Mapa de guías CCN-STIC

Mapa de qué guía CCN-STIC te aplica según tu categoría y perfil

Material propio, de elaboración original (Ángel Ortega Castro / Summum Marketing), construido a partir del texto público del RD 311/2022 (excluido de propiedad intelectual por el art. 13 LPI: es una disposición reglamentaria). No reproduce ninguna guía CCN-STIC; organiza en un único mapa lo que el CCN publica repartido en 40 documentos distintos. Este es el contenido real del imán — no una copia del PDF de nadie.

Paso 1 · Mide el nivel de cada dimensión, no la categoría todavía

El ENS valora cinco dimensiones de seguridad por separado. Para cada una, asigna el nivel (BAJO, MEDIO, ALTO, o «no afectada» si el incidente no tendría consecuencias en esa dimensión):

Dimensión	Pregunta que la fija	Nivel
Confidencialidad	Si esta información se filtrase, ¿el perjuicio sería limitado, grave o muy grave?	☐ Bajo ☐ Medio ☐ Alto
Integridad	Si alguien la alterase sin permiso, ¿qué tan grave sería el daño?	☐ Bajo ☐ Medio ☐ Alto
Trazabilidad	Si no pudieras demostrar quién hizo qué, ¿qué consecuencias tendría?	☐ Bajo ☐ Medio ☐ Alto
Autenticidad	Si alguien pudiera suplantar a un usuario o falsear el origen del dato, ¿qué pasaría?	☐ Bajo ☐ Medio ☐ Alto
Disponibilidad	Si el servicio cayera un día entero, ¿qué tan grave sería?	☐ Bajo ☐ Medio ☐ Alto

Esto es exactamente lo que desarrolla la guía CCN-STIC 803 (Valoración de sistemas en el ENS): el procedimiento para pasar de «esto nos afectaría bastante» a un nivel concreto por dimensión.

Paso 2 · Tu categoría es el nivel MÁS ALTO de las cinco — no la media, no la moda

Error normativo real, ya publicado y corregido en este sitio: mezclar «categoría» (una propiedad del SISTEMA completo) con «nivel» (una propiedad de CADA DIMENSIÓN). Son cosas distintas y el RD 311/2022 las separa a propósito (Anexo I, apartado 4):

- Si **ninguna** dimensión pasa de BAJO → tu sistema es **categoría BÁSICA**.
- Si **al menos una** dimensión llega a MEDIO (y ninguna a ALTO) → **categoría MEDIA**.
- Si **al menos una** dimensión llega a ALTO → **categoría ALTA**.

Basta con que UNA dimensión suba para que suba la categoría entera, aunque las otras cuatro se queden en bajo. Es la trampa más común: un sistema con disponibilidad ALTA (por ejemplo, un servicio 24/7 crítico) es categoría ALTA aunque su confidencialidad sea irrelevante.

Paso 3 · Tabla de decisión: qué te toca según tu categoría

Tu categoría	Cómo se llega	Guías CCN-STIC que aplican siempre	Auditoría y conformidad
BÁSICA	Ninguna dimensión pasa de nivel bajo	801 (roles) · 803 (valoración) · 805 (política de seguridad) · 806 (plan de adecuación)	Autoevaluación por tu propio personal (guía 808 como referencia de qué comprobar) → **Declaración** de conformidad (guía 809), publicada en tu sede electrónica o web. No exige auditor externo, aunque puedes pedirla voluntariamente.
MEDIA	Al menos una dimensión en nivel medio, ninguna en alto	Las mismas 801, 803, 805, 806, y además entra en juego el marco de	Auditoría obligatoria por entidad certificadora (guías 802 + 808)

Tu categoría	Cómo se llega	Guías CCN-STIC que aplican siempre	Auditoría y conformidad
		medidas reforzado del Anexo II	al menos cada 2 años → **Certificación** de conformidad (guía 809), publicada obligatoriamente
ALTA	Al menos una dimensión en nivel alto	Las mismas de MEDIA, con los refuerzos de seguridad más exigentes del Anexo II (los marcados «rojo» en la tabla de medidas del CCN)	Auditoría obligatoria igual que MEDIA; con el matiz de que ante hallazgos graves el responsable del sistema puede suspender temporalmente el servicio (art. 31.6 RD 311/2022) hasta corregirlos

Paso 4 · Tu perfil cambia el CÓMO, no el SI

- **Administración pública** (ayuntamiento, organismo autónomo, universidad pública…): obligada directamente por el art. 2 del RD 311/2022. Aplica a todos sus sistemas de información, sin excepción de tamaño.
- **Empresa que presta servicios TIC a la Administración** (alojamiento, desarrollo de software, gestión documental, plataformas, ciberseguridad…): obligada por la vía contractual. Desde 2024, sin certificación o declaración de conformidad ENS no se puede firmar o renovar el contrato con la Administración. El proceso es idéntico al de la Administración: la categoría la fija el análisis de impacto del propio servicio contratado, no el tamaño de la empresa proveedora.

Cómo se usa este mapa en la práctica (orden real de trabajo)

1. Valora tus dimensiones (Paso 1 → guía 803).
2. Fija tu categoría por el máximo, nunca por la media (Paso 2).
3. Nombra los cuatro roles y documenta tu política de seguridad (guías 801 y 805) — esto va primero porque el resto de guías dan por hecho que estas figuras ya existen.
4. Redacta el plan de adecuación con tus huecos reales frente al Anexo II (guía 806).
5. Verifica el cumplimiento: autoevaluación si eres básica, auditoría si eres media o alta (guías 802 y 808).

6. Declara o certifica la conformidad y publícala en tu sede o web (guía 809).

Elaborado el 4 de septiembre de 2026 a partir del texto del RD 311/2022 (BOE-A-2022-7191, descargado y verificado línea a línea). No sustituye la lectura de las guías CCN-STIC oficiales, enlazadas desde la página, ni el asesoramiento de un auditor acreditado para casos límite entre categorías o dimensiones no contempladas aquí.