Organizan

TEDAE Defensa, Seguridad, Aeronáutica y Espacio

Comité calidad de TEDAE

AEC Asociación Española para la Calidad

6ª Jornada Técnica

"Herramientas prácticas para el sector de Defensa, Seguridad y Aeroespacial"

Madrid, 23 de junio de 2026

"Integración de la ciberdefensa en los sistemas de calidad"

Jorge Arroyo Lázaro

Responsable IT, PAP TECNOS Innovación

www.linkedin.com/in/jorge-arroyo-2a72a133

@ jarroyo@paptecnos.es

¿Quién ha hecho posible esta guía?

- Alfonso López López
- Fernando R. Armada García (NAVANTIA)
- Jorge Arroyo Lázaro (PAP TECNOS Innovación)
- Laura Monsálvez Víctor

Objetivo: construir el puente

Proporcionar un marco para integrar la ciberdefensa en sistemas de gestión de calidad, especialmente donde hay requisitos normativos, contractuales o de defensa.

No se trata de un manual técnico. Es un marco de referencia para integrar lo **invisible en lo tangible**: Blindar el Sistema de Gestión de Calidad frente a la nueva guerra híbrida.

Calidad

procesos · trazabilidad · auditoría

Ciberdefensa

riesgos · amenazas · resiliencia

Contrato

requisitos · evidencias · cumplimiento

No sustituye normas ni metodologías: ayuda a que el Sistema de Calidad las absorba de forma coherente.

Alcance: dónde entra la ciberdefensa en calidad

Trascendemos el código, abarcando:

- El producto: hardware y software.
- El proceso: de la ingeniería a la cadena de suministro.
- Las personas: formación como barrera de ciberdefensa.
- El entorno: salas seguras y repositorios blindados.

La seguridad no se "añade al final"; se incorpora al ciclo normal del sistema.

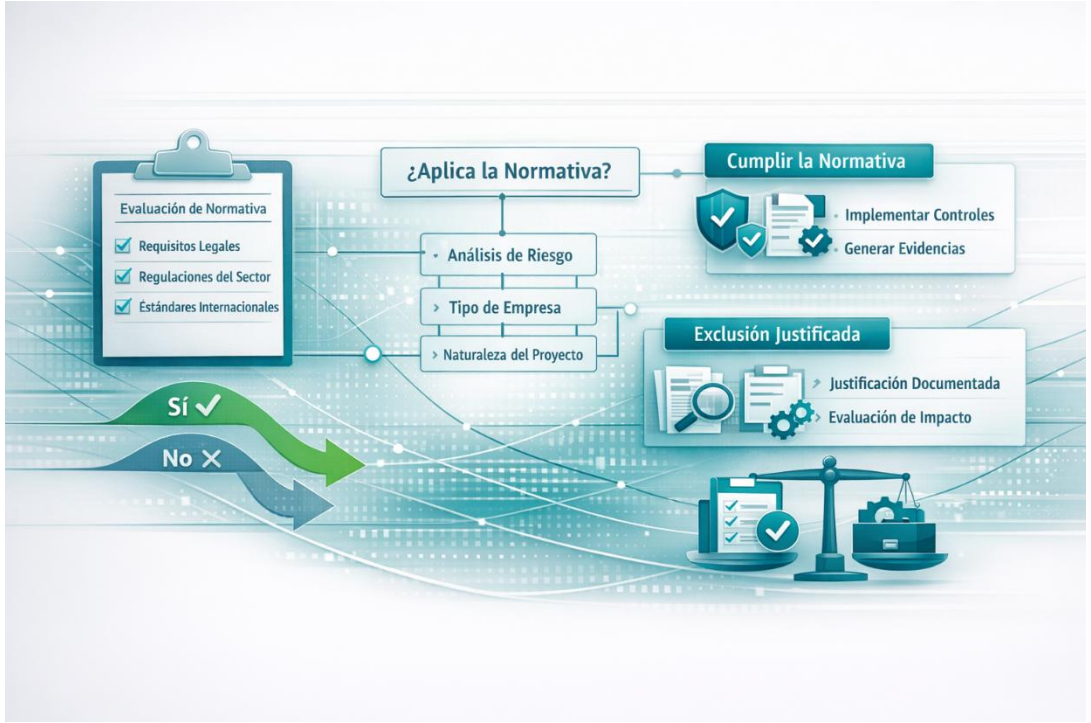
¿Para qué sirve realmente?

Traducir — Convertir exigencias de ciberseguridad en lenguaje de procesos, registros y auditoría.

Priorizar — Saber qué revisar primero según sector, contrato, producto y riesgo.

Preguntar — Disponer de checklists para abrir conversaciones útiles con TI, ingeniería y proveedores.

Evidenciar — Evitar sistemas paralelos y construir un repositorio común de evidencias.



La seguridad ya no es una opción del cliente, es una responsabilidad legal del fabricante (CRA)

Ciberseguridad y ciberdefensa no compiten…

… se complementan, respondiendo a preguntas distintas.

Ciberseguridad

¿Cómo reducimos vulnerabilidades antes de que sean explotadas?

Prevención · Protección · Reacción · Recuperación

Enfoque **preventivo:** Proteger la información y los activos digitales de la empresa de forma reactiva y defensiva.

Ciberdefensa

¿Cómo detectamos, resistimos y respondemos ante amenazas concretas?

Detección · Respuesta · Inteligencia · Resiliencia operativa

Enfoque **activo:** Estrategias para garantizar la libertad de acción en el ciberespacio Estatal y militar. Resistencia ante ataques persistentes.

La clave no es elegir una: es saber cómo se convierten ambas en requisitos verificables

Desarrollo seguro: cuatro capas

1. Desarrollo seguro

Diseño, codificación, revisión y validación.

2. Desarrollo ciberseguro

Resistencia a ataques, cifrado, autenticación, vulnerabilidades.

3. Entorno seguro

Personas, salas, documentación, repositorios, segregación.

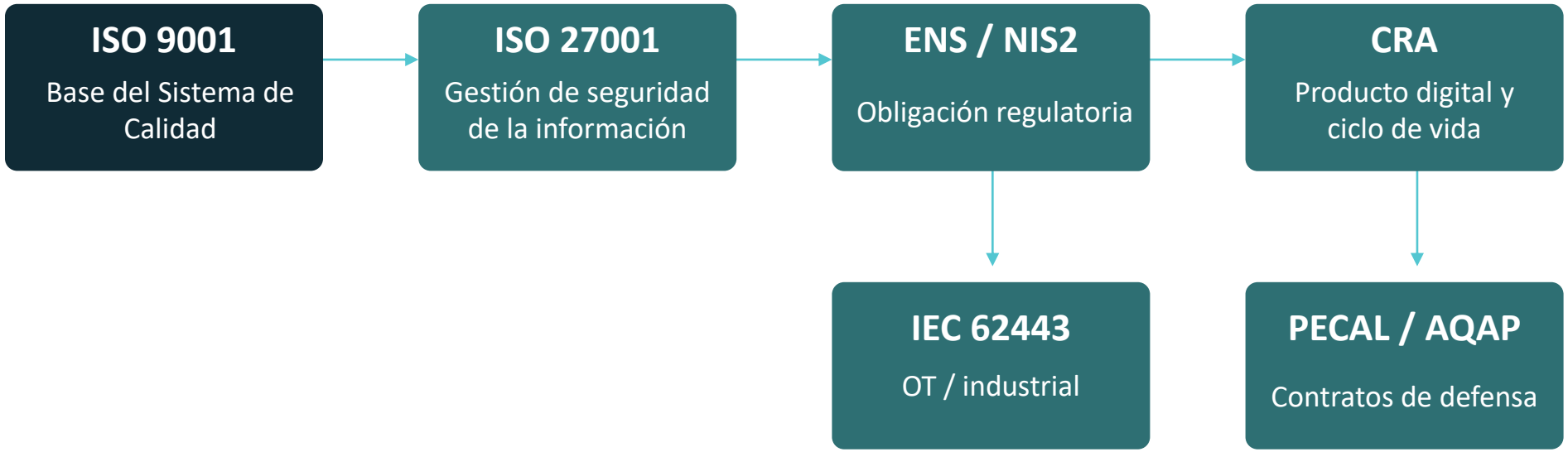
4. Entorno ciberseguro

Redes, servidores, nube, centro de datos, parches, monitorización.

Un producto "bien hecho" puede seguir siendo frágil si el entorno, la configuración o la cadena de evidencias fallan.

Normativa: aplicabilidad

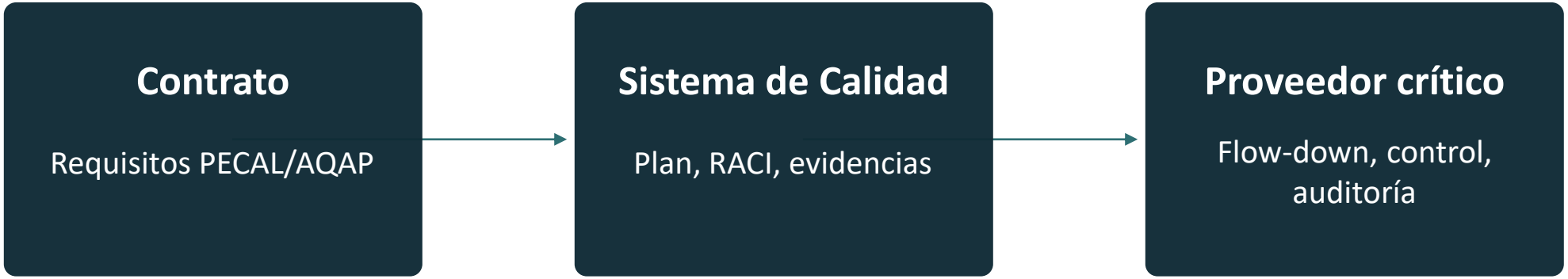
¿qué me aplica por sistema, por sector, por contrato o por producto?



Recomendado: analizar el caso de uso de cada organización, no empezar por la tabla normativa.

En defensa, la calidad se demuestra en cadena

Los requisitos no deben quedarse en el contratista principal: deben bajar a proveedores críticos.
Debemos validar cada componente de la cadena de suministro como si ya estuviera comprometido.



Hay que convertir el "esto es del proveedor", en una pregunta de aseguramiento contractual.

Formación: de trámite anual a control auditable

¿Quién debe saber qué?

Alta dirección, usuarios, equipos técnicos, Desarrollo, terceros…

¿Cómo se demuestra?

No solo asistencia: matriz de competencias, evaluación de eficacia, registros y seguimiento.

¿Cómo mejora?

Indicadores, campañas, simulaciones, auditorías, no conformidades y revisión por dirección.

Debemos pasar de "formar por cumplir" a "formar para reducir riesgo y generar evidencia".

Cómo leer la guía sin perderse

1	**Sitúa tu contexto**	Sector, contrato, producto, tecnología, proveedores
2	**Elige el hilo de lectura**	Normativa, desarrollo seguro, formación o buenas prácticas
3	**Usa los checklists**	No para "aprobar", sino para descubrir brechas y evidencias faltantes
4	**Convoca a las áreas**	Calidad, IT, Seguridad, Ingeniería, Compras, Contrato
5	**Cierra con un plan**	Responsables, plazos, registros y revisión

Tres preguntas que deberíamos hacernos

1. **¿Dónde aparece hoy la ciberseguridad en mi Sistema de Calidad?**
2. **¿Qué requisitos ya estamos cumpliendo, pero sin evidencias trazables?**
3. **¿Qué proveedor, producto o contrato podría exponernos mañana?**

Hay que convertir una preocupación técnica, en una conversación de gestion.

Muchas gracias por su atención