobernanza ENS: Guías y Roles

Su valor radica en que evitan una visión excesivamente tecnológica del ENS. La seguridad no depende sólo de herramientas, sino de decisiones y de una perspectiva de negocio o competencial. Alguien debe determinar qué información es crítica, qué servicios requieren mayor disponibilidad, qué riesgos son aceptables, qué medidas deben financiarse, qué proveedores pueden intervenir, qué incidentes deben escalarse y qué acciones correctoras deben priorizarse. Las guías de gobernanza ayudan a ordenar esas decisiones y asignarlas a niveles jerárquicos o de decisión concretos.

Desde el punto de vista jurídico, la correcta definición de roles facilita la rendición de cuentas. La diferenciación de responsabilidades permite identificar quién decide, quién valida, quién opera, quién supervisa y quién responde. Esto es especialmente relevante en el sector público, donde las decisiones de seguridad pueden afectar a servicios públicos, derechos de ciudadanos, cumplimiento normativo, protección de datos personales y contratación. Además, facilita la visibilidad del modelo dentro de la organización, de manera que los usuarios internos conocen los órganos con responsabilidad respecto a la seguridad de la información.

Desde el punto de vista organizativo, estas guías promueven una cultura de seguridad transversal. La seguridad deja de ser una función exclusivamente técnica y

pasa a integrarse en dirección, contratación, recursos humanos, servicios jurídicos, protección de datos, continuidad, gestión económica y relación con proveedores. Esta transversalidad es indispensable para la eficacia del ENS. Cuestiones como la identificación y respuesta ante incidentes de seguridad o la seguridad en la cadena de suministro requieren de una participación horizontal de toda la organización.

Desde la perspectiva institucional, las guías de gobernanza permiten presentar el ENS como un modelo de responsabilidad directiva y madurez organizativa. Este mensaje es especialmente importante para públicos ejecutivos: el ENS no es sólo "ciberseguridad técnica", sino un sistema de gobierno para proteger servicios públicos digitales y generar confianza. Una estructura con herramientas transversales y empleables a todos los niveles de la organización.

6.8. GUÍAS SOBRE MEDIDAS DE PROTECCIÓN, SERVICIOS CLOUD, CONTRATACIÓN Y EXTERNALIZACIÓN

La evolución tecnológica ha convertido la seguridad de proveedores, servicios cloud, servicios gestionados, plataformas externas, software de terceros y cadenas de suministro en una cuestión central. El sector público ya no opera todos sus sistemas de forma exclusivamente interna. Buena parte de los servicios digitales dependen de proveedores privados, infraestructuras compartidas, plataformas cloud, integradores, desarrolladores, subcontratistas y servicios especializados. Las guías de la serie 800 relacionadas con medidas de protección, contratación, externalización y servicios cloud son esenciales para aplicar el ENS en este escenario.

Estas guías permiten orientar la selección e implantación de medidas de seguridad sobre activos concretos: instalaciones, equipos, comunicaciones, soportes, aplicaciones, servicios externos, información, control de acceso, registros, continuidad, cifrado, monitorización o protección frente a código dañino. Su función es traducir el Anexo II en criterios prácticos de protección.

En materia de **servicios cloud y externalización**, las guías ayudan a resolver uno de los problemas más complejos del ENS: **cómo mantener la responsabilidad de la entidad pública cuando parte del sistema o del servicio depende de un tercero**. Externalizar no significa transferir la responsabilidad última sobre la seguridad. La entidad debe conservar capacidad de gobierno, exigencia contractual, supervisión, acceso a evidencias, gestión de incidentes y verificación de cumplimiento. Es por ello que se introduce un conjunto de orientaciones en relación al reparto de responsabilidades en materia de seguridad entre el proveedor y la entidad cliente, permitiendo su configuración por parte de las entidades.

Las guías sobre **contratación permiten incorporar el ENS a pliegos, contratos, encargos, acuerdos de nivel de servicio, cláusulas de seguridad, requisitos de certificación, obligaciones de notificación de incidentes, derechos de auditoría, subcontratación, ubicación de datos, continuidad, reversibilidad y conservación de evidencias.** Esta dimensión es especialmente importante porque el ENS se proyecta sobre entidades privadas que prestan servicios o suministran soluciones al sector público. Estas indicaciones suponen una primera capa de seguridad que permite

seleccionar a proveedores que dispongan de garantías suficientes en relación al manejo de información e interacción con sistemas de información que soportan servicios públicos.

Desde una **perspectiva de mercado, estas guías contribuyen a disciplinar la cadena de suministro**. Los proveedores conocen mejor qué se espera de ellos, las Administraciones pueden exigir requisitos más claros y los órganos de contratación pueden utilizar la conformidad ENS como herramienta de gestión de riesgos. Esto favorece un mercado público digital más profesional, transparente y seguro.

Desde el **punto de vista estratégico, las guías sobre cloud, externalización y contratación son un elemento especialmente atractivo para Europa**. La seguridad de la cadena de suministro, la dependencia tecnológica, la soberanía digital, la resiliencia de servicios críticos y la contratación segura son prioridades crecientes que se han trasladado a las últimas novedades legislativas. El ENS ofrece una experiencia dilatada y práctica para abordar esas cuestiones desde un marco nacional de seguridad verificable.

En **términos de comunicación, estas guías permiten transmitir una idea relevante: el ENS no se queda dentro de la Administración; se proyecta sobre el ecosistema tecnológico que la sostiene**. Esta capacidad de extender la seguridad desde la entidad pública hacia sus proveedores es una de las fortalezas más importantes del modelo español.

6.9. GUÍAS RELEVANTES PARA ENTIDADES CON REQUISITOS ESPECÍFICOS O DE MENOR DIMENSIÓN: LOS PERFILES DE CUMPLIMIENTO ESPECÍFICO.

La aplicación del ENS en entidades locales y organizaciones de menor dimensión plantea retos específicos. Muchas de estas entidades carecen de una estructura organizativa o equipos técnicos amplios, presupuestos suficientes, estructuras maduras de seguridad o experiencia previa en auditoría y certificación. Sin embargo, también prestan servicios públicos digitales, tratan información relevante y forman parte del ecosistema público que debe protegerse. La serie 800 y las herramientas del CCN cumplen aquí una función particularmente valiosa.

Las guías orientadas a entidades de menor dimensión permiten adaptar el cumplimiento a contextos con recursos limitados. No se trata de reducir la exigencia del ENS de forma injustificada, sino de hacerla comprensible y abordable. La proporcionalidad y la progresividad es clave: las entidades deben empezar a aplicar las medidas que correspondan a sus sistemas, categorías y riesgos, pero necesitan metodologías que les permitan hacerlo sin convertir el proceso en una carga inasumible.

Estas guías ayudan a ordenar prioridades. En entidades pequeñas, la dificultad no suele estar sólo en saber qué exige el ENS, sino en decidir por dónde empezar, cómo documentar lo esencial, cómo asignar roles cuando no existe una estructura compleja, cómo gestionar proveedores, cómo preparar una autoevaluación, cómo utilizar herramientas de apoyo y cómo sostener la mejora continua.

Su valor es también territorial. En un Estado descentralizado, la seguridad del conjunto depende en buena medida de la seguridad de sus eslabones más vulnerables. Una entidad local pequeña puede gestionar información sensible, prestar servicios críticos para sus ciudadanos o depender de proveedores compartidos. Elevar el nivel de seguridad de estas entidades contribuye a reducir el riesgo sistémico.

Por otra parte, y siguiendo estos principios de apoyo a entidades singulares, nos encontramos con perfiles de cumplimiento específicos, incorporados al catálogo de guías de la serie 800 y que abordan, desde un punto de vista práctico, aquellas medidas de seguridad y criterios de aplicación de medidas que se añaden a los ya existentes para entidades menores y que cubren sistemas de información entidades con particularidades concretas, como Universidades, entidades locales como Diputaciones o Cabildos Insulares, o servicios concretos como la atención primaria en centros de salud, dirigiéndose en gran parte de los casos a dotar de criterios de aplicación concretos y de un catálogo de medidas de seguridad extraído del Anexo II del ENS y que se han considerado como elementales en atención al marco de servicios o competencias de dichas entidades. De esta manera, se baja un escalón más en cuanto al apoyo al cumplimiento, con directrices claras para casos concretos. Estos perfiles de cumplimiento a su vez, se están incrementando paulatinamente a medida en que se conocen las necesidades y peculiaridades de cada sector de actividad o tipo de entidad.

Desde el punto de vista institucional, esta dimensión permite presentar el ENS como un modelo inclusivo y escalable. No está pensado únicamente para grandes organismos públicos o entidades con alta capacidad técnica. Dispone de guías y herramientas para facilitar su aplicación en realidades organizativas diversas. Esta escalabilidad es fundamental para defender el ENS como modelo nacional.

> **La existencia de guías específicas o especialmente útiles para entidades locales, universidades u otros colectivos permite además reforzar la idea de adaptación sectorial. El ENS combina una base común de seguridad con orientaciones prácticas para distintos tipos de entidades. Esta combinación entre unidad y flexibilidad es uno de los factores que explican su madurez.**

En términos de certificación, estas guías también pueden facilitar la preparación de entidades con menor experiencia o con necesidades singulares o sectoriales. Ayudan a comprender evidencias, documentación, roles, medidas y procesos de verificación. De este modo, contribuyen a que la certificación o declaración de conformidad no se perciba como un obstáculo reservado a organizaciones genéricas o muy grandes, sino como una meta alcanzable mediante metodología y acompañamiento.

6.10. HERRAMIENTAS DE APOYO DEL CCN: INES, AMPARO Y OTRAS SOLUCIONES ORIENTADAS AL CUMPLIMIENTO.

Las herramientas de apoyo del CCN completan la función de las guías. **Mientras las guías proporcionan doctrina, metodología y orientación, las herramientas facilitan la ejecución práctica de tareas relacionadas con la adecuación, implantación, medición,**

gestión de riesgos, auditoría y certificación. Esta combinación es uno de los rasgos más potentes del modelo ENS: conocimiento técnico y soporte operativo y funcional para dar cobertura a las obligaciones de cumplimiento.

INES, AMPARO y otras muchas forman parte de las herramientas de gobernanza de la ciberseguridad nacional puestas a disposición para facilitar el proceso completo de adecuación al ENS. Su función debe explicarse de forma integrada, no como aplicaciones aisladas. En conjunto, ayudan a que las entidades puedan abordar el cumplimiento de forma más ordenada, trazable y homogénea. Constituyen por tanto un cuadro de mandos básico para conocer el alcance y situación actual de los sistemas de información y la progresión de la entidad en cuanto al cumplimiento del ENS.

Por ejemplo, **INES** está vinculada al Informe del Estado de la Seguridad y a la medición del grado de madurez y situación de seguridad de las entidades. Su valor estratégico reside en que permite recopilar información, estructurar variables y contribuir a una visión agregada de la ciberseguridad en el sector público. Constituye un catálogo completo de métricas e indicadores de cumplimiento para observar la progresión en el cumplimiento normativo y en aspectos tan cruciales como la gestión de incidentes de seguridad. En un modelo nacional, medir es tan importante como regular. INES permite avanzar hacia una seguridad pública basada en datos.

AMPARO facilita el proceso de adecuación al ENS, proporcionando soporte para la gestión de documentación, identificación de tareas, seguimiento de cumplimiento y preparación de evidencias. Su valor es especialmente relevante para entidades que necesitan acompañamiento metodológico. Reduce la complejidad del proceso y favorece una implantación más ordenada a través de pasos secuenciales que se acompañan con modelos predefinidos de documentación, registros y listados de verificación que ayudan a completar todas las tareas previstas para una adecuación al ENS.

PILAR se relaciona con la gestión de riesgos. Su utilidad debe entenderse en conexión con la lógica del ENS: categorización, identificación y análisis de riesgos, selección de medidas y mejora continua. Una herramienta de gestión de riesgos facilita que las decisiones de seguridad estén justificadas y documentadas. Esto es esencial para la Declaración de Aplicabilidad, la auditoría y la certificación.

Además de estas herramientas, el ecosistema de herramientas CCN cuenta con otros muchos instrumentos y servicios que contribuyen a la implantación y seguimiento de la seguridad. Su función general es reforzar la capacidad de las entidades para cumplir el ENS de forma efectiva.

El valor no reside únicamente en cada herramienta individual, sino en el hecho de que el modelo español proporciona soporte operativo y funcional al cumplimiento de manera directa y con el respaldo de aplicaciones contrastadas.

Desde el punto de vista organizativo, estas herramientas permiten mejorar la coordinación interna. Ayudan a estructurar tareas, responsabilidades, evidencias, estados de avance, riesgos, medidas y resultados. En proyectos de adecuación e implantación del ENS, donde intervienen perfiles jurídicos, técnicos, responsables de

sistemas, responsables de seguridad, responsables de servicio y proveedores, disponer de herramientas comunes facilita la gestión y la aplicación práctica de conceptos y elementos aplicables a cualquier tipo de entidad o sistema de información.

Desde el punto de vista de certificación, las herramientas contribuyen a mejorar la calidad de las evidencias. Una entidad que gestiona su adecuación de forma estructurada estará mejor preparada para auditorías, certificaciones, renovaciones y seguimiento. Esto reduce el riesgo de cumplimiento improvisado o meramente documental.

Desde una perspectiva institucional, las herramientas permiten formular uno de los mensajes más fuertes del ENS: el modelo español no sólo regula y orienta, sino que también ayuda a ejecutar. Esta es una diferencia relevante respecto de otros marcos. El ENS se presenta como un sistema que acompaña a las entidades desde la planificación hasta la certificación.

6.11. VALOR DE LAS GUÍAS Y HERRAMIENTAS PARA LA HOMOGENEIZACIÓN, ESCALABILIDAD Y SOSTENIBILIDAD DEL ENS

El valor conjunto de las guías CCN-STIC de la serie 800 y de las herramientas de apoyo del CCN puede resumirse en tres ideas: **homogeneización, escalabilidad y sostenibilidad.**

La homogeneización consiste en aplicar el ENS con criterios comunes. Las guías reducen la dispersión interpretativa y las herramientas facilitan que los procesos se estructuren de forma comparable. Esto es fundamental para que las auditorías y certificaciones sean coherentes, para que las entidades entiendan qué se espera de ellas y para que los proveedores puedan operar en un mercado con reglas claras.

La escalabilidad significa que el ENS puede aplicarse a un conjunto amplio y diverso de entidades. Un modelo nacional de ciberseguridad sólo es útil si puede desplegarse en ministerios, comunidades autónomas, entidades locales, universidades, organismos públicos, sociedades públicas y proveedores privados. Las guías y herramientas permiten que esa aplicación sea más viable. Sin ellas, el ENS podría percibirse como un marco excesivamente complejo para muchas organizaciones.

La sostenibilidad se refiere a la capacidad de mantener la conformidad en el tiempo. El ENS no termina con la obtención de una declaración o certificación. Exige revisión, auditoría, gestión de incidentes, actualización documental, mantenimiento de medidas, reevaluación de riesgos y mejora continua. Las guías y herramientas ayudan a que esta continuidad sea gestionable.

Estas tres funciones refuerzan la credibilidad del ENS como modelo de confianza. Una norma sin criterios comunes genera inseguridad. Una norma sin herramientas puede resultar difícil de aplicar. Una norma sin mecanismos de mantenimiento puede convertirse en cumplimiento puntual. El ENS evita esos riesgos mediante un ecosistema de apoyo técnico y operativo.

Desde la perspectiva de España, las guías y herramientas son un activo institucional.

Permiten elevar el nivel de seguridad del sector público, mejorar la calidad de las auditorías, apoyar a entidades con menor capacidad, facilitar la certificación y reforzar la confianza en proveedores.
Desde la perspectiva internacional, son un elemento exportable del modelo. Otros países pueden encontrar en la experiencia española una referencia no sólo normativa, sino metodológica y operativa.

Por ello, la serie 800 y las herramientas del CCN son una de las razones por las que el ENS funciona como ecosistema. La norma establece el deber; las ITS concretan obligaciones críticas; las guías explican cómo aplicarlas; las herramientas ayudan a ejecutarlas; la auditoría verifica; la certificación acredita; y la mejora continua sostiene el modelo.

En la siguiente tabla se recoge la clasificación funcional de las guías CCN-STIC de la serie 800, detallando su finalidad, destinatarios principales y el valor que aportan al Esquema Nacional de Seguridad:

Bloque funcional	Finalidad principal	Destinatarios principales	Valor para el ENS
Guías generales y terminológicas	Explicar conceptos, estructura y lenguaje común del ENS	Directivos, responsables ENS, equipos jurídicos y técnicos	Facilitan comprensión y coherencia conceptual
Guías de adecuación y cumplimiento	Orientar el proceso de implantación del ENS	Entidades obligadas, consultores y responsables de seguridad	Transforman la obligación normativa en plan de acción
Guías de auditoría y certificación	Preparar y homogeneizar la verificación del cumplimiento	Auditores, entidades de certificación y entidades auditadas	Refuerzan la confianza en la conformidad ENS
Guías de análisis y gestión de riesgos	Apoyar categorización, valoración de impacto y selección de medidas	Responsables de seguridad, responsables del sistema y equipos técnicos	Conectan seguridad con riesgo y proporcionalidad
Guías de gobernanza, roles y organización	Definir responsabilidades, política de seguridad y gobierno interno	Órganos directivos, responsables ENS y comités de seguridad	Integran la seguridad en la organización
Guías sobre medidas técnicas y protección	Orientar la implantación de controles y medidas del Anexo II	Equipos técnicos, responsables de sistemas y proveedores	Facilitan seguridad operativa verificable
Guías sobre cloud, contratación y externalización	Gestionar proveedores, servicios externos y cadenas de	Órganos de contratación, responsables jurídicos,	Proyectan el ENS sobre el mercado público digital

Bloque funcional	Finalidad principal	Destinatarios principales	Valor para el ENS
	suministro	proveedores y seguridad	
Guías para entidades o sectores específicos	Adaptar el ENS a colectivos con necesidades comunes	Entidades locales, universidades, organismos sectoriales y entidades pequeñas	Aumentan escalabilidad y viabilidad del modelo

Figura 6.2 Clasificación funcional de las guías CCN-STIC de la serie 800

Para comprender la cobertura del ecosistema del CCN en todo el ciclo de vida del *compliance*, la tabla expuesta a continuación detalla las principales herramientas de apoyo y su encuadre metodológico:

Herramienta	Función principal	Momento del ciclo ENS	Mensaje de valor
INES	Recopilación, estructuración y comunicación de información sobre el estado de seguridad	Medición, seguimiento e informe del estado de seguridad	El ENS permite conocer y medir la ciberseguridad pública
AMPARO	Apoyo a la adecuación, implantación, documentación y seguimiento del cumplimiento	Planificación, adecuación, evidencias y preparación de auditoría	El ENS proporciona acompañamiento operativo
PILAR	Apoyo a la gestión y análisis de riesgos	Categorización, análisis de riesgos, selección de medidas y revisión	El ENS convierte la seguridad en gestión racional del riesgo
LUCIA	Sistema de gestión de tickets e incidentes de seguridad	Respuesta ante incidentes y coordinación técnica	El ENS permite una respuesta ágil y coordinada ante ciberataques
REYES	Intercambio de información de ciberamenazas (Ciberinteligencia)	Vigilancia continua y compartición de amenazas	El ENS fortalece la resiliencia mediante la cooperación nacional
CARMEN	Defensa frente a ataques avanzados y amenazas persistentes (APT)	Detección de intrusión y monitorización avanzada	El ENS protege los activos críticos contra los atacantes más sofisticados
CLARA	Auditoría de	Verificación técnica y	El ENS asegura

Herramienta	Función principal	Momento del ciclo ENS	Mensaje de valor
	cumplimiento del ENS en sistemas operativos Windows	auditoría de conformidad	configuraciones de seguridad verificables y objetivas
ANA	Automatización y normalización de procesos de auditoría	Verificación y evaluación del cumplimiento	El ENS simplifica y estandariza la labor de auditoría y supervisión
GLORIA	Gestión de registros (logs) para responder ante incidentes y amenazas	Vigilancia continua y registro de la actividad	El ENS optimiza la visibilidad operativa mediante la correlación de eventos
CLAUDIA / MicroClaudia	Detección de amenazas complejas en el puesto de usuario y centro de vacunación	Protección frente a código dañino (malware)	El ENS blinda el puesto de trabajo frente al ransomware y el fraude
OLVIDO	Borrado seguro de datos y gestión de metadatos	Protección de la información y de los soportes	El ENS garantiza la confidencialidad y el ciclo de vida seguro del dato
ELSA	Análisis de la superficie de ataque y exposición local	Vigilancia y detección de vulnerabilidades externas	El ENS permite identificar y reducir la visibilidad de activos frente a internet
ÁNGELES	Portal de formación y capacitación en ciberseguridad	Concienciación y formación del personal	El ENS sitúa a las personas como el primer nivel de defensa de la entidad
ATENEA	Plataforma de desafíos y retos de seguridad (gamificación)	Capacitación técnica y mejora continua	El ENS fomenta el talento y la destreza técnica de los especialistas
VANESA	Plataforma de grabaciones y emisiones multimedia en streaming	Difusión de cultura de seguridad y comunicación	El ENS promueve la cultura de seguridad mediante recursos didácticos de referencia
Otras soluciones y servicios del CCN	Apoyo técnico, metodológico y operativo	Implantación, supervisión, respuesta y mejora	El ENS se apoya en un ecosistema público de capacidades

Herramienta	Función principal	Momento del ciclo ENS	Mensaje de valor
	complementario		

Figura 6.3 Herramientas de apoyo del CCN en el ciclo ENS

La figura siguiente sintetiza la evolución metodológica del modelo español, mostrando la transición lógica desde la doctrina técnica inicial hasta la consecución de una confianza verificable:

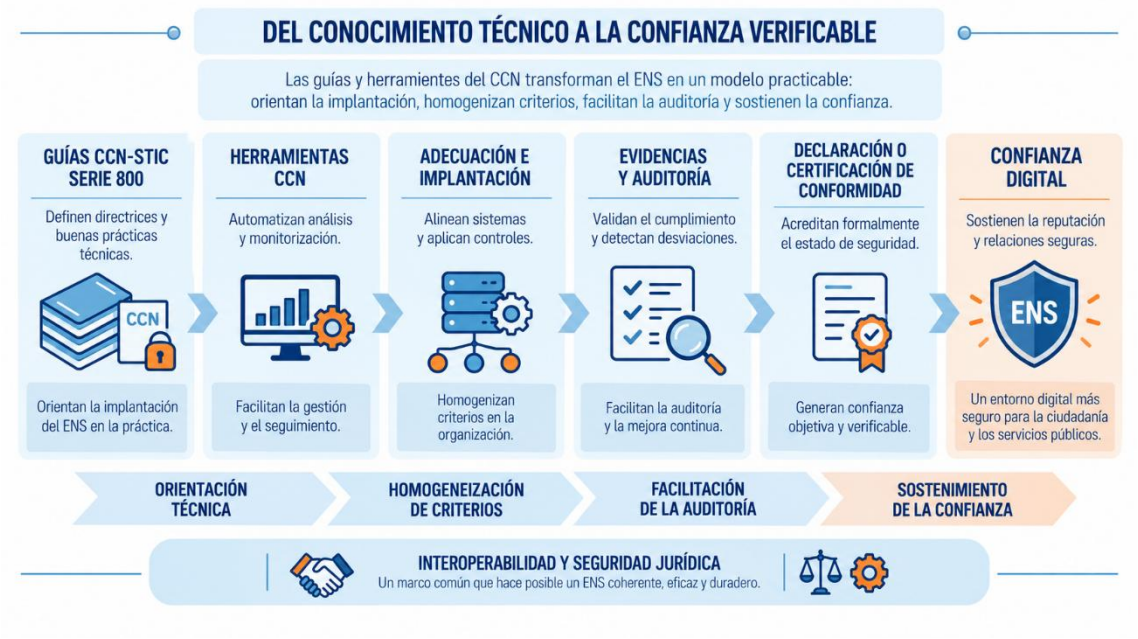


Figura 6.4 Del conocimiento técnico a la confianza verificable

6.12 RESUMIENDO...

Las guías CCN-STIC de la serie 800 y las herramientas de apoyo del CCN son una pieza decisiva para comprender el valor real del ENS. El Real Decreto 311/2022 establece el marco jurídico; las Instrucciones Técnicas de Seguridad concretan aspectos críticos; pero las guías y herramientas permiten que el modelo se implante, se interprete, se audite y se mantenga de forma efectiva.

Su función no es accesoria. Sin guías y herramientas, el ENS sería más difícil de aplicar, más costoso de interpretar y más vulnerable a criterios heterogéneos. Con ellas, el ENS se convierte en un sistema acompañado, metodológico, escalable y sostenible. Esta es una de las grandes fortalezas del modelo español.

Desde la perspectiva técnica, las guías y herramientas permiten aplicar medidas y gestionar riesgos. Desde la perspectiva organizativa, ayudan a estructurar responsabilidades, documentación y procesos. Desde la perspectiva de certificación, mejoran la calidad de las evidencias y la consistencia de auditorías. Desde la perspectiva institucional, refuerzan la confianza en el sistema. Y desde la perspectiva de visualización internacional, permiten presentar el ENS como algo más que una

norma: como un modelo completo de gobernanza pública de la ciberseguridad, dotado de doctrina, metodología, herramientas y capacidad de acompañamiento.

En definitiva, la serie 800 y las herramientas del CCN son uno de los elementos que hacen del ENS un modelo singularmente robusto. Gracias a ellas, la seguridad deja de ser una exigencia abstracta y se convierte en una práctica organizada, asistida, verificable y orientada a la mejora continua.

7. AUDITORÍA, CERTIFICACIÓN Y ACREDITACIÓN: EL SISTEMA DE CONFIANZA DEL ENS

El Esquema Nacional de Seguridad no se limita a establecer obligaciones jurídicas y medidas técnicas de protección de los sistemas de información. Su verdadera fortaleza reside en que **convierte el cumplimiento en confianza verificable.** Para ello, articula un sistema que contempla tanto la realización de controles y auditorías internas hasta la obtención de la certificación de conformidad, pasando por los hitos de la auditoría, la declaración de conformidad, la obtención del certificado y la gestión de no conformidades. **Este conjunto de instrumentos permite que el cumplimiento del ENS no quede reducido a una afirmación interna de la entidad, sino que pueda ser comprobado, evidenciado y reconocido frente a terceros.**

Esta dimensión es esencial para comprender el valor institucional del modelo español. En materia de ciberseguridad, la confianza no puede descansar únicamente en la buena voluntad, en declaraciones genéricas de diligencia o en documentos internos no contrastados, o en la simple declaración de intenciones de la entidad. Se requiere un modelo de verificación.

> **La confianza exige método, evidencias, revisión independiente, trazabilidad de decisiones, competencia técnica de quienes evalúan y coherencia entre entidades evaluadas, auditores, certificadores y organismos de acreditación.**
> **El ENS incorpora todos esos elementos y los integra en un modelo nacional de evaluación de la conformidad.**

Desde una **perspectiva técnica**, **la auditoría permite verificar que el sistema de información se ha categorizado correctamente, que se han identificado y gestionado los riesgos, que se han seleccionado las medidas aplicables, que dichas medidas se han implantado y que existen evidencias suficientes para sostener el cumplimiento**.

Por consiguiente, nos encontramos con un modelo que incorpora los principios y procesos clásicos de las auditorías de los sistemas de gestión, de manera que se puede equiparar a otros estándares internacionales similares.

Desde una **perspectiva organizativa**, **la auditoría obliga a ordenar responsabilidades, documentación, procedimientos, registros, gestión de incidentes, continuidad y mejora continua**.

Desde una **perspectiva jurídica**, **la declaración o Certificación de Conformidad permite acreditar el cumplimiento de un marco normativo obligatorio**. Y desde una **perspectiva estratégica**, **la certificación ENS opera como una señal de confianza para**

el sector público, proveedores, órganos de contratación, ciudadanos, empresas, instituciones europeas y terceros países.

El ENS no es sólo un marco regulatorio: es un sistema de confianza supervisada. Permite pasar de la obligación a la evidencia, de la evidencia a la certificación y de la certificación a la confianza.

Esta arquitectura diferencia al modelo español de otros marcos de seguridad que pueden contener controles o buenas prácticas, pero que no siempre disponen de un sistema tan estructurado de verificación externa y reconocimiento de conformidad que, además, cuenta con mecanismos de publicidad que permiten fiscalizar los certificados de conformidad en vigor, su alcance y caducidad.

7.1. DECLARACIÓN DE CONFORMIDAD Y CERTIFICACIÓN DE CONFORMIDAD

El ENS distingue entre Declaración de Conformidad y Certificación de Conformidad. Ambas figuras tienen una finalidad común: permitir que una entidad acredite que un sistema de información cumple las exigencias aplicables del Esquema Nacional de Seguridad. Sin embargo, su naturaleza, intensidad y función dentro del modelo son distintas.

La **Declaración de Conformidad** se asocia a sistemas de **categoría Básica**. En estos casos, la entidad responsable puede acreditar la adecuación al ENS mediante un proceso de **autoevaluación y declaración formal**, en los términos previstos por el Real Decreto 311/2022 y por la Instrucción Técnica de Seguridad de Conformidad con el ENS. La Declaración tiene valor porque obliga a la entidad a asumir expresamente su responsabilidad respecto del cumplimiento y a hacer visible su conformidad. No es, por tanto, una mera manifestación informal, sino una expresión documentada de cumplimiento bajo responsabilidad de la propia organización.

La **Certificación de Conformidad**, en cambio, se reserva ordinariamente para sistemas de **categoría Media o Alta**. En estos casos, **el cumplimiento debe ser verificado mediante una auditoría y certificado por una entidad de certificación acreditada o por el órgano que corresponda en el ámbito del sector público**. La Certificación introduce una garantía adicional: el cumplimiento no es afirmado únicamente por la entidad titular del sistema, sino evaluado por una auditoría de tercera parte, a cargo de una entidad con competencia técnica y sometido a reglas de acreditación, imparcialidad y trazabilidad.

Esta distinción refleja una de las ideas centrales del ENS: **la intensidad de la verificación debe ser proporcional a la criticidad del sistema**. No todos los sistemas presentan el mismo impacto potencial, por lo que no todos requieren el mismo nivel de comprobación externa. El modelo permite así equilibrar rigor y proporcionalidad. Exige mayor verificación allí donde el impacto de un incidente puede ser más relevante y evita imponer cargas innecesarias cuando el nivel de riesgo y categoría del sistema no lo justifican.

La Declaración y la Certificación cumplen también una función de transparencia.

Permiten que terceros conozcan el estado de conformidad de una entidad o sistema, favoreciendo la confianza en la Administración digital y en los proveedores que participan en la prestación de servicios públicos.
Además, la publicidad de las declaraciones y certificaciones de conformidad fomentan la transparencia del modelo y potencia la elección de proveedores de garantías para los sistemas y servicios públicos.

En la **contratación pública**, la certificación ENS puede convertirse en una evidencia especialmente relevante para valorar la adecuación de un proveedor o de un servicio. En las **relaciones interadministrativas**, permite identificar sistemas que han alcanzado un determinado nivel de madurez. En la **proyección internacional**, permite explicar que el modelo español no se limita a exigir seguridad, sino que permite demostrarla.

No obstante, debe evitarse una interpretación puramente formal de ambas figuras. Ni la Declaración ni la Certificación deben concebirse como fines en sí mismos. Su valor depende de la calidad del proceso previo de categorización, análisis de riesgos, selección de medidas, implantación efectiva, documentación, auditoría y mantenimiento. Un distintivo de conformidad sólo tiene valor real si está respaldado por un sistema vivo de seguridad, evidencias suficientes y mejora continua. Por ello, el ENS vincula la conformidad con la auditoría, el seguimiento y la reevaluación periódica.

Desde una **perspectiva institucional,** la existencia de declaración y Certificación de Conformidad permite formular un mensaje claro: **el ENS convierte la ciberseguridad en una garantía demostrable**. No se trata sólo de que una entidad afirme que aplica buenas prácticas, sino de que pueda mostrar, mediante mecanismos reconocidos, que su sistema ha sido adecuado al marco nacional de seguridad y que, periódicamente, se revise que el nivel de gestión y madurez de los sistemas es mantenido y mejorado.

7.2. SISTEMAS DE CATEGORÍA BÁSICA, MEDIA Y ALTA

La categorización de los sistemas es determinante para entender el sistema de auditoría y certificación del ENS. La categoría Básica, Media o Alta no sólo condiciona las medidas de seguridad aplicables, sino también la forma de verificar el cumplimiento y de acreditar la conformidad. Por ello, la auditoría y certificación no pueden analizarse de manera aislada respecto de la categorización del sistema.

Los **sistemas de categoría Básica** son **aquellos en los que el impacto de un incidente, atendidas las dimensiones de seguridad aplicables, no alcanza niveles medios o altos.** Ello no significa que estén exentos de medidas ni de responsabilidades. Todo sistema sujeto al ENS debe cumplir los principios básicos, requisitos mínimos y medidas aplicables. La diferencia radica en que, para estos sistemas, la conformidad puede acreditarse mediante Declaración de Conformidad basada en autoevaluación, sin perjuicio de que la entidad pueda optar por someterse a procesos de verificación más intensos si lo considera oportuno o si considera que la madurez de los sistemas permite cumplir con los requisitos de niveles mayores.

Los **sistemas de categoría Media** representan un nivel superior de exigencia. En ellos, **la afectación de alguna dimensión de seguridad puede producir impactos relevantes sobre la información, los servicios, la organización o los derechos e**

intereses afectados. Por esa razón, el ENS exige auditoría y Certificación de Conformidad. La intervención de un tercero aporta mayor objetividad y refuerza la confianza en que el sistema cumple efectivamente los requisitos aplicables.

Los **sistemas de categoría Alta** son aquellos en los que **la afectación de alguna dimensión puede producir consecuencias especialmente graves**. En estos casos, la auditoría y certificación adquieren una importancia máxima. No basta con implantar medidas; es necesario demostrar de forma sólida que la organización mantiene controles adecuados, evidencia suficiente, gestión de riesgos, continuidad, vigilancia, respuesta a incidentes y capacidad de mejora. La categoría Alta exige una aproximación de seguridad estratégica, no meramente documental.

La conexión entre categoría y conformidad es una de las fortalezas del ENS. Permite graduar el nivel de exigencia y evitar soluciones uniformes.

En términos de **comunicación**, el mensaje es sencillo y potente: **cuanto mayor sea el impacto potencial de un incidente, mayor debe ser el nivel de verificación**. Esta regla hace que el modelo sea razonable para las entidades obligadas, defendible desde el punto de vista jurídico y comprensible para terceros países.

Desde la **perspectiva de certificación**, **la categoría delimita también el alcance de la auditoría.** El auditor debe evaluar el sistema conforme a su categoría, medidas aplicables y, en su caso, perfil de cumplimiento específico. Por ello, una categorización incorrecta compromete todo el proceso. Si el sistema se categoriza por debajo de su impacto real, la auditoría y certificación podrían otorgar una confianza insuficiente. Si se categoriza por encima sin justificación, podrían imponerse cargas innecesarias.

Desde el **punto de vista de mercado**, **la diferenciación entre categorías ayuda a los proveedores**. Les permite conocer qué nivel de exigencia será esperable según el servicio prestado y el sistema afectado. También permite que las Administraciones incluyan requisitos proporcionados en pliegos y contratos. **La certificación ENS, adecuadamente vinculada a la categoría del sistema, se convierte así en un instrumento de confianza contractual.**

7.3. PROCEDIMIENTO DE AUDITORÍA

La auditoría es el mecanismo que permite verificar el cumplimiento del ENS mediante **una evaluación ordenada, objetiva y basada en evidencias**. Su finalidad no es sólo constatar la existencia de documentos o controles, sino comprobar si el sistema de información cumple de forma efectiva los requisitos aplicables a su categoría y si la entidad dispone de una organización de seguridad adecuada para mantener dicho cumplimiento en el tiempo.

El procedimiento de auditoría debe comenzar con una delimitación precisa del alcance. **Debe identificarse el sistema objeto de evaluación, los servicios soportados, la información tratada, la categoría del sistema, los activos relevantes, las medidas aplicables, los proveedores implicados y los límites de la evaluación**. Sin un alcance bien definido, la auditoría pierde valor, porque no resulta claro qué se ha evaluado ni qué confianza puede otorgarse al resultado. Tal y como se indicaba anteriormente, una

categorización del sistema y una declaración de aplicabilidad correctas tendrán un impacto en la determinación no solo del alcance del sistema sino también de los límites de la auditoría.

Una vez delimitado el alcance, la auditoría debe revisar la categorización del sistema y el análisis de riesgos. Esta revisión es esencial, porque de ella depende la selección de medidas y la intensidad de la evaluación. La auditoría no puede limitarse a verificar medidas preseleccionadas sin comprobar si la base sobre la que se han elegido es correcta. La coherencia entre categoría, riesgos, medidas y Declaración de Aplicabilidad es uno de los ejes de una auditoría ENS rigurosa.

La auditoría debe analizar también la política de seguridad, la organización de responsabilidades, los procedimientos internos, la gestión de personal, los controles de acceso, la protección de instalaciones, la adquisición y contratación de productos y servicios, la gestión de cambios, la continuidad, la monitorización, la gestión de incidentes, la protección de la información y la existencia de evidencias. El alcance exacto dependerá del sistema, su categoría y las medidas aplicables, pero la lógica general es siempre la misma: verificar que el ENS se ha implantado de manera real, documentada y mantenible, verificando además que existe un alineamiento entre los objetivos de la entidad en cuanto a sus funciones y competencias, y los objetivos marcados para la seguridad de la información.

La evaluación debe apoyarse en evidencias. La evidencia es lo que permite distinguir entre cumplimiento afirmado y cumplimiento demostrado. Puede consistir en documentación aprobada, registros de actividad, configuraciones, actas, informes, contratos, procedimientos, resultados de pruebas, planes de continuidad, registros de formación, informes de vulnerabilidades, evidencias de gestión de incidentes o cualquier otro elemento que permita sostener objetivamente el cumplimiento. En definitiva, se debe demostrar que la entidad está en disposición de cumplir una medida; que la cumple, de acuerdo a dicha intención y que ésta es eficaz en relación a los objetivos propuestos.

El informe de auditoría debe recoger los trabajos realizados, los criterios aplicados, las evidencias examinadas, los hallazgos identificados, las no conformidades detectadas y las conclusiones alcanzadas. Este informe es una herramienta de gran valor para la entidad. Permite conocer el grado real de cumplimiento, priorizar medidas correctoras, justificar inversiones, reforzar la trazabilidad de las decisiones y preparar la certificación o el mantenimiento de la conformidad.

La auditoría ENS no debe concebirse como un examen meramente sancionador o documental. Su valor principal es mejorar la seguridad.

> **Una auditoría bien realizada ayuda a identificar debilidades antes de que se conviertan en incidentes, a corregir desviaciones antes de que supongan incumplimientos, a elevar la madurez de la organización y a asegurar que el certificado, cuando se emite, descansa sobre una evaluación consistente.**

Desde el **punto de vista organizacional**, **la auditoría es un instrumento de aprendizaje institucional.**

En términos de **posicionamiento internacional**, **la auditoría refuerza la credibilidad del modelo español.** El ENS no confía únicamente en declaraciones internas, sino que exige verificación periódica y basada en evidencias. Esta característica permite presentar el modelo como una arquitectura de cumplimiento real, especialmente alineada con la creciente exigencia europea de diligencia demostrable, responsabilidad y gestión de riesgos.

7.4. PROCEDIMIENTO DE CERTIFICACIÓN

La certificación de conformidad con el ENS es el proceso mediante el cual se acredita formalmente que un sistema de información cumple los requisitos del Esquema Nacional de Seguridad aplicables a su categoría.

La certificación se apoya en la auditoría, pero no se confunde con ella. La auditoría verifica; la certificación reconoce formalmente la conformidad cuando los resultados de la evaluación lo permiten.

El procedimiento de certificación debe partir de un alcance claramente definido. El certificado debe identificar el sistema o sistemas cubiertos, la entidad titular o responsable, la categoría de seguridad, el alcance funcional, las condiciones aplicables y el periodo de validez. Esta precisión es esencial. Un certificado de conformidad no debe interpretarse como una garantía genérica de toda la organización, sino como **una evidencia relativa al sistema y alcance concretos que han sido evaluados.**

La entidad que solicita la certificación debe haber realizado previamente un proceso de adecuación al ENS. Esto incluye la categorización del sistema, el análisis de riesgos, la selección de medidas aplicables, la elaboración de la Declaración de Aplicabilidad, la implantación de controles, la preparación de evidencias, la organización de responsabilidades y la corrección de deficiencias detectadas.

La entidad de certificación debe evaluar la información disponible, revisar los resultados de auditoría, comprobar las evidencias, valorar las no conformidades y determinar si procede o no la emisión del certificado. Esta decisión debe adoptarse con independencia, competencia técnica y trazabilidad. La credibilidad del sistema ENS depende de que la certificación no se convierta en un trámite automático ni en una mera formalización comercial, sino en una decisión técnica fundamentada.

La certificación no sustituye al proceso de adecuación; lo culmina y lo somete a verificación externa.

La certificación tiene efectos relevantes:

- Para la **entidad certificada**, supone una evidencia de cumplimiento frente a ciudadanos, órganos de control, órganos de contratación, entidades públicas y clientes.
- Para los **proveedores privados**, puede operar como un elemento de acceso o posicionamiento en el mercado público digital.
- Para las **Administraciones contratantes**, permite disponer de una señal objetiva de seguridad.

- Para **terceros países**, muestra que España ha desarrollado un modelo de confianza basado en evaluación de la conformidad.

El certificado debe mantenerse en el tiempo. El sistema certificado puede cambiar, las medidas pueden degradarse, los proveedores pueden modificarse, los riesgos pueden evolucionar y las amenazas pueden intensificarse. Por ello, **la certificación debe vincularse a seguimiento, renovación, auditorías periódicas y gestión de cambios**. Un sistema que fue conforme en un momento determinado puede dejar de serlo si no mantiene sus controles y evidencias. Por tanto la certificación de la conformidad se convierte en una herramienta de medición de la mejora continua en los sistemas y en la seguridad.

Desde la **perspectiva institucional**, la certificación ENS constituye uno de los elementos más visibles del modelo. **Permite convertir la seguridad en un signo reconocible.** No obstante, el mensaje debe formularse con precisión: la certificación no es sólo un distintivo, sino el resultado de una arquitectura de categorización, medidas, auditoría, acreditación y seguimiento. Su valor está en todo el sistema que la sostiene.

7.5. VIGENCIA, SEGUIMIENTO, RENOVACIÓN, SUSPENSIÓN Y RETIRADA DE CERTIFICADOS

La Certificación de Conformidad no debe entenderse como un estado permanente e inalterable. Su valor depende de que el sistema evaluado mantenga en el tiempo las condiciones que justificaron la emisión del certificado.

> **El modelo ENS debe contemplarse como un ciclo de certificación, seguimiento y renovación, en el que la conformidad se conserva mediante control continuo, revisión periódica y corrección de desviaciones, en un claro ejemplo de aplicación del principio de mejora continua.**

La vigencia del certificado determina el periodo durante el cual la entidad puede utilizarlo como evidencia de conformidad, siempre que se mantengan las condiciones evaluadas. Durante ese periodo, la entidad debe conservar las medidas implantadas, gestionar cambios, mantener documentación, tratar incidentes, corregir no conformidades, actualizar evidencias y comunicar, cuando proceda, modificaciones relevantes que puedan afectar al alcance o validez de la certificación.

El seguimiento es esencial para evitar que la certificación se convierta en una fotografía estática. Un sistema certificado puede sufrir cambios técnicos, organizativos, contractuales o funcionales. Puede migrar a la nube, incorporar nuevos módulos, externalizar servicios, modificar proveedores, cambiar responsables, integrar nuevas plataformas o experimentar incidentes relevantes. Cada uno de estos cambios puede afectar a la conformidad. Por ello, la entidad debe mantener una gestión activa de la certificación.

La renovación implica una nueva evaluación del sistema, dirigida a comprobar si siguen cumpliéndose los requisitos aplicables. No debe ser tratada como una mera actualización formal del certificado, sino como una oportunidad para revisar la

madurez del sistema, incorporar lecciones aprendidas, corregir debilidades y adaptar las medidas al contexto actualizado de riesgos. La renovación refuerza la lógica de mejora continua del ENS.

La suspensión o retirada del certificado debe contemplarse como una consecuencia necesaria cuando se incumplen las condiciones de conformidad o cuando el sistema deja de reunir los requisitos exigibles. Esta posibilidad es esencial para preservar la credibilidad del modelo. Si los certificados no pudieran suspenderse o retirarse ante incumplimientos relevantes, perderían valor como garantía frente a terceros.

La **gestión de no conformidades** ocupa un lugar central en este proceso. Las no conformidades deben identificarse, clasificarse, documentarse, analizarse y corregirse mediante acciones adecuadas. La entidad debe demostrar que no se limita a recibir hallazgos de auditoría, sino que los transforma en acciones correctoras eficaces. La gestión de no conformidades es, por tanto, una evidencia de madurez organizativa.

Desde la **perspectiva del mercado y de la contratación pública**, la vigencia y mantenimiento del certificado son cuestiones críticas. **Un órgano de contratación no debería valorar únicamente la existencia de un certificado, sino su alcance, categoría, vigencia, sistema cubierto y condiciones de mantenimiento**. Del mismo modo, un proveedor debe asegurarse de que su certificación cubre realmente el servicio o sistema que ofrece.

Desde la **perspectiva de proyección internacional**, **esta dimensión permite reforzar la idea de que el ENS no es un modelo de certificación puntual, sino un sistema de confianza sostenida**. La confianza no se concede una vez para siempre; se mantiene mediante seguimiento, renovación y, cuando sea necesario, suspensión o retirada. Este enfoque resulta coherente con los modelos modernos de evaluación de la conformidad y con la evolución europea hacia la supervisión continua de la ciberseguridad.

7.6. ENTIDADES DE CERTIFICACIÓN DEL ENS

Las entidades de certificación del ENS desempeñan una función esencial dentro del ecosistema de confianza**. Son las encargadas de evaluar, en los términos aplicables, si un sistema de información cumple los requisitos del ENS y de emitir, cuando proceda, la Certificación de Conformidad**. Su intervención introduce un elemento externo de objetividad y refuerza la credibilidad del cumplimiento frente a terceros.

La función de estas entidades no puede entenderse como una mera prestación comercial. Actúan dentro de un modelo de confianza pública y, por tanto, **deben operar con independencia, imparcialidad, competencia técnica y sujeción a criterios de acreditación**. El certificado ENS sólo tendrá valor si quienes lo expiden ofrecen garantías suficientes de rigor, solvencia y trazabilidad. De lo contrario, el mercado de certificación podría debilitar la confianza que el ENS pretende generar.

Las entidades de certificación deben evaluar sistemas concretos, no organizaciones de manera genérica. Esto exige delimitar adecuadamente el alcance del certificado,

revisar la categoría del sistema, analizar la Declaración de Aplicabilidad, comprobar evidencias, valorar hallazgos y adoptar una decisión técnica motivada.

La precisión del alcance es especialmente importante en servicios externalizados, plataformas *cloud*, sistemas compartidos o proveedores que prestan múltiples servicios a distintas Administraciones.

El modelo ENS exige que las entidades de certificación estén acreditadas en el ámbito correspondiente. Esta exigencia permite garantizar que disponen de procedimientos adecuados, personal competente, independencia, mecanismos de decisión imparcial y capacidad para evaluar de forma consistente. La acreditación no sustituye al juicio técnico de la entidad de certificación, pero proporciona una garantía institucional sobre su competencia.

Las entidades de certificación tienen también un papel indirecto en la mejora del ecosistema. A través de sus evaluaciones, contribuyen a identificar errores recurrentes, problemas interpretativos, debilidades documentales, deficiencias de implantación y ámbitos en los que resulta necesario reforzar guías o criterios comunes. Su actividad forma parte del aprendizaje del modelo ENS.

Desde el punto de vista de las entidades públicas y privadas, la elección de una entidad de certificación debe hacerse con criterio. No se trata únicamente de seleccionar un proveedor, sino de elegir un actor que va a evaluar una pieza crítica de la confianza institucional. La calidad de la certificación depende de la competencia del equipo auditor, de la rigurosidad del proceso, de la correcta delimitación del alcance y de la consistencia de la decisión de certificación.

Desde la **perspectiva institucional**, **la existencia de entidades de certificación acreditadas permite mostrar que el ENS dispone de un mercado profesional de evaluación de la conformidad.** Este mercado no opera al margen del modelo público, sino integrado en él. Esa combinación de iniciativa especializada, acreditación y marco público refuerza la idea del ENS como ecosistema de confianza público-privado.

7.7. FUNCIÓN DE ENAC EN LA ACREDITACIÓN DE ENTIDADES DE CERTIFICACIÓN

La **Entidad Nacional de Acreditación (en adelante, ENAC)** desempeña un papel fundamental en la arquitectura de confianza del ENS. **Su función consiste en acreditar a las entidades de certificación que desean operar en el ámbito del Esquema Nacional de Seguridad, verificando que cumplen los requisitos de competencia técnica, imparcialidad, independencia y consistencia exigibles.** Esta intervención es esencial para que la certificación ENS sea creíble.

La acreditación no certifica directamente los sistemas de información sujetos al ENS. Su función es distinta: evalúa a quienes certifican.

ENAC actúa como garantía de segundo nivel. Mientras la entidad de certificación evalúa el sistema de información, ENAC evalúa la competencia de la entidad que certifica.

Esta estructura de niveles refuerza la confianza del conjunto: sistema evaluado, certificado emitido por entidad competente, entidad certificadora acreditada por el organismo nacional de acreditación.

Esta función es especialmente relevante para evitar una proliferación descontrolada de certificados sin garantías suficientes. Si cualquier entidad pudiera emitir certificados ENS sin acreditación, el valor del distintivo se degradaría rápidamente. La intervención de ENAC preserva la integridad del modelo, establece reglas de competencia, supervisa a las entidades acreditadas y contribuye a que los certificados expedidos tengan un valor homogéneo.

La acreditación aporta confianza a varios destinatarios:

- A las **entidades públicas**, porque pueden confiar en que las entidades certificadoras cumplen requisitos técnicos y de imparcialidad.
- A los **proveedores privados**, porque les permite obtener certificados emitidos por entidades reconocidas.
- A los **órganos de contratación**, porque les ofrece una base objetiva para aceptar certificaciones.
- A los **interlocutores internacionales**, porque conecta el ENS con prácticas reconocibles de evaluación de la conformidad.

La función de ENAC refuerza además la posición internacional del ENS. La acreditación es un lenguaje conocido en los mercados regulados y en los sistemas internacionales de evaluación de la conformidad. Señalar que la certificación ENS se apoya en entidades acreditadas facilita su comprensión fuera de España, permitiendo presentar el modelo como una arquitectura alineada con estándares internacionales de confianza y no como un procedimiento administrativo puramente nacional.

Desde una **perspectiva estratégica**, **ENAC aporta al ENS una garantía institucional de imparcialidad**. El CCN actúa como autoridad técnica de referencia en el ecosistema ENS; las entidades de certificación evalúan la conformidad de sistemas; ENAC acredita la competencia de dichas entidades; y las entidades obligadas aplican el marco. Esta distribución de funciones es uno de los elementos más sólidos del modelo.

El mensaje de valor es claro: **el ENS no sólo certifica sistemas, sino que acredita a quienes certifican**. Esa capa adicional de garantía es una de las razones por las que el modelo español puede presentarse como una infraestructura de confianza robusta, profesionalizada y susceptible de reconocimiento más allá del ámbito nacional.

7.8. USO DE UNE-EN ISO/IEC 17065 COMO NORMA DE REFERENCIA PARA LA ACREDITACIÓN DE ENTIDADES CERTIFICADORAS

La **norma UNE-EN ISO/IEC 17065** ocupa un lugar central en el sistema de acreditación de las entidades de certificación del ENS. **Esta norma establece requisitos para organismos que certifican productos, procesos y servicios, y proporciona un marco internacionalmente reconocible para evaluar la competencia, imparcialidad y consistencia de las entidades certificadoras.**

Su utilización en el ámbito ENS tiene una importancia estratégica. **Permite conectar el modelo español con una referencia internacional de evaluación de la conformidad.** Esto facilita que los certificados ENS se perciban como resultado de un proceso apoyado en estándares reconocibles y no como una práctica aislada o exclusivamente doméstica. Para interlocutores europeos e internacionales, esta conexión es especialmente relevante.

La UNE-EN ISO/IEC 17065 aporta garantías sobre aspectos esenciales del proceso de certificación. Entre ellos se encuentran la **independencia de la decisión de certificación, la imparcialidad frente a conflictos de interés, la competencia del personal, la gestión de procedimientos, la trazabilidad de las evaluaciones, la confidencialidad, la gestión de reclamaciones, el control de documentación y la consistencia de las decisiones**. Todos estos elementos son necesarios para que la certificación ENS tenga valor.

Debe destacarse que la acreditación conforme a esta norma no convierte a la entidad certificadora en responsable del cumplimiento permanente de la entidad certificada. La responsabilidad primaria de mantener la conformidad corresponde a la entidad titular o responsable del sistema. La entidad de certificación evalúa, verifica y certifica en un momento y bajo un alcance determinados. La acreditación asegura que dicha evaluación se realiza por un organismo competente.

Desde el **punto de vista del mercado**, **la referencia a ISO/IEC 17065 proporciona seguridad**. Las Administraciones pueden exigir certificaciones emitidas por entidades acreditadas; los proveedores pueden obtener certificados con reconocimiento técnico; los auditores pueden operar dentro de un marco consistente; y los órganos de contratación pueden valorar evidencias con mayor confianza.

Desde la **perspectiva internacional**, este punto debe destacarse con claridad. **El ENS es un modelo español, pero no cerrado sobre sí mismo. Su sistema de certificación dialoga con normas internacionales de evaluación de la conformidad.** Esto permite presentarlo como un modelo nacional con lenguaje internacional: una norma pública española, una certificación ENS y una acreditación basada en estándares reconocibles globalmente.

La utilización de UNE-EN ISO/IEC 17065 también **refuerza la profesionalización del ecosistema**. Obliga a las entidades certificadoras a mantener procedimientos, competencias, independencia y sistemas de gestión adecuados. De este modo, el ENS no sólo eleva la seguridad de las entidades certificadas, sino también la calidad del mercado de certificación.

7.9. NORMATIVA INTERNA DE ENAC APLICABLE A ENTIDADES ACREDITADAS O EN PROCESO DE ACREDITACIÓN

Además de la norma UNE-EN ISO/IEC 17065, el proceso de acreditación de entidades de certificación ENS se apoya en criterios, procedimientos y documentos específicos de ENAC. Estos documentos permiten adaptar la lógica general de la acreditación al esquema concreto de Certificación de Conformidad con el ENS. Su

función es ordenar cómo se solicita, evalúa, concede, mantiene y supervisa la acreditación en este ámbito.

La normativa interna de ENAC aplicable al esquema ENS es relevante porque concreta las expectativas sobre las entidades certificadoras. No basta con invocar genéricamente la norma ISO/IEC 17065. Es necesario determinar cómo se aplica al contexto específico del ENS, qué alcance de acreditación se solicita, qué competencias debe acreditar el personal, qué procedimientos deben existir, cómo se gestionan expedientes, cómo se toman decisiones de certificación, cómo se tratan conflictos de interés y cómo se mantienen las condiciones de acreditación.

Para entidades acreditadas o en proceso de acreditación, estos documentos tienen un valor operativo evidente. Les permiten conocer qué debe preparar la organización, qué evidencias debe aportar, qué requisitos debe cumplir su sistema de gestión, qué capacidades debe demostrar y qué mecanismos de supervisión puede esperar. La acreditación no es un acto puntual, sino un proceso continuo de evaluación y mantenimiento de competencia.

Desde el **punto de vista del ENS**, **esta normativa interna refuerza la coherencia del sistema de certificación**. Permite que las entidades certificadoras se sometan a criterios comunes y que la acreditación no dependa de interpretaciones informales. Esto contribuye a preservar la confianza de las entidades públicas y privadas que utilizan certificados ENS como evidencia de cumplimiento.

Desde el **punto de vista de los órganos de contratación y entidades usuarias**, **la existencia de criterios de acreditación específicos proporciona seguridad adicional**. Un certificado emitido por una entidad acreditada no se apoya sólo en la reputación de esa entidad, sino en un proceso estructurado de acreditación y supervisión. Esto permite que la certificación ENS sea utilizada con mayor seguridad jurídica y técnica.

Desde una **perspectiva de proyección internacional**, este punto **permite explicar que el ENS no sólo dispone de un modelo de certificación, sino también de reglas para acreditar y controlar a quienes certifican**. Esta capa de confianza es especialmente importante para interlocutores extranjeros, porque permite comprender que el sistema no depende de certificadores no supervisados, sino de un organismo nacional de acreditación y de criterios específicos aplicables al esquema.

7.10. IMPARCIALIDAD, COMPETENCIA TÉCNICA, TRAZABILIDAD Y SUPERVISIÓN

La confianza en el sistema ENS depende de cuatro **garantías esenciales**: **imparcialidad, competencia técnica, trazabilidad y supervisión**. Estas garantías afectan tanto a la auditoría como a la certificación y acreditación. Sin ellas, la conformidad podría convertirse en una práctica formal, inconsistente o carente de valor frente a terceros.

La imparcialidad exige que la entidad que certifica actúe sin conflictos de interés y sin comprometer la independencia de su decisión. Esta exigencia es especialmente relevante cuando una misma organización presta servicios de consultoría, adecuación,

auditoría o certificación en ámbitos próximos. El sistema debe evitar que quien ayuda a implantar el cumplimiento acabe validando sin independencia el resultado de su propia actuación. La separación de funciones y la gestión de conflictos de interés son esenciales para preservar la credibilidad del certificado.

La competencia técnica exige que las personas y organizaciones que auditan o certifican dispongan de conocimientos suficientes sobre el ENS, seguridad de la información, gestión de riesgos, auditoría, sistemas de información, medidas del Anexo II, evidencias, contratación tecnológica, servicios externalizados y, cuando proceda, cloud, continuidad, incidentes y protección de datos. La certificación ENS no puede ser una revisión superficial; requiere capacidad técnica real.

La trazabilidad implica que las decisiones adoptadas durante el proceso de auditoría y certificación deben estar documentadas y ser reconstruibles. Debe poder saberse qué sistema se evaluó, con qué alcance, bajo qué categoría, qué medidas eran aplicables, qué evidencias se revisaron, qué hallazgos se detectaron, cómo se trataron las no conformidades y por qué se concedió, mantuvo, suspendió o retiró un certificado. La trazabilidad protege a la entidad certificada, al certificador, al órgano de contratación y al propio modelo ENS.

La supervisión garantiza que el sistema no se degrade. ENAC supervisa a las entidades acreditadas; las entidades de certificación realizan seguimiento de los certificados; las auditorías periódicas revisan la conformidad; y el propio ecosistema ENS dispone de espacios de coordinación y criterios técnicos para mantener coherencia. Esta supervisión es la que permite que la certificación no sea una foto fija, sino una garantía sometida a control.

Estas cuatro garantías tienen un **valor jurídico, técnico y reputacional**. **Jurídico**, porque permiten defender la validez y utilidad de la certificación como evidencia de cumplimiento. **Técnico**, porque aseguran que la evaluación se realiza con rigor. **Reputacional**, porque preservan la confianza del mercado y de las Administraciones. Estratégico, porque permiten presentar el ENS como un modelo serio ante otros países.

Desde la **perspectiva institucional**, conviene formular esta idea con claridad:



Figura 7.1 Cadena de confianza de las Certificaciones de conformidad con el ENS

El valor de un certificado ENS no reside únicamente en el documento emitido, sino en la cadena de confianza que lo sostiene:
Categorización → Medidas → Evidencias → Auditoría → Certificación → Acreditación → Seguimiento → Supervisión.
Cuanto más sólida sea esa cadena, mayor será el valor nacional e internacional del ENS.

7.11. VALOR DE LA ACREDITACIÓN PARA LA CONFIANZA NACIONAL E INTERNACIONAL DEL ENS

La acreditación aporta al ENS una dimensión de confianza que resulta especialmente valiosa en el plano nacional e internacional. En el **plano nacional**, **permite que Administraciones, entidades públicas, proveedores privados y órganos de contratación confíen en que las certificaciones de conformidad han sido emitidas por entidades técnicamente competentes e imparciales**. En el **plano internacional, facilita la comprensión del modelo español mediante categorías reconocibles en los sistemas globales de evaluación de la conformidad.**

El valor nacional de la acreditación se manifiesta, en primer lugar, en la **seguridad jurídica**. Cuando una Administración exige certificación ENS en un contrato, debe poder confiar en que esa certificación ha sido emitida por una entidad competente. La acreditación aporta esa garantía. En segundo lugar, se manifiesta en la **homogeneidad del mercado**. Las entidades certificadoras acreditadas deben operar bajo criterios comunes, lo que reduce la dispersión y facilita la comparabilidad. En tercer lugar, se

manifiesta en la protección del valor del distintivo ENS. Si la certificación se emitiera sin control suficiente, el distintivo perdería credibilidad.

Para los proveedores privados, la acreditación también tiene **valor competitivo.** Obtener una certificación ENS emitida por una entidad acreditada permite demostrar solvencia, madurez y capacidad de cumplir requisitos de seguridad exigibles en el mercado público digital. Esta certificación puede ser especialmente relevante para proveedores cloud, desarrolladores, integradores, operadores de servicios gestionados, consultoras tecnológicas y empresas que tratan información pública o soportan servicios públicos.

Para las entidades públicas, la acreditación contribuye a **profesionalizar la relación con proveedores**. Permite incorporar la conformidad ENS en pliegos y contratos con mayor precisión, exigir evidencias objetivas y reducir la dependencia de declaraciones unilaterales. Esto mejora la gestión de riesgos de la cadena de suministro y refuerza la seguridad de los servicios externalizados.

En el **plano internacional**, la acreditación **permite presentar el ENS como un modelo comprensible para otros Estados, instituciones europeas y organizaciones internacionales**. La certificación basada en entidades acreditadas conforme a normas internacionales ofrece un lenguaje común. Otros países pueden reconocer más fácilmente un modelo que combina norma pública, evaluación de sistemas, Certificación de Conformidad y acreditación de certificadores.

Este punto es especialmente importante para la proyección europea del ENS.

En un entorno en el que la Unión Europea impulsa normas sobre ciberseguridad, resiliencia, certificación, seguridad de proveedores y gestión de riesgos, el ENS puede presentarse como una experiencia nacional madura que ya incorpora mecanismos de conformidad verificable y acreditación.

La acreditación permite reforzar la tesis de que…

… el ENS no es un marco puramente interno, sino un modelo con vocación de interoperabilidad conceptual con los sistemas europeos e internacionales de confianza.

La acreditación también aporta **reputación al Estado**. **Un país que dispone de un esquema nacional de seguridad con certificación y acreditación puede mostrar que su Administración digital se apoya en garantías verificables**. Esto tiene valor para la confianza ciudadana, para la contratación pública, para la cooperación internacional y para la posición de España en debates europeos sobre certificación y gobernanza de la ciberseguridad.

En definitiva, la acreditación es una de las claves del sistema de confianza del ENS.

La entidad certificada demuestra cumplimiento; la entidad de certificación emite una certificación; ENAC acredita la competencia del certificador; y el conjunto del sistema genera una confianza que puede ser utilizada en el mercado, en la Administración y en la proyección internacional del modelo español.

A fin de estructurar la implementación del marco normativo en la gestión de compras y licitaciones, la siguiente tabla detalla las exigencias recomendables del ENS a lo largo del **ciclo contractual**:

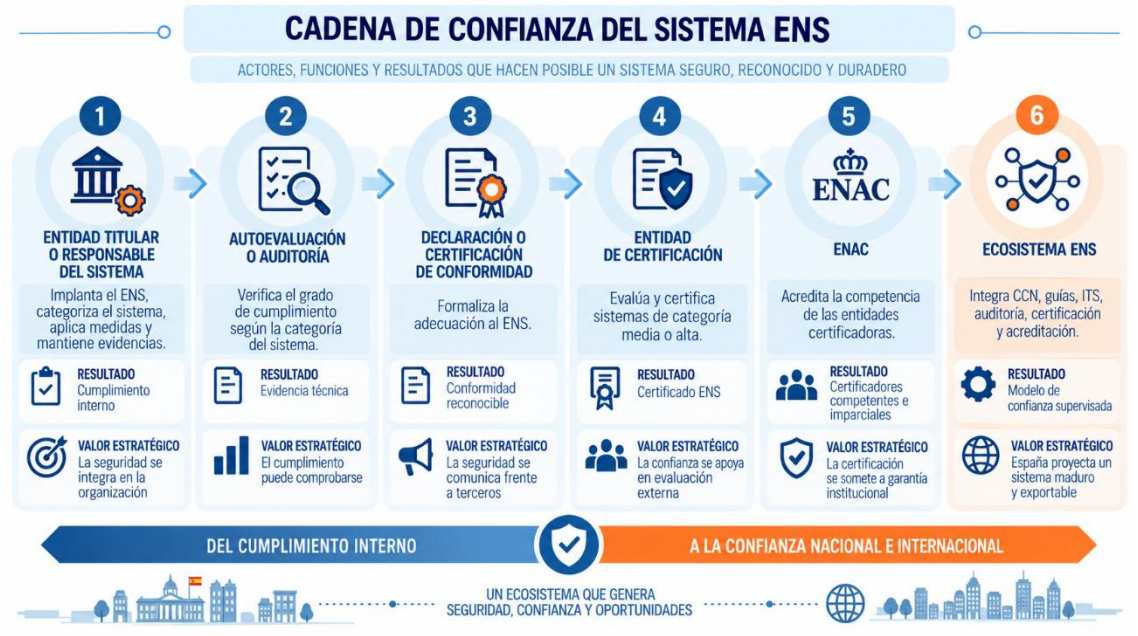


Figura 7.2 Cadena de confianza del sistema ENS

En la tabla siguiente se identifican los principales riesgos derivados de una mala integración del ENS en la contratación pública y las correspondientes medidas correctoras:

Elemento	Declaración de Conformidad	Certificación de Conformidad
Categoría ordinariamente vinculada	Sistemas de categoría básica	Sistemas de categoría media o alta
Mecanismo principal	Autoevaluación y declaración responsable de la entidad	Auditoría y evaluación por entidad certificadora
Intensidad de verificación	Interna	Externa
Valor principal	Transparencia y responsabilidad	Confianza reforzada frente a terceros
Uso habitual	Acreditar cumplimiento en sistemas de menor impacto	Acreditar cumplimiento en sistemas de mayor criticidad
Riesgo a evitar	Declaración formal sin evidencias suficientes	Certificación entendida como mero distintivo comercial
Mensaje de valor	La entidad asume y publica su conformidad	Un tercero competente verifica la conformidad

Tabla 7.3 Declaración de Conformidad y Certificación de Conformidad

A continuación, se ilustra conceptualmente la función de la contratación pública como motor de tracción de la ciberseguridad y generador de confianza en el ecosistema público-privado:



Figura 7.4 Del cumplimiento interno a la confianza internacional

7.12 RESUMIENDO…

La auditoría, la certificación y la acreditación constituyen el sistema de confianza del ENS.

2.1 La auditoría verifica el cumplimiento;
2.2 La Declaración y la Certificación de Conformidad lo hacen visible;
2.3 Las entidades de certificación aportan evaluación externa;
2.4 ENAC acredita la competencia de quienes certifican; y
2.5 El seguimiento, la renovación, la suspensión o retirada de certificados preservan la credibilidad del modelo en el tiempo.

Este sistema permite que el ENS vaya más allá del cumplimiento interno. **Una entidad no sólo aplica medidas, sino que puede demostrar que las aplica. Un proveedor no sólo afirma que es seguro, sino que puede acreditar la conformidad de sus sistemas. Un órgano de contratación no sólo exige seguridad, sino que puede apoyarse en evidencias verificables. Un país no sólo declara que protege su Administración digital, sino que puede mostrar un modelo estructurado de confianza.**

Este es uno de los argumentos más potentes para la proyección del ENS en Europa y fuera de Europa. **España dispone de un marco que combina regulación, gestión de riesgos, medidas de seguridad, auditoría, certificación, acreditación y mejora continua**. Esa arquitectura convierte al ENS en un modelo de confianza pública digital,

útil para proteger servicios, disciplinar proveedores, profesionalizar el mercado y ofrecer una referencia avanzada de gobernanza de la ciberseguridad.

8. EL ENS COMO MODELO DE CONFIANZA PARA LA CONTRATACIÓN PÚBLICA Y LA COLABORACIÓN PÚBLICO-PRIVADA

El Esquema Nacional de Seguridad no opera únicamente dentro del perímetro interno de las entidades públicas. Una de sus funciones más relevantes es proyectar las **exigencias de seguridad sobre el conjunto de relaciones mediante las cuales el sector público obtiene, desarrolla, externaliza, mantiene o explota servicios digitales.** En una Administración crecientemente dependiente de proveedores tecnológicos, plataformas cloud, servicios gestionados, desarrolladores, integradores, consultoras, centros de proceso de datos, soluciones SaaS, servicios de soporte, comunicaciones y cadenas de suministro complejas, la seguridad pública ya no puede garantizarse sólo mediante controles internos. Debe extenderse, de forma jurídicamente ordenada y técnicamente verificable, a los sistemas que soportan la prestación efectiva de los servicios públicos digitales.

Esta es una de las aportaciones más importantes del Real Decreto 311/2022, de 3 de mayo. Su artículo 2.3 establece que…

> **… el ENS se aplica también a los sistemas de información de las entidades del sector privado cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.**

La norma añade, además, que **los pliegos de prescripciones administrativas o técnicas de los contratos celebrados por entidades del sector público deben contemplar los requisitos necesarios para asegurar la conformidad con el ENS** de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, incluyendo, cuando proceda, la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS.

El valor estratégico de esta previsión es notable. El ENS convierte la contratación pública en una palanca de ciberseguridad.

> **Permite que la exigencia de seguridad no se detenga en la Administración contratante, sino que alcance a los proveedores que participan en la prestación del servicio, a los sistemas que utilizan, a las plataformas que operan y, cuando resulte necesario conforme al análisis de riesgos, a su propia cadena de suministro.**

De este modo, **el ENS actúa como instrumento de gobernanza contractual, disciplina del mercado tecnológico y construcción de confianza público-privada.**

Desde una **perspectiva técnica**, **el ENS permite exigir medidas de seguridad proporcionadas a la categoría del sistema y al riesgo real del servicio contratado.** Desde una **perspectiva jurídica, proporciona una base normativa para incorporar obligaciones de conformidad, evidencias, auditoría, notificación de incidentes, continuidad, subcontratación y seguimiento en los pliegos y contratos.** Desde una **perspectiva organizativa**, **obliga a que responsables de contratación, responsables de**

seguridad, responsables del sistema, responsables jurídicos y unidades promotoras trabajen de forma coordinada. Desde una **perspectiva institucional**, **permite presentar a España como un país que no sólo regula la seguridad de su sector público, sino que crea un mercado público digital basado en confianza verificable.**

Este epígrafe analiza precisamente esa dimensión: el ENS como modelo de confianza para la contratación pública y para la colaboración público-privada. Su finalidad es mostrar que la certificación ENS puede ser una evidencia de cumplimiento y madurez, pero también advertir frente al riesgo de convertirla en un requisito puramente formal, desvinculado del sistema, del servicio, del contrato y del riesgo real.

8.1. INCORPORACIÓN DEL ENS EN PLIEGOS, CONTRATOS Y ENCARGOS PÚBLICOS

La incorporación del ENS a la contratación pública debe realizarse desde el diseño del expediente contractual, no como una cláusula añadida al final del proceso. Cuando el objeto del contrato incluya servicios tecnológicos, desarrollo o mantenimiento de aplicaciones, alojamiento, explotación de infraestructuras, servicios cloud, comunicaciones, servicios gestionados de seguridad, soporte, tratamiento de información pública o cualquier otra actividad que pueda sostener servicios públicos digitales, el órgano de contratación debe analizar si los sistemas de información del adjudicatario quedan dentro del ámbito funcional del ENS.

El punto de partida debe ser la identificación del servicio público o función administrativa afectada. No se trata de exigir el ENS de forma indiscriminada a todo contratista, sino de determinar si el contrato implica que sistemas del proveedor sustenten servicios prestados por la entidad pública, traten información pública, intervengan en procesos administrativos o formen parte de la infraestructura necesaria para el ejercicio de competencias y potestades administrativas**. Esta aproximación funcional permite aplicar el ENS con proporcionalidad y seguridad jurídica.**

Los pliegos deben concretar el alcance de la obligación. Una referencia genérica al "cumplimiento del ENS" puede resultar insuficiente. **Conviene precisar qué sistemas o servicios quedan afectados, qué categoría de seguridad se estima aplicable o cómo deberá determinarse, qué medidas o requisitos mínimos deberán cumplirse, qué declaración o certificación de conformidad deberá aportarse, en qué momento, con qué alcance, con qué vigencia y respecto de qué sistema concreto**.

La seguridad contractual exige precisión.

También debe establecerse **qué evidencias deberán aportarse durante la licitación y cuáles durante la ejecución**. En algunos casos podrá exigirse que la certificación ENS exista ya en el momento de presentar la oferta, especialmente cuando el servicio dependa de una plataforma ya operativa. En otros, podrá admitirse un compromiso de obtención de conformidad en un plazo determinado, siempre que ello sea compatible con el riesgo del servicio y la continuidad de la prestación. La decisión debe justificarse en función del objeto contractual y del análisis de riesgos.

Los pliegos deben prever igualmente obligaciones de mantenimiento de la conformidad durante toda la vida del contrato. No basta con aportar un certificado al inicio. El sistema puede cambiar, el proveedor puede modificar su arquitectura, subcontratar componentes, migrar servicios, introducir nuevas herramientas, cambiar centros de datos, renovar tecnología o sufrir incidentes. Por ello, el contrato debe exigir que la conformidad se mantenga, que se comuniquen cambios relevantes y que se aporten evidencias actualizadas cuando proceda.

En encargos a medios propios, convenios, acuerdos interadministrativos u otras fórmulas de colaboración pública, el ENS también debe integrarse adecuadamente. La forma jurídica de la relación no debe ocultar la realidad funcional: si un sistema soporta servicios públicos digitales o trata información dentro del ámbito del ENS, la seguridad debe estar prevista, asignada, documentada y verificada.

Desde el punto de vista de **posicionamiento institucional**, esta capacidad de incorporar el ENS a pliegos y contratos es uno de los grandes activos del modelo. **Permite convertir la contratación pública en un instrumento de transformación del mercado. Los proveedores que quieran operar con el sector público deben acreditar seguridad, madurez, evidencias y capacidad de mantener la conformidad. Esto eleva el nivel general del ecosistema tecnológico.**

8.2. PROVEEDORES TECNOLÓGICOS Y PRESTADORES DE SERVICIOS EXTERNALIZADOS

Los proveedores tecnológicos desempeñan un papel cada vez más relevante en la prestación de servicios públicos digitales. Desarrollan aplicaciones, alojan plataformas, gestionan infraestructuras, prestan soporte, operan servicios, monitorizan sistemas, proporcionan soluciones de seguridad, tratan información, administran bases de datos, mantienen redes, suministran software y participan en procesos esenciales para la continuidad administrativa. Esta realidad exige que la seguridad se proyecte sobre ellos de forma clara y exigible.

El ENS permite ordenar esa proyección. No convierte automáticamente a todo proveedor en sujeto obligado en términos absolutos, pero sí somete al marco ENS los sistemas de información de las entidades privadas cuando, en virtud de una relación contractual, presten servicios o provean soluciones a entidades del sector público para el ejercicio de sus competencias y potestades administrativas. La clave está en el sistema y en el servicio, no en una etiqueta genérica del proveedor.

Esta aproximación tiene especial valor jurídico. Evita tanto la infraaplicación como la sobrerregulación. La infraaplicación se produciría si la Administración entendiera que la externalización desplaza fuera del ENS los sistemas del proveedor. La sobrerregulación se produciría si se exigiera conformidad ENS a cualquier actividad empresarial sin conexión real con servicios públicos o información sometida al ámbito del ENS. El criterio correcto es funcional: deben quedar cubiertos los sistemas que sostienen el servicio público o la solución contratada.

La relación con proveedores debe incorporar obligaciones claras: cumplimiento del

ENS, política de seguridad, medidas de seguridad aplicables, declaración o certificación de conformidad, cooperación en auditorías, conservación y entrega de evidencias, notificación de incidentes, continuidad, reversibilidad, control de subcontratistas, confidencialidad, protección de datos, ubicación de la información, trazabilidad de accesos y gestión de cambios.

La externalización no elimina la responsabilidad de la entidad pública sobre la seguridad del servicio. Puede trasladar la ejecución de determinadas funciones, pero no la necesidad de gobernar el riesgo. Por ello, **el contrato debe asegurar que la entidad pública mantiene capacidad de supervisión, acceso a evidencias, derecho de auditoría o verificación, información sobre subcontratación y mecanismos de respuesta ante incidentes.**

Para los proveedores, el ENS puede convertirse en un activo competitivo. La conformidad o certificación ENS demuestra que el proveedor dispone de sistemas adecuados para operar en el mercado público digital. Permite diferenciarse frente a competidores, facilitar la participación en licitaciones, reducir fricciones contractuales y generar confianza en los órganos de contratación.

Bien comunicado, el ENS no es sólo una carga regulatoria, sino un elemento de posicionamiento empresarial.

Para las Administraciones, trabajar con proveedores alineados con el ENS reduce riesgos de seguridad, mejora la trazabilidad contractual, facilita auditorías y contribuye a elevar la madurez del servicio. Para el conjunto del mercado, crea un lenguaje común entre Administración, empresas, auditores y certificadores. Esta es una de las razones por las que el ENS debe presentarse como modelo de colaboración público-privada: no se limita a imponer obligaciones al proveedor, sino que crea un marco compartido de confianza.

8.3. SERVICIOS CLOUD Y SERVICIOS GESTIONADOS DE SEGURIDAD

Los servicios cloud y los servicios gestionados de seguridad merecen una atención específica. La nube aporta escalabilidad, flexibilidad, eficiencia, resiliencia potencial, innovación y acceso a capacidades tecnológicas avanzadas. Los servicios gestionados de seguridad permiten a muchas entidades disponer de monitorización, detección, respuesta, análisis, gestión de vulnerabilidades y soporte especializado que difícilmente podrían mantener por sí solas. Sin embargo, **ambos modelos introducen dependencias, concentración de riesgos, complejidad contractual, subcontratación, problemas de trazabilidad y retos de soberanía, continuidad y control.**

El ENS ofrece un marco para gestionar estos riesgos, siempre que se incorpore desde el diseño del servicio y desde la fase contractual.

En **servicios cloud**, **deben analizarse cuestiones como el modelo de servicio —IaaS, PaaS, SaaS u otros—, el reparto de responsabilidades entre proveedor y cliente, la ubicación de datos, la subcontratación, la administración de accesos, la segregación de entornos, la continuidad, la reversibilidad, la portabilidad, la gestión de incidentes, la conservación de evidencias, el cifrado, la monitorización y la capacidad de auditoría.**

En servicios gestionados de seguridad, deben definirse con precisión las obligaciones del proveedor: alcance de la monitorización, fuentes de información, tratamiento de registros, tiempos de detección y respuesta, comunicación de alertas, clasificación de incidentes, escalado, custodia de evidencias, coordinación con CCN-CERT o INCIBE-CERT cuando proceda, confidencialidad, personal autorizado, herramientas empleadas y régimen de subcontratación.

Una dificultad habitual en servicios cloud es la tendencia a confundir la certificación del proveedor con la conformidad del sistema concreto que soporta el servicio público. Una plataforma cloud puede disponer de certificaciones, pero el cumplimiento ENS debe analizarse en relación con el sistema, servicio, configuración, responsabilidades y uso concreto. La seguridad real depende de cómo se configura y opera la solución, qué medidas corresponden al proveedor, cuáles a la entidad pública y cuáles son compartidas.

Por ello, **el contrato debe incluir matrices de responsabilidad**. Estas matrices permiten identificar qué parte asume cada medida o control: proveedor cloud, proveedor de servicios gestionados, entidad pública, integrador, desarrollador u otro subcontratista. Sin esta delimitación, pueden aparecer zonas grises que comprometan la seguridad y dificulten la auditoría. El modelo de responsabilidad compartida debe documentarse y vincularse a evidencias verificables.

Los servicios cloud y gestionados pueden ser una oportunidad para fortalecer el ENS. Permiten escalar capacidades, profesionalizar servicios, mejorar la resiliencia y facilitar la obtención de evidencias, siempre que se gestionen con rigor contractual y técnico. El riesgo no está en la externalización como tal, sino en la externalización sin gobierno, sin control, sin evidencias y sin claridad sobre responsabilidades.

Desde una **perspectiva institucional**, **el ENS puede presentarse como un marco especialmente útil para ordenar la adopción segura de servicios cloud y gestionados en el sector público. No bloquea la innovación, sino que la disciplina**. Permite contratar tecnología avanzada sin renunciar a gobernanza, trazabilidad, auditoría y conformidad. Esta combinación es especialmente atractiva en Europa, donde la confianza en proveedores cloud, la resiliencia y la autonomía estratégica ocupan un lugar central en la agenda digital.

8.4. CONTROL DE LA CADENA DE SUMINISTRO

La cadena de suministro tecnológica es uno de los principales vectores de riesgo en la ciberseguridad contemporánea. Un servicio público digital puede depender de múltiples capas: proveedor principal, subcontratistas, fabricantes de software, proveedores cloud, operadores de comunicaciones, servicios de soporte, componentes de código abierto, servicios de identidad, herramientas de monitorización, APIs, integradores y plataformas de terceros. Una debilidad en cualquiera de esas capas puede afectar a la seguridad del servicio final.

El Real Decreto 311/2022 reconoce expresamente esta realidad al extender la cautela sobre los requisitos ENS a la cadena de suministro de los contratistas, en la medida necesaria y de acuerdo con los resultados del análisis de riesgos. Esta

previsión es estratégica. Permite que la seguridad contractual no se detenga en el adjudicatario principal, sino que alcance a los actores que realmente intervienen en la prestación del servicio cuando su participación tenga relevancia para el riesgo.

El control de la cadena de suministro exige **identificar subcontratistas críticos, componentes relevantes, ubicaciones de procesamiento, flujos de información, dependencias operativas, accesos privilegiados, servicios de soporte remoto, herramientas de administración, proveedores de continuidad y terceros con capacidad de afectar a la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad del sistema.** Esta identificación debe formar parte del análisis de riesgos y del diseño contractual.

Los contratos deben regular la subcontratación con precisión. Deben prever autorización previa o comunicación de subcontratistas relevantes, obligación de trasladar requisitos ENS cuando proceda, conservación de evidencias, cooperación en auditorías, notificación de incidentes que afecten a subcontratistas, restricciones de acceso, requisitos de confidencialidad, medidas de continuidad y capacidad de sustitución o reversibilidad.

Una cadena de suministro opaca es incompatible con una seguridad verificable. La entidad pública no necesita conocer todos los detalles comerciales irrelevantes del proveedor, pero sí debe disponer de información suficiente para valorar riesgos, verificar cumplimiento y reaccionar ante incidentes. El equilibrio entre confidencialidad empresarial y control público debe resolverse mediante cláusulas proporcionadas, pero no mediante renuncia al control.

El control de la cadena de suministro tiene también una dimensión de mercado. Si el ENS se exige adecuadamente, los proveedores principales tenderán a seleccionar subcontratistas más maduros, a mejorar sus propios procesos de seguridad y a documentar mejor sus relaciones. Esto produce un efecto expansivo: la exigencia de seguridad en la contratación pública eleva la seguridad del ecosistema empresarial que la rodea.

Desde la **perspectiva internacional**, este es uno de los argumentos más potentes para presentar el ENS como modelo avanzado. Muchos Estados están preocupados por la seguridad de sus cadenas de suministro digitales. **El ENS ofrece una respuesta clara: incorporar la seguridad al contrato, exigir conformidad, vincular la cadena de suministro al análisis de riesgos y convertir la certificación y las evidencias en instrumentos de control**. Esta lógica convierte la contratación pública en política pública de ciberseguridad.

8.5. BENEFICIOS PARA ENTIDADES PÚBLICAS

Para las entidades públicas, el ENS aporta beneficios que van más allá del cumplimiento normativo.

El ENS:



Figura 8.1 Beneficios del ENS para las entidades públicas

Desde una **perspectiva estratégica**, **el ENS ayuda a que las entidades públicas compren mejo**r. No se limita a imponer seguridad, sino que proporciona un marco para definir, exigir, verificar y mantener requisitos de seguridad. Esto convierte al ENS en una herramienta de profesionalización de la contratación pública tecnológica.

8.6. BENEFICIOS PARA EMPRESAS PRIVADAS PROVEEDORAS DEL SECTOR PÚBLICO

Para las **empresas privadas**, el ENS puede percibirse inicialmente como una carga regulatoria. Sin embargo, bien entendido, **constituye también una oportunidad de posicionamiento en el mercado público digital.** La conformidad o certificación ENS permite demostrar que una empresa dispone de sistemas, procesos y controles adecuados para prestar servicios a entidades públicas con garantías de seguridad.

El primer beneficio para las empresas es la **diferenciación competitiva**. En licitaciones donde el ENS sea exigible o valorable, disponer de conformidad adecuada puede facilitar el acceso al contrato, reducir incertidumbres y mejorar la posición del proveedor frente a competidores menos maduros. La seguridad se convierte en atributo de calidad y confianza.

El segundo beneficio es la **profesionalización interna**. Prepararse para el ENS obliga a la empresa a ordenar su política de seguridad, categorizar sistemas, gestionar riesgos, documentar medidas, controlar accesos, mejorar continuidad, gestionar incidentes, revisar subcontratistas y conservar evidencias. Estas mejoras no sólo sirven para contratar con el sector público; elevan la madurez general de la organización.

El tercer beneficio es la **reducción de fricción contractual**. Un proveedor que dispone de certificación ENS sobre el sistema adecuado puede responder con mayor rapidez a exigencias de órganos de contratación, auditorías, solicitudes de evidencias o procesos de homologación. Esto reduce costes de transacción y facilita relaciones a largo plazo con entidades públicas.

El cuarto beneficio es **reputacional**. La certificación ENS puede utilizarse como señal de confianza ante clientes, socios, inversores y otras Administraciones. En un mercado donde la ciberseguridad es cada vez más relevante, demostrar conformidad con un marco público exigente puede aportar valor comercial.

El quinto beneficio es la **preparación frente a otras obligaciones regulatorias**. La implantación del ENS puede ayudar a ordenar capacidades que también resultan útiles en marcos europeos o sectoriales relacionados con gestión de riesgos, seguridad de redes y sistemas, protección de datos, resiliencia operativa, servicios cloud o continuidad. Aunque el ENS no sustituye automáticamente esos marcos, sí proporciona una base de madurez.

Un beneficio estratégico fundamental para las empresas es que el ENS se perfila actualmente como la **vía maestra para el cumplimiento de la Directiva NIS2**. Conforme al Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, se prevé que el Perfil de Cumplimiento Específico del ENS se configure como un mecanismo válido para acreditar el cumplimiento de las medidas de gestión de riesgos exigidas por la normativa europea. Esta integración permitirá a los proveedores privados utilizar su certificación nacional (especialmente en categoría Alta) como evidencia sólida de madurez ante requerimientos de la Unión Europea, reduciendo drásticamente las duplicidades de auditoría y los costes de cumplimiento para operar en el mercado único digital.

El sexto beneficio es la **mejora de la relación con subcontratistas**. Las empresas proveedoras que deben responder ante la Administración por la seguridad de su cadena de suministro tenderán a exigir mejores prácticas a sus propios proveedores. Esto puede fortalecer el ecosistema empresarial y reducir riesgos operativos.

Desde la **perspectiva institucional** del ENS, este punto debe comunicarse con claridad: **el ENS no sólo impone obligaciones a las empresas, sino que crea un mercado de confianza**. Las empresas que invierten en seguridad y certificación pueden

obtener ventajas competitivas. La Administración gana proveedores más seguros. El mercado gana reglas más claras. El ciudadano gana servicios públicos digitales más confiables.

8.7. RIESGOS DE CUMPLIMIENTO MERAMENTE FORMAL

El principal riesgo en la incorporación del ENS a la contratación pública es convertirlo en un requisito formal, documental o meramente reputacional. Esto ocurre cuando los pliegos exigen "cumplir el ENS" sin concretar el sistema afectado, la categoría aplicable, las medidas exigibles, la declaración o certificación necesaria, las evidencias requeridas, el régimen de subcontratación, la notificación de incidentes o los mecanismos de supervisión durante la ejecución.

También se produce cumplimiento formal cuando se exige una certificación ENS sin comprobar su alcance real. Un certificado puede referirse a un sistema distinto del que se utilizará en el contrato, a una categoría insuficiente, a un servicio parcial o a una plataforma que no cubre la configuración concreta ofrecida. En estos casos, la certificación puede generar una falsa sensación de seguridad.

Otro riesgo es **utilizar el ENS como barrera injustificada de acceso al mercado**. La exigencia de conformidad debe ser proporcionada al objeto del contrato, al riesgo y al sistema afectado. Requisitos excesivos, mal justificados o desconectados de la prestación pueden restringir la competencia sin mejorar realmente la seguridad. La correcta aplicación del ENS exige equilibrio: rigor en sistemas relevantes y proporcionalidad en servicios de menor impacto.

Existe igualmente **riesgo de cumplimiento inicial sin mantenimiento**. Un proveedor puede aportar evidencias al inicio de la licitación, pero modificar después la arquitectura del servicio, cambiar subcontratistas, alterar ubicaciones de datos o degradar controles sin comunicación adecuada. Por ello, el contrato debe prever seguimiento, actualización de evidencias, comunicación de cambios y consecuencias ante pérdida de conformidad.

En **servicios cloud, el riesgo formal puede consistir en asumir que la certificación del proveedor cloud cubre automáticamente cualquier uso que la entidad haga de la plataforma**. La realidad es más compleja. El cumplimiento depende de la configuración, del reparto de responsabilidades, de los controles activados, de la gestión de identidades, del cifrado, de la monitorización, de la continuidad y del servicio concreto. La certificación del proveedor es relevante, pero no sustituye el análisis del sistema.

Otro riesgo es **no controlar la cadena de suministro**. El adjudicatario principal puede cumplir determinados requisitos, pero apoyarse en subcontratistas críticos que no estén sometidos a obligaciones equivalentes. El artículo 2.3 del Real Decreto 311/2022 permite extender cautelas a la cadena de suministro conforme al análisis de riesgos. No utilizar esta posibilidad en contratos relevantes puede dejar expuesto el servicio.

Finalmente, existe un **riesgo de desconexión entre contratación y seguridad**. Si los responsables de seguridad no participan en la preparación de pliegos, si los servicios jurídicos desconocen el alcance técnico, si la unidad promotora no identifica correctamente el sistema o si el órgano de contratación no traduce los requisitos en cláusulas verificables, el ENS puede quedar mal incorporado. El resultado será un contrato aparentemente seguro, pero difícil de supervisar.

8.8. BUENAS PRÁCTICAS CONTRACTUALES

Un elenco razonable de requisitos contractuales debe contemplar las siguientes buenas prácticas:

1. **Realizar un análisis previo del alcance ENS antes de redactar los pliegos.** La unidad promotora, el responsable de seguridad, el responsable del sistema, los servicios jurídicos y el órgano de contratación deben identificar si el contrato afecta a sistemas de información sujetos al ENS, qué servicios se prestan, qué información se trata, qué categoría resulta aplicable, qué proveedores intervienen y qué riesgos deben gestionarse.
2. **Evitar cláusulas genéricas**. El pliego debe concretar el sistema o servicio afectado, la categoría de seguridad, la declaración o certificación exigible, el plazo para aportarla, el alcance que debe cubrir, las evidencias requeridas, el régimen de mantenimiento, la obligación de comunicar cambios, las consecuencias de pérdida de conformidad y los mecanismos de supervisión. La precisión contractual es una condición de seguridad.
3. **Utilizar matrices de responsabilidad**. En contratos con proveedores cloud, servicios gestionados, integradores o subcontratistas, debe identificarse qué medidas corresponden a cada actor. Esta matriz debe alinearse con la Declaración de Aplicabilidad y con el análisis de riesgos. Sin reparto claro de responsabilidades, las medidas pueden quedar sin dueño.
4. **Exigir evidencias proporcionadas**. La certificación ENS puede ser una evidencia relevante, pero no siempre será suficiente por sí sola. Puede ser necesario solicitar Declaración de Aplicabilidad, alcance del certificado, informes de auditoría en la medida procedente, planes de continuidad, procedimientos de incidentes, compromisos de subcontratación, registros de pruebas, cláusulas de reversibilidad o evidencias de configuración segura. La exigencia debe ser proporcionada y compatible con la protección de información sensible del proveedor.
5. **Regular la notificación de incidentes.** El contrato debe establecer plazos, canales, información mínima, obligación de cooperación, conservación de evidencias, comunicación de incidentes de subcontratistas y coordinación con los centros de respuesta que correspondan. La gestión de incidentes no puede improvisarse durante la crisis.
6. **Regular la subcontratación**. Deben identificarse subcontratistas críticos, exigir autorización o comunicación previa cuando proceda, trasladar obligaciones de

seguridad, prever derechos de auditoría o acceso a evidencias, y establecer consecuencias ante incumplimientos. La cadena de suministro debe formar parte del contrato, no quedar fuera de él.

7. **Prever continuidad, reversibilidad y salida ordenada.** La seguridad del servicio público no depende sólo de la prestación ordinaria, sino también de la capacidad de mantener o recuperar el servicio ante incidentes, incumplimientos, finalización del contrato o sustitución del proveedor. Las cláusulas de reversibilidad, portabilidad de datos, entrega de documentación, conservación de evidencias y asistencia en transición son esenciales.

8. **Incorporar mecanismos de seguimiento durante la ejecución**. El contrato debe prever reuniones de seguridad, actualización periódica de evidencias, revisión de certificados, auditorías, informes de cumplimiento, comunicación de cambios y tratamiento de no conformidades. La seguridad contractual no termina con la adjudicación.

9. **Coordinar ENS y protección de datos cuando el servicio implique tratamiento de datos personales**. Deben alinearse las obligaciones del ENS con el Reglamento General de Protección de Datos, la Ley Orgánica 3/2018 y, en su caso, la Ley Orgánica 7/2021. La seguridad ENS puede apoyar el cumplimiento del artículo 32 del RGPD, pero no sustituye por sí sola el conjunto de obligaciones de protección de datos.

10. **Utilizar el ENS como criterio de calidad del mercado público digital**. Cuando se incorpora correctamente, el ENS permite seleccionar proveedores más maduros, reducir riesgos, mejorar servicios, profesionalizar la contratación y generar confianza. Esta debe ser la idea final: la contratación pública no sólo compra tecnología; también compra seguridad, continuidad, trazabilidad y confianza.

11. **Procurar que los pliegos garanticen la independencia técnica y la imparcialidad del proceso de certificación**. Conforme a la Guía CCN-CERT IC-02/20 Guía para la contratación de auditorías de certificaciones del ENS, no es admisible que una empresa consultora encargada de la adecuación subcontrate, a su vez, a la Entidad de Certificación que realizará la auditoría. Este conflicto de interés invalidaría la certificación, por lo que el órgano de contratación debe asegurar que la auditoría de certificación se contrate de forma independiente a cualquier servicio de consultoría previo, ya sea mediante lotes separados o licitaciones independientes en el tiempo.

12. **Garantizar la Integración de la Sostenibilidad** (Principio DNSH)**.** En cumplimiento de la disposición adicional tercera del ENS los pliegos de contratación relacionados con el ENS, especialmente aquellos vinculados a proyectos financiados con fondos del Plan de Recuperación, Transformación y Resiliencia (PRTR), deben incorporar de forma preceptiva el respeto al principio de «no causar un perjuicio significativo» al medioambiente (DNSH). Esto conlleva que la adquisición de componentes tecnológicos y la contratación de servicios derivados de las medidas de seguridad del Esquema deben cumplir

con los criterios de etiquetado climático y digital de la Unión Europea, integrando de forma efectiva la resiliencia ciber con la sostenibilidad institucional.

A fin de estructurar la implementación del marco normativo en la gestión de compras y licitaciones, la siguiente tabla detalla las exigencias recomendables del ENS a lo largo del ciclo contractual:

Fase contractual	Pregunta clave	Exigencia ENS recomendable	Resultado esperado
Preparación del contrato	¿El servicio o solución afecta a sistemas sujetos al ENS?	Análisis previo de alcance, información, servicio, categoría y riesgo	Pliego proporcionado y jurídicamente sólido
Redacción de pliegos	¿Qué debe exigirse al proveedor?	Requisitos ENS concretos, declaración/certificación, evidencias y medidas aplicables	Obligaciones claras y verificables
Licitación	¿Cómo se acredita la capacidad del licitador?	Certificación o compromiso de conformidad, alcance del certificado, solvencia técnica y plan de adecuación	Selección de proveedores más confiables
Adjudicación y formalización	¿Qué queda obligado a cumplir el adjudicatario?	Cláusulas de seguridad, responsabilidades, subcontratación, incidentes, continuidad y auditoría	Contrato alineado con el riesgo del servicio
Ejecución	¿Se mantiene la conformidad durante el contrato?	Seguimiento, actualización de evidencias, auditorías, comunicación de cambios y no conformidades	Seguridad sostenida, no sólo inicial
Finalización o transición	¿Cómo se protege el servicio al terminar el contrato?	Reversibilidad, portabilidad, devolución o destrucción de información, conservación de evidencias	Continuidad y salida ordenada

Figura 8.2 Incorporación del ENS al ciclo contractual

En la tabla expuesta a continuación se identifican los principales riesgos derivados de una mala integración del ENS en la contratación pública y las correspondientes medidas correctoras:

Riesgo	Consecuencia	Medida correctora
Cláusula genérica de "cumplimiento ENS"	Inseguridad jurídica y dificultad de supervisión	Concretar sistema, categoría, medidas, evidencias y conformidad exigible
Certificado ENS no alineado con el servicio	Falsa apariencia de cumplimiento	Verificar alcance, categoría, sistema cubierto y vigencia del certificado

Riesgo	Consecuencia	Medida correctora
Falta de control de subcontratistas	Riesgo oculto en la cadena de suministro	Regular subcontratación crítica y traslado de obligaciones ENS
Ausencia de seguimiento durante la ejecución	Conformidad sólo inicial	Exigir evidencias periódicas, auditorías, comunicación de cambios y mantenimiento
Servicios cloud sin matriz de responsabilidad	Zonas grises de cumplimiento	Definir responsabilidades entre entidad, proveedor cloud, integrador y subcontratistas
Incidentes no regulados contractualmente	Respuesta tardía o descoordinada	Establecer plazos, canales, evidencias y obligaciones de cooperación
Requisitos desproporcionados	Restricción de competencia sin mejora real de seguridad	Ajustar exigencias al objeto, categoría y análisis de riesgos
Falta de coordinación interna	Pliegos técnicamente incompletos o jurídicamente débiles	Involucrar seguridad, sistemas, contratación, jurídico y unidad promotora

Figura 8.3 Riesgos de mala incorporación del ENS y medidas correctoras

A continuación, se ilustra conceptualmente la función de la contratación pública como motor de tracción de la ciberseguridad y generador de confianza en el ecosistema público-privado:



Figura 8.4 La contratación pública como palanca de confianza ENS

8.9. RESUMIENDO…

El ENS es una herramienta especialmente potente para la contratación pública y la colaboración público-privada. Su artículo 2.3 permite proyectar sus exigencias sobre los sistemas de información de entidades privadas que prestan servicios o proveen soluciones al sector público, y exige que los pliegos incorporen los requisitos necesarios para asegurar la conformidad con el ENS de los sistemas que sustenten los servicios contratados. Esta previsión convierte al ENS en un instrumento de gobernanza contractual.

Su valor no reside sólo en exigir certificados, sino en ordenar la seguridad del servicio contratado: identificar el sistema, determinar su categoría, exigir medidas proporcionadas, controlar proveedores y subcontratistas, regular incidentes, mantener evidencias, supervisar la ejecución y garantizar continuidad.

El ENS permite pasar de la contratación tecnológica a la contratación confiable.

Para las **entidades públicas**, **el ENS reduce riesgos, mejora la calidad de los contratos, facilita la supervisión y refuerza la diligencia institucional**. Para las **empresas privadas**, **crea un mercado de confianza en el que la seguridad y la certificación pueden convertirse en ventajas competitivas**. Para el **conjunto del ecosistema**, **eleva la madurez de la cadena de suministro**. Y para la **proyección internacional**, **ofrece un mensaje claro: el modelo ENS demuestra cómo la contratación pública puede utilizarse como palanca de ciberseguridad, confianza digital y colaboración público-privada responsable.**

9. ALINEAMIENTO EUROPEO E INTERNACIONAL DEL ENS

El Esquema Nacional de Seguridad es modelo nacional sólidamente alineado con las principales tendencias europeas e internacionales en materia de ciberseguridad, resiliencia, gestión de riesgos, certificación y confianza digital. Su valor no reside únicamente en ser un marco obligatorio para el sector público español y para determinados proveedores privados vinculados a la prestación de servicios públicos digitales. Su relevancia estratégica deriva también de su **capacidad para dialogar con otros marcos regulatorios y técnicos, especialmente con la Directiva NIS2, el Reglamento de Ciberseguridad de la Unión Europea, los esquemas europeos de certificación, las normas ISO/IEC 27001 e ISO/IEC 27002, la norma ISO/IEC 17065 y el Reglamento General de Protección de Datos.**

El ENS no es una singularidad española desconectada del contexto europeo, sino que constituye una experiencia nacional avanzada que anticipa y concreta muchas de las exigencias que hoy caracterizan la política europea de ciberseguridad: enfoque basado en riesgos, responsabilidad organizativa, medidas técnicas y organizativas proporcionadas, gestión de incidentes, continuidad, auditoría, certificación, control de proveedores, mejora continua y confianza verificable.

En este sentido, **el ENS constituye una infraestructura nacional de confianza digital compatible con la evolución del Derecho de la Unión.**

Esta compatibilidad no significa equivalencia automática ni sustitución plena de otros marcos. El ENS tiene su propio ámbito de aplicación, su propia lógica normativa y su propio sistema de certificación de conformidad. NIS2, el Reglamento de Ciberseguridad, el RGPD, las normas ISO y los futuros esquemas europeos de certificación tienen funciones distintas. No obstante, existe una clara convergencia conceptual: todos ellos buscan elevar la madurez de la ciberseguridad, ordenar la gestión de riesgos, reforzar la responsabilidad de las entidades y generar confianza en productos, servicios, sistemas y organizaciones.

Desde una **perspectiva técnica**, **el ENS aporta una metodología concreta para proteger sistemas de información mediante categorización, medidas de seguridad, auditoría y conformidad**. Desde una **perspectiva jurídica**, **ofrece un marco obligatorio y verificable**. Desde una **perspectiva organizativa**, **introduce roles, políticas, responsabilidades, gestión de riesgos y mejora continua.** Desde una **perspectiva institucional**, **permite presentar a España como un Estado que dispone de un modelo maduro, operativo y exportable de gobernanza pública de la ciberseguridad.**

La finalidad de este epígrafe es situar el ENS dentro de ese ecosistema europeo e internacional. Para ello, se analizará su relación con los principales marcos normativos y técnicos de referencia, destacando tanto las conexiones como las diferencias. El objetivo no es afirmar que el ENS sustituye a todos esos marcos, sino mostrar que puede operar como un instrumento nacional complementario, interoperable en términos conceptuales y útil para reforzar la posición española en Europa.

9.1. ENS Y DIRECTIVA NIS2

La Directiva (UE) 2022/2555, conocida como Directiva NIS2, constituye una de las piezas centrales del marco europeo de ciberseguridad. Su finalidad es alcanzar un elevado nivel común de ciberseguridad en la Unión mediante obligaciones aplicables a entidades esenciales e importantes, medidas de gestión de riesgos, notificación de incidentes, supervisión y responsabilidad. Aunque su ámbito subjetivo y funcional no coincide plenamente con el del ENS, existe una clara afinidad entre ambos modelos.

La NIS2 se orienta principalmente a sectores esenciales e importantes, incluyendo energía, transporte, banca, infraestructuras de mercados financieros, salud, agua potable, aguas residuales, infraestructuras digitales, gestión de servicios TIC, administración pública, espacio, servicios postales, gestión de residuos, fabricación, producción y distribución de productos químicos, producción y distribución de alimentos, fabricación de determinados productos, proveedores digitales y otros sectores. Su lógica es sectorial y de resiliencia sistémica. **El ENS, en cambio, se articula en torno a la seguridad de los sistemas de información que soportan la actuación del sector público, la prestación de servicios públicos digitales y determinados servicios o soluciones prestados por proveedores privados al sector público.**

En el ámbito financiero, el ENS presenta una alta convergencia con **el Reglamento (UE) 2022/2554 (DORA)**. Si bien DORA constituye la *lex specialis* para el sector financiero, el ENS proporciona a los organismos públicos con competencias en este mercado y a sus proveedores tecnológicos un marco de controles técnicos y

organizativos que facilitan el cumplimiento de las obligaciones de gestión de riesgos TIC, notificación de incidentes y vigilancia de terceros proveedores exigidos por el reglamento europeo. Esta alineación permite que las entidades financieras sujetas a ambas normativas puedan reutilizar las evidencias de cumplimiento del ENS para satisfacer gran parte de los requerimientos de resiliencia operativa digital de la Unión Europea.

La diferencia de ámbito no impide una fuerte convergencia. Tanto NIS2 como ENS se basan en la gestión de riesgos. Ambos exigen medidas técnicas, operativas y organizativas adecuadas. Ambos otorgan importancia a la continuidad, la gestión de incidentes, la seguridad de la cadena de suministro, la responsabilidad de la organización y la mejora continua.

La NIS2 establece un marco europeo de obligaciones para entidades esenciales e importantes; el ENS proporciona, en el ámbito español, una metodología concreta de seguridad, categorización, medidas, auditoría y conformidad.

El ENS puede desempeñar una función especialmente útil respecto de las entidades del sector público incluidas en NIS2. En la medida en que la Administración pública forma parte del ámbito de la Directiva, el ENS ofrece un marco nacional ya consolidado para articular medidas de seguridad, gestión de riesgos, responsabilidades y verificación. No sustituye por sí solo a la transposición ni a la aplicación completa de NIS2, pero puede servir como instrumento práctico de cumplimiento y como base nacional para demostrar madurez en seguridad.

También es relevante la coincidencia en materia de proveedores y cadena de suministro. NIS2 refuerza la atención a la seguridad de proveedores y prestadores de servicios TIC. **El ENS, por su parte, proyecta sus exigencias sobre entidades privadas que prestan servicios o proveen soluciones al sector público, e impone que los pliegos incorporen requisitos para asegurar la conformidad con el ENS cuando los sistemas sustenten los servicios contratados**. Esta coincidencia permite presentar el ENS como una herramienta nacional idónea para aplicar, en el sector público español, la lógica europea de gestión del riesgo de terceros.

La notificación de incidentes es otro punto de conexión. NIS2 refuerza el régimen europeo de comunicación de incidentes significativos. El ENS dispone de una Instrucción Técnica de Seguridad específica sobre notificación de incidentes, que ordena la comunicación y gestión de incidentes en sistemas afectados. De nuevo, no existe identidad plena, pero sí convergencia funcional: ambos modelos entienden que la resiliencia exige detectar, comunicar, gestionar y aprender de los incidentes.

Desde una perspectiva de **posicionamiento europeo**, el mensaje debe ser claro: **el ENS es un marco nacional ya operativo que comparte la lógica de NIS2 y puede facilitar su aplicación en el sector público español.**

La existencia de un modelo como el ENS permite a España presentarse ante la Unión Europea no como un Estado que parte de cero, sino como un Estado que ya cuenta con una arquitectura avanzada de seguridad pública digital, auditoría, certificación y mejora continua.

9.2. ENS Y REGLAMENTO DE CIBERSEGURIDAD DE LA UNIÓN EUROPEA

El **Reglamento (UE) 2019/881, conocido como Reglamento de Ciberseguridad o Cybersecurity Act (CSA),** reforzó el mandato de ENISA y estableció un marco europeo de certificación de la ciberseguridad para productos, servicios y procesos TIC. Su objetivo es crear esquemas europeos de certificación que permitan aumentar la confianza en el mercado digital y facilitar el reconocimiento de garantías de ciberseguridad en la Unión.

El ENS y el Reglamento de Ciberseguridad responden a lógicas distintas, pero complementarias. El Reglamento europeo se centra en la creación de esquemas de certificación de productos, servicios y procesos TIC a escala de la Unión. El ENS se centra en la seguridad de sistemas de información que soportan servicios públicos digitales y en la conformidad de dichos sistemas con un marco nacional de seguridad. El primero tiene una vocación horizontal europea en materia de certificación TIC; el segundo tiene una función nacional de gobernanza, cumplimiento y certificación de sistemas en el ámbito público y público-privado.

La complementariedad entre la CSA y el ENS es evidente.
Los esquemas europeos de certificación pueden aportar garantías sobre productos, servicios o procesos TIC concretos.
El ENS, por su parte, permite evaluar cómo esos productos, servicios o procesos se integran en un sistema de información determinado, con una categoría, una Declaración de Aplicabilidad, unas medidas, unos responsables, unos proveedores, unos riesgos y un servicio público concreto.

La certificación de un producto o servicio no sustituye automáticamente la conformidad ENS del sistema en el que se integra; pero puede constituir una evidencia relevante dentro de ese sistema.

El Reglamento de Ciberseguridad proporciona, además, un lenguaje europeo de certificación, niveles de garantía y evaluación de la conformidad. El ENS puede dialogar con ese lenguaje desde su propio sistema de certificación nacional.

La existencia de entidades de certificación acreditadas, la utilización de la UNE-EN ISO/IEC 17065 y la intervención de ENAC permiten presentar el esquema de certificación ENS como un modelo nacional compatible conceptualmente y equivalente funcionalmente con la cultura europea de evaluación de la conformidad.

Desde la perspectiva de España, este punto tiene importancia estratégica. **El ENS no debe presentarse como competidor de los esquemas europeos de certificación, sino como complemento nacional equivalente**. Allí donde un esquema europeo certifique un producto, servicio o proceso TIC, el ENS puede seguir siendo necesario para verificar la seguridad del sistema concreto que soporta un servicio público. Del mismo modo, allí donde el ENS exige medidas o evidencias, una certificación europea puede ayudar a acreditar determinados componentes de seguridad.

En términos de **proyección internacional**, esta relación permite formular un mensaje equilibrado:

El ENS no pretende sustituir los esquemas europeos, sino integrarse conceptualmente

con ellos. Su valor reside en cubrir una dimensión diferente: la seguridad del sistema público digital en su contexto organizativo, contractual y operativo.

Esa dimensión sistémica es precisamente una de las fortalezas del modelo español.

9.3. ENS Y ESQUEMAS EUROPEOS DE CERTIFICACIÓN DE CIBERSEGURIDAD

El desarrollo de esquemas europeos de certificación de ciberseguridad es una de las líneas más relevantes de la política europea. El primer esquema europeo adoptado ha sido el EUCC, basado en Common Criteria, mediante el Reglamento de Ejecución (UE) 2024/482 de la Comisión. Este esquema establece disposiciones de aplicación del Reglamento de Ciberseguridad en relación con la certificación basada en criterios comunes.

La existencia del EUCC y el futuro desarrollo de otros esquemas europeos obligan a situar correctamente el ENS. El ENS no es un esquema europeo de certificación adoptado conforme al Reglamento de Ciberseguridad. Es un marco nacional de seguridad y conformidad de sistemas de información. Sin embargo, puede relacionarse con los esquemas europeos de varias formas:

1º. **Los esquemas europeos pueden proporcionar evidencias relevantes para el cumplimiento ENS**. Si un producto, servicio o componente TIC cuenta con una certificación europea aplicable, esa certificación puede ser considerada en el análisis de riesgos, en la selección de medidas, en la contratación y en la auditoría ENS, siempre que el certificado cubra efectivamente el componente, uso y nivel de garantía necesarios. La certificación europea no sustituye por sí sola la adecuación del sistema, pero puede reforzarla.

2º. **El ENS puede actuar como marco integrador**. Un sistema de información público puede estar compuesto por productos, servicios y procesos certificados bajo esquemas europeos, pero seguirá necesitando gobernanza, categorización, responsabilidades, configuración segura, controles operacionales, medidas organizativas, gestión de incidentes, continuidad y auditoría. El ENS proporciona ese marco sistémico.

3º. **El ENS puede servir de referencia para defender la utilidad de los esquemas nacionales en el ecosistema europeo**. La creación de esquemas europeos no elimina la necesidad de marcos nacionales que regulen la seguridad de la Administración digital, la contratación pública, la conformidad de sistemas y la gestión de proveedores. La seguridad pública digital requiere tanto garantías sobre componentes como garantías sobre sistemas y servicios concretos.

4º**. La experiencia española puede contribuir al debate europeo sobre reconocimiento, equivalencia o interoperabilidad entre marcos nacionales y esquemas europeos**. El ENS dispone de elementos que facilitan esa conversación: categorización por impacto, medidas de seguridad, auditoría, certificación, acreditación de entidades certificadoras, guías técnicas y herramientas públicas de apoyo.

El principal riesgo en esta materia sería confundir planos. Una certificación europea de producto no equivale automáticamente a una certificación ENS del sistema; y una certificación ENS no equivale necesariamente a una certificación europea de producto, servicio o proceso TIC. Cada certificado responde a un objeto, alcance, metodología y finalidad distintos. La clave está en construir relaciones de complementariedad y uso cruzado de evidencias.

Desde la **perspectiva institucional**, la conclusión es clara:

> **El ENS permite a España entrar en el debate europeo de certificación desde una posición de madurez. España dispone de un modelo nacional que ya utiliza certificación, acreditación y auditoría para generar confianza. Esa experiencia puede proyectarse como contribución al desarrollo de una Europa digital segura y resiliente.**

9.4. ENS E ISO/IEC 27001 E ISO/IEC 27002

Las normas ISO/IEC 27001 e ISO/IEC 27002 constituyen referencias internacionales ampliamente utilizadas en materia de sistemas de gestión de seguridad de la información y controles de seguridad. **ISO/IEC 27001** establece requisitos para implantar, mantener y mejorar un sistema de gestión de seguridad de la información. **ISO/IEC 27002** proporciona un catálogo de controles y orientaciones para su aplicación. Ambas normas son instrumentos reconocidos globalmente y forman parte del lenguaje internacional de la ciberseguridad corporativa.

El ENS comparte con estas normas varios elementos: gestión de riesgos, mejora continua, medidas de seguridad, documentación, responsabilidades, evaluación, auditoría y orientación a la protección de la información. Sin embargo, no debe confundirse con ellas. El ENS es un marco jurídico-técnico obligatorio en su ámbito de aplicación, regulado por el Derecho español, con categorización de sistemas, medidas del Anexo II, declaración o certificación de conformidad y un ecosistema propio de guías, ITS, herramientas, auditoría y acreditación. ISO/IEC 27001 es una norma internacional de sistema de gestión, generalmente adoptada de forma voluntaria salvo que una norma o contrato la exija.

La relación entre ENS e ISO/IEC 27001 puede ser muy positiva. Una organización que disponga de un sistema de gestión de seguridad de la información conforme a ISO/IEC 27001 contará normalmente con elementos útiles para abordar el ENS: análisis de riesgos, política de seguridad, gestión documental, mejora continua, auditoría interna, gestión de activos, control de accesos, continuidad, incidentes y revisión por la dirección. No obstante, deberá mapear esos elementos con las exigencias específicas del ENS, su categorización, medidas y requisitos de conformidad.

ISO/IEC 27002 puede ayudar a interpretar o reforzar controles técnicos y organizativos, pero tampoco sustituye al Anexo II del ENS. Las medidas del ENS tienen su propio contexto normativo y deben aplicarse conforme a la categoría del sistema, la Declaración de Aplicabilidad y las guías CCN-STIC. Las normas ISO pueden ser complementarias, pero la conformidad ENS exige cumplir el marco ENS.

Esta relación de complementariedad es útil para empresas privadas que ya trabajan con estándares ISO. Para ellas, el ENS puede explicarse como un marco específico del sector público español que puede apoyarse en capacidades ya existentes, pero que exige una adaptación propia. Este mensaje reduce barreras de entrada: el ENS no es incompatible con ISO, sino que puede aprovechar estructuras de gestión ya maduras.

Para interlocutores internacionales, la conexión con ISO/IEC 27001 e ISO/IEC 27002 facilita la comprensión del ENS. Permite explicar que el modelo español comparte lenguaje y principios con estándares globales, pero añade una dimensión pública: obligatoriedad normativa, categorización nacional, medidas específicas, auditoría, certificación de conformidad y papel del CCN. Esta combinación de lenguaje internacional y especificidad nacional refuerza la posición del ENS como modelo exportable.

9.5. ENS, ISO/IEC 17065 Y ACREDITACIÓN DE CERTIFICADORES

La norma ISO/IEC 17065 es especialmente relevante para el sistema de certificación del ENS porque establece requisitos para organismos que certifican productos, procesos y servicios. En el modelo ENS, esta norma sirve como referencia para la acreditación de entidades de certificación de conformidad, reforzando la competencia técnica, imparcialidad, independencia y trazabilidad del sistema.

La utilización de ISO/IEC 17065 aporta al ENS una conexión directa con el lenguaje internacional de evaluación de la conformidad. Esto es estratégicamente importante.

La certificación ENS no se presenta como una simple declaración administrativa interna, sino como un proceso apoyado en entidades certificadoras acreditadas conforme a una norma reconocible internacionalmente.

Esta característica facilita la confianza de órganos de contratación, proveedores, autoridades, instituciones europeas y terceros países.

La **acreditación de certificadores** permite distinguir entre dos **niveles de garantía**. En el primer nivel, **el sistema de información es auditado y certificado conforme al ENS**. En el segundo, **la entidad que certifica es acreditada para demostrar que tiene competencia técnica y actúa con imparcialidad**. Esta cadena de confianza es uno de los elementos diferenciales del modelo español: no sólo se evalúa el sistema; también se controla a quien evalúa.

La conexión con ISO/IEC 17065 es especialmente útil para la proyección europea e internacional del ENS. Los organismos de acreditación y los esquemas de evaluación de la conformidad utilizan un lenguaje común basado en normas ISO/IEC. Presentar el ENS desde esa perspectiva permite que interlocutores extranjeros comprendan rápidamente la seriedad del modelo. No se trata de un certificado sin supervisión, sino de un esquema apoyado en acreditación.

Conviene destacar, no obstante, que ISO/IEC 17065 no define por sí misma las medidas ENS ni el contenido material del cumplimiento. Su función es establecer requisitos para los organismos certificadores. El contenido de la certificación procede

del Real Decreto 311/2022, de las ITS, de las guías CCN-STIC y del esquema de certificación aplicable. Esta distinción debe mantenerse para evitar confusiones.

Desde la **perspectiva institucional,** este punto es especialmente potente:

El ENS combina contenido normativo nacional con garantía internacional de evaluación de la conformidad. Esa combinación refuerza su credibilidad y facilita su defensa como modelo de referencia para otros Estados que quieran crear esquemas nacionales de ciberseguridad certificable.

9.6. ENS Y REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

El Reglamento General de Protección de Datos ocupa un lugar relevante en cualquier análisis de seguridad de la información, porque su artículo 32 exige al responsable y al encargado del tratamiento aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. Entre esas medidas se incluyen, cuando proceda, la seudonimización y cifrado, la capacidad de garantizar confidencialidad, integridad, disponibilidad y resiliencia permanentes, la capacidad de restaurar la disponibilidad y acceso a los datos personales en caso de incidente y un proceso de verificación, evaluación y valoración regular de la eficacia de las medidas.

La relación entre ENS y RGPD es especialmente estrecha cuando los sistemas sometidos al ENS tratan datos personales.

El ENS proporciona un marco de medidas, organización, auditoría y gestión de riesgos que puede contribuir al cumplimiento de las obligaciones de seguridad del tratamiento.

En particular, la categorización, las dimensiones de seguridad, la protección de la información, el control de accesos, la trazabilidad, la gestión de incidentes, la continuidad y la auditoría son elementos directamente útiles para acreditar diligencia en materia de protección de datos.

No obstante, el ENS no sustituye por completo al RGPD. El RGPD regula un régimen más amplio: licitud del tratamiento, transparencia, derechos de las personas, responsabilidad proactiva, encargados del tratamiento, transferencias internacionales, evaluaciones de impacto, registro de actividades, brechas de seguridad de datos personales y supervisión por autoridades de protección de datos. El ENS puede apoyar la dimensión de seguridad, pero no cubre por sí solo todo el cumplimiento de protección de datos.

La **conexión práctica** se produce especialmente en tres ámbitos:

1º. **Análisis de riesgos**: el ENS analiza riesgos para la información y los servicios; el RGPD exige considerar riesgos para los derechos y libertades de las personas. En sistemas que tratan datos personales, ambos análisis deben coordinarse.

2º. **Contratación con encargados del tratamiento**: el RGPD exige que el responsable recurra únicamente a encargados que ofrezcan garantías suficientes; la conformidad

ENS puede ser una evidencia relevante cuando el encargado presta servicios sujetos al ENS.

3º. **Gestión de incidentes y brechas**: un incidente de seguridad ENS puede constituir también una brecha de datos personales que active obligaciones específicas de notificación a la autoridad de control y, en su caso, a los interesados.

Desde la **perspectiva institucional, la relación ENS-RGPD permite presentar el ENS como un instrumento que refuerza la confianza en el tratamiento público de datos.** Los ciudadanos esperan que sus datos sean tratados por Administraciones y proveedores con garantías. El ENS proporciona un marco verificable de seguridad que puede contribuir a esa confianza, especialmente en servicios públicos digitales intensivos en datos.

En el **plano internacional**, esta conexión es relevante porque el RGPD se ha convertido en una referencia global. **Explicar que el ENS puede apoyar la seguridad del tratamiento bajo el RGPD facilita su comprensión por terceros países y organizaciones internacionales. Permite presentar el modelo español como un marco que no sólo protege servicios, sino también información y derechos.**

9.7. EL ENS COMO MODELO NACIONAL COMPLEMENTARIO A MARCOS EUROPEOS E INTERNACIONALES

El ENS configura un modelo nacional complementario a los marcos europeos e internacionales, no como un sistema cerrado ni autosuficiente. Su valor reside en que cubre un espacio específico: la seguridad de los sistemas de información que soportan la Administración digital y determinados servicios o soluciones vinculados al sector público. Desde ese espacio, puede interactuar con NIS2, Cybersecurity Act, EUCC, RGPD, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 17065 y otros marcos sectoriales.

La complementariedad puede explicarse mediante una idea sencilla: **los marcos europeos e internacionales proporcionan obligaciones, estándares o esquemas de certificación en distintos planos; el ENS permite integrarlos en la seguridad concreta de sistemas públicos digitales**. NIS2 aporta una lógica de resiliencia y gestión de riesgos para entidades esenciales e importantes. El Cybersecurity Act aporta el marco europeo de certificación TIC. EUCC certifica determinados productos TIC bajo Common Criteria. ISO/IEC 27001 aporta un sistema de gestión. ISO/IEC 27002 aporta controles. ISO/IEC 17065 aporta garantías sobre organismos certificadores. El RGPD exige seguridad del tratamiento de datos personales. El ENS conecta esos elementos con la protección concreta de sistemas del sector público español.

Esta posición complementaria tiene gran valor estratégico. Permite defender que **los marcos nacionales no son obstáculos a la armonización europea, sino instrumentos necesarios para hacerla operativa en contextos concretos**. La Unión Europea establece objetivos, obligaciones y esquemas comunes; los Estados necesitan marcos nacionales que los implementen, coordinen y adapten a sus estructuras administrativas, contractuales y tecnológicas. El ENS puede presentarse como uno de esos marcos.

El ENS aporta varias ventajas como **modelo complementario**. En primer lugar, **obligatoriedad jurídica en su ámbito**. En segundo lugar, **categorización proporcional de sistemas**. En tercer lugar, **catálogo propio de medidas**. En cuarto lugar, **auditoría y certificación de conformidad**. En quinto lugar, **acreditación de entidades certificadoras**. En sexto lugar, **guías técnicas y herramientas públicas**. En séptimo lugar, **integración de proveedores privados del sector público**. En octavo lugar, **orientación a mejora continua**.

Estas características permiten que el ENS actúe como una plataforma nacional de cumplimiento. Una entidad pública o proveedor puede utilizar el ENS para ordenar su seguridad y, al mismo tiempo, mapear sus controles frente a otras obligaciones europeas o estándares internacionales. Esta posibilidad de mapeo es especialmente importante para reducir cargas, evitar duplicidades y construir evidencias reutilizables.

Desde la **perspectiva internacional**, esta idea debe ocupar un lugar central: **el ENS es un modelo nacional que habla el lenguaje europeo de la ciberseguridad. Utiliza riesgo, responsabilidad, auditoría, certificación, acreditación, continuidad, incidentes, proveedores, medidas técnicas y organizativas. Por ello, puede ser entendido, comparado y eventualmente tomado como referencia por otros Estados.**

Asimismo, el ENS se alinea con el **Reglamento (UE) 2024/1689 sobre Inteligencia Artificial**. En virtud de la madurez del modelo español, la seguridad de los sistemas de IA debe integrarse plenamente en la gobernanza del ENS. Según establecen las guías CCN-STIC 801 (Responsabilidades y Funciones) y CCN-STIC 805 (Política de Seguridad de la Información), las organizaciones que desarrollen o desplieguen sistemas de IA en el ámbito público deben incorporar en su Política de Seguridad los requisitos de ciberseguridad y supervisión exigidos por la normativa europea. Esto incluye la necesidad de contar con un informe preceptivo del Responsable de la Seguridad que evalúe los riesgos específicos de la IA, garantizando que su implementación no comprometa las dimensiones de seguridad del sistema de información en el que se integra.

9.8. POSIBLES VÍAS DE RECONOCIMIENTO, EQUIVALENCIA O INTEROPERABILIDAD INTERNACIONAL

La proyección internacional del ENS requiere distinguir entre tres conceptos: **reconocimiento, equivalencia funcional e interoperabilidad**. El reconocimiento implicaría que otro Estado, institución u organización aceptara formalmente la conformidad ENS como evidencia válida para determinados fines. La equivalencia implicaría considerar que el ENS ofrece garantías sustancialmente comparables a otro marco o esquema, aunque no sean idénticas. La interoperabilidad implicaría que el ENS pueda dialogar con otros marcos mediante correspondencias, mapeos, uso cruzado de evidencias o integración metodológica.

A corto plazo, la vía más evidente es la **interoperabilidad**. **El ENS puede compararse con NIS2, RGPD, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 17065 y esquemas europeos de certificación para identificar correspondencias funcionales**. Por ejemplo, medidas ENS pueden mapearse con controles ISO; requisitos de gestión de riesgos pueden

vincularse con NIS2; medidas de seguridad pueden apoyar el artículo 32 RGPD; la acreditación bajo ISO/IEC 17065 puede facilitar la comprensión internacional del esquema de certificación ENS; y certificados de productos bajo esquemas europeos pueden utilizarse como evidencias parciales en sistemas ENS.

Además de ello, cabe contemplar igualmente la **equivalencia funcional** en determinados ámbitos. Por ejemplo, **en contratación pública internacional, cooperación administrativa, proyectos europeos, servicios cloud para Administraciones o reconocimiento de proveedores**, la certificación ENS aporta garantías suficientes para determinados requisitos de seguridad. Esta equivalencia debería ser prudente y basada en análisis técnico, porque los marcos tienen objetos distintos.

El **reconocimiento** formal podría plantearse en el futuro mediante **acuerdos, instrumentos europeos, marcos de cooperación, cláusulas de contratación o mecanismos de aceptación recíproca.**

La interoperabilidad requiere también evitar afirmaciones excesivas. No debe afirmarse que cumplir el ENS equivale automáticamente a cumplir NIS2, RGPD o ISO/IEC 27001. Tampoco debe afirmarse que una certificación ENS sustituye a un esquema europeo de certificación. Lo correcto es sostener que el ENS proporciona una base sólida y verificable que puede apoyar el cumplimiento, facilitar correspondencias y reducir duplicidades cuando se gestiona adecuadamente.

Desde una **perspectiva institucional**, la formulación debe ser ambiciosa pero precisa: **el ENS es un modelo español de confianza digital con alto potencial de interoperabilidad europea e internacional. Su estructura de riesgo, medidas, auditoría, certificación, acreditación, guías y herramientas lo convierte en una referencia útil para otros países y para el debate europeo sobre marcos nacionales de ciberseguridad.**

En la siguiente tabla se recogen las principales correspondencias funcionales entre el ENS y los marcos normativos, estándares y regulaciones de referencia a nivel europeo e internacional:

Marco	Finalidad principal	Punto de conexión con el ENS	Mensaje de valor
Directiva NIS2	Elevar el nivel común de ciberseguridad en la UE mediante gestión de riesgos, incidentes y supervisión	Gestión de riesgos, medidas de seguridad, incidentes, cadena de suministro, responsabilidad organizativa	El ENS facilita una aplicación nacional madura de la lógica NIS2 en el sector público
Reglamento de Ciberseguridad	Marco europeo para ENISA y para esquemas europeos de certificación de ciberseguridad	Certificación, confianza, evaluación de conformidad y posible complementariedad con sistemas nacionales	El ENS dialoga con la cultura europea de certificación
EUCC	Esquema europeo de certificación basado en	Evidencias de seguridad de productos o componentes	Certificaciones europeas pueden

Marco	Finalidad principal	Punto de conexión con el ENS	Mensaje de valor
	Common Criteria para productos TIC	integrables en sistemas ENS	reforzar evidencias dentro del ENS
ISO/IEC 27001	Sistema de gestión de seguridad de la información	Gestión de riesgos, mejora continua, auditoría, controles y gobierno de seguridad	Organizaciones con ISO 27001 pueden aprovechar capacidades para adecuarse al ENS
ISO/IEC 27002	Controles y buenas prácticas de seguridad de la información	Orientación complementaria para controles técnicos y organizativos	El ENS es compatible con el lenguaje internacional de controles
ISO/IEC 17065	Requisitos para organismos que certifican productos, procesos y servicios	Acreditación de entidades certificadoras ENS	La certificación ENS se apoya en garantías internacionales de evaluación de la conformidad
RGPD	Protección de datos personales y seguridad del tratamiento	Medidas técnicas y organizativas, confidencialidad, integridad, disponibilidad, resiliencia, incidentes	El ENS puede apoyar la seguridad del tratamiento en sistemas públicos
Reglamento IA	Establecer normas armonizadas para una IA segura y fiable	Requisitos de seguridad técnica y gobernanza en sistemas de IA	El ENS ayuda a operativizar la seguridad exigida por el Reglamento IA en el sector público

Figura 9.1 Correspondencias funcionales entre el ENS y marcos europeos e internacionales

A continuación, se presenta un esquema conceptual que ilustra cómo el ENS actúa como puente integrador entre la Administración digital española y el ecosistema europeo e internacional de ciberseguridad:



Figura 9.2 El ENS como puente entre Administración digital española y ecosistema europeo de ciberseguridad

9.9. RESUMIENDO…

El ENS es un marco nacional plenamente alineado con la evolución europea e internacional de la ciberseguridad. Comparte con **NIS2** la lógica de gestión de riesgos, medidas organizativas y técnicas, incidentes, resiliencia y cadena de suministro. Dialoga con el **Reglamento de Ciberseguridad** y los esquemas europeos de certificación desde su propio sistema nacional de conformidad. Es compatible con **ISO/IEC 27001 e ISO/IEC 27002** como referencias internacionales de gestión y controles. Utiliza **ISO/IEC 17065** para reforzar la acreditación de entidades certificadoras. Y puede apoyar el cumplimiento de la seguridad del tratamiento exigida por el **RGPD** cuando los sistemas ENS tratan datos personales.

Su valor estratégico está precisamente en esa capacidad de conexión. El ENS no es un modelo aislado, ni una peculiaridad administrativa española, ni un simple catálogo de medidas. Es una infraestructura nacional de confianza digital que habla el lenguaje europeo de la ciberseguridad: riesgo, gobernanza, medidas proporcionadas, auditoría, certificación, acreditación, incidentes, proveedores y mejora continua.

El ENS proporciona una base nacional madura, verificable y potencialmente interoperable para aplicar, demostrar y proyectar ciberseguridad en el sector público y en su cadena de suministro. Esa es su principal fuerza como modelo español exportable a Europa y al ámbito internacional.

10. VALOR DIFERENCIAL DEL ENS Y RAZONES PARA SU PROYECCIÓN INTERNACIONAL

El Esquema Nacional de Seguridad presenta un valor diferencial que excede su función estrictamente normativa. No es sólo el marco jurídico español para proteger los sistemas de información del sector público y de determinados proveedores privados; **es también un modelo completo de confianza digital, gobernanza de la ciberseguridad, cumplimiento verificable y colaboración público-privada. Esa condición explica su interés como referencia nacional y como modelo proyectable en el ámbito europeo e internacional.**

La singularidad del ENS deriva de la combinación de elementos que lo integran. Muchos marcos de ciberseguridad ofrecen principios, buenas prácticas, controles técnicos, requisitos organizativos o mecanismos de certificación.

El ENS, en cambio, articula todos esos elementos dentro de una arquitectura pública común: norma obligatoria, ámbito definido, principios básicos, requisitos mínimos, categorización de sistemas, medidas de seguridad, Instrucciones Técnicas de Seguridad, guías CCN-STIC, herramientas de apoyo, auditoría, declaración o certificación de conformidad, acreditación de entidades certificadoras, gestión de incidentes, informe del estado de seguridad y mejora continua.

Esta integración es el principal argumento para su proyección.

El ENS no se presenta en Europa ni ante terceros países como una norma técnica más, sino como un ecosistema nacional de confianza digital.

Su valor no reside únicamente en lo que exige, sino en cómo organiza el cumplimiento, cómo lo hace verificable, cómo acompaña a las entidades, cómo extiende la seguridad a proveedores y cómo convierte la ciberseguridad en una política pública operativa.

Desde una **perspectiva técnica**, **el ENS proporciona medidas y criterios concretos. Desde una perspectiva jurídica, convierte la seguridad en obligación exigible**. Desde una **perspectiva organizativa**, **asigna responsabilidades y ordena la gobernanza**. Desde una **perspectiva de mercado**, **disciplina la contratación pública tecnológica**. Desde una **perspectiva de certificación**, **genera evidencias verificables**. Desde una **perspectiva internacional**, **ofrece un modelo nacional maduro que puede inspirar a otros Estados en el diseño de marcos de ciberseguridad pública.**

10.1. EL ENS COMO SISTEMA COMPLETO, NO COMO MERO ESTÁNDAR TÉCNICO

El primer valor diferencial del ENS es su **carácter sistémico**. El ENS no es un estándar técnico aislado, ni un catálogo voluntario de controles, ni una certificación sectorial desconectada de la realidad administrativa. Es **un sistema completo de gobernanza de la seguridad de la información aplicable a sistemas que soportan la actuación del sector público, la prestación de servicios públicos digitales y determinadas relaciones con proveedores privados.**

Esta condición sistémica se manifiesta en varios planos:

- En el **plano normativo**, **el ENS se apoya en el Real Decreto 311/2022 y en las Instrucciones Técnicas de Seguridad**.
- En el **plano técnico**, **incorpora principios, requisitos mínimos y medidas de seguridad**.
- En el **plano organizativo**, **exige política de seguridad, roles, responsabilidades, procedimientos y gestión de riesgos**.
- En el **plano operativo**, **se apoya en guías, herramientas y procesos de adecuación**.
- En el **plano de confianza**, **incorpora auditoría, declaración o certificación de conformidad y acreditación de entidades certificadoras**.

El ENS ofrece, por tanto, una cadena completa: regular, organizar, implantar, verificar, certificar, medir y mejorar.

Esta cadena es lo que lo diferencia de marcos más limitados. Un estándar técnico puede proporcionar controles; el ENS proporciona un sistema de cumplimiento. Una certificación puede acreditar un producto o servicio; el ENS permite evaluar la seguridad de sistemas que soportan servicios públicos. Una guía puede orientar buenas prácticas; el ENS integra guías dentro de un marco jurídico y de auditoría.

Esta visión sistémica es especialmente valiosa para terceros países. Muchos Estados no necesitan únicamente listas de controles, sino modelos completos para proteger sus Administraciones digitales.

El ENS ofrece una experiencia concreta de cómo convertir la ciberseguridad pública en un sistema regulado, aplicable y certificable, lo que constituye una de sus principales fortalezas como modelo exportable.

Desde la **perspectiva de comunicación institucional**, el mensaje es claro:

El ENS no es un producto documental, sino una infraestructura nacional de confianza digital. Su valor está en el conjunto, no en cada pieza aislada.

Asimismo, un valor diferencial emergente es la capacidad del ENS para integrar la gobernanza de la **Inteligencia Artificial**. Según establece la **Guía CCN-STIC 805 ENS. Política de Seguridad de la Información (actualizada en junio 2025)**, el modelo español proporciona el marco necesario para que el despliegue de sistemas de IA en el sector público cumpla con los requisitos de seguridad y supervisión exigidos por el **Reglamento (UE) 2024/1689 Reglamento de Inteligencia Artificial**. Esto asegura que la innovación tecnológica no comprometa las dimensiones de seguridad del sistema de información y se realice bajo un informe de riesgos preceptivo del Responsable de Seguridad, situando al ENS como un marco pionero para la protección de servicios públicos basados en IA.

10.2. OBLIGATORIEDAD JURÍDICA Y APLICABILIDAD AL SECTOR PÚBLICO

El segundo valor diferencial del ENS es su obligatoriedad jurídica en el ámbito del sector público. Muchos marcos de seguridad se basan en adopción voluntaria,

incentivos reputacionales o compromisos contractuales. **El ENS, por el contrario, se integra en el ordenamiento jurídico español como marco obligatorio para las entidades incluidas en su ámbito de aplicación**. Esta obligatoriedad aporta fuerza, coherencia y capacidad de despliegue.

La seguridad de los servicios públicos digitales no puede depender exclusivamente de decisiones voluntarias de cada entidad. En un Estado descentralizado, con múltiples Administraciones, organismos, entidades públicas y sistemas interconectados, la fragmentación de criterios puede generar debilidades sistémicas. **El ENS proporciona una base común de seguridad para todo el sector público afectado, reduciendo la dispersión y elevando el nivel mínimo de protección.**

La obligatoriedad jurídica tiene también un **efecto organizativo: obliga a las entidades a incorporar la seguridad en su gobierno interno, asignar responsabilidades, aprobar políticas, categorizar sistemas, implantar medidas, documentar evidencias, gestionar incidentes y someterse a verificación**. La seguridad deja de ser una práctica deseable y se convierte en una exigencia institucional.

Desde el punto de vista de la **confianza ciudadana**, esta obligatoriedad es especialmente importante. Los ciudadanos y empresas que se relacionan electrónicamente con la Administración no pueden evaluar por sí mismos la seguridad de cada sistema público. Necesitan confiar en que existe un marco común que exige protección adecuada. El ENS cumple esa función: **ofrece una garantía estructural sobre la seguridad de la Administración digital.**

Desde una **perspectiva internacional**, **la obligatoriedad del ENS muestra cómo un Estado puede transformar una política pública de ciberseguridad en obligaciones concretas**.

> **Esta capacidad de pasar de la estrategia a la norma, de la norma a las medidas y de las medidas a la certificación es uno de los rasgos más atractivos del modelo español.**

10.3. EXTENSIÓN A PROVEEDORES PRIVADOS DEL SECTOR PÚBLICO

El tercer valor diferencial del ENS es su **proyección sobre entidades privadas que prestan servicios o proveen soluciones al sector público**. Esta característica es decisiva en el entorno tecnológico actual. La Administración digital depende cada vez más de proveedores cloud, desarrolladores, integradores, operadores de servicios gestionados, consultoras, fabricantes, plataformas, servicios de soporte y cadenas de suministro complejas. Proteger sólo los sistemas internos de la Administración sería insuficiente.

El ENS ofrece una respuesta normativa clara: **cuando los sistemas de información de entidades privadas sustentan servicios o soluciones para el sector público en el ejercicio de competencias y potestades administrativas, las exigencias del ENS pueden proyectarse sobre dichos sistemas.** Además, los pliegos deben contemplar los requisitos necesarios para asegurar la conformidad ENS cuando proceda. Esta previsión convierte la contratación pública en una herramienta de ciberseguridad.

Esta extensión al proveedor tiene un **efecto disciplinador del mercado**. Las empresas que quieran operar en el mercado público digital deben ser capaces de demostrar seguridad, madurez y cumplimiento. **La certificación ENS se convierte así en una señal de confianza y en un elemento de diferenciación competitiva**. La Administración obtiene proveedores más seguros; las empresas maduras obtienen una ventaja; y el ciudadano recibe servicios públicos digitales más confiables.

La extensión a proveedores permite también **gestionar mejor la cadena de suministro**. El riesgo no reside sólo en el contratista principal, sino también en subcontratistas, plataformas, servicios de terceros, herramientas de soporte, centros de datos y componentes tecnológicos. El ENS permite incorporar esos riesgos al análisis contractual y exigir evidencias proporcionadas.

Desde una **perspectiva europea e internacional**, este punto es especialmente relevante. **La seguridad de proveedores y cadenas de suministro es una prioridad creciente**. El ENS ofrece un modelo nacional que no se limita a proclamar esa preocupación, sino que la integra en la contratación pública y en el sistema de conformidad. Esta característica lo convierte en una referencia útil para otros países que quieran reforzar la seguridad de sus mercados públicos digitales.

10.4. CATEGORIZACIÓN PROPORCIONAL BASADA EN IMPACTO

El cuarto valor diferencial del ENS es su sistema de **categorización proporcional basada en impacto**. El ENS no aplica la misma exigencia a todos los sistemas, sino que **determina la categoría en función del impacto que tendría un incidente sobre dimensiones esenciales de seguridad: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad**. Esta lógica permite adaptar las medidas y la verificación al nivel real de criticidad.

La proporcionalidad es uno de los elementos que hacen viable el modelo. Un marco de seguridad que imponga exigencias idénticas a todos los sistemas corre el riesgo de ser excesivo para unos e insuficiente para otros. El ENS evita esa rigidez. Permite distinguir entre sistemas de categoría básica, media y alta, vinculando la intensidad de las medidas, la auditoría y la certificación al impacto potencial.

Este enfoque tiene **valor técnico** porque **ayuda a asignar recursos de forma racional**. Tiene **valor jurídico** porque **justifica las obligaciones exigidas**. Tiene **valor organizativo** porque **obliga a conocer los sistemas y servicios**. Tiene **valor de mercado** porque **permite exigir a proveedores requisitos proporcionados**. Y tiene **valor internacional** porque **ofrece una metodología clara para graduar la seguridad pública digital.**

La categorización basada en impacto es también un mensaje de credibilidad. Permite defender que el ENS es exigente, pero no arbitrario. No impone seguridad por intuición, sino por análisis. No se basa en el tamaño de la entidad, sino en el impacto del sistema. No busca cumplimiento uniforme, sino protección adecuada.

Desde el punto de vista de la **proyección internacional**, **esta característica facilita la adaptación del modelo a otros contextos nacionales**. Cada Estado puede tener

estructuras administrativas, riesgos y capacidades distintas, pero la idea de categorizar sistemas según impacto resulta fácilmente comprensible y replicable. Es uno de los elementos más exportables del ENS.

10.5. AUDITORÍA Y CERTIFICACIÓN VERIFICABLES

El quinto valor diferencial del ENS es su **sistema de auditoría y certificación**. La confianza digital exige evidencias. No basta con que una entidad afirme que cumple; debe poder demostrarlo. **El ENS incorpora mecanismos para verificar la conformidad mediante autoevaluación, auditoría, Declaración de Conformidad y Certificación de Conformidad, en función de la categoría del sistema.**

La auditoría permite comprobar si la categorización es correcta, si el análisis de riesgos es adecuado, si las medidas aplicables se han implantado, si la documentación es coherente y si existen evidencias suficientes. La certificación permite transformar ese proceso de evaluación en una evidencia reconocible frente a terceros. De este modo, el ENS convierte el cumplimiento interno en confianza externa.

Este elemento tiene gran valor para la Administración: **permite acreditar diligencia, reforzar la rendición de cuentas, mejorar la gestión de proveedores y demostrar que los sistemas que soportan servicios públicos han sido evaluados**. También tiene valor para las empresas proveedoras, porque les permite diferenciarse en el mercado mediante una señal de conformidad verificable.

> **La certificación ENS no debe presentarse como un simple distintivo. Su valor reside en la cadena que la sostiene: categorización, medidas, Declaración de Aplicabilidad, evidencias, auditoría, entidad certificadora, acreditación, seguimiento y mejora continua. Esta cadena es lo que convierte el certificado en una garantía útil.**

Desde la **perspectiva internacional**, **la auditoría y certificación son piezas centrales del argumento de venta**. Muchos modelos nacionales de ciberseguridad tienen dificultades para demostrar cumplimiento. El ENS ofrece un mecanismo para hacerlo. Esto permite posicionar a España como un país que ha sabido convertir la seguridad pública digital en evidencia evaluable.

10.6. ACREDITACIÓN DE ENTIDADES CERTIFICADORAS

El sexto valor diferencial del ENS es la **acreditación de las entidades certificadoras.** La certificación sólo genera confianza si quien certifica es competente, imparcial y está sometido a supervisión. **El modelo ENS incorpora esta garantía mediante la intervención de la Entidad Nacional de Acreditación (ENAC) y la referencia a la UNE-EN ISO/IEC 17065 como norma aplicable a organismos que certifican productos, procesos y servicios.**

La acreditación aporta una segunda capa de confianza: la entidad certificadora evalúa el sistema; ENAC evalúa la competencia de la entidad certificadora. Esta estructura evita que el mercado de certificación se degrade y permite que los certificados ENS sean emitidos por organizaciones sometidas a criterios técnicos y de imparcialidad.

El valor de esta capa es evidente:

- **Para las Administraciones, permite confiar en que los certificados aportados por proveedores han sido emitidos por entidades competentes**.
- **Para las empresas, ofrece un marco reconocido para acreditar conformidad**.
- **Para los órganos de contratación, proporciona una base objetiva para aceptar evidencias**.
- **Para interlocutores internacionales, facilita la comprensión del modelo mediante el lenguaje global de la evaluación de la conformidad.**

La acreditación refuerza también la reputación del ENS. Un certificado sin control del certificador tiene un valor limitado. Un certificado emitido por una entidad acreditada dentro de un esquema nacional supervisado tiene mayor credibilidad. Esta diferencia debe subrayarse en cualquier presentación internacional.

Desde la **perspectiva institucional**, la idea puede formularse así: **el ENS no sólo certifica sistemas; acredita a quienes certifican. Esta garantía de segundo nivel es uno de los elementos que permiten presentar el modelo español como una infraestructura de confianza robusta.**

10.7. PAPEL DEL CCN COMO AUTORIDAD TÉCNICA DE REFERENCIA

El séptimo valor diferencial del ENS es **el papel del Centro Criptológico Nacional (CCN)** como autoridad técnica de referencia. El CCN no es un actor periférico del modelo.

> **La función del CCN en la interpretación, desarrollo, implantación y evolución del ENS resulta esencial para mantener coherencia técnica, orientar a las entidades, elaborar guías, proporcionar herramientas, apoyar la respuesta a incidentes y acompañar la maduración del ecosistema.**

La existencia de una autoridad técnica de referencia evita que el ENS quede fragmentado en interpretaciones dispersas. En un marco aplicado por múltiples entidades, auditores, certificadores, consultores y proveedores, la coherencia técnica es imprescindible. El CCN proporciona doctrina, criterios, guías, herramientas y capacidades que permiten sostener esa coherencia.

El papel del CCN refuerza además la conexión entre cumplimiento y ciberseguridad real. El ENS no es sólo un esquema documental; está vinculado a capacidades técnicas nacionales, al conocimiento de amenazas, a la gestión de incidentes, a la elaboración de guías y al acompañamiento de las entidades. Esta conexión entre norma y capacidad técnica es uno de los elementos más valiosos del modelo.

Desde la **perspectiva de las entidades obligadas**, **el CCN proporciona referencia y apoyo**. Desde la **perspectiva de auditores y certificadores**, **ofrece criterios técnicos y documentación de apoyo**. Desde la **perspectiva de proveedores**, **clarifica expectativas**. Desde la **perspectiva internacional**, **permite presentar el ENS como un modelo respaldado por una autoridad nacional especializada.**

Este punto es especialmente relevante para la proyección exterior. Muchos países pueden aprobar normas de ciberseguridad, pero no todos cuentan con una autoridad técnica capaz de sostener su aplicación mediante guías, herramientas, criterios y apoyo operativo. La presencia del CCN convierte al ENS en un modelo institucionalmente sólido.

10.8. GUÍAS, HERRAMIENTAS Y ACOMPAÑAMIENTO TÉCNICO

El octavo valor diferencial del ENS es la existencia de **guías, herramientas y acompañamiento técnico**.

La serie CCN-STIC 800, junto con herramientas como INES, AMPARO, LUCIA y otras muchas soluciones de apoyo, permite que el cumplimiento del ENS sea practicable. Esta dimensión distingue al modelo español de marcos que imponen obligaciones sin proporcionar una metodología suficiente para cumplirlas.

- Las **guías** ayudan a interpretar el marco, organizar la adecuación, aplicar medidas, preparar auditorías, gestionar riesgos, ordenar roles, abordar contratación, externalización, cloud y entidades de menor dimensión.
- Las **herramientas** permiten estructurar información, medir el estado de seguridad, gestionar riesgos, documentar evidencias y facilitar el seguimiento.
- El **acompañamiento técnico** reduce incertidumbre y favorece la homogeneidad.

Esta combinación tiene **valor práctico inmediato:**

- Las entidades públicas no parten de cero.
- Los proveedores conocen mejor las expectativas.
- Los auditores y certificadores cuentan con referencias.
- Las entidades pequeñas disponen de apoyo para abordar un marco que, de otro modo, podría resultar complejo.
- La implantación se vuelve más escalable.

Desde una **perspectiva institucional**, este es uno de los mensajes más eficaces: **el ENS no sólo exige, sino que ayuda. No sólo regula, sino que proporciona doctrina. No sólo certifica, sino que acompaña el camino hacia la certificación**. Esa dimensión de apoyo es esencial para presentar el ENS como modelo exportable.

En términos internacionales, las guías y herramientas son elementos especialmente transferibles. Otros países pueden inspirarse no sólo en la norma, sino en la idea de acompañar el cumplimiento mediante documentación técnica, herramientas públicas y autoridad de referencia. Esta es una de las aportaciones más valiosas del modelo español.

10.9. MADUREZ, TRAZABILIDAD Y MEJORA CONTINUA

El noveno valor diferencial del ENS es su **orientación a la madurez, la trazabilidad y la mejora continua**. El modelo no se agota en la obtención inicial de una declaración o certificación de conformidad. Exige mantener el cumplimiento, revisar riesgos, gestionar incidentes, actualizar medidas, conservar evidencias, someterse a auditoría y corregir no conformidades.

La **madurez** se manifiesta en la capacidad de integrar la seguridad en la organización. **Una entidad madura no sólo implanta controles, sino que sabe por qué los implanta, quién responde de ellos, cómo los documenta, cómo los verifica y cómo los mejora**. El ENS impulsa precisamente esa transición desde la seguridad reactiva hacia la seguridad gobernada.

La **trazabilidad** es igualmente central. **El ENS exige documentar decisiones, justificar la categoría, reflejar medidas aplicables, conservar evidencias, registrar actividad, gestionar incidentes y mantener información sobre el estado de seguridad**. Esta trazabilidad permite auditar, certificar, supervisar y aprender. Sin trazabilidad, la confianza se debilita.

La **mejora continua** **garantiza que el modelo no se convierta en una fotografía estática.** Los sistemas cambian, las amenazas evolucionan, los proveedores se modifican y las tecnologías se transforman. El ENS incorpora auditoría periódica, revisión, actualización y aprendizaje. Esto lo convierte en un modelo vivo.

Desde la **perspectiva internacional**, **este punto permite presentar el ENS como un marco sostenible. No es sólo un requisito de entrada ni un certificado puntual. Es una disciplina de gestión continuada de la seguridad**. Esta característica resulta especialmente valiosa para Administraciones y Estados que buscan modelos duraderos, no soluciones de cumplimiento coyuntural.

10.10. ELEMENTOS EXPORTABLES DEL MODELO ESPAÑOL

La proyección internacional del ENS permite mostrar los elementos que pueden servir de referencia a otros países, sabiendo que cada Estado tiene su propio marco constitucional, administrativo, tecnológico e institucional. Pese a ello, **el ENS contiene componentes de diseño especialmente transferibles:**

1. **La idea de un marco nacional obligatorio para la seguridad de los sistemas públicos digitales**. La transformación digital de la Administración exige una base común de seguridad, y el ENS ofrece un ejemplo de cómo estructurarla.
2. **La categorización proporcional basada en impacto.** Esta metodología puede adaptarse a distintos contextos nacionales porque se basa en una idea universal: los sistemas deben protegerse según el impacto que tendría su compromiso.
3. **La combinación de medidas organizativas, operacionales y de protección**. Esta estructura permite evitar una visión puramente tecnológica y construir seguridad desde la gobernanza, la operación y los activos.

4. **El sistema de declaración, auditoría y certificación de conformidad.** Muchos países necesitan mecanismos para demostrar cumplimiento. El ENS ofrece una arquitectura clara para hacerlo.
5. **La acreditación de entidades certificadoras**. Esta capa de confianza permite profesionalizar el mercado y evitar certificados sin garantías suficientes.
6. **El papel de una autoridad técnica nacional que elabora guías, proporciona herramientas, orienta la implantación y sostiene el modelo**. Sin una autoridad técnica de referencia, los marcos nacionales corren el riesgo de fragmentarse.
7. **La extensión del marco a proveedores privados y a la contratación pública**. Esta dimensión es especialmente relevante para países que dependen de empresas tecnológicas para prestar servicios públicos digitales.
8. **El ecosistema de guías y herramientas**. La norma es necesaria, pero no suficiente. Los Estados necesitan acompañar el cumplimiento con metodología, documentación, herramientas y capacidades.
9. **La orientación a mejora continua**. Un marco de ciberseguridad debe poder evolucionar con las amenazas, la tecnología y los modelos de prestación de servicios.

Finalmente, el ENS incorpora un valor diferencial de responsabilidad institucional al vincular legalmente la ciberseguridad con la **sostenibilidad medioambiental**. En cumplimiento de la **disposición adicional tercera del ENS**, todas las actuaciones de implantación y adecuación del Esquema (especialmente aquellas vinculadas al **Plan de Recuperación, Transformación y Resiliencia (PRTR)**) deben respetar de forma preceptiva el principio de **«no causar un perjuicio significativo» al medioambiente (DNSH)**. Esta integración conlleva que la adquisición de componentes tecnológicos y la contratación de servicios derivados de las medidas de seguridad deban cumplir con los criterios de **etiquetado climático y digital** de la Unión Europea, alineando la resiliencia digital con los objetivos de desarrollo sostenible del Estado y sus instituciones.

A fin de sintetizar la propuesta de valor del ENS, la siguiente tabla detalla la contribución específica de cada uno de sus elementos diferenciales, tanto para el contexto nacional como para su proyección internacional:

Elemento diferencial	Qué aporta	Valor para España	Valor para terceros países
Marco jurídico obligatorio	Convierte la seguridad en exigencia normativa	Homogeneidad y seguridad jurídica	Referencia para construir marcos nacionales
Aplicación al sector público	Protege servicios públicos digitales	Confianza ciudadana y continuidad administrativa	Modelo de seguridad para Administración digital
Extensión a proveedores	Proyecta seguridad sobre contratistas y cadena de suministro	Mercado público digital más seguro	Herramienta para controlar proveedores tecnológicos

Elemento diferencial	Qué aporta	Valor para España	Valor para terceros países
Categorización por impacto	Gradúa exigencias según criticidad	Proporcionalidad y eficiencia	Metodología adaptable a distintos contextos
Medidas del Anexo II	Traduce principios en controles concretos	Seguridad operativa verificable	Catálogo estructurado de referencia
Auditoría y certificación	Permite demostrar cumplimiento	Confianza frente a terceros	Modelo de conformidad replicable
Acreditación de certificadores	Garantiza competencia e imparcialidad	Credibilidad del sistema	Lenguaje internacional de evaluación de conformidad
Papel del CCN	Aporta autoridad técnica, guías y herramientas	Coherencia y acompañamiento	Ejemplo de gobernanza técnica nacional
Mejora continua	Mantiene la seguridad en el tiempo	Resiliencia institucional	Modelo sostenible y evolutivo

Figura 10.1 Propuesta de valor del ENS

Para articular de manera eficaz la estrategia de proyección internacional del modelo, la tabla expuesta a continuación recoge los mensajes clave adaptados a cada público objetivo:

Público destinatario	Mensaje principal	Argumento de apoyo
Instituciones europeas	El ENS es un marco nacional alineado con la lógica europea de riesgo, resiliencia y certificación	Combina gestión de riesgos, auditoría, certificación, proveedores e incidentes
Otros Estados	El ENS ofrece una arquitectura práctica para proteger Administraciones digitales	Norma, medidas, guías, herramientas, certificación y autoridad técnica
Organismos de certificación y acreditación	El ENS dispone de una cadena de confianza evaluable	Certificación de sistemas y acreditación de certificadores
Proveedores tecnológicos	El ENS crea un mercado público digital basado en confianza	La conformidad ENS puede ser ventaja competitiva
Administraciones públicas españolas	El ENS no es sólo cumplimiento: es madurez, continuidad y reputación	Ordena responsabilidades, medidas, auditoría y mejora continua
Ciudadanía y empresas	El ENS refuerza la confianza en los servicios públicos digitales	Protege información, servicios, trazabilidad y disponibilidad

Figura 10.2 Mensajes clave para la proyección internacional del ENS

A continuación, se presenta de forma ilustrada la arquitectura integral del ENS como "producto-país" de confianza digital y su secuencia operativa de implantación:



Figura 10.3 El ENS como producto-país de confianza digital

10.11. RESUMIENDO…

El valor diferencial del ENS reside en su **carácter integral**.

El ENS es norma jurídica, marco técnico, modelo organizativo, sistema de auditoría, esquema de certificación, arquitectura de acreditación, herramienta de contratación pública, mecanismo de control de proveedores, cuerpo doctrinal mediante guías, ecosistema de herramientas y proceso de mejora continua. Esa combinación lo convierte en una infraestructura nacional de confianza digital.

La proyección internacional del ENS se sustenta en esa integración. España presenta el ENS como un modelo maduro, operativo, verificable y adaptable. No como una norma aislada, sino como una política pública completa de ciberseguridad aplicada a la Administración digital y a su ecosistema proveedor.

La propuesta de valor es clara:

El ENS permite pasar de la ciberseguridad como aspiración a la ciberseguridad como sistema; de la obligación al cumplimiento; del cumplimiento a la evidencia; de la evidencia a la certificación; y de la certificación a la confianza.

Esa cadena convierte al ENS en un activo estratégico del Estado español y en una referencia útil para Europa y para terceros países.

11. CONCLUSIONES

El Esquema Nacional de Seguridad debe ser entendido como una de las principales infraestructuras regulatorias de confianza digital del Estado español. Su relevancia no deriva únicamente de su carácter obligatorio ni de la existencia de un catálogo de medidas de seguridad, sino de haber construido **un modelo completo que conecta Derecho público, seguridad de la información, gestión de riesgos, gobernanza, contratación tecnológica, auditoría, certificación, acreditación, guías técnicas, herramientas de apoyo y mejora continua.**

A lo largo del documento se ha sostenido una tesis central: el ENS no es una mera obligación administrativa ni un estándar técnico aislado. **Es un sistema público de confianza que permite proteger servicios digitales, ordenar responsabilidades, disciplinar proveedores, generar evidencias de cumplimiento, verificar la seguridad alcanzada y proyectar internacionalmente una experiencia nacional madura.**

Las conclusiones que siguen sintetizan ese valor. Están formuladas para cerrar el documento con una lectura institucional y estratégica del modelo, sin perder el rigor técnico-jurídico que exige su naturaleza.



Figura 11.1. El ENS como infraestructura de confianza digital.

11.1. EL ENS COMO INFRAESTRUCTURA NACIONAL DE CONFIANZA DIGITAL

El ENS constituye una **infraestructura nacional de confianza digital porque proporciona una base común para proteger la información tratada y los servicios prestados por medios electrónicos en el ámbito del sector público y en su ecosistema**

proveedor. En un contexto en el que la Administración digital depende de sistemas interconectados, plataformas externas, servicios cloud, proveedores tecnológicos y cadenas de suministro complejas, la confianza no puede descansar en decisiones aisladas de cada entidad. Requiere un marco común, obligatorio, verificable y actualizado.

Esa infraestructura se articula mediante una lógica integral. **El ENS define principios básicos, requisitos mínimos, categorías de sistemas, medidas de seguridad, roles, política de seguridad, procedimientos de auditoría, declaración y certificación de conformidad, notificación de incidentes, informe del estado de seguridad, guías técnicas y herramientas de apoyo**. La seguridad se convierte así en una capacidad institucional, no en una suma de controles inconexos.

La confianza que genera el ENS es especialmente relevante para ciudadanos y empresas. Quien se relaciona electrónicamente con una Administración no puede verificar por sí mismo la seguridad de cada plataforma, expediente, registro, sede electrónica o servicio digital. El ENS cumple esa función de garantía estructural: permite confiar en que existe un marco público que exige seguridad, proporcionalidad, evidencias y revisión periódica.

11.2. EL ENS COMO ACTIVO ESTRATÉGICO DEL ESTADO ESPAÑOL

El ENS es un activo estratégico del Estado español porque convierte la ciberseguridad pública en un modelo regulado, operativo y evaluable. España no se limita a declarar la importancia de proteger sus servicios públicos digitales; dispone de un marco que permite organizar esa protección, exigirla jurídicamente, implantarla técnicamente, verificarla mediante auditoría y acreditarla frente a terceros.

Este valor estratégico se manifiesta en varios planos:

- En el **plano institucional**, refuerza la resiliencia de la Administración digital.
- En el **plano jurídico**, proporciona seguridad normativa.
- En el **plano organizativo,** obliga a distribuir responsabilidades y a integrar la seguridad en el gobierno de las entidades.
- En el **plano técnico**, ofrece medidas y criterios de implantación.
- En el **plano económico**, disciplina el mercado público tecnológico, y
- En el **plano internacional**, permite presentar un modelo nacional con elementos exportables.

El papel del CCN es esencial en esta arquitectura. Su función como autoridad técnica de referencia aporta coherencia, doctrina, herramientas, guías, criterios de interpretación y capacidad de acompañamiento. Sin esa referencia técnica, el ENS correría el riesgo de fragmentarse en interpretaciones dispersas. Con ella, el modelo se consolida como un ecosistema público de conocimiento, apoyo y confianza.

11.3. EL ENS COMO MODELO DE GOBERNANZA, CUMPLIMIENTO Y CERTIFICACIÓN

El ENS debe valorarse como un **modelo de gobernanza** **porque sitúa la seguridad en la dirección y gestión de las entidades, y no sólo en los equipos técnicos.** La diferenciación entre responsables de información, servicio, seguridad y sistema, la exigencia de política de seguridad, la documentación de decisiones, la gestión de riesgos y la mejora continua muestran que la seguridad es una función organizativa transversal.

También es un **modelo de cumplimiento** **porque transforma principios generales en obligaciones concretas.** La categorización de sistemas, la valoración de dimensiones de seguridad, la selección de medidas del Anexo II, la Declaración de Aplicabilidad y la conservación de evidencias permiten pasar de la obligación normativa a una práctica verificable. El ENS no exige seguridad de forma abstracta: define cómo debe organizarse, justificarse, implantarse y mantenerse.

Finalmente, es un **modelo de certificación** **porque convierte el cumplimiento en confianza externa**. La Declaración de Conformidad, la Certificación de Conformidad, la auditoría, la acreditación de entidades certificadoras por ENAC y la referencia a UNE-EN ISO/IEC 17065 permiten que la seguridad no dependa sólo de afirmaciones internas. La conformidad ENS puede ser mostrada, evaluada, contrastada y utilizada en la contratación pública, en la relación con proveedores y en la proyección internacional del modelo español.

Idea fuerza	Implicación para el modelo ENS
No es sólo **norma**	Es una infraestructura de confianza digital que integra obligaciones, medidas, guías, herramientas, auditorías y certificación.
No es sólo **tecnología**	Es gobernanza: roles, responsabilidades, políticas de seguridad, gestión de riesgos y mejora continua.
No es sólo **cumplimiento**	Es evidencia verificable mediante declaración, certificación, auditoría, acreditación y seguimiento.
No se limita al **sector público interno**	Se proyecta sobre proveedores privados, contratación pública, servicios externalizados, *cloud* y cadena de suministro.
No es un **modelo aislado**	Dialoga con NIS2, Ciberseguridad Act, RGPD, ISO/IEC 27001, ISO/IEC 27002 y ISO/IEC 27035.
No es una **fotografía estática**	Debe actualizarse mediante guías, herramientas, criterios técnicos y evolución normativa cuando proceda.

Figura 11.2 Mensajes finales para cerrar la propuesta de valor del ENS.

11.4. EL ENS COMO REFERENCIA ÚTIL PARA OTROS PAÍSES

El ENS puede ser útil para otros países porque **ofrece una experiencia práctica de cómo estructurar un marco nacional de ciberseguridad pública**. Su valor exportable no consiste en que pueda ser copiado mecánicamente, sino en que **aporta principios**

de diseño trasladables: obligatoriedad en el sector público, extensión funcional a proveedores, categorización proporcional basada en impacto, catálogo de medidas, guías técnicas, herramientas públicas, auditoría, certificación, acreditación y mejora continua.

En el **contexto europeo**, **el ENS se alinea con tendencias regulatorias como la gestión de riesgos, la responsabilidad de las entidades, la notificación de incidentes, la seguridad de la cadena de suministro, la certificación, la resiliencia y la confianza digital.** No sustituye automáticamente a NIS2, al Reglamento de Ciberseguridad, al RGPD ni a las normas ISO, pero dialoga con todos ellos y puede servir como plataforma nacional para ordenar evidencias, reducir duplicidades y reforzar la posición española en debates de equivalencia, interoperabilidad o reconocimiento.

Para **terceros Estados y organizaciones internacionales**, **el ENS muestra que la ciberseguridad pública puede convertirse en un sistema: norma, medidas, roles, guías, herramientas, auditoría, certificación y acreditación.** Esta combinación lo diferencia de aproximaciones basadas únicamente en buenas prácticas o en compromisos voluntarios. El modelo español aporta una experiencia de institucionalización de la confianza digital.

11.5. NECESIDAD DE PRESERVAR, REFORZAR Y PROYECTAR INTERNACIONALMENTE EL MODELO ENS

El ENS **debe preservarse** porque constituye una ventaja institucional acumulada. Su existencia permite a España disponer de un marco común para proteger la Administración digital, controlar proveedores, mejorar la contratación tecnológica, profesionalizar el mercado de servicios de ciberseguridad y generar confianza en ciudadanos, empresas e instituciones. Preservarlo significa mantener la coherencia del modelo, evitar su banalización y asegurar que la certificación conserva valor real.

El ENS **debe reforzarse de forma continua** porque la tecnología, las amenazas y la regulación evolucionan. Servicios cloud, inteligencia artificial, servicios gestionados, cadena de suministro, automatización, tecnologías criptográficas emergentes y nuevos marcos europeos exigirán adaptar guías, herramientas, criterios de auditoría, cláusulas contractuales y mecanismos de coordinación. Reforzar el ENS no significa sustituirlo, sino aprovechar su arquitectura para mantenerlo como modelo vivo.

El ENS **debe proyectarse internacionalmente** porque España dispone de una experiencia valiosa. Esa proyección exige una narrativa clara: el ENS es un modelo español de confianza digital verificable. También exige materiales ejecutivos, traducciones, diagramas, tablas de correspondencia, explicación del sistema de certificación y casos de uso. La proyección debe ser ambiciosa, pero prudente: no debe afirmar equivalencias automáticas, sino demostrar alineamiento, complementariedad y potencial de interoperabilidad.

> **El ENS debe ser preservado, desarrollado y promovido como una referencia avanzada de gobernanza pública de la ciberseguridad y como activo institucional del Estado español**.



Figura 11.3 Prioridades estratégicas para preservar, reforzar y proyectar el ENS.

ANEXO I. CUADRO RESUMEN DEL REAL DECRETO 311/2022

PARTE I: ESTRUCTURA DE CAPÍTULOS Y ARTÍCULOS (DEL 1 AL 41)

CAPÍTULO / ARTÍCULO	RÚBRICA / TÍTULO	CONTENIDO Y REQUISITOS CLAVE DEL ENS
CAPÍTULO I	**Disposiciones generales**	**Ámbito, objeto, datos personales y definiciones aplicables.**
Artículo 1	Objeto	Regular el ENS establecido en la Ley 40/2015, fijando principios básicos y requisitos mínimos para proteger la información y los servicios públicos por medios electrónicos.
Artículo 2	Ámbito de aplicación	Obligatorio para todo el sector público en los términos del artículo 2 de la Ley 40/2015. Se aplica también a los sistemas de información de entidades privadas que, en virtud de una relación contractual, presten servicios o provean soluciones a entidades del sector público para el ejercicio de sus competencias y potestades administrativas. Los pliegos deben incluir los requisitos necesarios para asegurar la conformidad ENS, incluyendo Declaración o Certificación cuando proceda, y esta cautela alcanza a la cadena de suministro en función del análisis de riesgos.
Artículo 3	Sistemas que traten datos personales	Cuando un sistema trate datos personales, será aplicable la normativa de protección de datos —RGPD, LOPDGDD y, en su caso, Ley Orgánica 7/2021—, así como los criterios de las autoridades de control, sin perjuicio de los requisitos del Real Decreto 311/2022. En estos casos, el análisis de riesgos y, cuando proceda, la evaluación de impacto contemplados en el ENS derivan asimismo del régimen de protección de datos.
Artículo 4	Definiciones	Las palabras, expresiones y términos técnicos se entenderán en el sentido indicado en el Glosario de términos del Anexo IV.
CAPÍTULO II	**Principios básicos**	**Los 7 pilares filosóficos y operativos que rigen el diseño de la seguridad.**
Artículo 5	Principios básicos	Enumera los principios rectores: seguridad integral; gestión basada en riesgos; prevención, detección, respuesta y conservación; líneas de defensa; vigilancia continua; reevaluación periódica; y diferenciación de responsabilidades.
Artículo 6	Seguridad integral	Concibe la seguridad como un proceso integral de

CAPÍTULO / ARTÍCULO	RÚBRICA / TÍTULO	CONTENIDO Y REQUISITOS CLAVE DEL ENS
		elementos humanos, materiales, técnicos, jurídicos y organizativos, excluyendo tratamientos coyunturales.
Artículo 7	Gestión basada en riesgos	El análisis y tratamiento de riesgos guiará la selección e implantación de las medidas de protección de forma proporcional.
Artículo 8	Prevención, detección, respuesta y conservación	Minimizar vulnerabilidades para evitar que las amenazas se materialicen o mitigar su impacto en tiempo oportuno, garantizando la conservación a largo plazo de los soportes electrónicos.
Artículo 9	Líneas de defensa	Implementación de barreras de protección de naturaleza organizativa, física y lógica para evitar que el fallo de un elemento comprometa todo el sistema.
Artículo 10	Vigilancia continua y reevaluación periódica	Monitorización permanente para detectar anomalías, corregir configuraciones, identificar vulnerabilidades y actualizar las salvaguardas periódicamente.
Artículo 11	Diferenciación de responsabilidades	Separación clara de funciones entre los roles de Gobernanza: Responsable de la Información, Responsable del Servicio, Responsable de la Seguridad y Responsable del Sistema. La política de seguridad detallará sus atribuciones y resolución de conflictos.
CAPÍTULO III	**Política de seguridad y requisitos mínimos**	**Gobernanza corporativa y controles mínimos de seguridad de obligado cumplimiento.**
Artículo 12	Política de seguridad	Directrices de gestión y protección. Debe incluir obligatoriamente: misión de la organización, marco regulatorio, roles, comités, estructura documental de seguridad y riesgos de datos personales. Aprobada por el titular del Departamento o por el órgano ejecutivo máximo en el sector privado.
Artículo 13	Organización e implantación	La seguridad compromete a toda la organización. El Responsable de Seguridad debe ser distinto del Responsable del Sistema (sin dependencia jerárquica). Los proveedores externos deben nombrar un Punto de Contacto (POC) de seguridad.
Artículo 14	Análisis y gestión de riesgos	Obligatoriedad de realizar análisis y gestión de riesgos periódicos empleando metodologías reconocidas internacionalmente (como MAGERIT) de forma proporcional.
Artículo 15	Gestión de personal	Formación y concienciación del personal, propio o

CAPÍTULO / ARTÍCULO	RÚBRICA / TÍTULO	CONTENIDO Y REQUISITOS CLAVE DEL ENS
		ajeno, sobre sus deberes, obligaciones y responsabilidades. Normas de seguridad de obligado cumplimiento aprobadas por la dirección.
Artículo 16	Profesionalidad	La seguridad debe ser atendida, revisada y auditada por personal cualificado en todo su ciclo de vida. Exigencia objetiva de niveles de madurez idóneos en la contratación de servicios de seguridad.
Artículo 17	Autorización y control de accesos	Limitación estricta de accesos exclusivamente a usuarios, procesos y dispositivos autorizados, aplicando el principio de necesidad de conocer.
Artículo 18	Protección de las instalaciones	Ubicación de infraestructuras en áreas físicas controladas con mecanismos de acceso proporcionales, conforme a la normativa de protección de infraestructuras críticas.
Artículo 19	Adquisición de productos y servicios	Empleo de productos y servicios de seguridad que tengan certificada su funcionalidad de seguridad (uso prioritario del catálogo CPSTIC de la serie CCN-STIC 105) en proporción a la categoría del sistema.
Artículo 20	Mínimo privilegio	Limitación de privilegios lógicos al mínimo necesario. Aplicación obligatoria de guías de configuración de seguridad del CCN para desactivar funciones innecesarias o inseguras.
Artículo 21	Integridad y actualización	Autorización formal previa para incluir o modificar cualquier activo lógico o físico. Monitorización permanente para parches de seguridad y detección temprana.
Artículo 22	Protección de información almacenada/tránsito	Atención prioritaria a equipos móviles, soportes portátiles y redes abiertas. Procedimientos de recuperación a largo plazo de documentos electrónicos.
Artículo 23	Prevención ante interconexiones	Protección del perímetro de red (especialmente si conecta a internet o redes públicas), controlando los puntos de unión de acuerdo con su ITS y análisis de riesgos específicos.
Artículo 24	Registro de actividad y código dañino	Registro de la actividad de los usuarios para monitorizar, investigar y documentar incidentes (identificando unívocamente al actor) respetando la limitación de la finalidad y la privacidad.
Artículo 25	Incidentes de seguridad	Procedimientos formales de gestión de incidentes (detección, clasificación, resolución y comunicación) conforme a su respectiva ITS.

CAPÍTULO / ARTÍCULO	RÚBRICA / TÍTULO	CONTENIDO Y REQUISITOS CLAVE DEL ENS
Artículo 26	Continuidad de la actividad	Copias de seguridad periódicas y planes de contingencia para asegurar la resiliencia y la continuidad operativa ante pérdidas físicas o lógicas del entorno habitual.
Artículo 27	Mejora continua	Evaluación periódica basada en métricas e indicadores nacionales e internacionales para madurar progresivamente el proceso de seguridad.
Artículo 28	Cumplimiento de requisitos mínimos	Adopción de las medidas del Anexo II en función del análisis de riesgos, activos y la categoría del sistema. Formalización mediante la **Declaración de Aplicabilidad**. Permite la adopción de medidas compensatorias siempre que se justifique documentalmente su equivalencia.
Artículo 29	Infraestructuras y servicios comunes	Promoción de infraestructuras y servicios comunes (como servicios cloud públicos compartidos, GRC, etc.) para favorecer la eficiencia y la sinergia de seguridad.
Artículo 30	Perfiles de cumplimiento específico	Posibilidad de implementar perfiles específicos de cumplimiento (PCE) validados por el CCN para sectores o colectivos concretos (ej. Sanidad, Justicia, Entidades Locales), flexibilizando y simplificando la adecuación.
CAPÍTULO IV	**Seguridad de los sistemas: auditoría, informe e incidentes**	**Verificación del estado de seguridad, notificación de incidentes y resiliencia.**
Artículo 31	Auditoría de la seguridad	Regula la auditoría de seguridad, que debe verificar el cumplimiento de los requerimientos del ENS con la periodicidad ordinaria prevista y, en su caso, mediante auditoría extraordinaria cuando se produzcan modificaciones sustanciales que puedan repercutir en las medidas de seguridad requeridas. La intensidad y modalidad de verificación se conecta con la categoría del sistema y con el régimen de declaración o certificación aplicable.
Artículo 32	Informe del estado de la seguridad	Recogida sistemática y periódica de variables de ciberseguridad a través de la Comisión Sectorial de Administración Electrónica y el CCN (mediante la plataforma **INES**) para generar cuadros de mando nacionales.
Artículo 33	Capacidad de respuesta a incidentes	Capacidad articulada en torno al **CCN-CERT** (sector público) e **INCIBE-CERT** (proveedores y sector privado). Notificación obligatoria de incidentes con

CAPÍTULO / ARTÍCULO	RÚBRICA / TÍTULO	CONTENIDO Y REQUISITOS CLAVE DEL ENS
		impacto significativo. Coordinación de CSIRTs nacionales.
Artículo 34	Prestación de servicios de respuesta	Servicios de soporte del CCN-CERT: tratamiento de vulnerabilidades, formación técnica de especialistas, alertas y publicación del catálogo de guías de las series CCN-STIC.
CAPÍTULO V	**Normas de conformidad**	**Procedimientos para evidenciar y publicitar la conformidad del sistema con el ENS.**
Artículo 35	Administración digital	La seguridad de la administración digital se rige por el ENS. El CCN es competente para garantizar la interoperabilidad cibersegura y criptográfica (Esquema Nacional de Interoperabilidad).
Artículo 36	Ciclo de vida de servicios y sistemas	Integración de las especificaciones y requisitos de seguridad desde la concepción, diseño e implantación de los sistemas y servicios TIC.
Artículo 37	Mecanismos de control	Establecimiento de canales internos de supervisión, verificación y seguimiento para garantizar de manera real y efectiva que el sistema cumple el ENS.
Artículo 38	Procedimientos de determinación de conformidad	Diferencia la Certificación de Conformidad para sistemas de categoría Media o Alta, que requiere auditoría, y la Declaración de Conformidad para sistemas de categoría Básica, que exige autoevaluación. Permite convertir el cumplimiento interno en evidencia formal y publicable.
CAPÍTULO VI	**Actualización del Esquema Nacional de Seguridad**	**Adaptación al estado de la ciberseguridad y las amenazas.**
Artículo 39	Actualización permanente	El ENS se mantendrá actualizado de forma permanente en paralelo al avance tecnológico, la evolución reglamentaria de la Unión Europea y los vectores de ataque.
CAPÍTULO VII	**Procedimiento de categorización de los sistemas**	**Graduación proporcional del nivel de protección.**
Artículo 40	Categorías de seguridad	Clasificación en Básica, Media y Alta, modulando el esfuerzo de seguridad de forma proporcional a la valoración del impacto.
Artículo 41	Facultades	La valoración de impacto en la información y los servicios corresponde a los Responsables de la Información y los Servicios. La determinación de la

CAPÍTULO / ARTÍCULO	RÚBRICA / TÍTULO	CONTENIDO Y REQUISITOS CLAVE DEL ENS
		categoría final del sistema corresponde al Responsable de la Seguridad.

PARTE II: DISPOSICIONES ADICIONALES, TRANSITORIAS Y FINALES

DISPOSICIÓN	TÍTULO / ÁMBITO	MANDATO Y REQUISITO TÉCNICO
Disposición Adicional 1ª	Formación	El CCN y el INAP desarrollarán programas continuos de formación, sensibilización y concienciación dirigidos al personal público para el despliegue del ENS.
Disposición Adicional 2ª	Desarrollo del ENS	Prevé la aprobación de Instrucciones Técnicas de Seguridad de obligado cumplimiento, a propuesta de la Comisión Sectorial de Administración Electrónica y a iniciativa del CCN, y atribuye al CCN la elaboración y difusión de las guías CCN-STIC, en particular las de la serie 800, para facilitar el mejor cumplimiento del ENS.
Disposición Adicional 3ª	Principio de «no causar un perjuicio significativo»	Las actuaciones realizadas en el marco del Plan de Recuperación, Transformación y Resiliencia deberán respetar el principio de «no causar un perjuicio significativo» al medioambiente y las condiciones de etiquetado climático y digital que resulten aplicables.
Disposición Transitoria Única	Adecuación de sistemas	Concede un plazo improrrogable de **veinticuatro meses** (vencido el 5 de mayo de 2024) para la plena adecuación de sistemas preexistentes al nuevo RD 311/2022.
Disposición Derogatoria Única	Derogación normativa	Queda completamente derogado el anterior Real Decreto 3/2010, de 8 de enero, así como cualquier norma de igual o inferior rango que se oponga al nuevo ENS.
Disposición Final 1ª	Títulos competenciales	Se dicta al amparo del artículo 149.1 de la Constitución Española, que atribuye competencia exclusiva al Estado en las bases del régimen jurídico de las Administraciones Públicas (18.ª), telecomunicaciones (21.ª) y seguridad pública (29.ª).
Disposición Final 2ª	Desarrollo normativo	Habilita al Ministerio competente en materia de transformación digital y función pública para dictar las disposiciones necesarias para la aplicación y desarrollo del Real Decreto, dentro de sus competencias.

DISPOSICIÓN	TÍTULO / ÁMBITO	MANDATO Y REQUISITO TÉCNICO
Disposición Final 3ª	Entrada en vigor	Entrada en vigor al día siguiente de su publicación en el Boletín Oficial del Estado (BOE).

PARTE III: LOS CUATRO ANEXOS TÉCNICOS DEL REAL DECRETO

ANEXO TÉCNICO	NOMBRE Y PROPÓSITO	SÍNTESIS Y LÓGICA TÉCNICA DE APLICACIÓN
ANEXO I	**Categorías de seguridad de los sistemas**	Establece el procedimiento de categorización formal. 4. **Valoración de impacto:** Se valora el impacto (Bajo, Medio, Alto) que tendría un incidente que comprometa cualquiera de las **cinco dimensiones de seguridad: Confidencialidad (C), Integridad (I), Disponibilidad (D), Autenticidad (A) y Trazabilidad (T)**. 5. **Determinación de la categoría del sistema:** El sistema se clasifica en **BÁSICA** (si el nivel máximo de cualquier dimensión es Bajo), **MEDIA** (si el nivel máximo es Medio y ninguno superior), o **ALTA** (si al menos una dimensión alcanza nivel Alto). 6. Las guías de la serie CCN-STIC 803 precisan estos criterios.
ANEXO II	**Medidas de Seguridad**	Detalla el catálogo de **73 medidas de seguridad** organizadas en tres bloques estructurales: 2.4 **Marco Organizativo (org - 4 medidas):** Política, normativa interna, procedimientos y autorización. 2.5 **Marco Operacional (op – 7 apartados, 33 medidas):** Planificación, control de acceso, explotación, recursos externos, continuidad, servicios en la nube y monitorización. 2.6 **Medidas de Protección (mp – 8 apartados, 36 medidas):** Instalaciones, personal, equipos, comunicaciones, soportes de información, aplicaciones, información y protección de servicios. Gradúa el nivel de aplicación mediante el uso de la voz *"aplica"* o *"n.a. (no aplica)"* y establece **refuerzos de seguridad (R)** incrementales según la categoría del sistema. Exige niveles de madurez específicos del proceso de seguridad: **L2 (Reproducible)** para categoría Básica, **L3 (Proceso definido)** para categoría Media, y **L4 (Gestionado y medible)** para categoría Alta.
ANEXO III	**Auditoría de la seguridad**	Define las condiciones para verificar de manera objetiva el cumplimiento del ENS: 1. **Objeto:** Constatar la gobernanza, segregación de

ANEXO TÉCNICO	NOMBRE Y PROPÓSITO	SÍNTESIS Y LÓGICA TÉCNICA DE APLICACIÓN
		funciones, análisis de riesgos y la Declaración de Aplicabilidad. 2. **Procedimiento:** Recopilación de evidencias (documentales, técnicas, entrevistas con personal). 3. **Evidencia de conformidad:** Informes de autoevaluación firmados para categoría Básica (auditoría opcional), e informes de auditoría de certificación formal para sistemas de categoría Media o Alta.
ANEXO IV	**Glosario de términos**	Contiene las definiciones normativas y conceptuales necesarias para la interpretación del esquema, incluyendo conceptos como *Activo, Distintivo de Conformidad, Perfil de Cumplimiento Específico, Firma Electrónica Cualificada, Dominio de Seguridad y Usuario Externo.*

A continuación, y a efectos de garantizar la máxima fidelidad jurídica y facilitar la consulta operativa de las salvaguardas exigibles, se incorpora, de forma íntegra y literal, la tabla de correspondencia de medidas de seguridad y sus respectivos refuerzos publicada en el Boletín Oficial del Estado (BOE) como parte del Anexo II del Real Decreto 311/2022. Este catálogo estructurado vincula cada una de las medidas organizativas, operacionales y de protección con las dimensiones de ciberseguridad afectadas (Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad), precisando rigurosamente su exigencia de aplicación técnica y los refuerzos obligatorios (R) que deben implementarse de manera proporcional según la categoría (Básica, Media o Alta) del sistema de información bajo el alcance:

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
org	**Marco organizativo**				
org.1	Política de seguridad	Categoría	aplica	aplica	aplica
org.2	Normativa de seguridad	Categoría	aplica	aplica	aplica
org.3	Procedimientos de seguridad	Categoría	aplica	aplica	aplica
org.4	Proceso de autorización	Categoría	aplica	aplica	aplica
op	**Marco operacional**				
op.pl	Planificación				
op.pl.1	Análisis de riesgos	Categoría	aplica	+ R1	+ R2
op.pl.2	Arquitectura de Seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.pl.3	Adquisición de nuevos componentes	Categoría	aplica	aplica	aplica
op.pl.4	Dimensionamiento/gestión de la capacidad	D	aplica	+ R1	+ R1

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
op.pl.5	Componentes certificados	Categoría	n.a.	aplica	aplica
op.acc	Control de acceso				
op.acc.1	Identificación	T A	aplica	+ R1	+ R1
op.acc.2	Requisitos de acceso	C I T A	aplica	aplica	+ R1
op.acc.3	Segregación de funciones y tareas	C I T A	n.a.	aplica	+ R1
op.acc.4	Proceso de gestión de derechos de acceso	C I T A	aplica	aplica	aplica
op.acc.5	Mecanismo de autenticación (usuarios externos)	C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	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
op.exp	Explotación				
op.exp.1	Inventario de activos	Categoría	aplica	aplica	aplica
op.exp.2	Configuración de seguridad	Categoría	aplica	aplica	aplica
op.exp.3	Gestión de la configuración de seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.exp.4	Mantenimiento y actualizaciones de seguridad	Categoría	aplica	+ R1	+ R1 + R2
op.exp.5	Gestión de cambios	Categoría	n.a.	aplica	+ R1
op.exp.6	Protección frente a código dañino	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
op.exp.7	Gestión de incidentes	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3
op.exp.8	Registro de la actividad	T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5
op.exp.9	Registro de la gestión de incidentes	Categoría	aplica	aplica	aplica
op.exp.10	Protección de claves criptográficas	Categoría	aplica	+ R1	+ R1
op.ext	Recursos externos				
op.ext.1	Contratación y acuerdos de nivel de servicio	Categoría	n.a.	aplica	aplica
op.ext.2	Gestión diaria	Categoría	n.a.	aplica	aplica
op.ext.3	Protección de la cadena de suministro	Categoría	n.a.	n.a.	aplica
op.ext.4	Interconexión de sistemas	Categoría	n.a.	aplica	+ R1
op.nub	Servicios en la nube				
op.nub.1	Protección de servicios en la nube	Categoría	aplica	+ R1	+ R1 + R2
op.cont	Continuidad del servicio				

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
op.cont.1	Análisis de impacto	D	n.a.	aplica	aplica
op.cont.2	Plan de continuidad	D	n.a.	n.a.	aplica
op.cont.3	Pruebas periódicas	D	n.a.	n.a.	aplica
op.cont.4	Medios alternativos	D	n.a.	n.a.	aplica
op.mon	Monitorización del sistema				
op.mon.1	Detección de intrusión	Categoría	aplica	+ R1	+ R1 + R2
op.mon.2	Sistema de métricas	Categoría	aplica	+ R1 + R2	+ R1 + R2
op.mon.3	Vigilancia	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 + R6
mp	Medidas de protección				
mp.if	Protección de las instalaciones e infraestructuras				
mp.if.1	Áreas separadas y con control de acceso	Categoría	aplica	aplica	aplica
mp.if.2	Identificación de las personas	Categoría	aplica	aplica	aplica
mp.if.3	Acondicionamiento de los locales	Categoría	aplica	aplica	aplica
mp.if.4	Energía eléctrica	D	aplica	+ R1	+ R1
mp.if.5	Protección frente a incendios	D	aplica	aplica	aplica
mp.if.6	Protección frente a inundaciones	D	n.a.	aplica	aplica
mp.if.7	Registro de entrada y salida de equipamiento	Categoría	aplica	aplica	aplica
mp.per	Gestión del personal				
mp.per.1	Caracterización del puesto de trabajo	Categoría	n.a.	aplica	aplica
mp.per.2	Deberes y obligaciones	Categoría	aplica	+ R1	+ R1
mp.per.3	Concienciación	Categoría	aplica	aplica	aplica
mp.per.4	Formación	Categoría	aplica	aplica	aplica
mp.eq	Protección de los equipos				
mp.eq.1	Puesto de trabajo despejado	Categoría	aplica	+ R1	+ R1
mp.eq.2	Bloqueo de puesto de trabajo	A	n.a.	aplica	+ R1
mp.eq.3	Protección de dispositivos portátiles	Categoría	aplica	aplica	+ R1 + R2
mp.eq.4	Otros dispositivos conectados a la red	C	aplica	+ R1	+ R1
mp.com	Protección de las comunicaciones				
mp.com.1	Perímetro seguro	Categoría	aplica	aplica	aplica
mp.com.2	Protección de la confidencialidad	C	aplica	+ R1	+ R1 + R2 + R3
mp.com.3	Protección de la integridad y de la autenticidad	I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
mp.com.4	Separación de flujos de información en la red	Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4
mp.si	Protección de los soportes de información				
mp.si.1	Marcado de soportes	C	n.a.	aplica	aplica
mp.si.2	Criptografía	C I	n.a.	aplica	+ R1 + R2
mp.si.3	Custodia	Categoría	aplica	aplica	aplica
mp.si.4	Transporte	Categoría	aplica	aplica	aplica
mp.si.5	Borrado y destrucción	C	aplica	+ R1	+ R1
mp.sw	Protección de las aplicaciones informáticas				
mp.sw.1	Desarrollo de aplicaciones	Categoría	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4
mp.sw.2	Aceptación y puesta en servicio	Categoría	aplica	+ R1	+ R1
mp.info	Protección de la información				
mp.info.1	Datos personales	Categoría	aplica	aplica	aplica
mp.info.2	Calificación de la información	C	n.a.	aplica	aplica
mp.info.3	Firma electrónica	I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4
mp.info.4	Sellos de tiempo	T	n.a.	n.a.	aplica
mp.info.5	Limpieza de documentos	C	aplica	aplica	aplica
mp.info.6	Copias de seguridad	D	aplica	+ R1	+ R1 + R2
mp.s	Protección de los servicios				
mp.s.1	Protección del correo electrónico	Categoría	aplica	aplica	aplica
mp.s.2	Protección de servicios y aplicaciones web	Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3
mp.s.3	Protección de la navegación web	Categoría	aplica	aplica	+ R1
mp.s.4	Protección frente a denegación de servicio	D	n.a.	aplica	+ R1

ANEXO II. CUADRO RESUMEN DE LAS CUATRO ITS

Las Instrucciones Técnicas de Seguridad (ITS) se configuran como normas técnicas de desarrollo de obligado cumplimiento, dictadas formalmente al amparo de la Disposición Adicional Segunda del Real Decreto 311/2022. Mientras que el artículo 156.2 de la Ley 40/2015 y el propio Real Decreto constituyen los cimientos legislativos y la base operativa fundamental del Esquema Nacional de Seguridad, las ITS actúan en un segundo nivel normativo con el propósito de detallar, concretar y dotar de operatividad real a las exigencias generales de la norma.

Su función primordial no es redefinir la arquitectura estructural del ENS, sino proporcionar los procedimientos, variables de datos y criterios técnicos necesarios para garantizar una aplicación homogénea, comparable y coordinada del modelo en todo el sector público y su cadena de suministro.

Asimismo, de conformidad con el mandato de actualización permanente, las ITS sirven como herramientas dinámicas que permiten adaptar el marco técnico a la rápida evolución de las amenazas y de la tecnología, preservando la estabilidad jurídica de la norma principal.




ITS de Auditoría de la Seguridad
Resolución: 27 de marzo de 2018
1
Resolución y objeto
Regular condiciones, metodología y mínimo del proceso.
2
Criterios técnicos
Auditoría regular ordinaria (cada 2 años para categoría media/alta)
Auditoría extraordinaria (modificaciones sustanciales)
Metodología (gobernanza, riesgos, Declaración de Aplicabilidad)
Documentos obligatorios (planes e informes)
3
Valor operativo
Garantiza una verificación independiente y eficaz, impidiendo que sea un mero trámite administrativo.
ENS · Instrucciones Técnicas de Seguridad


ITS de Notificación de Incidentes
Resolución: 13 de abril de 2018
1
Resolución y objeto
Regular el procedimiento técnico de notificación, gestión e intercambio de información.
2
Criterios técnicos
Notificación obligatoria a CCN-CERT (impacto significativo)
Determinación del impacto (criterios y plazos)
Procedimientos de respuesta (evidencias y cadena de custodia)
Coordinación y estadísticas (CCN-CERT / INCIBE-CERT)
3
Valor operativo
Articula un modelo de resiliencia nacional: del incidente individual al aprendizaje colectivo. La ventanilla única agiliza la respuesta.
ENS · Instrucciones Técnicas de Seguridad



Figura Anexo II.1 Resumen Esquema de las ITS del ENS

ANEXO III. RELACIÓN DE GUÍAS CCN-STIC DE LA SERIE 800

La serie 800 de las Guías de Seguridad de las Tecnologías de la Información y la Comunicación (CCN-STIC) constituye el pilar técnico y práctico indispensable para la operatividad del Esquema Nacional de Seguridad.

Su función primordial, fundamentada en la disposición adicional segunda del Real Decreto 311/2022, es orientar a las organizaciones en la implantación, interpretación y auditoría del modelo de seguridad español. Mientras que el Real Decreto y las Instrucciones Técnicas de Seguridad (ITS) definen el marco obligatorio, las Guías CCN-STIC explican detalladamente cómo aplicar correctamente dichas medidas, asegurando una homogeneización de criterios en todo el Sector Público y su cadena de suministro. Este cuerpo documental, que integra desde directrices de gobernanza hasta perfiles de cumplimiento específicos, es una pieza clave del ecosistema de confianza y se incorpora preceptivamente al conjunto de evidencias analizadas en los procesos de certificación.

Al igual que ocurre con las Instrucciones Técnicas de Seguridad, las Guías CCN-STIC son objeto de una constante revisión y actualización, adaptándose a nuevas realidades organizativas y técnicas, e introduciendo nuevos criterios de aplicación que permitan albergar la mayor casuística posible dentro de las distintas vertientes de la administración públicas.

Asimismo, conscientes de la singularidad de algunas situaciones o entidades (sector público, universidades, diputaciones), este modelo de guías técnicas alberga dichas situaciones, proponiendo modelos que encajan en dichas casuísticas, permitiendo un acercamiento más eficaz y ajustado a las necesidades de dichas entidades.



Figura Anexo III.1 Catálogo de Guías y documentos de apoyo del ENS

A continuación, se presenta una relación operativa de referencia de las guías y documentos de la serie 800. Al tratarse de un catálogo vivo, la relación debe contrastarse para usos formales con la carpeta oficial vigente del CCN-CERT, especialmente cuando se utilice en contextos europeos o internacionales:

Documento		Descripción
CCN-STIC 800	Glosario de términos y abreviaturas del ENS	Define formalmente la terminología, abreviaturas y conceptos técnicos y jurídicos de la seguridad de la información para unificar el lenguaje entre administraciones, proveedores y auditores.
CCN-STIC 801	ENS. Responsabilidades y funciones	Desarrolla el modelo de gobernanza del ENS, delimitando las atribuciones y competencias específicas de los roles de Responsable de la Información, del Servicio, de la Seguridad, del Sistema, así como el resto de roles que puedan verse implicados.
CCN-STIC 802	ENS. Guía de auditorías de cumplimiento	Fija los criterios técnicos, directrices metodológicas y evidencias documentales requeridas para planificar y ejecutar con rigor las auditorías de conformidad ordinarias y extraordinarias.
CCN-STIC 803	ENS. Valoración de los sistemas	Proporciona los criterios de impacto para analizar y graduar la criticidad de la información y los servicios en las cinco dimensiones de ciberseguridad, determinando la categoría del sistema.
CCN-STIC 804	Medidas de implantación del ENS	Traduce las salvaguardas abstractas del Anexo II del Real Decreto en especificaciones de control concretas para orientar la ejecución técnica de las mismas.
CCN-STIC 805	ENS. Política de Seguridad de la Información	Proporciona las directrices, secciones estructurales y modelos prácticos para la redacción, aprobación formal y revisión continuada de la Política de Seguridad requerida por los criterios del ENS.
CCN-STIC 806	Plan de Adecuación al ENS	Detalla la metodología y el cronograma de hitos operativos para transicionar ordenadamente desde un diagnóstico inicial hasta la obtención del certificado de conformidad.
CCN-STIC 807	Criptología de empleo en el ENS	Detalla los algoritmos criptográficos, longitudes de clave, protocolos de tránsito seguro y parámetros de cifrado que se encuentran

Documento		Descripción
		nominalmente autorizados por el CCN para salvaguardar información sensible.
CCN-STIC 808	Verificación del cumplimiento	Ofrece un inventario detallado de controles e indicadores concretos para auditar y monitorizar si cada una de las medidas del Anexo II ha sido efectivamente implantada y es evaluable en el tiempo.
CCN-STIC 809	Declaración, certificación y aprobación provisional de conformidad con el ENS y distintivos de cumplimiento	Exhibe los modelos oficiales para la Declaración de Conformidad con el ENS y la Certificación de Conformidad con el ENS, y contiene el régimen de los Distintivos de Conformidad (sellos) visibles que deben publicarse en las sedes electrónicas o páginas web para evidenciar el cumplimiento.
CCN-STIC 810	Creación de CERT's	Guía en la planificación, dotación presupuestaria, requisitos de personal técnico, infraestructuras y procedimientos necesarios para constituir un equipo de respuesta ante incidentes (CSIRT) integrado.
CCN-STIC 811	Interconexión en el Esquema Nacional de Seguridad	Regula las condiciones técnicas fronterizas, cortafuegos, pasarelas e interconexiones lógicas que deben aplicarse cuando el sistema del organismo intercambia información con redes o sistemas externos.
CCN-STIC 812	Seguridad en Entornos y Aplicaciones Web	Define los criterios de configuración segura, mitigación de vulnerabilidades de inyección de código, validación de entradas y protección específica para portales corporativos y sedes electrónicas.
CCN-STIC 813	Ciberseguridad de espacio de datos	Establece directrices para la protección, gobernanza e intercambio ciberseguro de flujos de datos a gran escala y entornos colaborativos multi-organización en línea con la soberanía digital.
CCN-STIC 814	Seguridad en el correo electrónico	Concreta las salvaguardas perimetrales, técnicas de filtrado de malware, mecanismos SPF/DKIM/DMARC y pautas de cifrado extremo a extremo para garantizar la confidencialidad del correo electrónico.
CCN-STIC 815	Indicadores y métricas en el ENS	Define el cuadro de mando de métricas operacionales que las organizaciones deben monitorizar de forma continua para medir de forma empírica la madurez real y efectividad de sus procesos de seguridad.

Documento		Descripción
CCN-STIC 816	Seguridad en las Redes Inalámbricas en el ENS	Detalla los protocolos de autenticación robusta, segmentación lógica de invitados y controles de radiofrecuencia necesarios para desplegar infraestructuras Wi-Fi seguras en dependencias públicas.
CCN-STIC 817	Gestión de Ciberincidentes	Normaliza los criterios comunes de clasificación de gravedad, impacto operativo, procedimientos de contención rápida y plazos formales para reportar ciberincidentes al CCN-CERT.
CCN-STIC 817	*National Security Framework cyber-incident management*	Versión inglesa de la guía CCN-STIC 817 sobre gestión de ciberincidentes en el marco del ENS.
CCN-STIC 818	Herramientas de Seguridad en el ENS	Presenta herramientas de seguridad de apoyo al ENS y orienta su uso para facilitar implantación, verificación y operación.
CCN-STIC 819	Medidas compensatorias	Orienta la justificación, documentación y uso de medidas compensatorias cuando una medida del ENS se sustituya por otra equivalente o superior.
CCN-STIC 820	Protección contra Denegación de Servicio	Establece criterios y pautas de protección frente a ataques de denegación de servicio, especialmente en servicios expuestos o de alta disponibilidad.
CCN-STIC 821	Normas de Seguridad en el ENS	Orienta la elaboración de normas internas de seguridad dentro del sistema documental del ENS.
CCN-STIC 822	Procedimientos de Seguridad	Orienta la elaboración de procedimientos de seguridad como desarrollo operativo de la política y normativa de seguridad.
CCN-STIC 823	Seguridad en entornos Cloud	Determina los requisitos y responsabilidades técnicas exigibles según el modelo de despliegue cloud (SaaS, PaaS, IaaS) y define las condiciones de auditoría para proveedores de nube pública.
CCN-STIC 823	*Use of Cloud Services*	
CCN-STIC 824	Información del Estado de Seguridad	Detalla los parámetros y la sistemática de reporte anual para que los organismos cumplimenten adecuadamente sus indicadores de ciberseguridad corporativos ante el CCN-CERT.
CCN-STIC 825	Esquema Nacional de Seguridad. Certificaciones 27001	Analiza las equivalencias de controles y regula la metodología de mapeo para que las entidades aprovechan de forma eficiente una certificación internacional ISO/IEC 27001 en su adecuación al ENS.

Documento		Descripción
CCN-STIC 825	*National Security Framework. 27001 Certifications*	Versión inglesa de la guía sobre certificaciones ISO/IEC 27001 y su relación con el ENS.
CCN-STIC 826	Implementación de Seguridad Nextcloud	Guía de implantación y configuración segura de Nextcloud en el marco del ENS.
CCN-STIC 827	Gestión y uso de dispositivos móviles	Define criterios para la gestión y uso seguro de dispositivos móviles en sistemas sometidos al ENS.
CCN-STIC 830	Ámbito de aplicación del ENS	Clarifica el ámbito subjetivo y objetivo de aplicación del ENS, incluyendo entidades públicas, sector privado proveedor y supuestos de aplicación funcional.
CCN-STIC 831	Registro de actividad de los usuarios	Detalla criterios sobre registro de actividad de los usuarios, trazabilidad, conservación y explotación de evidencias.
CCN-STIC 834	Protección ante el Código Dañino en el ENS	Guía para prevención, detección y respuesta frente a código dañino en sistemas incluidos en el ámbito del ENS.
CCN-STIC 835	Borrado de metadatos en el marco del ENS	Establece pautas para el borrado de metadatos en documentos y ficheros dentro del marco del ENS.
CCN-STIC 836	Seguridad en VPN en el marco del ENS	Establece pautas de diseño, configuración y operación segura de redes privadas virtuales en el marco del ENS.
CCN-STIC 837	ENS. Seguridad en Bluetooth	Identifica los vectores de ataque en redes de área personal de proximidad y establece directrices para restringir, desactivar o parametrizar el emparejamiento ciberseguro de periféricos.
CCN-STIC 844	Manual de usuario de INES	Guía técnica y de interfaz para facilitar a los CISO y responsables públicos la introducción sistemática y consolidación de sus datos de ciberseguridad en la plataforma estatal de reporte.
CCN-STIC 845 A	LUCIA. Manual de usuario	Conjunto de manuales operativos para el despliegue de la herramienta de gestión federada de tickets de incidentes de seguridad e interconexión con el sistema de alerta nacional del CCN-CERT.
CCN-STIC 845 B	LUCIA. Manual de usuario SAT	
CCN-STIC 845 C	LUCIA. Manual instalación organismo	

Documento		Descripción
CCN-STIC 852	Perfil de cumplimiento específico. Organismos pagadores	Perfil de Cumplimiento Específico que adapta de manera proporcional y concreta las salvaguardas del Anexo II para los sistemas que gestionan fondos agrícolas y de la PAC.
CCN-STIC 852	*Specific Compliance Profile. Paying Agencies*	
CCN-STIC 857	Requisitos Seguridad para aplicaciones de Cibersalud	Establece las medidas técnicas, autenticación de pacientes y protección de datos médicos requeridos por el ENS para el desarrollo y despliegue seguro de apps sanitarias de cara al ciudadano.
CCN-STIC 857	*Security requirements for E-Healthy Applications in the context of the ENS*	
CCN-STIC 858	Implantación de sistemas SaaS en modo local (on premise)	Regula el régimen de control y auditoría necesario cuando un organismo aloja en infraestructuras propias plataformas de Software como Servicio que habitualmente operan en nube remota.
CCN-STIC 860	Seguridad en el servicio OWA Exchange Server 2010	Guía técnica de bastionado y mitigación de riesgos de exposición para el acceso web al servicio de correo electrónico corporativo bajo infraestructuras Microsoft legadas.
CCN-STIC 869	Implementación de Applocker en el Esquema Nacional de Seguridad	Detalla cómo configurar y desplegar políticas de restricción de software basadas en listas blancas a través de Applocker para evitar la ejecución de ejecutables no autorizados en el puesto de trabajo.
CCN-STIC 875	Implementación del ENS con MS SCCM 2012 R2	Guía práctica para utilizar Microsoft System Center Configuration Manager en la distribución centralizada de parches, auditoría de software y control de inventario técnico.
CCN-STIC 881	Adecuación al ENS para Universidades	Adapta las directrices de adecuación del ENS y unifica los criterios de control y alcance de auditoría específicos para los sistemas de información de los entornos universitarios públicos.
CCN-STIC 881 A	Perfil de cumplimiento específico Universidades	
CCN-STIC 882	Guía de Análisis de Riesgos para Entidades Locales	Proporciona una metodología de análisis simplificada y adaptada para ayuntamientos y diputaciones, alineada con MAGERIT y asistida por la herramienta PILAR
CCN-STIC 883	Guía de Implementación del	Ofrece el catálogo de Perfiles de Cumplimiento Específicos para ayuntamientos de menos de

Documento		Descripción
	ENS para Entidades Locales	2.000 hab., menos de 20.000 hab., entre 20.000 y 75.000 hab. y para Diputaciones
CCN-STIC 883 A	Perfil de cumplimiento específico Ayuntamientos pequeños y con limitados recursos (hasta 5000 habitantes)	
CCN-STIC 883 B	Perfil de cumplimiento específico Ayuntamientos de menos de 20000 habitantes	
CCN-STIC 883 C	Perfil de cumplimiento específico Ayuntamientos entre 20000 y 75000 habitantes	
CCN-STIC 883 D	Perfil de cumplimiento específico Diputaciones	
CCN-STIC 884	Perfil de cumplimiento específico Azure	Define el perfil y las guías detalladas para el bastionado seguro de servicios e infraestructuras en la nube de Microsoft Azure, abarcando Kubernetes, SQL Databases, servicios de IA, Sentinel e Intune
CCN-STIC 884	*Specific Compliance Profile for Azure Corporate Cloud Service*	
CCN-STIC 884 A	Guía de Configuración para Azure	
CCN-STIC 884 B	Guía de Configuración segura para Kubernetes Services	
CCN-STIC 884 B	*Secure configuration guide for Azure Kubernetes Services*	
CCN-STIC 884 C	Guía de configuración segura para SQL Database	
CCN-STIC 884 D	Guía de configuración segura para servicios de IA	
CCN-STIC 884 E	Guía de configuración segura para Microsoft	

Documento		Descripción
	Sentinel	
CCN-STIC 884 F	Guía de configuración segura para Microsoft Intune	
CCN-STIC 885	Perfil de cumplimiento específico Office 365	Detalla la arquitectura de seguridad y la configuración técnica de bastionado para las herramientas de Microsoft 365, incluyendo Teams, Exchange Online, Sharepoint y Defender.
CCN-STIC 885	*Specific compliance profile Corporate Cloud Service*	
CCN-STIC 885 ES	Escenario de nube para el manejo de información sensible en Microsoft Office 365	
CCN-STIC 885 A	Guía de configuración segura para Office 365	
CCN-STIC 885 B	Guía de configuración segura para Sharepoint Online	
CCN-STIC 885 C	Guía de configuración segura para Exchange Online	
CCN-STIC 885 C	*Secure configuration guide for Exchange Online*	
CCN-STIC 885 D	Guía de configuración segura para Microsoft Teams	
CCN-STIC 885 D	*Secure configuration guide for Microsoft Teams*	
CCN-STIC 885 E	Guía de configuración segura para Microsoft Defender for Endpoint	
CCN-STIC 885 F	Guía de configuración segura para Microsoft Defender for Identity	
CCN-STIC 885 G	Guía de configuración segura para Microsoft Defender for Office 365	
CCN-STIC 886	Perfil de cumplimiento	Especificaciones técnicas del perfil de

Documento		Descripción
	específico para LORETO-NG BASE	cumplimiento y bastionado para la solución corporativa de almacenamiento en la nube de forma segura y centralizada del CCN.
CCN-STIC 887	Perfil de cumplimiento específico para AWS Servicio de Cloud Corporativo	Establece las pautas y configuraciones detalladas para garantizar que el despliegue de servicios e infraestructuras en Amazon Web Services cumple el ENS, incluyendo conectividad híbrida y monitorización.
CCN-STIC 887 A	Guía de configuración segura AWS	
CCN-STIC 887 B	Guía rápida de Prowler	
CCN-STIC 887 C	Guía de Configuración Segura de Conectividad Híbrida en AWS	
CCN-STIC 887 D	Guía de configuración segura Multi Cuenta AWS	
CCN-STIC 887 E	Guía de configuración segura Amazon WorkSpaces	
CCN-STIC 887 F	Guía de respuesta a incidentes en AWS	
CCN-STIC 887 G	Guía de Configuración segura para Monitorización y gestión AWS	
CCN-STIC 888	Perfil de Cumplimiento específico para Google Cloud Servicio de Cloud Corporativo	Define el perfil de conformidad y el bastionado paso a paso para el uso seguro de las plataformas corporativas de Google Cloud y Google Workspace en la administración digital.
CCN-STIC 888 A	Guía de configuración segura para Google WorkSpace	
CCN-STIC 888 B	Guía de configuración segura para GCP	
CCN-STIC 888 C	Guía de Configuración Segura para Contenedores	
CCN-STIC 889	Perfil de cumplimiento especifico Oracle Cloud	Regula las especificaciones de cumplimiento y el bastionado de bases de datos, sistemas híbridos,

Documento		Descripción
	Servicio de Cloud Corporativo	IAM, Oracle SaaS y sistemas de despliegue en entornos federados de Oracle.
CCN-STIC 889 A	Guía de configuración segura para IAM y servicios de seguridad	
CCN-STIC 889 B	Guía de configuración segura para monitorización y gestión	
CCN-STIC 889 C	CS Oracle OCI Arquitecturas Híbridas	
CCN-STIC 889 D	CS Oracle OCI Database Instancias VM	
CCN-STIC 889 E	CS Oracle OCI Compute Instancias VM y Bare Metal	
CCN-STIC 889 F	CS Oracle C@C Sistemas Exadata Autonomous DB	
CCN-STIC 889 G	Perfil de Cumplimiento Específico Oracle Cloud SaaS Servicio de Cloud Corporativo	
CCN-STIC 889 H	Guía de Configuración segura para Oracle SaaS Enterprise Performance Management EPM	
CCN-STIC 889 I	Guía de Configuración segura para Oracle SaaS FusionApplications	
CCN-STIC 889 J	Guía de configuración segura de Oracle SaaS Fusion y EPM Applications bajo entorno EURA	
CCN-STIC 889 K	Guía de Configuración Segura de Oracle Roving Edge Infrastructure	
CCN-STIC 890	Adecuación al ENS conforme al Perfil de	Establece un modelo simplificado y ágil de cumplimiento de requisitos técnicos mínimos

Documento		Descripción
	Cumplimiento Específico de Requisitos Fundamentales de Seguridad	esenciales enfocado especialmente en Entidades Locales de pequeño tamaño.
CCN-STIC 890 A	Perfil de Cumplimiento Específico de Requisitos Fundamentales de Seguridad - Entidades Locales	
CCN-STIC 890 C	Perfil de Cumplimiento Específico de Requisitos Fundamentales de Seguridad - Entidades de menor tamaño	
CCN-STIC 891	Perfil de Cumplimiento Específico para Salud Prestación sanitaria a pacientes (Atención Primaria y Atención Especializada)	Perfil de Cumplimiento Específico para Salud, relativo a la prestación sanitaria a pacientes en Atención Primaria y Atención Especializada.
CCN-STIC 896	Perfil de Cumplimiento Específico para Servicios de Seguridad Gestionados / PCE-SSG	Perfil de Cumplimiento Específico para Servicios de Seguridad Gestionados / PCE-SSG.
CCN-STIC 897	Perfil de Cumplimiento Específico para la Administración de Justicia	Perfil de Cumplimiento Específico para la Administración de Justicia.

Complementando el catálogo de la serie 800, existe un conjunto de Guías e Informes de Buenas Prácticas, si bien se encuadran en otras series del Centro Criptológico Nacional, resultan de obligada referencia y especial relevancia para la implantación práctica del ENS:

Documento		Descripción
CCN-STIC 105	Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación	Esta guía recoge el **Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC)** del CCN, el cual relaciona los productos y servicios de seguridad cualificados y aprobados por el organismo. Su propósito principal es servir de referencia para seleccionar de forma proporcionada los componentes que formarán parte de la arquitectura de seguridad del sistema.
CCN-	Organización y gestión	Se trata de una guía específica de gobernanza orientada

Documento		Descripción
STIC 201	para la seguridad de las TIC	a establecer un marco de referencia y definir responsabilidades para la organización y gestión de la seguridad de las tecnologías de la información y las comunicaciones (TIC) en entidades que manejan información clasificada.
CCN-CERT BP/01	Principios y recomendaciones básicas en Ciberseguridad	Se trata de un **Informe de Buenas Prácticas** enfocado en proporcionar las directrices, principios y recomendaciones esenciales para elevar la postura de ciberseguridad de las organizaciones.
CCN-CERT BP/14	Declaración de aplicabilidad ENS	El objetivo principal es explicar de forma clara y detallada el procedimiento para definir y elaborar la Declaración de Aplicabilidad (DdA) en el ámbito del Esquema Nacional de Seguridad (ENS).
CCN-CERT BP/20	Buenas prácticas en la gestión de cibercrisis	El objetivo principal del documento es proporcionar a las organizaciones una guía estructurada para preparar, gestionar y superar de forma eficaz una crisis de ciberseguridad, evitando respuestas puramente reactivas frente a incidentes graves

ANEXO IV. RESUMEN SINTÉTICO DE LAS GUÍAS CCN-STIC DE LA SERIE 800 DE ESPECIAL RELEVANCIA PRÁCTICA

El presente anexo ofrece una síntesis de las Guías de Seguridad de las Tecnologías de la Información y la Comunicación (CCN-STIC) de la serie 800 que poseen una mayor trascendencia operativa para la adecuación al Esquema Nacional de Seguridad. Estas guías, cuya elaboración y difusión corresponde al Centro Criptológico Nacional en virtud de la disposición adicional segunda del Real Decreto 311/2022, constituyen el soporte técnico y metodológico indispensable para la correcta interpretación e implantación de los principios, requisitos y medidas de seguridad del modelo español. Mientras que el Real Decreto y las Instrucciones Técnicas de Seguridad definen el marco normativo de obligado cumplimiento, las Guías CCN-STIC concretan de forma práctica cómo las organizaciones deben articular sus capacidades de gobernanza, operación y protección de activos.

A continuación, se presentan aquellas guías de la serie 800 que revisten una especial relevancia y aplicabilidad práctica en el marco del citado Esquema:

CCN-STIC 801: RESPONSABILIDADES Y FUNCIONES EN EL ENS

Esta guía desarrolla el principio de diferenciación de responsabilidades, esencial para que la seguridad sea una función organizativa estratégica. El marco define cuatro figuras clave con misiones diferenciadas: el Responsable de la Información (que determina los requisitos de los datos), el Responsable del Servicio (que define los requisitos de la prestación), el Responsable de la Seguridad (encargado de las decisiones para satisfacer los requisitos técnicos) y el Responsable del Sistema (responsable de la implementación y operación diaria). Esta estructura evita que la seguridad sea una cuestión reactiva, asignando deberes claros en cada nivel.

Para evitar el "atrapamiento operacional" donde las decisiones de seguridad quedan supeditadas a la explotación técnica, la guía impone la obligatoriedad de la independencia jerárquica entre el responsable de seguridad y el del sistema. Esta separación actúa como un control interno irrenunciable para evitar conflictos de interés, el primero decide qué salvaguardas son necesarias, mientras el segundo ejecuta su integración. Solo en casos excepcionales por falta de recursos se admite la coincidencia de roles, siempre que se documenten formalmente medidas compensatorias que preserven la integridad del modelo.

CCN-STIC 802: GUÍA DE AUDITORÍA DEL ENS

El objeto de esta guía es regular la auditoría regular ordinaria que debe realizarse obligatoriamente al menos cada dos años. Su función es verificar de manera sistemática y objetiva que el sistema cumple con los requerimientos del ENS, validando que la categorización sea correcta y que las medidas de seguridad implantadas sean efectivas ante los riesgos reales. La auditoría conecta la documentación de seguridad con la realidad técnica de los sistemas, asegurando que la protección no sea una fotografía estática sino un proceso dinámico de mejora continua.

La guía sintetiza los niveles de auditoría y detalla la obligatoriedad de presentar el informe final ante los responsables del sistema y de seguridad. Este documento debe identificar los hallazgos de cumplimiento y las deficiencias detectadas, sirviendo de base preceptiva para que el responsable del sistema adopte las medidas correctoras necesarias. La supervisión de estos informes garantiza que la dirección de la entidad posea una visión fidedigna de su superficie de exposición y de la diligencia debida en la protección de los servicios públicos digitales.

CCN-STIC 803: VALORACIÓN DE SISTEMAS EN EL ENS

Esta directriz establece el procedimiento técnico para valorar el impacto de incidentes sobre las funciones y activos de la organización. La valoración se fundamenta en el análisis de seis dimensiones esenciales de seguridad, conforme al estándar absoluto del RD 311/2022: Confidencialidad, Integridad, Trazabilidad, Autenticidad, Disponibilidad (C-I-T-A-D). Este enfoque integral permite medir el perjuicio potencial —limitado, grave o muy grave— que un compromiso de la seguridad causaría sobre la entidad o los ciudadanos.

La valoración obtenida determina los niveles de seguridad específicos (Bajo, Medio o Alto) para cada una de las dimensiones mencionadas. En última instancia, esta evaluación técnica es la que fija la categoría del sistema (Básica, Media o Alta), modulando de forma proporcional el esfuerzo de seguridad requerido. Al vincular directamente la importancia de la información con las salvaguardas necesarias, la guía asegura que los recursos de ciberseguridad se asignen de manera eficiente y equilibrada a la criticidad de los servicios sustentados.

CCN-STIC 804: MEDIDAS DE IMPLANTACIÓN DEL ENS

La guía define la estructura operativa de las medidas de seguridad, organizándolas en tres marcos fundamentales: Organizativo (gestión global), Operacional (protección de la operación integral) y de Protección (activos específicos como comunicaciones o soportes). Esta división permite un despliegue ordenado de controles que cubren los ámbitos humano, material y técnico del sistema. La correcta aplicación de estos marcos garantiza que la seguridad se integre en todas las capas del servicio, desde la política de gobernanza hasta el último dispositivo periférico.

Para asegurar una protección ajustada al riesgo, la guía detalla la aplicación de refuerzos de seguridad (R) en función de la categoría del sistema. Estos refuerzos se añaden a los requisitos base de cada medida para elevar la resiliencia de forma granular. El resultado final se formaliza en la Declaración de Aplicabilidad, donde se seleccionan y justifican las salvaguardas precisas. Este método asegura que la entidad implemente una protección proporcionada, evitando cargas innecesarias en sistemas de baja criticidad y garantizando robustez extrema en infraestructuras críticas.

CCN-STIC 805: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta guía detalla el contenido mínimo obligatorio de la Política de Seguridad, el documento de mayor nivel en la gobernanza de la información. Debe integrar los objetivos de la organización, el marco regulatorio, la definición de roles y la estructura de los comités de gestión. Al establecer las directrices de alto nivel, la política garantiza que la ciberseguridad sea tratada como una función estratégica dirigida por la gerencia, y no meramente como un apéndice técnico de los departamentos de informática.

La política actúa como el pilar de la gobernanza y debe ser aprobada formalmente por el órgano que ostente las máximas competencias ejecutivas de la entidad. Su aprobación formal vincula a todo el personal y manifiesta el compromiso de la dirección con el cumplimiento normativo. Una vez establecida, debe ser conocida por todos los miembros de la organización y servir como base jerárquica para el desarrollo de la normativa técnica y los procedimientos operativos que concretan la seguridad en el día a día.

CCN-STIC 806: PLAN DE ADECUACIÓN AL ENS

La guía describe el proceso estructurado de transición para que tanto los sistemas preexistentes como los nuevos alcancen la plena conformidad con el ENS. Para los sistemas nuevos, se enfatiza el principio de seguridad desde el diseño, integrando los requisitos desde su concepción. Para los sistemas ya operativos, establece un marco cronológico de adecuación (con un plazo de 24 meses según la transitoria única) que permite identificar brechas y planificar medidas correctoras sin interrumpir la prestación del servicio.

En este proceso, la guía destaca hitos críticos de adecuación, incluyendo el inventario detallado de activos y la realización del análisis de riesgos inicial. Estos elementos son los cimientos sobre los que se construye el sistema de gestión de seguridad. El plan de adecuación culmina con la obtención del distintivo de conformidad, una evidencia pública de que la entidad ha integrado satisfactoriamente los principios básicos y requisitos mínimos exigidos por el Real Decreto 311/2022.

CCN-STIC 808: VERIFICACIÓN DEL CUMPLIMIENTO DEL ENS

Esta guía explica la función operativa del Anexo III del ENS a través de la Tabla de Verificación, una herramienta indispensable para auditores y responsables de seguridad. La tabla desglosa cada medida en criterios de cumplimiento objetivos y verificables, facilitando una comprobación técnica rigurosa. Su uso estandariza los procesos de revisión a nivel nacional, asegurando que cualquier sistema, independientemente de su ubicación geográfica o administrativa, sea evaluado bajo criterios homogéneos y transparentes.

El documento detalla el uso de los niveles de cumplimiento para generar evidencias tangibles sobre el estado real de la seguridad. Al asignar valoraciones a la implementación de cada control, los responsables pueden detectar áreas críticas de

mejora y justificar inversiones tecnológicas. Esta metodología de verificación transforma los requisitos normativos en datos de gestión estratégica, permitiendo una toma de decisiones basada en hechos y la corrección proactiva de no conformidades antes de que estas deriven en incidentes.

CCN-STIC 809: DECLARACIÓN DE CONFORMIDAD CON EL ENS

La guía establece la distinción fundamental entre la Declaración de Conformidad y la Certificación de Conformidad. Para los sistemas de categoría Básica, el cumplimiento se acredita mediante una autoevaluación interna que culmina en una Declaración firmada por la entidad. Sin embargo, para sistemas de categoría Media o Alta, es preceptiva la Certificación, la cual requiere una auditoría externa realizada por entidades acreditadas o por órganos de auditoría técnica del sector público bajo criterios de independencia.

Para formalizar este proceso, la guía explica los anexos A y B, que estandarizan la documentación del cumplimiento. Asimismo, se subraya la obligación de dar visibilidad a estos distintivos en las sedes electrónicas y portales de internet. Esta transparencia no es solo un requisito administrativo, sino una garantía de confianza para el ciudadano, informando fehacientemente de que sus trámites digitales se realizan en un entorno que cumple con los estándares nacionales de seguridad y protección de datos.

CCN-STIC 831: REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS

Esta guía aborda la necesidad de mantener un registro detallado de la actividad del sistema para garantizar la dimensión de trazabilidad. El registro de eventos debe capturar la información necesaria para monitorizar y documentar acciones no autorizadas, permitiendo reconstruir la secuencia de hechos tras un incidente. Esta capacidad es vital para el análisis forense y para la atribución de responsabilidades, asegurando que cada acción realizada en el sistema pueda vincularse unívocamente a una identidad.

En la implementación de estos registros, la guía vincula estrictamente la vigilancia técnica con el respeto al derecho al honor y la protección de datos personales (RGPD). El registro de actividad debe limitarse a lo estrictamente necesario para fines de seguridad, aplicando principios de minimización y limitación de la conservación. De este modo, se garantiza que la capacidad de monitorización del sistema no vulnere los derechos fundamentales de los usuarios, manteniendo un equilibrio proporcional entre vigilancia y privacidad.

CCN-STIC 817: GESTIÓN DE CIBERINCIDENTES

Esta guía debe presentarse como referencia para la gestión de ciberincidentes en el marco del ENS. Su utilidad práctica reside en ordenar la prevención, detección, clasificación, análisis, respuesta, registro y aprendizaje posterior al incidente, evitando que la reacción dependa de actuaciones improvisadas.

En la lógica del documento, su importancia deriva de que conecta la seguridad del sistema con la resiliencia institucional: los incidentes relevantes deben gestionarse con evidencias, trazabilidad, comunicación adecuada y coordinación con los órganos competentes, especialmente cuando afectan a servicios públicos, datos personales o proveedores.

CCN-STIC 823: SEGURIDAD EN ENTORNOS CLOUD

Esta directriz trata la protección de servicios en la nube bajo la medida operativa op.nub.1, fundamentándose en un modelo de corresponsabilidad. Aunque el proveedor cloud cuente con certificaciones de seguridad, la entidad pública (el cliente) mantiene la responsabilidad última sobre la configuración de seguridad del servicio y la protección de la información tratada. No se debe caer en la falsa asunción de que la externalización alivia a la entidad de sus deberes de gobernanza y control sobre el dato.

La guía especifica los requisitos de seguridad que deben cumplir los prestadores cloud para operar con la Administración Pública, exigiendo evidencias de conformidad con el ENS. Se deben valorar aspectos como la ubicación del dato, las garantías de disponibilidad y los mecanismos de salida (exit strategy). Este marco asegura que la adopción de servicios en la nube no suponga una degradación de los niveles de protección exigidos por el Real Decreto 311/2022, manteniendo la soberanía sobre la información pública en entornos compartidos.

CCN-STIC 830: ÁMBITO DE APLICACIÓN DEL ENS

Esta guía es especialmente relevante para delimitar el ámbito subjetivo y objetivo del ENS. Permite explicar con mayor precisión cuándo el marco se aplica a entidades del sector público, cuándo se proyecta sobre entidades privadas proveedoras y cómo debe entenderse la aplicación funcional del ENS en servicios, soluciones y sistemas vinculados a la actuación administrativa.

Su valor para la proyección internacional del modelo reside en que clarifica una de las notas diferenciales del ENS: la seguridad no se limita al perímetro administrativo formal, sino que puede alcanzar a los sistemas privados que sostienen servicios públicos digitales, siempre con arreglo al objeto del contrato, al sistema afectado y al análisis de riesgos.

CCN-STIC 827: GESTIÓN Y USO DE DISPOSITIVOS MÓVILES

Esta guía aborda el análisis de riesgos específico para equipos portátiles y dispositivos periféricos, activos que, por su naturaleza, presentan una mayor exposición al robo, pérdida o acceso no autorizado. La movilidad introduce vectores de ataque externos a las áreas controladas de la organización, lo que exige salvaguardas adicionales para asegurar que el acceso a la red institucional no comprometa la integridad global del sistema.

Para la protección de estos dispositivos, la guía se enfoca en la medida mp.eq.3, prescribiendo controles como el cifrado de datos en reposo y mecanismos de borrado remoto. Asimismo, detalla los requisitos para el control de acceso remoto seguro mediante túneles protegidos y autenticación reforzada. Estas medidas permiten que el personal trabaje en movilidad con plenas garantías, asegurando que la información sensible permanezca protegida incluso fuera del perímetro físico de la entidad.

CCN-STIC 824: INFORMACIÓN DEL ESTADO DE SEGURIDAD

Esta guía debe vincularse al conocimiento agregado del estado de seguridad y a la comunicación de indicadores, no a la gestión de incidentes —materia propia de la CCN-STIC 817 y de la ITS de Notificación de Incidentes—. Su finalidad es facilitar la recopilación homogénea de variables que permitan conocer la madurez y evolución de la seguridad en el sector público.

Desde la perspectiva de política pública, su valor consiste en transformar la seguridad en información medible: permite detectar tendencias, orientar recursos, alimentar decisiones de mejora y reforzar la capacidad del Estado para conocer la situación real de su ecosistema público digital.

CCN-STIC 807: CRIPTOLOGÍA DE EMPLEO EN EL ENS

Basada en los artículos 19 y 22, esta guía regula el uso de productos criptográficos para garantizar la confidencialidad, integridad y autenticidad. Es imperativo utilizar productos que figuren en el Catálogo de Productos y Servicios de Seguridad (CPSTIC) del CCN para sistemas de categoría Media o Alta, asegurando que sus funcionalidades han sido validadas por la autoridad competente. El uso de criptología no certificada puede generar una falsa sensación de seguridad que comprometa la soberanía de la información.

Un aspecto crítico es la protección de las claves criptográficas como activos de máxima prioridad, según la medida op.exp.10. El ciclo de vida de las claves —desde su generación y custodia hasta su destrucción segura— debe estar estrictamente regulado y auditado. Dado que la robustez de cualquier mecanismo de cifrado reside en la seguridad de sus claves, su gestión adecuada es un requisito irrenunciable para mantener la integridad del patrimonio digital y el secreto de las comunicaciones administrativas.

CCN-STIC 812: SEGURIDAD EN ENTORNOS Y APLICACIONES WEB

Esta guía se centra en la medida mp.s.2, promoviendo el desarrollo de aplicaciones informáticas seguras desde sus fases iniciales. El objetivo es minimizar las vulnerabilidades intrínsecas en el código que sustenta los servicios de administración electrónica, evitando que errores de lógica o programación se conviertan en puertas de entrada para atacantes. La seguridad por diseño es el enfoque prescriptivo para garantizar la resiliencia de los servicios web públicos.

La guía detalla la importancia de realizar auditorías de código y pruebas de penetración antes de la puesta en servicio. Se hace hincapié en la protección frente a amenazas recurrentes como la inyección de código y la validación de datos de entrada. Al aplicar controles técnicos internos y asegurar la integridad del software, la Administración garantiza que sus servicios digitales sean robustos ante intentos de intrusión, protegiendo así la confianza de los ciudadanos que interactúan con sus portales web.

CCN-STIC 883: GUÍA DE IMPLANTACIÓN DEL ENS PARA ENTIDADES LOCALES

Esta directriz desarrolla las posibilidades de eficiencia organizativa para el ámbito local, permitiendo que municipios pequeños alcancen niveles de seguridad elevados mediante la colaboración. Menciona explícitamente la posibilidad de que varias entidades locales compartan una Política de Seguridad de la Información común, vinculada al Artículo 12 del ENS. Esto facilita que organismos de mayor nivel, como las Diputaciones, asuman la gobernanza de seguridad de municipios que carecen de recursos técnicos propios.

La guía destaca la eficiencia de compartir infraestructuras y servicios comunes (nubes privadas provinciales, SOC compartidos) para facilitar el cumplimiento normativo. Al unificar criterios y recursos, las entidades locales profesionalizan su gestión de seguridad y simplifican el proceso de auditoría. Este enfoque cooperativo es la única vía practicable para asegurar que la seguridad de los ciudadanos sea homogénea en todo el territorio, independientemente de la capacidad presupuestaria de su ayuntamiento.

CCN-STIC 823 — ANEXO: CLAUSULADO Y ACUERDOS DE NIVEL DE SERVICIO

Para servicios externalizados y cloud, resulta más preciso remitir a la CCN-STIC 823 y a su anexo de clausulado y acuerdos de nivel de servicio, sin perjuicio de otras guías o perfiles que puedan resultar aplicables. La cuestión central no es una guía autónoma de “servicios externalizados”, sino la incorporación contractual de obligaciones ENS, matrices de responsabilidad, evidencias, subcontratación, reversibilidad y notificación de incidentes.

Esta corrección evita atribuir a la CCN-STIC 883 un contenido que corresponde a entidades locales. El mensaje sustantivo se mantiene: la externalización exige cláusulas ENS precisas, control de proveedores, evidencias verificables y seguimiento durante toda la vida del contrato.

CCN-STIC 890: ADECUACIÓN AL ENS CONFORME AL PERFIL DE CUMPLIMIENTO ESPECÍFICO DE REQUISITOS FUNDAMENTALES DE SEGURIDAD

Esta guía introduce el concepto de "Perfil de Cumplimiento Específico" amparado por el Artículo 30 del ENS. Estos perfiles no suponen bajo ningún concepto una rebaja o excepción a las exigencias del Esquema, sino que constituyen una forma de hacer el cumplimiento "practicable" y operativo para sectores con riesgos similares o recursos limitados. Permiten concretar qué conjunto de medidas son idóneas tras un análisis de riesgos tipo, optimizando el despliegue de salvaguardas sin comprometer la eficacia de la protección.

El perfil de requisitos fundamentales racionaliza los recursos de la organización al enfocarlos en los controles que aportan el mayor valor de mitigación de riesgo. Este enfoque permite que el ENS sea sostenible y escalable para una amplia diversidad de colectivos, asegurando que la protección sea real y verificable. Los perfiles facilitan una aplicación proporcionada del Real Decreto 311/2022, garantizando que la ciberseguridad sea un objetivo alcanzable para todas las entidades que forman parte del sector público.

CCN-STIC 891: PERFIL DE CUMPLIMIENTO ESPECÍFICO PARA SALUD

Este perfil resulta relevante para sistemas vinculados a la prestación sanitaria a pacientes. Su interés no está en microservicios o contenedores, sino en la adaptación de los requisitos ENS a un entorno sanitario en el que confluyen datos personales especialmente sensibles, continuidad asistencial, disponibilidad de sistemas clínicos, trazabilidad y seguridad de proveedores tecnológicos.

Desde la perspectiva internacional, el PCE-Salud permite mostrar cómo el ENS puede adaptarse a sectores con necesidades específicas sin perder coherencia general: mantiene la base común del ENS, pero concreta expectativas de cumplimiento para un ámbito de alto impacto social y jurídico.

CCN-STIC 896: PERFIL DE CUMPLIMIENTO ESPECÍFICO PARA SERVICIOS DE SEGURIDAD GESTIONADOS / PCE-SSG

Este perfil debe presentarse como referencia para servicios de seguridad gestionados. Su relevancia es elevada en un mercado público digital en el que muchas entidades externalizan capacidades de monitorización, detección, respuesta, análisis de vulnerabilidades, SOC, operación de herramientas y soporte especializado.

El PCE-SSG permite ordenar qué garantías deben exigirse a estos servicios, cómo deben documentarse las responsabilidades, qué evidencias son relevantes y cómo se preserva la confianza cuando capacidades críticas de ciberseguridad son prestadas por terceros.

CCN-STIC 897: PERFIL DE CUMPLIMIENTO ESPECÍFICO PARA LA ADMINISTRACIÓN DE JUSTICIA

Este perfil debe vincularse a los sistemas de la Administración de Justicia, no a una guía general de vigilancia continua. Su importancia radica en adaptar el ENS a un ámbito institucional con especiales exigencias de disponibilidad, integridad, trazabilidad, confidencialidad, interoperabilidad y garantía de derechos.

Desde la perspectiva de proyección exterior, el PCE para la Administración de Justicia demuestra que el ENS puede especializarse en sectores públicos complejos y sensibles, manteniendo una arquitectura común de seguridad, auditoría, certificación y mejora continua.

ANEXO V. HERRAMIENTAS DE APOYO DEL CCN PARA LA IMPLANTACIÓN Y SEGUIMIENTO DEL ENS Y SUS FUNCIONES.

El Esquema Nacional de Seguridad se configura como el pilar fundamental del ordenamiento jurídico español para estructurar la gobernanza, la gestión de riesgos y la defensa de la administración digital. La fundamentación legal del marco emana del artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que preceptúa el ENS como el instrumento articulador para garantizar la seguridad, integridad, disponibilidad, autenticidad, trazabilidad y conservación de los datos e información procesados en las relaciones electrónicas del Sector Público.

Para articular la aplicación práctica de principios como la vigilancia continua, la reevaluación periódica y la mejora continua, y para reducir la brecha entre las exigencias normativas y la realidad operativa de las entidades, el Centro Criptológico Nacional ha desarrollado un ecosistema de soluciones y servicios de apoyo. Estas herramientas no sustituyen la responsabilidad de cada entidad ni constituyen por sí mismas prueba completa de conformidad, pero facilitan la gestión de riesgos, la medición, el seguimiento, la notificación de incidentes y la preparación de evidencias.

La trascendencia operativa de estas soluciones radica en su capacidad para actuar como facilitadores y homogeneizadores del marco nacional de ciberdefensa:

1. **Estandarización y Armonización:** Proporcionan métricas, metodologías e indicadores unificados que permiten valorar de forma homogénea el estado de ciberseguridad en la Administración Pública y su cadena de suministro.
2. **Sostenibilidad Operativa y Eficiencia:** Automatizan tareas complejas de auditoría, gestión de vulnerabilidades, monitorización y reporte de incidentes, reduciendo la carga administrativa y optimizando la inversión de recursos públicos.
3. **Generación de Inteligencia Colectiva:** Articulan el principio de *Prevención, Detección y Respuesta* (Art. 8) mediante plataformas centralizadas de intercambio de ciberinteligencia en tiempo real, permitiendo que la detección de una amenaza en un organismo sirva para proteger preventivamente al conjunto del Sector Público.
4. **Soporte al Cumplimiento Normativo:** Constituyen el soporte técnico directo sobre el que se sustenta la evidencia del cumplimiento ante las auditorías de certificación y la rendición de cuentas institucional.

A continuación, se desarrolla en detalle el catálogo de herramientas de apoyo organizadas según su función operativa en la arquitectura del ENS.

Ámbito de aplicación	Herramienta	Propósito	Desarrollo y valor ENS
Gobernanza, riesgos y cumplimiento	**PILAR (Metodología y Análisis de Riesgos)**	Entorno diseñado para la implementación formal de la metodología Magerit	Apoya el artículo 14 del ENS, al facilitar el empleo de una metodología reconocida de análisis y gestión de riesgos. No

Ámbito de aplicación	Herramienta	Propósito	Desarrollo y valor ENS
		(Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) desarrollada por el CCN.	debe presentarse como la única herramienta posible, aunque su uso sea especialmente coherente con el ecosistema CCN.
	INÉS (Informe Nacional del Estado de la Seguridad)	Plataforma web centralizada para la recogida, consolidación y tratamiento estadístico de los indicadores del nivel de madurez y estado de ciberseguridad.	Facilita el cumplimiento de las obligaciones de información sobre el estado de la seguridad y la elaboración de indicadores homogéneos. Su valor reside en la medición agregada y en la disciplina de seguimiento.
	AMPARO (Adecuación y Perfiles de Cumplimiento)	Plataforma orientada a la simplificación y guiado del proceso de adecuación al ENS, especialmente enfocada en Entidades Locales y organismos de complejidad o recursos reducidos.	Apoya la aplicación de perfiles de cumplimiento específico y procesos de adecuación, especialmente en entidades con menor capacidad. Su uso debe entenderse como ayuda metodológica, no como sustitución de la responsabilidad de la entidad.
Gestión de incidentes	**LUCÍA (Gestión y Notificación de Incidentes)**	Sistema de gestión de tickets e incidentes de seguridad de la información diseñado de forma nativa para el entorno del Sector Público.	Apoya la gestión y notificación de incidentes en el ecosistema público. Debe integrarse con los procedimientos internos de la entidad y con las obligaciones contractuales de proveedores cuando proceda.

Ámbito de aplicación	Herramienta	Propósito	Desarrollo y valor ENS
	REYES (Intercambio de ciberinteligencia)	Plataforma centralizada de ciberinteligencia que consolida, analiza y distribuye Indicadores de Compromiso (IoCs) y cibermedidas en tiempo real.	Sustenta operativamente el principio de **Prevención, detección y respuesta (Artículo 8)**. Al integrar fuentes de inteligencia nacionales e internacionales, REYES permite automatizar la inyección de reglas de bloqueo e indicadores de amenaza en las infraestructuras perimetrales de las entidades conectadas, transformando el conocimiento de un ciberataque aislado en protección colectiva inmediata.
	CARMEN (Detección de amenazas avanzadas- APT)	Plataforma de análisis de tráfico de red y registros centrada en la identificación de intrusiones complejas y Amenazas Persistentes Avanzadas.	Fundamentada en el requerimiento de detección temprana y respuesta ante ciberataques de alto impacto. CARMEN utiliza capacidades de analítica avanzada sobre grandes volúmenes de tráfico (*Big Data*) para descubrir patrones exfiltración de datos o comportamientos anómalos que eluden los sistemas de detección tradicionales.
Auditoría, Vigilancia y Verificación Técnica	**CLARA (Auditoría Técnica de Configuraciones)**	Herramienta de auditoría técnica que evalúa de forma automatizada la configuración de seguridad (*bastionado* o *hardening*) en sistemas operativos y plataformas clave.	Da soporte al **Artículo 31 (Auditoría de la seguridad)** y a las medidas del Anexo II relativas al principio de **Mínimo privilegio (Art. 20)**. CLARA analiza los parámetros del sistema respecto a las Guías CCN-STIC de bastionado (serie 800), emitiendo informes con la desviación detectada y la nota técnica de cumplimiento normativo.

Ámbito de aplicación	Herramienta	Propósito	Desarrollo y valor ENS
	ANA (Auditoría de Vulnerabilidades)	Plataforma de escaneo y monitorización automatizada de la superficie de exposición externa e interna y detección de vulnerabilidades.	Articula el cumplimiento de los **Artículos 10 (Vigilancia continua) y 21 (Integridad y actualización del sistema)**. ANA identifica fallos de seguridad, puertos abiertos y parches faltantes en los activos de la organización, clasificándolos por nivel de severidad para priorizar su remediación antes de que puedan ser explotados por terceros.
	GLORIA (Gestión de Eventos y Registros - SIEM)	Solución orientada a la recolección, correlación analítica y almacenamiento seguro de registros de eventos (*logs*).	Cumple con la medida **[op.exp.8] Registro de actividad (Anexo II)** y apoya el **Artículo 24 (Trazabilidad y registro de la actividad)**. Garantiza la conservación e integridad de las trazas del sistema, permitiendo reconstruir la secuencia de eventos durante una investigación forense y detectando desviaciones de comportamiento en tiempo real.
Protección de Activos y Herramientas Operativas	**CLAUDIA / microCLAUDIA (Detección y Respuesta en el Puesto de Trabajo - EDR)**	Solución para la prevención, detección y neutralización de código dañino (*malware*) y amenazas avanzadas en el puesto final mediante agentes livianos.	Apoya las exigencias del **Artículo 8 (Prevención, detección, respuesta y conservación)** y la medida **[op.exp.6] (Protección contra código dañino)**. microCLAUDIA permite aplicar vacunas y políticas de contención masivas de forma inmediata ante oleadas de *ransomware* o exploits desconocidos, aislando el equipo comprometido sin interrumpir el resto de la red.

Ámbito de aplicación	Herramienta	Propósito	Desarrollo y valor ENS
	OLVIDO / metaOLVIDO (Borrado Seguro y Limpieza de Metadatos)	Suite de herramientas destinadas al sanitizado digital, borrado seguro de archivos y eliminación automatizada de metadatos adjuntos en documentos electrónicos	Es una herramienta clave para la **Protección de la información (Art. 22)** y la **Protección de datos personales (Art. 3)**. Evita la fuga inadvertida de información sensible (nombres de usuario, rutas de red, versiones de software) oculta en los documentos públicos, garantizando además la destrucción irreversible de soportes de información cuando estos finalizan su ciclo de vida.
	ELSA (Descubrimiento y Visibilidad de Activos)	Herramienta orientada al descubrimiento de red y visibilidad técnica en tiempo real.	Da soporte al **Artículo 21 (Integridad y actualización del sistema)**, al **Artículo 28 (Cumplimiento de los requisitos mínimos)** y a la **medida [op.exp.1],** que exige disponer de un inventario exhaustivo y actualizado de todos los componentes del sistema. ELSA permite identificar activos *sombra* (*Shadow IT*) no autorizados conectados a la infraestructura corporativa.
Formación y Concienciación	**Ángeles (Portal de Formación en Ciberseguridad)**	Plataforma e-learning centralizada destinada a la capacitación técnica, legal y organizativa de Responsables de Seguridad, administradores de sistemas y auditores.	Apoya las obligaciones relativas a la **Concienciación y formación (Anexo II, [mp.per.3] y [mp.per.4])**. Imparte itinerarios formativos oficiales alineados con la normativa ENS, fortaleciendo el perfil profesional de las figuras clave del marco de seguridad.

Ámbito de aplicación	Herramienta	Propósito	Desarrollo y valor ENS
	ATENEA (Plataforma de Desafíos Técnicos)	Entorno práctico de ciberejercicios (*Capture The Flag* - CTF) para la puesta a prueba y perfeccionamiento de habilidades técnicas ofensivas y defensivas.	Permite el entrenamiento de los equipos de respuesta ante incidentes y administradores en escenarios simulados de ataques reales, asegurando que el personal disponga de la cualificación y destreza técnica exigida en la gestión de crisis.
	VANESA (Materiales y Píldoras de Concienciación)	Repositorio de contenidos multimedia, infografías y campañas periódicas de sensibilización orientadas al usuario final.	Proporciona a las organizaciones los materiales necesarios para cumplir con la obligación de concienciar de forma permanente a todo el personal empleado público sobre el uso seguro de los puestos de trabajo y la gestión de la información.

El catálogo de Soluciones CCN-STIC representa una infraestructura tecnológica de valor inestimable que simplifica significativamente la transición hacia la conformidad con el Esquema Nacional de Seguridad. La adopción integral de este ecosistema permite a las administraciones públicas y a sus operadores tecnológicos trascender el enfoque meramente formalista del cumplimiento administrativo, dotándolos de capacidades reales, verificables y en constante evolución para la protección de la información.

A través del despliegue coordinado de estas herramientas, que pueden complementarse con la selección de productos y servicios incluidos en el Catálogo de Productos y Servicios de Seguridad (CPSTIC) cuando resulte procedente, las organizaciones pueden reforzar su capacidad de gobierno, operación, monitorización y acreditación de evidencias. Esta formulación debe evitar presentarlas como garantía automática de soberanía tecnológica o de cumplimiento pleno: su valor es instrumental y debe integrarse en la arquitectura ENS de cada sistema.

ANEXO VI. ESQUEMA GRÁFICO DEL CICLO DE CUMPLIMIENTO DEL ENS.

A continuación, se visualiza, mediante un modelo circular de ocho fases secuenciales interconectadas, el tránsito que deben recorrer los sistemas de información desde el diagnóstico inicial y la categorización hasta la auditoría, la certificación de conformidad y el mantenimiento del nivel de seguridad mediante la mejora continua, cumpliendo así con todo el ciclo de adecuación al ENS:



Figura Anexo VI.III. Ciclo de cumplimiento del ENS

ANEXO VII. ESQUEMA GRÁFICO DEL SISTEMA DE AUDITORÍA, CERTIFICACIÓN Y ACREDITACIÓN

A continuación, se detalla la arquitectura institucional y técnica que articula el **Sistema de Auditoría, Certificación y Acreditación del ENS**, estructurado conforme a los principios de independencia y doble garantía de confianza digital regulados en el Real Decreto 311/2022. Este esquema gráfico describe de forma integral los organismos, roles y flujos que intervienen en cada nivel de control, asegurando la validez técnica de las evaluaciones y la transparencia en la acreditación de la conformidad de los sistemas de información.

El gráfico ilustra de forma clara la distribución jerárquica de competencias y el flujo de certificación:



Figura I- Anexo VII. Esquema del sistema de auditoría, certificación y acreditación

ANEXO VIII. TABLA DE CORRESPONDENCIAS ENTRE ENS, ISO/IEC 27001, ISO/IEC 27002, NIS2, CYBERSECURITY ACT Y RGPD

Esta tabla de correspondencias ofrece una aproximación funcional entre las 73 medidas de seguridad del Anexo II del Esquema Nacional de Seguridad, ISO/IEC 27001:2022 e ISO/IEC 27002:2022, las áreas de medidas de gestión de riesgos de la Directiva NIS2, el Reglamento General de Protección de Datos, el marco europeo de certificación de la ciberseguridad y, como referencia de trabajo, el documento del NIS Cooperation Group sobre medidas de seguridad para entidades sujetas a NIS2. Debe leerse como instrumento de análisis e interoperabilidad, no como equivalencia automática ni como matriz oficial de cumplimiento cruzado.

A continuación, se presenta un mapeo técnico de carácter orientativo, estructurado de acuerdo con objetivos y subobjetivos funcionales del documento de referencia del NIS Cooperation Group, con el fin de facilitar la lectura comparada del ENS frente a otros marcos europeos e internacionales:

Objetivo / subobjetivo NCG (junio de 2026)	Medidas ENS (Anexo II RD 311/2022)	Controles ISO/IEC 27001 / 27002:2022	Directiva NIS2 (Art. 21 / 20)	RGPD (Medidas de Control)	Cybersecurity Act / DORA / Otros
2.1 Compromiso y Responsabilidad de la Alta Dirección **- Implicación activa y aprobación directiva.**	org.1 (Política de seguridad) Art. 12 (Aprobación por máxima autoridad) Art. 11 (Segregación de roles)	5.1 Políticas de seguridad de la información 5.2 Roles y responsabilidades Cláusula 5 (Liderazgo)	Art. 20 (Gobernanza, aprobación y formación obligatoria de directivos)	Art. 24 (Responsabilidad del responsable) Art. 25 (Garantía de cumplimiento)	No aplica directamente (enfoque en gobernanza y responsabilidad corporativa).
2.2 Política de Seguridad de Redes y Sistemas **- Misión, ámbito y estructura documental.**	org.1 (Política) org.2 (Normativa) org.3 (Procedimientos) org.4 (Autorización)	5.1 Políticas de SI 5.2 Roles y responsabilidades 5.3 Segregación de tareas 5.4 Gestión del SGSI	Art. 21(2)(a) Políticas de análisis de riesgos y seguridad de sistemas de información.	Art. 24 (Políticas de protección de datos adecuadas) Art. 25 (Privacidad desde el diseño)	Gobernanza cibersegura alineada con políticas organizativas nacionales.
2.3.1 Marco de Gestión de Riesgos **- Metodología, análisis y tratamiento de riesgos.**	op.pl.1 (Análisis de riesgos) | Art. 14 (metodología reconocida de análisis y gestión de riesgos; p. ej., MAGERIT/PILAR) | Guía CCN-STIC 882 (análisis de riesgos en entidades locales, cuando proceda)	Cláusula 6.1.2 (Evaluación de riesgos) Cláusula 6.1.3 (Tratamiento de riesgos)	Art. 21(1) Obligatoriedad de adoptar un enfoque basado en riesgos proporcional.	Art. 32(1) Evaluación de riesgos específicos sobre los derechos y libertades.	El análisis de riesgos guía la exigencia de componentes de seguridad certificados (EUCC).
2.3.2 Monitoreo de Cumplimiento **- Verificación e indicadores continuos.**	op.mon.2 (Sistema de métricas e indicadores) Art. 27 (Mejora continua) Guía CCN-STIC 815	Cláusula 9.1 (Seguimiento, medición, análisis y evaluación del SGSI)	Art. 21(2)(f) Políticas y procedimientos para evaluar la eficacia de las medidas.	Art. 32(1)(d) Proceso de verificación y evaluación regular de la seguridad.	Sincronización anual mediante indicadores ciberseguros (INES).
2.3.3 Revisión Independiente **- Auditoría formal del sistema.**	Art. 31 (Auditoría de seguridad ordinaria/extraordinaria) Anexo III (Criterios) Guía CCN-STIC 802	Cláusula 9.2 (Auditoría interna) 5.36 Revisión independiente de la seguridad	Art. 21(2)(f) Verificación externa e independiente del gobierno de seguridad.	Art. 32(1)(d) Auditoría e informes de cumplimiento e impacto del tratamiento.	Acreditación de entidades de certificación bajo estándar internacional ISO/IEC 17065 (ENAC).
2.4.1 a 2.4.3 Detección y Registro de Incidentes **- Monitorización de eventos y**	op.exp.8 (Registro de actividad) op.mon.1 (Detección de	8.15 Registro de logs 8.16 Supervisión de eventos 8.17 Protección de logs	Art. 21(2)(b) Manejo de incidentes (prevención, detección y reporte).	Art. 32(1) Trazabilidad del acceso a datos personales para evitar	Sondas y sistemas de monitorización calificados en el

Objetivo / subobjetivo NCG (junio de 2026)	Medidas ENS (Anexo II RD 311/2022)	Controles ISO/IEC 27001 / 27002:2022	Directiva NIS2 (Art. 21 / 20)	RGPD (Medidas de Control)	Cybersecurity Act / DORA / Otros
correlación de registros.	intrusiones) Guía CCN-STIC 831 (Logs)			brechas de seguridad.	catálogo CPSTIC.
2.4.4 Clasificación de Eventos - Gravedad, taxonomía e impacto.	op.exp.7 (Gestión de incidentes) Guía CCN-STIC 817 (Gestión ciberincidentes)	5.24 Planeación de incidentes 5.25 Evaluación de eventos	Art. 21(2)(b) Clasificación de la criticidad del incidente y su repercusión social.	Art. 33 Evaluación inmediata del impacto fidedigno de la brecha.	Uso de la taxonomía del CCN-CERT para el reporte unificado nacional.
2.4.5 y 2.4.6 Respuesta y Revisión Post-incidente - Contención y mitigación de amenazas.	op.exp.7 (Gestión de incidentes) op.exp.9 (Registro de incidentes) Resolución ITS de Notificación	5.26 Respuesta a incidentes 5.27 Aprendizaje de incidentes	Art. 21(2)(b) Mitigación de impactos y coordinación ágil con el CSIRT nacional.	Arts. 33 y 34 RGPD: notificación de brechas de datos personales a la autoridad de control y, cuando proceda, comunicación a los interesados. El plazo de 72 horas se refiere a la notificación a la autoridad de control, no a toda comunicación de seguridad.	Sistemas federados de ticketing e intercambio de amenazas (plataforma LUCÍA / REYES).
2.5.1 Plan de Continuidad y BCP - Planificación de contingencia y resiliencia.	op.cont.1 (Análisis de impacto) op.cont.2 (Plan de continuidad) op.cont.3 (Pruebas periódicas)	5.29 Seguridad en continuidad 5.30 Preparación de TIC para continuidad	Art. 21(2)(c) Continuidad de las actividades, gestión de crisis y resiliencia.	Art. 32(1)(b) Capacidad de garantizar la resiliencia permanente de los sistemas.	Alineamiento sectorial con los requisitos de resiliencia operativa del Reglamento DORA.
2.5.2 Respaldo y Gestión de Redundancia - Copias de seguridad periódicas y aisladas.	mp.info.6 (Copias de seguridad) mp.si.2.r2 (Cifrado de respaldos) Guía CCN-STIC 804 (Medidas)	8.13 Copias de seguridad de la información	Art. 21(2)(c) Gestión de copias de seguridad robustas, cifradas y aisladas (air-gapped).	Art. 32(1)(c) Capacidad de restaurar la disponibilidad de los datos rápidamente.	Despliegue de tecnologías de backup inmutable del catálogo CPSTIC.

Objetivo / subobjetivo NCG (junio de 2026)	Medidas ENS (Anexo II RD 311/2022)	Controles ISO/IEC 27001 / 27002:2022	Directiva NIS2 (Art. 21 / 20)	RGPD (Medidas de Control)	Cybersecurity Act / DORA / Otros
2.6 Seguridad de la Cadena de Suministro **- Control de riesgos de terceros y subcontratistas.**	op.ext.1 (Contratación) op.ext.3 (Cadena de suministro) Guía CCN-STIC 830 (Contratos)	5.19 Relaciones con proveedores 5.20 Seguridad en acuerdos con proveedores	Art. 21(2)(d) Seguridad de la cadena de suministro y vulnerabilidades de socios.	Art. 28 Deber de diligencia en la elección de encargados del tratamiento.	Exigencia obligatoria en pliegos de contratación pública de cumplimiento ENS (Art. 2.3).
2.7.1 y 2.7.2 Adquisición y Desarrollo Seguro (SDLC) **- Seguridad desde el diseño del software.**	op.pl.3 (Adquisición) mp.sw.1 (Desarrollo seguro) mp.sw.2 (Aceptación de apps)	8.25 Ciclo de vida de desarrollo seguro 8.27 Requisitos de adquisición	Art. 21(2)(e) Seguridad en adquisición, desarrollo y mantenimiento de sistemas.	Art. 25 Privacidad desde el diseño y por defecto en sistemas lógicos.	Uso de Common Criteria y esquemas europeos EUCC del Cybersecurity Act.
2.7.3 a 2.7.6 Configuración, Cambios y Parches **- Mantener endurecimiento del sistema (hardening).**	op.exp.2 (Configuración) op.exp.3 (Gestión de la configuración) op.exp.4 (Mantenimiento) op.exp.5 (Cambios)	8.9 Gestión de la configuración 8.19 Gestión de vulnerabilidades 8.32 Gestión de cambios	Art. 21(2)(e) Gestión, control de cambios, mantenimiento y parcheado de seguridad.	Art. 32(1) Preservar integridad de servidores de bases de datos de carácter personal.	Aplicación de guías de configuración de seguridad oficiales del CCN (hardening).
2.7.10 Gestión y Divulgación de Vulnerabilidades **- Identificación y reporte coordinado.**	op.exp.6 (Protección malware) op.mon.3 (Vigilancia e informes) Guía CCN-STIC 808 / 817	8.19 Gestión de vulnerabilidades técnicas 5.28 Inteligencia de amenazas	Art. 21(2)(e) Políticas de divulgación coordinada de vulnerabilidades y escaneo.	Indirecto: Prevención de accesos no autorizados a repositorios sensibles.	Coordinación técnica nacional a través de las capacidades del CCN-CERT e INCIBE-CERT.
2.7.7 y 2.7.8 Seguridad de Red y Segmentación **- Cierre perimetral y segmentación lógica.**	mp.com.1 (Perímetro seguro) mp.com.4 (Separación de flujos) op.ext.4 (Interconexión)	8.20 Seguridad de redes 8.21 Seguridad de servicios 8.22 Segregación de redes	Art. 21(2)(e) Ciberseguridad de redes, filtrado y segmentación en zonas seguras.	Art. 32(1) Cifrado de flujos y aislamiento de la red de datos de carácter personal.	Implementación de cortafuegos perimetrales y VPNs certificadas del catálogo CPSTIC.
2.10 Criptografía y Cifrado **- Cifrado robusto del tránsito y reposo.**	mp.si.2 (Criptografía) mp.com.2 (Confidencialidad) op.exp.10 (Claves criptográficas)	8.24 Uso de la criptografía	Art. 21(2)(h) Políticas y procedimientos sobre el uso de criptografía y cifrado.	Art. 32(1)(a) Seudonomización y cifrado de datos personales en el tratamiento.	Aplicación de algoritmos y longitudes de clave autorizados por el CCN (Guía CCN-STIC 807).

Objetivo / subobjetivo NCG (junio de 2026)	Medidas ENS (Anexo II RD 311/2022)	Controles ISO/IEC 27001 / 27002:2022	Directiva NIS2 (Art. 21 / 20)	RGPD (Medidas de Control)	Cybersecurity Act / DORA / Otros
2.12 Control de Acceso y MFA - Autenticación multifactor y privilegios mínimos.	op.acc.1 a op.acc.6 (Control de acceso) Art. 20 (Mínimo privilegio)	5.15 Control de acceso 5.18 Derechos de acceso 8.5 Autenticación segura	Art. 21(2)(j) Uso de soluciones de autenticación multifactor (MFA) robustas.	Art. 32(1) Garantía de que solo personal autorizado accede a datos (necesidad de conocer).	Gestores de identidad y llaves MFA homologadas por el CCN.
2.13 Gestión de Activos - Inventariado y destrucción segura de soportes.	op.exp.1 (Inventario de activos) mp.si.1 (Marcado) mp.si.5 (Borrado y destrucción)	5.9 Inventario de activos 5.12 Clasificación 7.10 Soportes	Art. 21(2)(i) Clasificación, gestión e inventariado actualizado de activos TIC y OT.	Art. 32(1) Destrucción fidedigna de soportes y borrado de metadatos (herramienta OLVIDO).	Gestión automatizada de activos mediante GRC y plataforma INES.
2.11 Seguridad de los Recursos Humanos - Contratación, deberes y terminación.	mp.per.1 (Caracterización puesto) mp.per.2 (Deberes) Guía CCN-STIC 801 (Roles)	6.1 Investigación de antecedentes 6.2 Términos y condiciones 6.5 Terminación	Art. 21(2)(i) Gestión del personal, contratos de confidencialidad y control de salidas.	Art. 32(1) Normativa de uso y compromiso expreso de confidencialidad firmado por empleados.	Garantía de profesionalidad del personal del organismo (Art. 16).
2.9 Higiene Cibernética y Formación - Concienciación general y especializada.	mp.per.3 (Concienciación) mp.per.4 (Formación) Disp. Adicional 1ª (Programas)	6.3 Concienciación, educación y formación en seguridad de la información	Art. 21(2)(g) Prácticas básicas de higiene cibernética y capacitación de empleados.	Art. 32(1) Formación obligatoria para el personal en protección de datos y privacidad.	Cursos continuos desarrollados en colaboración con el INAP y la plataforma ÁNGELES del CCN.

ANEXO IX. GLOSARIO DE TÉRMINOS BÁSICOS DEL ENS

MARCO GENERAL Y ÁMBITO

Término	Definición / descripción
ENS (Esquema Nacional de Seguridad)	Constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos.
Ámbito de aplicación	Todo el sector público (art. 2 Ley 40/2015); sistemas que tratan información clasificada; sistemas de información de entidades del sector privado que, por relación contractual, presten servicios o provean soluciones a entidades del sector público para el ejercicio de sus competencias y potestades administrativas.
Sistema de información	(1) Las redes de comunicaciones electrónicas que utilice la entidad sobre las que posea capacidad de gestión; (2) todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí en el que uno o varios realicen, mediante un programa, el tratamiento automático de datos digitales.

PRINCIPIOS BÁSICOS

Referencia / alcance	Descripción
Seguridad como proceso integral	La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información; excluye cualquier actuación puntual o tratamiento coyuntural.
Gestión de la seguridad basada en los riesgos	El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad; debe ser una actividad continua y permanentemente actualizada.
Prevención, detección, respuesta y conservación	Conjunto de acciones orientadas a minimizar vulnerabilidades, evitar que las amenazas se materialicen o, si lo hacen, que no afecten gravemente a la información o a los servicios; incluye la conservación de datos e información en soporte electrónico durante todo el ciclo vital.
Líneas de defensa	Estrategia de protección constituida por múltiples capas de seguridad (organizativas, físicas y lógicas) dispuesta de forma que, si una capa es comprometida, permita reaccionar y minimizar el impacto final.
Vigilancia continua y reevaluación periódica	Permite la detección de actividades o comportamientos anómalos y su respuesta oportuna; las medidas de seguridad se reevalúan y

Referencia / alcance	Descripción
	actualizan periódicamente.
Diferenciación de responsabilidades	Roles diferenciados: responsable de la información, responsable del servicio, responsable de la seguridad y responsable del sistema.

ROLES DE RESPONSABILIDAD

Término	Descripción
Responsable de la información	Determina los requisitos de la información tratada.
Responsable del servicio	Determina los requisitos de los servicios prestados.
Responsable de la seguridad	Determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios; supervisa la implantación de las medidas necesarias y reporta sobre ello. Debe ser distinto del responsable del sistema, sin dependencia jerárquica entre ambos (salvo situaciones excepcionales justificadas, con medidas compensatorias).
Responsable del sistema	Desarrolla la forma concreta de implementar la seguridad en el sistema y supervisa su operación diaria, por sí o mediante recursos propios o contratados; puede delegar en administradores u operadores.
POC de seguridad (Punto o Persona de Contacto)	En servicios externalizados, designado por la organización prestataria para canalizar y supervisar el cumplimiento de los requisitos de seguridad del servicio y las comunicaciones relativas a incidentes; será el propio Responsable de Seguridad de la organización contratada o tendrá comunicación directa con él.

POLÍTICA DE SEGURIDAD Y REQUISITOS MÍNIMOS

Término	Descripción
Política de seguridad de la información	Conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta.
Requisitos mínimos de seguridad	15 bloques definidos en el art. 12.6: organización e implantación del proceso de seguridad; análisis y gestión de riesgos; gestión de personal; profesionalidad; autorización y control de accesos; protección de instalaciones; adquisición de productos/servicios de seguridad; mínimo privilegio; integridad y actualización del sistema; protección de información almacenada y en tránsito; prevención ante sistemas interconectados; registro de actividad y detección de código dañino; incidentes de seguridad; continuidad de la actividad; mejora continua.
Mínimo privilegio	Diseño y configuración de los sistemas otorgando los mínimos privilegios necesarios para su correcto desempeño (funcionalidad imprescindible,

Término	Descripción
	funciones mínimas necesarias, eliminación de funciones innecesarias, guías de configuración segura).
Declaración de Aplicabilidad	Documento, firmado por el responsable de la seguridad, que formaliza la relación de medidas de seguridad seleccionadas (Anexo II) para el sistema, incluyendo, en su caso, la correspondencia con medidas compensatorias.

CATEGORIZACIÓN DE SISTEMAS Y DIMENSIONES DE SEGURIDAD (ANEXO I ENS)

Término	Descripción
Dimensiones de seguridad	Confidencialidad [C], Integridad [I], Trazabilidad [T], Autenticidad [A], Disponibilidad [D].
Nivel de seguridad (BAJO / MEDIO / ALTO)	Nivel asignado a cada dimensión de seguridad afectada por un incidente, en función del perjuicio (limitado / grave / muy grave) sobre las funciones, activos o individuos de la organización.
Categoría de seguridad (BÁSICA / MEDIA / ALTA)	Categoría del sistema determinada por el nivel más alto alcanzado por cualquiera de sus dimensiones de seguridad: ALTA si alguna dimensión alcanza nivel ALTO; MEDIA si alguna alcanza MEDIO sin llegar a ALTO; BÁSICA si alguna alcanza BAJO sin niveles superiores.

MEDIDAS DE SEGURIDAD (ANEXO II ENS)

Término	Descripción
Marco organizativo [org]	Conjunto de medidas relacionadas con la organización global de la seguridad (política, normativa, procedimientos, proceso de autorización).
Marco operacional [op]	Medidas para proteger la operación del sistema como conjunto integral de componentes para un fin (planificación, control de acceso, explotación, recursos externos, servicios en la nube, continuidad, monitorización).
Medidas de protección [mp]	Medidas centradas en proteger activos concretos (instalaciones, personal, equipos, comunicaciones, soportes, aplicaciones, información, servicios).
Refuerzo (R)	Exigencia adicional que se suma a los requisitos base de una medida de seguridad, en función del nivel de seguridad de la dimensión afectada o de la categoría del sistema; no siempre son incrementales entre sí.
Medida compensatoria	Medida distinta de las previstas en el Anexo II que puede reemplazar a estas si se justifica documentalmente que ofrece una protección igual o mejor y satisface los principios básicos y requisitos mínimos; se recoge en la Declaración de Aplicabilidad.

Término	Descripción
Perfil de cumplimiento específico	Conjunto de medidas de seguridad, derivado del preceptivo análisis de riesgos, idóneo para una categoría de seguridad concreta, aplicable a determinadas entidades o sectores de actividad, validado y publicado por el CCN.

AUDITORÍA, INFORME Y CONFORMIDAD (CAPÍTULOS IV Y V; ANEXO III ENS)

Término	Descripción
Auditoría de la seguridad	Auditoría regular ordinaria (mínimo cada dos años) que verifica el cumplimiento de los requerimientos del ENS; también con carácter extraordinario ante modificaciones sustanciales del sistema.
Informe del estado de la seguridad	Recopilación por la Comisión Sectorial de Administración Electrónica, con apoyo del CCN, de la información sobre el estado de la seguridad de los sistemas comprendidos en el ámbito de aplicación, plasmada en un informe.
Declaración de conformidad	Documento por el que los sistemas de categoría BÁSICA acreditan el cumplimiento del ENS mediante autoevaluación.
Certificación de conformidad	Documento requerido para sistemas de categoría MEDIA o ALTA, obtenido mediante auditoría (que puede coincidir con la auditoría de seguridad del art. 31).

INCIDENTES Y RESPUESTA

Término	Descripción
CCN (Centro Criptológico Nacional)	Organismo que, entre otras funciones, articula la respuesta a incidentes de seguridad, coordina a nivel nacional e internacional, y valida perfiles de cumplimiento y esquemas de acreditación.
CCN-CERT	Estructura mediante la cual el CCN articula la respuesta a los incidentes de seguridad (acrónimo de Computer Emergency Response Team).
CSIRT	Equipo de respuesta a incidentes de seguridad informática (Computer Security Incident Response Team); el CCN ejerce la coordinación nacional de la respuesta técnica de los CSIRT en materia de seguridad de redes y sistemas de información del sector público.
INCIBE-CERT	Centro de respuesta a incidentes de seguridad de referencia para ciudadanos y entidades de derecho privado en España, operado por INCIBE; recibe notificaciones de organizaciones del sector privado que prestan servicios a entidades públicas y las traslada al CCN-CERT.
ESPDEF-CERT	Capacidad de respuesta a incidentes de seguridad de referencia para el ámbito de la Defensa Nacional, del Mando Conjunto del Ciberespacio (MCCE).

Término	Descripción
Guías CCN-STIC	Series de documentos elaborados por el CCN (particularmente la serie 800) que ofrecen normas, instrucciones, guías, recomendaciones y mejores prácticas para aplicar el ENS; se incorporan al conjunto documental usado en las auditorías de seguridad.
Instrucción Técnica de Seguridad (ITS)	Disposición de obligado cumplimiento aprobada en desarrollo del ENS (p. ej., sobre auditoría de la seguridad, notificación de incidentes, esquema de certificación de responsables de seguridad).

GLOSARIO OFICIAL — ANEXO IV DEL RD 311/2022

Término	Definición literal (Anexo IV)
Activo	Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.
Administrador del sistema/de la seguridad del sistema	Persona encargada de la instalación y el mantenimiento de un sistema de información, implantando los procedimientos y la configuración de seguridad que se haya establecido en el marco de la política de seguridad del organismo.
Análisis de riesgos	Estudio de las consecuencias previsibles de un posible incidente de seguridad, considerando su impacto en la organización (en la protección de sus activos, en su misión, en su imagen o reputación, o en sus funciones) y la probabilidad de que ocurra.
Área controlada	Zona o área en la que una organización considera cumplidas las medidas de seguridad físicas y procedimentales requeridas para la protección de la información y los sistemas de información ubicados en ella.
Arquitectura de seguridad	Conjunto de elementos físicos y lógicos que forman parte de la arquitectura del sistema y cuyo objetivo es la protección de los activos dentro del sistema y en las interconexiones con otros sistemas.
Auditoría de la seguridad	Proceso sistemático, independiente y documentado que persigue la obtención de evidencias objetivas y su evaluación objetiva para determinar en qué medida se cumplen los criterios de auditoría en relación con la idoneidad de los controles de seguridad adoptados, el cumplimiento de la política de seguridad, las normas y los procedimientos operativos establecidos, y detectando desviaciones a los antedichos criterios.
Autenticación	Ratificación de la identidad de un usuario, proceso o dispositivo.
Autenticación	Exigencia de dos o más factores de autenticación para ratificar una

Término	Definición literal (Anexo IV)
multifactor	autenticación como válida.
Autenticador	Algo, físico o inmaterial, que posee el usuario bajo su exclusivo control y que le distingue de otros usuarios.
Autenticidad	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
Biometría (factor de autenticación)	Reconocimiento de los individuos en base a sus características biológicas o de comportamiento.
Cadena de suministro	Conjunto relacionado de recursos y procesos que comienza con la provisión de materias primas y se extiende a través de la entrega de productos o servicios al usuario final a través de los modos de transporte. Incluye a los proveedores (primer, segundo y tercer nivel), los almacenes de materia prima (directa o indirecta), las líneas de producción, los almacenes de productos terminados y los canales de distribución (mayoristas y minoristas), hasta llegar al cliente final.
Categoría de seguridad de un sistema	Es un grado, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema de información a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría de seguridad del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.
Certificado de firma electrónica (factor de autenticación)	Una declaración electrónica que vincula los datos de validación de una firma con una persona física o jurídica y confirma, al menos, el nombre o el seudónimo de esa persona.
Certificado cualificado de firma electrónica	Un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I del Reglamento (UE) 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
Ciberamenaza	Amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste.
Ciberataque	Cualquier conducta dolosa de individuos u organizaciones, conocidos o no, desarrollada a través del ciberespacio contra sistemas de información, con el propósito de sustraer, alterar, abusar, desestabilizar, inutilizar, destruir o eliminar activos.
Ciberespacio	Dominio global y dinámico compuesto por infraestructuras de tecnología de la información -incluyendo internet-, redes de telecomunicaciones y sistemas de información que configuran un ámbito virtual.
Ciberincidente	Incidente relacionado con la seguridad de las tecnologías de la información y las comunicaciones que se produce en el

Término	Definición literal (Anexo IV)
	ciberespacio.
Ciberseguridad (seguridad de los sistemas de información)	La capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.
Compromiso de la seguridad	Incidente de seguridad en el que, debido a una violación de las medidas técnicas u organizativas de seguridad, una información o un servicio quedan expuestos, o potencialmente expuestos, a un acceso no autorizado.
Confidencialidad	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
Contraseña	Un secreto memorizado por el usuario, compuesto por varios caracteres según unas reglas de complejidad frente a ataques de adivinación o fuerza bruta.
Contraseña de un solo uso (OTP - One-Time Password)	Contraseña generada dinámicamente y que solamente se puede usar una vez y durante un periodo limitado.
Disponibilidad	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
Dispositivo de autenticación (token)	Autenticador físico.
Distintivo de Certificación de Conformidad con el ENS	Documento electrónico, en formato PDF-A, firmado electrónicamente por la Entidad de Certificación responsable de la evaluación de los sistemas de información concernidos, incluyendo un enlace a la Certificación de Conformidad con el ENS que, mientras se mantenga su vigencia, permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada, respectivamente, de que se trate.
Distintivo de Declaración de Conformidad con el ENS	Documento electrónico, en formato PDF-A, firmado o sellado electrónicamente por la entidad bajo cuya responsabilidad se encuentre el sistema de información en cuestión, incluyendo un enlace a la Declaración de Conformidad con el ENS que, mientras se mantenga su vigencia, permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada de que se trate.
Dominio de seguridad	Colección de activos uniformemente protegidos, típicamente bajo una única autoridad. Los dominios de seguridad se utilizan para diferenciar entre zonas en el sistema de información. Por ejemplo:

Término	Definición literal (Anexo IV)
	a) Instalaciones centrales, sucursales, comerciales trabajando con portátiles; b) Servidor central (host), frontal Unix y equipos administrativos; c) Seguridad física, seguridad lógica.
Evento de seguridad	Ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información, una falla de los controles o una situación desconocida que puede ser relevante para la seguridad.
Factor de autenticación	Hay 3 tipos de factores de autenticación: (1) algo que se sabe, un secreto; (2) algo que se tiene, un autenticador; y (3) algo que se es, biometría.
Firma electrónica	Los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.
Firma electrónica avanzada	La firma electrónica que cumple los requisitos contemplados en el artículo 26 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
Firma electrónica cualificada	Una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.
Gestión de incidentes	Procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante éste.
Gestión de riesgos	Actividades coordinadas para dirigir y controlar a una organización con respecto a los riesgos.
Incidente de seguridad (ciberincidente o incidente)	Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información.
Integridad	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
Lista de componentes software	Documento que detalla los componentes software utilizados para construir algo, sea una aplicación o un servicio.
Medidas de seguridad	Conjunto de disposiciones encaminadas a proteger al sistema de información de los riesgos a los que estuviere sometido, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.
Mínimo privilegio	Principio que determina que el diseño de la arquitectura de seguridad de un sistema garantiza el uso de los servicios y permisos mínimos necesarios para su correcto funcionamiento.

Término	Definición literal (Anexo IV)
Monitorización continua	Proceso de gestión dinámica de la seguridad basado en el seguimiento de indicadores críticos de seguridad y parcheo de las vulnerabilidades descubiertas en los componentes del sistema de información.
Observatorio Digital	Un observatorio digital, en su propósito de conocer realidades de la información que se transmite a través de medios digitales, es un conjunto de capacidades para la toma de decisiones dedicado a la detección y seguimiento de anomalías en el origen, definición o diseminación de contenidos digitales, las cuales pudieran representar indicadores de amenaza.
Perfil de cumplimiento específico	Conjunto de medidas de seguridad, comprendidas o no en el anexo II de este real decreto, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad, y que haya sido habilitado por el CCN.
PIN	Un secreto memorizado por el usuario, compuesto por unos pocos caracteres, siguiendo unas ciertas reglas frente a ataques de adivinación.
Política de firma electrónica, sello electrónico y certificados	Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas y sellos electrónicos, incluyendo las características exigibles a los certificados de firma o sello electrónicos.
Política de seguridad (Política de seguridad de la información)	Conjunto de directrices plasmadas en un documento, que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta.
Principios básicos de seguridad	Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.
Proceso	Conjunto organizado de actividades que se llevan a cabo para producir un producto o prestar un servicio, que tiene un principio y fin delimitados, que implica recursos y da lugar a un resultado.
Proceso de seguridad	Método que se sigue para alcanzar los objetivos de seguridad de la organización. El proceso se diseña para identificar, medir, gestionar y mantener bajo control los riesgos a que se enfrenta el sistema en materia de seguridad.
Proceso TIC	Conjunto de actividades llevadas a cabo para la concepción, elaboración, suministro y mantenimiento de un producto o servicio TIC.
Producto TIC	Elemento o grupo de elementos de las redes o los sistemas de información.
Requisitos mínimos	Exigencias mínimas necesarias para asegurar la información tratada

Término	Definición literal (Anexo IV)
de seguridad	y los servicios prestados.
Secreto memorizado (factor de autenticación)	Algo que solamente sabe el usuario autorizado. Típicamente, se concreta en una contraseña o un PIN.
Sistema de información	Cualquiera de los elementos siguientes: 1.º Las redes de comunicaciones electrónicas que utilice la entidad del ámbito de aplicación de este real decreto sobre las que posea capacidad de gestión. 2.º Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales. 3.º Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1.º y 2.º anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.
TEMPEST	Término que hace referencia a las investigaciones y estudios de emanaciones comprometedoras (emisiones electromagnéticas no intencionadas, producidas por equipos eléctricos y electrónicos que, detectadas y analizadas, puedan llevar a la obtención de información) y a las medidas aplicadas a la protección contra dichas emanaciones.
Trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad.
USO OFICIAL	Designa información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.
Usuarios de la organización	Personal del organismo, propio o contratado, estable o circunstancial, que acceden al sistema para desarrollar las funciones o actividades que les han sido encomendadas por la organización.
Usuarios externos	Usuarios con acceso al sistema que no entran en el conjunto de usuarios de la organización. En particular, los ciudadanos administrados.