Guía de soporte para su implementación y utilización

Integración de la ciberdefensa

en los sistemas de calidad

2026

TEDAE
Defensa, Seguridad, Aeronáutica y Espacio

GRUPO DE TRABAJO

- Alfonso López López. SENER Aeroespacial y Defensa
- Fernando R. Armada García. NAVANTIA
- Jorge Arroyo Lázaro. Independiente
- Laura Monsálvez Víctor. Independiente

índice

01 Terminología

- **Base de Conocimiento:** Los datos constituyen la base de cualquier sistema de IA. Es fundamental establecer una infraestructura para la recopilación, almacenamiento y gestión de grandes volúmenes de datos en un datalake que nos posibilite la creación de una base de conocimiento centralizada.

- **Amenaza Avanzada Persistente (APT):** Ataques prolongados y dirigidos a objetivos específicos para robar información o causar daño.

- **Arquitecturas Zero-trust (ZTA):** Modelo de seguridad que asume que ninguna entidad, interna o externa, es de confianza por defecto.

- **Ataque de denegación de servicio (DDoS):** Ataque que busca hacer que un sistema o red sea inaccesible mediante la sobrecarga de tráfico.

- **Automatización y Orquestación de Respuestas de Seguridad (SOAR):** Herramientas que automatizan la respuesta a incidentes de seguridad.

- **Ciberamenaza:** Acto malicioso que busca hacer daño a datos, robar información o afectar la vida digital en general, aprovechando vulnerabilidades para interrumpir, destruir o amenazar la actividad normal de individuos o empresas.

- **Ciberataque:** Ataque contra un sistema informático. Tiene como objetivo principal perjudicar a una persona, entidad o Estado. Los ciberataques afectan los sistemas de información ingresando a bases de datos o las redes computacionales para poder espiar o extorsionar; o anulando información importante o los servicios informáticos por completo. Existen diferentes tipos de ciberataques. A continuación, mencionamos algunos:
  - Phishing.
  - Malware.
  - Inyección de SQL.
  - Ataque de denegación de servicio.

- **Ciberinteligencia:** Uso de datos y análisis para anticipar, identificar y mitigar amenazas cibernéticas.

Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio
C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24
info@tedae.org
www.tedae.org

- **Cifrado de Datos:** Técnica para proteger la confidencialidad de los datos mediante la conversión de información en un formato ilegible para usuarios no autorizados.
- **Computer Security Incident Response Team (CSIRT):** Equipo especializado en la gestión y respuesta a incidentes de seguridad informática, encargado de detectar, prevenir y remediar ciberataques.
- **Firewall:** Dispositivo o software que controla el tráfico de red entrante y saliente basado en reglas de seguridad predeterminadas.
- **Gestión de Identidad y Acceso (IAM):** Soluciones para gestionar y controlar el acceso de los usuarios a sistemas y datos.
- **Herramientas de Análisis de Comportamiento de Usuarios (UBA):** Monitoreo y análisis de las actividades de los usuarios para detectar comportamientos anómalos.
- **Ingeniería Social:** Técnicas utilizadas por los atacantes para manipular a las personas y obtener información confidencial.
- **Inteligencia Artificial (IA):** Tecnología utilizada para mejorar las defensas cibernéticas mediante el análisis de grandes volúmenes de datos y la detección de patrones.
- **Malware:** Software malicioso diseñado para infiltrarse, dañar o deshabilitar sistemas informáticos.
- **Phishing:** Técnica utilizada para engañar a las personas y obtener información confidencial, como contraseñas y datos bancarios, mediante correos electrónicos falsos o sitios web fraudulentos.
- **Plataformas de Gestión de Eventos e Información de Seguridad (SIEM):** Sistemas que recopilan y analizan datos de seguridad en tiempo real para detectar y responder a incidentes.
- **Ransomware:** Tipo de malware que cifra los archivos de la víctima y exige un rescate para desbloquearlos.
- **Recuperación ante Desastres:** Estrategias y procedimientos para restaurar sistemas y datos después de un incidente de seguridad.
- **Seguridad informática:** Se refiere específicamente a la protección de los sistemas informáticos contra todo tipo de amenazas, ya sean daños físicos, fallos en el software, robo o pérdida de datos. Su objetivo es asegurar que los datos sean confidenciales, íntegros y accesibles solo para usuarios autorizados.
- **Sistema de Detección de Intrusos (IDS):** Tecnología que monitorea el tráfico de red en busca de actividades sospechosas.
- **Sistema de Prevención de Intrusos (IPS):** Tecnología que no solo detecta, sino que también previene actividades sospechosas en la red.
- **Sistemas de Respuesta a Incidentes (IR):** Tecnologías y procesos para gestionar y mitigar los efectos de un ciberataque.

02 Propósito y Alcance

La presente guía tiene como objetivo proporcionar un marco de referencia para integrar de forma coherente la ciberdefensa en los sistemas de gestión de la calidad, especialmente en organizaciones que desarrollan, suministran o mantienen productos, servicios o software en entornos con requisitos normativos, contractuales o de defensa.

Su alcance comprende la clarificación conceptual entre ciberdefensa y ciberseguridad, la incorporación del desarrollo seguro, la identificación de normativa y marcos aplicables, la relación con los contratos de defensa y estándares PECAL, así como la formación, concienciación y adopción de buenas prácticas organizativas y técnicas.

Esta guía está dirigida principalmente a responsables de calidad, responsables de seguridad de la información, dirección, gestores de contrato, equipos técnicos y de desarrollo, así como a aquellas organizaciones de la base industrial y tecnológica de la defensa que necesiten alinear sus procesos de calidad con requisitos crecientes de seguridad y resiliencia.

Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio
C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24
info@tedae.org
www.tedae.org

Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio

C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24

info@tedae.org
www.tedae.org

03 Introducción

En el contexto actual, la calidad de los productos, servicios y desarrollos de software no puede entenderse al margen de la ciberdefensa. La creciente exposición a amenazas cibernéticas, junto con la aparición de requisitos regulatorios, contractuales y operativos cada vez más exigentes, obliga a las organizaciones a integrar estas materias dentro de sus sistemas de gestión, y no tratarlas como ámbitos separados o exclusivamente técnicos.

Desde esta perspectiva, la ciberdefensa debe incorporarse al sistema de calidad como elemento que influye directamente en la planificación, el análisis de riesgos, la definición de requisitos, el diseño y desarrollo, la gestión de proveedores, la formación, la gestión documental, la trazabilidad, las auditorías y la mejora continua. Esta integración permite a la organización disponer de un enfoque único y coherente, mejorar la resiliencia de sus procesos y productos, demostrar cumplimiento ante clientes, reguladores y organismos contratantes, y generar evidencias objetivas de control a lo largo de todo el ciclo de vida.

En entornos de defensa, además, esta relación adquiere una relevancia especial, ya que los requisitos de calidad, seguridad y aseguramiento del software convergen en marcos como PECAL, en las obligaciones derivadas de la normativa aplicable y en la necesidad de garantizar la fiabilidad, integridad y protección de los sistemas suministrados.

04 Distinción entre Ciberdefensa y Ciberseguridad

La ciberdefensa y la ciberseguridad son conceptos relativamente nuevos que pueden ser desconocidos o fáciles de confundir. Ambas son pilares básicos para protegerse en el mundo digital actual frente a las amenazas cibernéticas. Por lo tanto, adoptar un enfoque proactivo en ciberdefensa y ciberseguridad es indispensable. Las diferencias entre ellas en concepto y alcance se reflejan en el uso de herramientas específicas.

La cooperación es fundamental en la seguridad de la información.

Y, la ciberseguridad y la ciberdefensa deben trabajar de forma sinérgica para garantizar una protección efectiva.

4.1 ¿Qué es la ciberdefensa?

4.1.1. Introducción

La ciberdefensa es el conjunto de estrategias implementadas para proteger activamente sistemas informáticos, redes, datos y dispositivos contra ataques cibernéticos. Estas estrategias incluyen herramientas y acciones destinadas a evitar, prevenir o responder a ciberataques, ofreciendo una resistencia activa.

A diferencia de la ciberseguridad, la ciberdefensa tiene un enfoque más concreto y se utiliza principalmente en el ámbito estatal o militar. En este contexto, la ciberdefensa se refiere a las operaciones activas o pasivas que el Estado emplea para garantizar la seguridad y el uso adecuado del ámbito digital del país, protegiéndolo de amenazas cibernéticas. Su objetivo es asegurar la libertad de acción de las Fuerzas Armadas en el ciberespacio.

En España, el Mando Conjunto del Ciberespacio (MCCE), dependiente del Estado Mayor de la Defensa, es el organismo encargado de implementar la ciberdefensa nacional mediante la planificación, coordinación, control y ejecución de las operaciones militares no presenciales.

Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio
C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24
info@tedae.org
www.tedae.org

La ciberdefensa juega un papel fundamental en la defensa de un Estado y en la gestión del riesgo informático en general. No solo abarca la protección contra la vulneración de sistemas, sino también la prevención de intrusiones en estructuras cibernéticas.

4.1.2. Principales aplicaciones

- Detección y respuesta ante amenazas, incluyendo ataques APT, malware y ransomware.
- Gestión de incidentes de seguridad.
- Gestión de accesos e identidades.
- Protección de redes, sistemas y dispositivos.
- Sistemas de Gestión de Información y Eventos de Seguridad (SIEM).
- Automatización y Orquestación de Respuestas de Seguridad (SOAR).
- Integración con Inteligencia de Amenazas.

4.1.3. Ejemplos de ciberdefensa

Históricamente, un hito significativo en la ciberdefensa fue el desarrollo del gusano informático “Creeper” en 1971, considerado el primer malware que se propagó a través de la red ARPANET. Para contrarrestarlo, Ray Tomlinson desarrolló “Reaper”, un gusano diseñado específicamente para localizar y eliminar a “Creeper”. Este evento marcó el inicio de la necesidad de estrategias de ciberdefensa para proteger sistemas informáticos y redes.

Desde entonces, la ciberdefensa ha evolucionado significativamente. En los años 80 y 90, surgieron nuevas amenazas como los virus informáticos y se implementaron medidas como los equipos de respuesta a incidentes de seguridad informática (CSIRT) y los sistemas de detección de intrusos (IDS). En el siglo XXI, la ciberdefensa se ha adaptado para enfrentar amenazas más sofisticadas como los ataques de denegación de servicio (DDoS) y el ransomware, utilizando tecnologías avanzadas como la inteligencia artificial y el aprendizaje automático. La cooperación internacional y el desarrollo continuo de estas tecnologías son esenciales para enfrentar las amenazas cibernéticas actuales y futuras.

Se incluyen:

- Firewalls, como defensa perimetral.
- Software antivirus.
- Sistemas de detección de intrusiones (IDS / IPS), que monitorean el tráfico en busca de actividades sospechosas y proporcionan respuesta.
- Cifrado de datos.
- Estrategias de autenticación de usuarios y análisis de comportamiento en busca de anomalías.

> **“LA COOPERACIÓN ES FUNDAMENTAL EN LA SEGURIDAD DE LA INFORMACIÓN”**

4.2. ¿Qué es la ciberseguridad?

4.2.1. Introducción

La ciberseguridad se refiere al conjunto de prácticas destinadas a proteger sistemas informáticos, redes, datos y dispositivos contra ciberamenazas. Esta disciplina abarca la protección de sistemas conectados a Internet, incluyendo hardware, software y datos en la nube, y es utilizada tanto por individuos como por empresas para evitar el acceso no autorizado a centros de datos y otros sistemas computarizados. Además, la ciberseguridad es crucial para prevenir ataques que buscan deshabilitar o interrumpir las operaciones de un sistema o dispositivo.

A diferencia de la ciberdefensa, que tiene un enfoque más concreto y reactivo, la ciberseguridad es un concepto más amplio y preventivo que abarca todos los dispositivos digitales. Puede incluir estrategias tanto públicas como privadas para proteger la información y los sistemas.

Una estrategia sólida de ciberseguridad proporciona una defensa robusta contra ataques maliciosos diseñados para acceder, alterar, eliminar, destruir o extorsionar los sistemas y datos confidenciales de una organización o usuario.

4.2.2. Etapas de la ciberseguridad

La ciberseguridad se desarrolla en varias etapas clave que aseguran una protección integral contra las amenazas cibernéticas.

- **Prevención:** Esta etapa implica el análisis de la infraestructura de seguridad de la empresa y la detección de posibles vulnerabilidades. Es fundamental identificar y evaluar los riesgos antes de que puedan ser explotados.

Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio
C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24
info@tedae.org
www.tedae.org

- **Protección:** Una vez identificadas las vulnerabilidades, se implementan las medidas y procesos de ciberseguridad necesarios para proteger los sistemas, redes y datos. Esto incluye la configuración de firewalls, el uso de software antivirus y la aplicación de políticas de seguridad.

- **Reacción:** En caso de un ciberataque, es crucial contar con tecnologías y capacidades para reaccionar de manera efectiva. Esta etapa se centra en la detección rápida de incidentes y la respuesta inmediata para mitigar el impacto del ataque.

- **Recuperación:** Finalmente, se llevan a cabo acciones para lidiar con las posibles consecuencias de un ataque. Esto incluye la restauración de sistemas y datos, así como la implementación de mejoras para prevenir futuros incidentes.

4.2.3. Ejemplos de ciberseguridad

La ciberseguridad abarca una amplia gama de prácticas y herramientas diseñadas para proteger sistemas, redes y datos. A continuación, se presentan algunos ejemplos clave:

- **Instalación de hardware y software de protección en tiempo real:** Incluye herramientas de ciberinteligencia capaces de bloquear amenazas instantáneamente y adaptarse a nuevas amenazas mediante algoritmos de aprendizaje automático.

- **Resolución de vulnerabilidades:** Identificación y corrección de fallos de seguridad en sistemas y aplicaciones.

- **Puesta en marcha de protocolos para la recuperación tras un ataque:** Estrategias y procedimientos para restaurar sistemas y datos después de un incidente de seguridad.

- **Herramientas de Análisis de Comportamiento de Usuarios (UBA):** Monitoreo y análisis de las actividades de los usuarios para detectar comportamientos anómalos.

- **Plataformas de Gestión de Eventos e Información de Seguridad (SIEM):** Recopilación y correlación de datos de registro de eventos de múltiples fuentes para una detección y respuesta rápida a incidentes.

- **Sistemas de Respuesta a Incidentes (IR):** Tecnologías y procesos para gestionar y mitigar los efectos de un ciberataque.

- **Herramientas de Análisis Forense:** Investigación de incidentes de seguridad para identificar la causa y el alcance del ataque.

- **Soluciones de Gestión de Identidad y Acceso (IAM):** Control y supervisión del acceso de los usuarios a sistemas y datos.

- **Herramientas de cifrado de datos:** Protección de la confidencialidad de los datos mediante técnicas de cifrado.

- **Soluciones para la gestión de políticas de seguridad:** Implementación y cumplimiento de políticas de seguridad en toda la organización.

- **Programas de formación y concienciación sobre ciberseguridad:** Capacitación de empleados y usuarios finales para prevenir ciberataques, especialmente aquellos que comienzan por descuidos o desconocimiento.

- **Plataformas para el cumplimiento regulatorio:** Herramientas que facilitan el cumplimiento de normativas y estándares de seguridad cibernética, como GDPR o HIPAA, incluyendo automatizaciones y generación de informes.

4.3. Diferencias entre ciberdefensa y ciberseguridad

La principal diferencia entre ciberseguridad y ciberdefensa radica en su alcance y enfoque. La ciberseguridad abarca un amplio espectro de medidas de protección destinadas a proteger sistemas interconectados y la información digital. Por otro lado, la ciberdefensa es una parte específica de la ciberseguridad que se centra en responder y poner freno a amenazas concretas, combatiendo a los ciberdelincuentes mediante procedimientos establecidos.

Para entender mejor esta diferencia, podemos usar una analogía. Si la empresa fuera un edificio, la ciberdefensa se centraría en construir defensas físicas como murallas, fosos y guardias de vigilancia para evitar ataques. En cambio, la ciberseguridad incluiría no solo estas defensas físicas, sino también el estudio de las estrategias de ataque del enemigo y la generación de simulaciones de ataque para prepararse mejor.

El enfoque de la ciberdefensa está muy centrado en los ataques: su objetivo es desarrollar capacidades para detectar ataques y establecer respuestas efectivas. En cambio, la ciberseguridad se enfoca en detectar y controlar vulnerabilidades antes de que sean explotadas por adversarios. Esto implica un amplio abanico de acciones, desde el desarrollo de políticas de seguridad hasta la formación de equipos humanos para prevenir ciberataques.

En resumen, aunque ambos conceptos deben actuar de forma complementaria, en entornos críticos o de defensa constituyen un componente esencial para alcanzar un nivel adecuado de ciberseguridad.

En esta guía, la ciberdefensa se aborda en relación con los entornos y contratos del sector defensa, mientras que la ciberseguridad se emplea como marco general de medidas prácticas integrables en el sistema de calidad.

4.4. Tendencias y soluciones en ciberdefensa y ciberseguridad

En el contexto actual, donde las amenazas digitales son cada vez más sofisticadas y frecuentes, es crucial que las organizaciones adopten un enfoque integral y adaptativo en ciberdefensa y ciberseguridad. Las tendencias y soluciones emergentes en estos campos no solo requieren un profundo conocimiento de sistemas y redes, sino también la capacidad de identificar con precisión las posibles vías de ataque. Trabajando en sinergia, estas estrategias permiten proteger eficazmente los sistemas, redes y dispositivos de una organización.

A continuación, se presentan algunas de las tendencias y soluciones más destacadas:

- **Aumento de la velocidad de respuesta a amenazas:** Implementación de herramientas avanzadas como los Next-Generation firewalls y las herramientas de automatización y respuesta SOAR.
- **Arquitecturas Zero-trust (ZTA):** Defensas que cubren el trabajo en remoto e híbrido, asegurando que solo los usuarios y dispositivos verificados puedan acceder a los recursos.
- **Analítica de comportamientos avanzada:** Identificación de actividades anómalas, tanto intencionadas como no intencionadas, y puesta en marcha de medidas de protección.
- **Automatización en ciberseguridad:** Uso de automatizaciones para procesos de menor riesgo, basándose en evaluaciones de riesgo para evitar la creación de nuevas vulnerabilidades.

Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio
C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24
info@tedae.org
www.tedae.org

- **Aplicación de inteligencia artificial:** Implementación de IA para mejorar las defensas, teniendo en cuenta que los hackers también utilizan herramientas avanzadas.

- **Medidas contra ransomware:** Creación de repositorios de datos resilientes, respuestas automáticas y sistemas de autenticación avanzados para prevenir ataques de ransomware.

Estas estrategias, cuando se implementan de manera conjunta, proporcionan una defensa robusta y adaptable frente a las amenazas digitales actuales.

> **“ESTAS ESTRATEGIAS, CUANDO SE IMPLEMENTAN DE MANERA CONJUNTA, PROPORCIONAN UNA DEFENSA ROBUSTA Y ADAPTABLE FRENTE A LAS AMENAZAS DIGITALES ACTUALES”**

05 Desarrollo Seguro

El desarrollo seguro debe entenderse como un enfoque integral orientado a garantizar que el software y los sistemas asociados se conciban, construyan, prueben, desplieguen y mantengan con criterios de seguridad desde su origen.

No se limita únicamente a la codificación, ni tampoco a la infraestructura técnica sobre la que se trabaja, sino que abarca tanto el propio producto software como el entorno organizativo, físico y tecnológico en el que dicho desarrollo tiene lugar.

Desde esta perspectiva, resulta útil distinguir entre cuatro conceptos complementarios: desarrollo seguro, desarrollo ciberseguro, desarrollo en entorno seguro y entorno ciberseguro.

Esta diferenciación permite delimitar responsabilidades, identificar controles aplicables y evitar la falsa percepción de que basta con proteger solo el código o solo la infraestructura.

5.1. Desarrollo seguro

El desarrollo seguro se centra en la seguridad del software desde las fases de diseño y codificación. Su objetivo principal es reducir defectos, errores de implementación y vulnerabilidades introducidas durante la construcción del producto.

En este ámbito se incluyen prácticas como la validación de entradas, el tratamiento seguro de errores, la codificación segura, la revisión de código y la incorporación de requisitos de seguridad dentro del ciclo de vida del desarrollo.

En consecuencia, el desarrollo seguro debe formar parte del proceso habitual de ingeniería, de forma que la seguridad no se trate como una revisión final, sino como una condición de calidad del propio producto.

Esta visión es coherente con el enfoque posterior del documento, donde se indica que la seguridad debe integrarse en el ciclo de vida del desarrollo de software y apoyarse en revisiones de código y pruebas específicas.

Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio
C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24
info@tedae.org
www.tedae.org

Concepto	Enfoque principal	Ejemplo práctico
Desarrollo seguro	Seguridad del software desde el diseño y codificación	Validación de entradas, control de errores, codificación segura
Desarrollo ciberseguro	Protección del software frente a amenazas externas y ciberataques	Cifrado, autenticación, cumplimiento ENS, análisis de vulnerabilidades
Desarrollo en entorno seguro	Buenas prácticas en el entorno físico y digital donde se desarrolla el software	Control de accesos, limpieza de escritorio, seguridad en salas de reuniones
Entorno ciberseguro	Infraestructura digital robusta y protegida frente a amenazas cibernéticas	Redes segmentadas, firewalls, monitorización continua, protección de datos en la nube

Tabla 1. Conceptos Desarrollo Seguro

5.2. Desarrollo ciberseguro

El desarrollo ciberseguro amplía el concepto anterior y pone el foco en la capacidad del software para resistir amenazas externas y ciberataques una vez que entra en operación.

Mientras que el desarrollo seguro se orienta principalmente a evitar errores de diseño e implementación, el desarrollo ciberseguro incorpora mecanismos de protección frente a ataques deliberados, tales como cifrado, autenticación robusta, análisis de vulnerabilidades, endurecimiento de componentes y cumplimiento de marcos o requisitos de seguridad aplicables.

En este sentido, no basta con que el software funcione correctamente: debe hacerlo de forma resiliente frente a accesos no autorizados, alteraciones, explotación de vulnerabilidades o compromisos de integridad y disponibilidad.

5.3. Desarrollo en entorno seguro

El desarrollo en entorno seguro hace referencia a las condiciones físicas, organizativas y operativas en las que se lleva a cabo el trabajo de desarrollo.

Su finalidad es proteger los activos utilizados durante el proceso de ingeniería —personas, documentación, equipos, credenciales, repositorios, salas y puestos de trabajo— frente a accesos indebidos, fugas de información, errores humanos o manipulaciones no autorizadas.

Dentro de este ámbito se encuadran medidas como el control de accesos, la política de mesa limpia, la protección de documentación sensible, la seguridad en reuniones, la segregación de funciones y, en general, todas aquellas buenas prácticas que preservan la confidencialidad e integridad del trabajo en curso.

Este concepto resulta especialmente relevante en proyectos con información sensible, requisitos contractuales estrictos o participación de terceros, ya que una parte importante del riesgo no reside solo en el código final, sino también en cómo se gestiona el proceso de desarrollo y quién puede intervenir sobre él.

5.4. Entorno ciberseguro

El entorno ciberseguro se refiere a la infraestructura digital sobre la que se apoya el desarrollo y la operación del software. Incluye redes, servidores, estaciones de trabajo, repositorios, servicios en la nube, sistemas de integración y despliegue, herramientas colaborativas y mecanismos de monitorización.

Su propósito es proporcionar una base tecnológica robusta y protegida frente a amenazas cibernéticas mediante medidas como la segmentación de redes, el uso de firewalls, la monitorización continua, la protección de datos en la nube, la gestión de vulnerabilidades, el control de identidades y la aplicación de parches.

En otras palabras, aunque el software se haya desarrollado con criterios adecuados, no puede considerarse suficientemente protegido si se ejecuta o mantiene sobre una infraestructura expuesta o mal securizada.

5.5. Relación entre los cuatro conceptos

Los cuatro conceptos anteriores no deben interpretarse como alternativas, sino como capas complementarias de un mismo enfoque.

Un software puede estar correctamente codificado y, sin embargo, ser vulnerable si carece de autenticación fuerte o cifrado; igualmente, puede incorporar controles de ciberseguridad adecuados y, aun así, desarrollarse en un entorno físico u organizativo débil que facilite accesos indebidos, fugas de información o alteraciones no controladas.

Del mismo modo, un equipo de desarrollo puede aplicar buenas prácticas internas y, pese a ello, trabajar sobre infraestructuras mal segmentadas o insuficientemente monitorizadas.

Por ello, para que exista un enfoque realmente sólido, la organización debe combinar seguridad en el código, resiliencia frente a amenazas, control del entorno de trabajo y protección de la infraestructura tecnológica. Esta visión integrada es coherente con el planteamiento general de la guía, que insiste en evitar sistemas paralelos y en incorporar la ciberdefensa de manera transversal al sistema de gestión.

5.6. Integración en el sistema de calidad

Desde el punto de vista de la calidad, el desarrollo seguro debe traducirse en requisitos definidos, responsabilidades claras, controles verificables y evidencias documentadas.

Esto implica incorporar criterios de seguridad en las especificaciones, mantener trazabilidad entre requisitos, diseño, pruebas e incidencias, registrar revisiones y validaciones, controlar cambios de configuración y asegurar que el personal implicado dispone de la competencia adecuada. Integrar estos elementos en el sistema de calidad permite que la seguridad deje de depender exclusivamente de iniciativas técnicas aisladas y pase a formar parte del funcionamiento normal de la organización, de sus auditorías y de su mejora continua. En entornos de defensa, además, esta integración adquiere especial relevancia por la convergencia entre requisitos contractuales, estándares PECAL y exigencias específicas aplicables al desarrollo de software.

5.6.1. Pasos para verificar la integración

El siguiente checklist permite verificar, de forma rápida, si el desarrollo seguro se encuentra integrado en el Sistema de Calidad de la organización como parte de sus requisitos,

Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio
C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24
info@tedae.org
www.tedae.org

controles, responsabilidades, evidencias y actividades de mejora continua. Su finalidad es servir como herramienta de autodiagnóstico y apoyo a la implantación.

5.6.2. Gestión del fin de vida útil

El Sistema de Calidad debe contemplar procedimientos específicos para la fase de retirada de los productos o software. Esto incluye:

- **Planificación de la obsolescencia:** Definir periodos de soporte de seguridad (mínimo 5 años según CRA) y comunicar proactivamente el fin de soporte a los clientes.

- **Borrado seguro de datos:** Establecer protocolos para la destrucción o borrado certificado de datos sensibles en soportes físicos o lógicos antes de su desecho o reutilización.

- **Gestión de la configuración post entrega:** Asegurar que las últimas versiones y parches de seguridad estén disponibles y documentados hasta el cierre definitivo del servicio

> **“EL ENTORNO CIBERSEGURO GARANTIZA QUE LA INFRAESTRUCTURA DONDE SE DESARROLLA, DESPLIEGA Y OPERA EL SOFTWARE ESTÉ PROTEGIDA FRENTE A AMENAZAS Y VULNERABILIDADES”**

Bloque	Qué verificar	Evidencia mínima esperable	Estado
1. Política y alcance	El Sistema de Calidad incluye de forma explícita el desarrollo seguro dentro de su alcance, política u objetivos. La seguridad del desarrollo se reconoce como un requisito de calidad del producto.	Política de calidad o sistema actualizada. Alcance del sistema revisado. Objetivos de calidad con referencia a seguridad.	☐ Sí ☐ Parcial ☐ No
2. Requisitos y planificación	Los proyectos incorporan requisitos de seguridad desde el inicio. La planificación contempla actividades de revisión, validación y pruebas de seguridad. Se identifican requisitos normativos, contractuales o del cliente.	Especificaciones con requisitos de seguridad. Plan de proyecto o plan de calidad. Matriz de requisitos.	☐ Sí ☐ Parcial ☐ No
3. Roles y responsabilidades	Existen responsabilidades claras para calidad, desarrollo, seguridad y gestión del proyecto. Se definen puntos de aprobación y decisión relacionados con seguridad.	Organigrama funcional. Matriz RACI. Descripciones de puesto o funciones. Actas de asignación.	☐ Sí ☐ Parcial ☐ No
4. Diseño y desarrollo seguro	El desarrollo seguro forma parte del proceso habitual de ingeniería. Se aplican prácticas de codificación segura, revisión de código y revisión técnica de diseño.	Procedimiento de desarrollo seguro. Guía de codificación segura. Registros de revisión de diseño y código.	☐ Sí ☐ Parcial ☐ No
5. Entorno de desarrollo y configuración	El entorno de desarrollo está protegido. Existen controles de acceso, protección de repositorios, credenciales, documentación y puestos de trabajo. Los cambios y versiones están controlados.	Procedimiento de control de accesos. Inventario de entornos y herramientas. Registros de cambios y configuración.	☐ Sí ☐ Parcial ☐ No
6. Verificación, validación y liberación	Además de pruebas funcionales, se realizan verificaciones de seguridad. Se revisan vulnerabilidades, configuraciones y componentes antes de liberar. Hay criterios de aceptación relacionados con seguridad.	Plan y resultados de pruebas. Registro de vulnerabilidades o incidencias. Checklist de liberación segura.	☐ Sí ☐ Parcial ☐ No
7. Competencia, formación y concienciación	El personal implicado recibe formación en desarrollo seguro según su rol. La organización conserva evidencias de competencia y formación.	Plan de formación. Registros de asistencia. Evaluaciones o evidencias de competencia. Requisitos de seguridad para terceros.	☐ Sí ☐ Parcial ☐ No
8. Auditoría, seguimiento y mejora continua	El desarrollo seguro se revisa en auditorías internas y en revisiones del sistema. Existen indicadores, acciones correctivas y seguimiento de mejoras.	Informes de auditoría. KPIs o indicadores. Acciones correctivas. Actas de revisión por la dirección.	☐ Sí ☐ Parcial ☐ No

Tabla 2. Checklist integración desarrollo seguro

Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio
C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24
info@tedae.org
www.tedae.org

5.7. Consideración final

“ES POSIBLE DESARROLLAR SOLUCIONES QUE MANTENGAN LA CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD Y TRAZABILIDAD EXIGIBLES”

En consecuencia, hablar de desarrollo seguro no debería limitarse a una única práctica técnica, sino a un marco de trabajo que combina ingeniería segura, protección frente a amenazas, control del entorno de desarrollo y robustez de la infraestructura tecnológica.

Solo mediante esta visión conjunta es posible desarrollar soluciones que no solo funcionen correctamente, sino que también mantengan la confidencialidad, integridad, disponibilidad y trazabilidad exigibles en contextos con requisitos elevados de calidad, seguridad y defensa.

06 Normativa aplicable. Guía para determinar si aplica o no la normativa

6.1. Introducción a la normativa aplicable.

NIS2 (Network and Information Systems Directive 2)

- **Descripción:** La Directiva NIS2, formalmente conocida como Directiva (UE) 2022/2555, es una normativa europea destinada a fortalecer la ciberseguridad en toda la Unión Europea. Su principal objetivo es garantizar que las empresas que gestionan infraestructuras críticas adopten medidas de seguridad adecuadas para protegerse contra amenazas cibernéticas.

- **Ámbito de Aplicación:** Aplica a entidades públicas y privadas de 18 sectores esenciales e importantes, divididos en “Sectores de Alta Criticidad” (anexo1) y “Otros Sectores Críticos” (anexo2). Factores como el tamaño de la empresa y el sector determinan si una organización está sujeta a la NIS2. Si tu empresa pertenece a alguno de estos sectores y tiene más de 50 empleados o una facturación superior a 10 millones de euros, es probable que esté obligada a cumplir con NIS2.

Por tamaño:

- Pequeña empresa: Menos de 50 empleados y menos de 10 millones de euros de facturación anual.
- Mediana empresa: Entre 50 y 250 empleados y entre 10 y 50 millones de euros de facturación anual.
- Gran empresa: Más de 250 empleados y más de 50 millones de euros de facturación anual.
- Sectores esenciales:
- Energía (electricidad, gas, petróleo).
- Transporte (ferroviario, aéreo, marítimo, carretera).
- Banca y mercados financieros.
- Sanidad y hospitales.

Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio
C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24
info@tedae.org
www.tedae.org

- Infraestructuras digitales y telecomunicaciones.
- Sectores importantes
- Servicios cloud y tecnología.
- Plataformas en línea y redes sociales.
- Administraciones públicas.
- Fabricación de productos críticos.
- Espacio (operadores de satélites y actividades espaciales).

- **Requisitos:** Incluye obligaciones de seguridad más estrictas y requisitos de reporte. Las empresas deben adoptar medidas de ciberseguridad adecuadas y reportar incidentes de seguridad significativos.
- **Certificación:** No es una norma certificable. Las organizaciones deben determinar si cumplen los criterios de tamaño y actividad para verificar su obligación de cumplimiento.
- **Requisitos clave para el cumplimiento normativo de NIS2**: Para adaptarse a la directiva, las empresas deben implementar:

1. *Evaluación y gestión de riesgos*

- Identificar vulnerabilidades y aplicar controles preventivos.
- Implementar cifrado, autenticación multifactor y segmentación de red.

2. *Respuesta a incidentes y notificación obligatoria*

- Establecer un plan de respuesta ante ciberataques.
- Informar incidentes graves en 24 horas y proporcionar informes detallados en 72 horas.

3. *Planes de continuidad del negocio*

- Asegurar copias de seguridad regulares y mecanismos de recuperación.
- Diseñar estrategias para minimizar interrupciones operativas.

4. *Gestión de la seguridad en la cadena de suministro*

- Exigir requisitos de seguridad a proveedores críticos.
- Incluir cláusulas de seguridad en los contratos.

5. *Gobernanza y responsabilidad de la alta dirección*

- Formación obligatoria en ciberseguridad para directivos.
- Supervisión proactiva de las medidas de cumplimiento.

ISO/IEC 27001

- **Descripción:** La norma ISO/IEC 27001 es un estándar internacional que especifica los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI).
- **Ámbito de Aplicación:** Aplica a cualquier organización, independientemente de su tamaño, tipo o sector. Es especialmente relevante para aquellas que manejan información sensible o crítica.
- **Requisitos:** Incluye la evaluación de riesgos, la implementación de controles de seguridad y la mejora continua del SGSI.
- **Certificación:** Es certificable, lo que significa que las organizaciones pueden obtener una certificación oficial que demuestre su conformidad con la norma.

ISO/IEC 62443

- **Descripción:** La norma ISA/IEC 62443 proporciona un marco integral de ciberseguridad específicamente diseñado para sistemas de control industrial (ICS).
- **Ámbito de Aplicación:** Aplica a industrias que utilizan sistemas de control industrial, como la energía, el agua, el transporte y la manufactura.
- **Requisitos:** Incluye la evaluación de riesgos, la implementación de controles de seguridad específicos para ICS y la gestión de la seguridad a lo largo del ciclo de vida de los sistemas.
- **Certificación:** Es certificable, permitiendo a las organizaciones demostrar su conformidad con los requisitos de ciberseguridad para sistemas de control industrial.

ENS (Esquema Nacional de Seguridad)

- **Descripción:** El ENS es una normativa española que establece los principios básicos y los requisitos de seguridad para la administración pública y sectores afines.
- **Ámbito de Aplicación:** Aplica a todas las entidades del sector público en España y a aquellas entidades privadas que colaboran con el sector público.
- **Requisitos:** Incluye la clasificación de la información, la implementación de medidas de seguridad y la verificación del cumplimiento de estas medidas.
- **Certificación:** Es certificable, lo que permite a las organizaciones obtener una certificación oficial que demuestre su conformidad con el ENS según su categoría de seguridad (básico, medio o alto).

> **“EL CRA SUPONE UN CAMBIO DE PARADIGMA: LA SEGURIDAD YA NO ES UNA OPCIÓN DEL CLIENTE, SINO UNA RESPONSABILIDAD LEGAL DEL FABRICANTE”**

CRA (Cyber Resilience Act - Reglamento UE 2024/2847)

- **Descripción:** Es el primer marco regulador a nivel europeo que establece requisitos horizontales de ciberseguridad para fabricantes, importadores y distribuidores de “productos con elementos digitales” (tanto hardware como software). Su objetivo es garantizar que los productos que se comercializan en la Unión Europea sean seguros a lo largo de todo su ciclo de vida.
- **Ámbito de Aplicación:** Aplica a cualquier producto conectable de forma directa o indirecta a otro dispositivo o red. En el sector defensa, aunque existen exclusiones para productos destinados exclusivamente a fines militares, afecta de lleno a todos los componentes de “doble uso” o productos comerciales que se integren en sistemas mayores.

Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio
C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24
info@tedae.org
www.tedae.org

- **Requisitos clave:**

- **Seguridad por diseño y por defecto:** Los productos deben entregarse sin vulnerabilidades conocidas y con configuraciones seguras de fábrica.

- **Gestión de vulnerabilidades:** Obliga a los fabricantes a documentar vulnerabilidades y a proporcionar actualizaciones de seguridad gratuitas durante un periodo de soporte determinado (generalmente 5 años).

- **Marcado CE de Ciberseguridad:** El cumplimiento de este reglamento será un requisito previo para obtener el marcado CE en productos digitales a partir de su plena aplicación (prevista para diciembre de 2027).

- **Relación con el Sistema de Calidad:** Obliga a integrar procesos de monitorización de vulnerabilidades y planes de respuesta post-venta dentro del sistema de gestión de la organización.

El CRA supone un cambio de paradigma: la seguridad ya no es una opción del cliente, sino una responsabilidad legal del fabricante. El Sistema de Calidad debe asegurar que existe un canal de reporte de vulnerabilidades activo y que la empresa tiene capacidad técnica para emitir parches de seguridad durante un periodo de hasta 5 años tras la venta, integrando este soporte en los procesos de post-venta de la norma ISO 9001.

Nota: Debido a la fase de transposición nacional de directivas como NIS2 o la entrada en vigor progresiva del CRA, se recomienda la consulta periódica de las Instrucciones Técnicas de Seguridad (ITS) publicadas por el CCN-CERT para asegurar que el Sistema de Calidad se mantiene actualizado con los últimos requisitos técnicos exigibles.

6.2. Guía para Determinar la Aplicabilidad de la Normativa

6.2.1. Evaluación del sector y tamaño de la Organización

- Determina si tu organización pertenece a alguno de los sectores críticos mencionados en la NIS2.

- Evalúa el tamaño de tu organización en términos de número de empleados y volumen de negocio para ver si cumple con los umbrales establecidos por la NIS2.

6.2.2. Revisión de Actividades y Procesos

- Identifica si tu organización maneja información sensible o crítica que requiera la implementación de un SGSI conforme a la ISO/IEC 27001.

- Verifica si tu organización utiliza sistemas de control industrial que deban cumplir con la norma ISA/IEC 62443.

6.2.3. Colaboración con el Sector Público

- Si tu organización colabora con el sector público en España, revisa los requisitos del ENS y asegúrate de cumplir con ellos.

6.2.4. Implementación y Verificación.

- Implementa las medidas de seguridad necesarias según las normativas aplicables.

- Realiza auditorías internas y externas para verificar el cumplimiento de las normativas.

Norma / marco	Qué es	Cuándo aplica	¿Obligatoria o voluntaria?	Relación con el Sistema de Calidad
ISO 9001:2015	Norma de sistemas de gestión de la calidad. Es certificable y se centra en procesos, cumplimiento de requisitos del cliente y mejora continua. (ISO)	Aplica a cualquier organización que quiera implantar o certificar un SGC. (ISO)	Voluntaria, salvo que un cliente o contrato la exija. Es certificable. (ISO)	Es el marco base para integrar la ciberseguridad en calidad: política, procesos, registros, auditorías, no conformidades y mejora continua. No define controles técnicos de ciberseguridad por sí sola. (ISO)
ISO/IEC 27001:2022	Norma de sistema de gestión de seguridad de la información (SGSI), basada en gestión de riesgos y mejora continua. Es certificable. (ISO)	Aplica a organizaciones que necesiten gobernar la seguridad de la información de forma sistemática. (ISO)	Voluntaria, salvo exigencia contractual o sectorial. Es certificable. (ISO)	Es la norma más natural para complementar ISO 9001 cuando quieres integrar ciberseguridad en el sistema de gestión. ISO 9001 organiza el sistema; ISO 27001 aporta la capa específica de seguridad. (ISO)
NIS2 / Directiva (UE) 2022/2555	Directiva europea que establece medidas para un alto nivel común de ciberseguridad en la UE, con gestión de riesgos, notificación de incidentes, supervisión y ejecución. (EUR-Lex)	Aplica a determinadas entidades esenciales e importantes de sectores críticos definidos por la norma y su transposición nacional. (EUR-Lex)	Obligatoria para las organizaciones incluidas en su ámbito de aplicación, una vez transpuesta y aplicada en cada Estado miembro. (EUR-Lex)	No sustituye al SGC, pero introduce exigencias regulatorias que deben integrarse en procesos de calidad: gestión de riesgos, cadena de suministro, gestión de incidentes, evidencias y gobierno. (EUR-Lex)
ENS / Real Decreto 311/2022	Marco español que regula el Esquema Nacional de Seguridad para garantizar la seguridad en el ámbito de la administración electrónica. (BOE)	Aplica al sector público español y a entidades privadas cuando prestan servicios o se relacionan con él en contextos donde se exige ENS. (BOE)	Obligatorio en su ámbito de aplicación. Puede acreditarse/ certificarse según el esquema correspondiente. (BOE)	Si trabajas con Administraciones públicas, el ENS debe integrarse en tu sistema documental y operativo: clasificación, medidas de seguridad, controles, auditorías y evidencias. (BOE)
IEC / ISA 62443	Serie de normas para la ciberseguridad de sistemas de automatización y control industrial (IACS/ OT). Define requisitos, procesos y ciclo de vida para entornos industriales. (isa.org)	Aplica cuando hay OT/industrial, por ejemplo, energía, agua, manufactura, transporte o automatización. (isa.org)	Normalmente voluntaria, salvo exigencia contractual, sectorial o de cliente. Algunas partes permiten certificación o evaluación asociada. (isa.org)	Es la referencia más útil cuando el Sistema de Calidad cubre productos, procesos o servicios industriales. Complementa a ISO 9001 e ISO 27001 con requisitos específicos de OT y ciclo de vida. (isa.org)
Cyber Resilience Act / Reglamento (UE) 2024/2847	Reglamento europeo sobre requisitos horizontales de ciberseguridad para productos con elementos digitales. Exige diseño y desarrollo seguros, gestión de vulnerabilidades y soporte durante el ciclo de vida. (EUR-Lex)	Aplica a fabricantes, importadores y distribuidores de productos con elementos digitales comercializados en la UE. (EUR-Lex)	Obligatorio dentro de su ámbito. La Comisión Europea indica que será plenamente aplicable desde el 11 de diciembre de 2027, con algunas obligaciones antes.	Es muy relevante si tu Sistema de Calidad cubre diseño, desarrollo, producción o mantenimiento de software o hardware conectable. Obliga a integrar ciberseguridad en requisitos, validación, gestión de vulnerabilidades y posventa. (EUR-Lex)

Tabla 3. Aplicabilidad de la normativa

Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio
C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24
info@tedae.org
www.tedae.org

6.2. Sinergias y Convalidación de marcos normativos

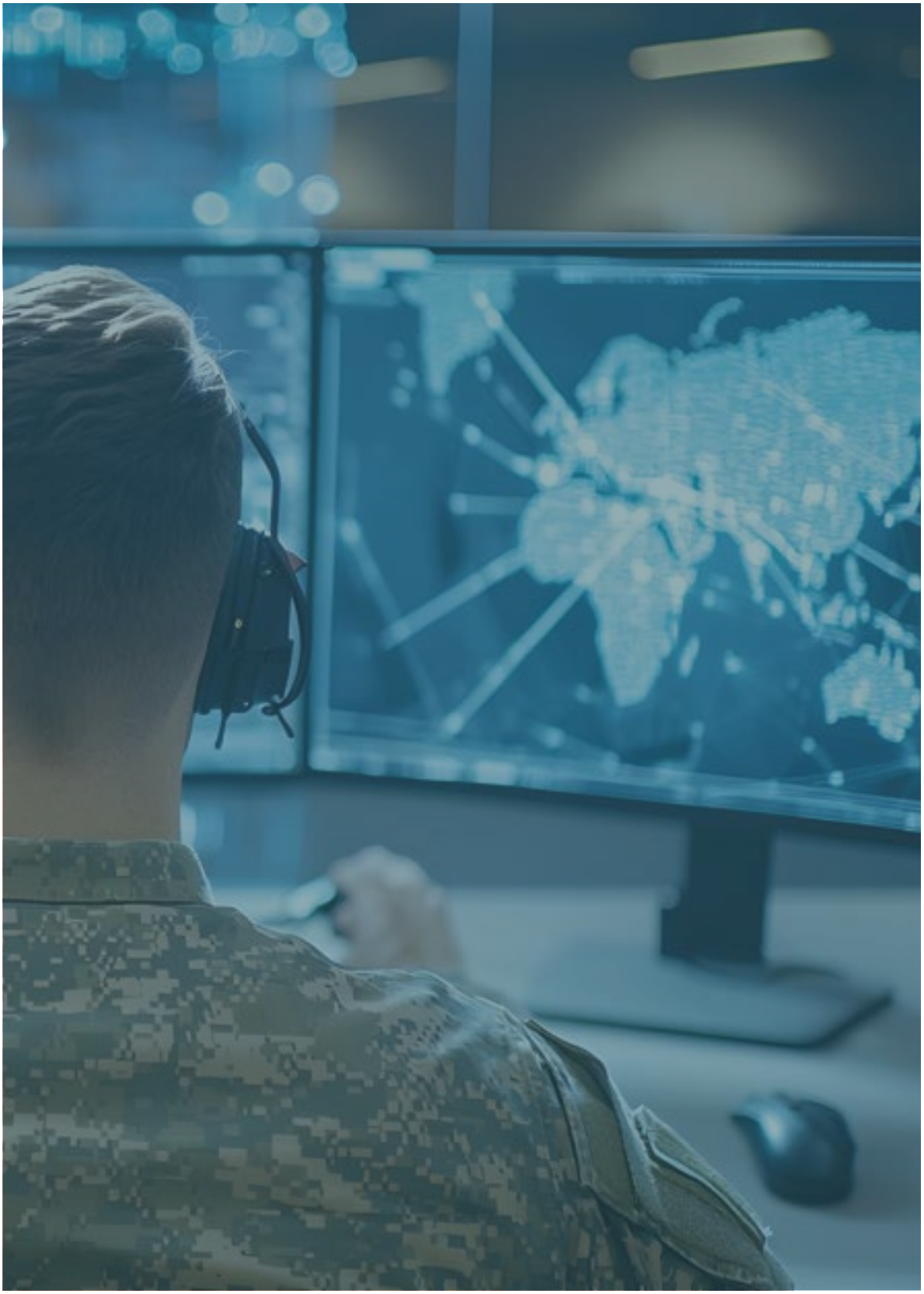
Aunque el panorama regulatorio pueda parecer fragmentado, existe una elevada convergencia (superior al 75%) entre los controles exigidos por la ISO 27001, el ENS y la Directiva NIS2. Una organización que haya implementado un Sistema de Gestión de Seguridad de la Información (SGSI) bajo ISO 27001 ya dispone de la base estructural necesaria para alcanzar el cumplimiento del ENS.

A su vez, el cumplimiento del ENS en su categoría media o alta se considera, de facto, la vía preferente para demostrar la conformidad con las obligaciones de la Directiva NIS2 en España. El enfoque de esta guía es el de "implementar una vez, cumplir con muchas", evitando la duplicidad de registros y simplificando las auditorías de calidad mediante un repositorio común de evidencias técnicas.

6.3. Sinergias y Convalidación de marcos normativos

Aunque el panorama regulatorio pueda parecer fragmentado, existe una elevada convergencia (superior al 75%) entre los controles exigidos por la ISO 27001, el ENS y la Directiva NIS2. Una organización que haya implementado un Sistema de Gestión de Seguridad de la Información (SGSI) bajo ISO 27001 ya dispone de la base estructural necesaria para alcanzar el cumplimiento del ENS.

A su vez, el cumplimiento del ENS en su categoría media o alta se considera, de facto, la vía preferente para demostrar la conformidad con las obligaciones de la Directiva NIS2 en España. El enfoque de esta guía es el de "implementar una vez, cumplir con muchas", evitando la duplicidad de registros y simplificando las auditorías de calidad mediante un repositorio común de evidencias técnicas.



Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio

C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24

info@tedae.org
www.tedae.org

6.4. Preguntas Frecuentes

- **¿Con el ENS cumplo NIS2?**

  El Esquema Nacional de Seguridad (ENS) y la Directiva NIS2 comparten un enfoque similar en la protección de la información y la ciberseguridad. Cumplir con el ENS puede ser un buen punto de partida para alinearse con la NIS2, ya que ambos marcos incluyen varias medidas de seguridad comunes. No obstante, es importante destacar que la conformidad con el ENS no asegura automáticamente el cumplimiento de la NIS2, ya que esta última puede tener requisitos adicionales específicos para ciertos sectores.

- **¿Es obligatorio certificar el Sistema de Calidad en Ciberdefensa?**

  No existe una "certificación de ciberdefensa" como tal. Lo que existe es la obligación de integrar controles de seguridad dentro de las certificaciones ya existentes (como ISO 9001 o EN 9100) y cumplir con las normativas obligatorias por ley (NIS2, ENS) o por contrato (PECAL 2210). La "certificación" se obtiene a través de la superación de las auditorías de calidad del cliente o de los organismos de certificación acreditados.

- **Si mi empresa es una PYME y solo es subcontratista, ¿me aplica el CRA?**

  Sí, si fabricas o desarrollas cualquier componente con elementos digitales que se comercialice o integre en la UE. Aunque no seas el contratista principal, el CRA te obliga a entregar productos sin vulnerabilidades conocidas y a gestionar parches de seguridad, ya que tu cliente (el contratista principal) te lo exigirá para poder obtener su propio marcado CE de ciberseguridad.

- **¿Tengo que auditar la ciberseguridad de todos mis proveedores?**

  No de todos, pero sí de los críticos. El Sistema de Calidad debe definir criterios de selección basados en el riesgo. Si un proveedor tiene acceso a tus planos, datos de diseño o desarrolla parte del software entregable, estás obligado por PECAL y NIS2 a verificar su madurez mediante cuestionarios, auditorías de segunda parte o exigencia de certificaciones.

- **¿Puede un auditor de Calidad (no técnico) auditar el Desarrollo Seguro?**

  Sí, siempre que su enfoque sea el cumplimiento del proceso. El auditor de calidad no necesita revisar el código línea por línea, sino verificar evidencias de que el proceso se ha seguido: ¿existe un informe del análisis SAST?, ¿se han cerrado las vulnerabilidades críticas antes de la entrega?, ¿están definidas las responsabilidades en la matriz RACI?

- **¿Qué debo cumplir? ¿NIS2, ENS o ISA 62443?**

  Es fundamental cumplir con las directrices PCE-NIS2 y CCN-CERT para garantizar el pleno cumplimiento de la Directiva NIS2 en España. Sin embargo, en entornos de tecnología operativa (OT), también es crucial priorizar la implementación de la norma IEC 62443, que complementa estas iniciativas.

  La norma IEC 62443 permite a las organizaciones establecer medidas de seguridad específicas para los sistemas de automatización y control industrial, reforzando así la seguridad y garantizando el cumplimiento de los requisitos de la Directiva NIS2.

07 Ciberdefensa y aseguramiento de la calidad en contratos de defensa

7.1. Objeto y contexto

En los contratos del ámbito de defensa, la calidad no se limita a la conformidad técnica del producto o servicio suministrado. También comprende el conjunto de actividades necesarias para proporcionar confianza al comprador sobre la capacidad del suministrador para cumplir, de forma controlada y verificable, los requisitos contractuales aplicables.

En este contexto, la ciberseguridad debe integrarse en el Sistema de Calidad cuando afecte a la protección de la información, a la gestión de riesgos, a la configuración del producto, a la cadena de suministro, a la trazabilidad de evidencias o al desarrollo de software. Su tratamiento no debe considerarse una actividad separada, sino una parte del aseguramiento global del contrato.

Por ello, cuando un contrato de defensa incorpore requisitos PECAL/AQAP, la organización deberá analizar su impacto sobre el Sistema de Calidad y asegurar que dichos requisitos quedan reflejados en sus procesos, planes, responsabilidades, evidencias y mecanismos de control.

7.2. Marco PECAL/ AQAP aplicable

Las PECAL son las Publicaciones Españolas de Calidad equivalentes a las AQAP de la OTAN y constituyen el marco de referencia para el aseguramiento oficial de la calidad en contratos de defensa.

Estos estándares aseguran que los sistemas y software desarrollados para la defensa cumplan con altos niveles de calidad y seguridad. En el contexto de la ciberdefensa, las PECAL incluyen requisitos específicos para la protección contra amenazas cibernéticas.

Dentro de este marco, resultan especialmente relevantes las siguientes publicaciones:

- **PECAL 2110,** aplicable a contratos que incluyen diseño, desarrollo y producción, basada en ISO 9001.
- **PECAL 2310**, aplicable a suministradores de aviación, espacio y defensa, basada en AS/EN 9100.
- **PECAL 210**5, relativa al plan de calidad contractual, aplicable cuando el contrato exige la presentación de dicho plan.

Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio
C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24
info@tedae.org
www.tedae.org

- **PECAL 2210**, aplicable como suplemento específico cuando el contrato incluye software orientado al proyecto o software entregable.

En consecuencia, el marco PECAL tiene un alcance muy amplio y afecta, con distinta intensidad, a cualquier organización que participe en contratos de defensa y deba demostrar capacidad de gestión, control y aseguramiento de la calidad frente al comprador.

7.3. Implicaciones para el Sistema de Calidad del suministrador

Cuando el contrato incorpore requisitos PECAL, la organización deberá asegurar que su Sistema de Calidad puede dar respuesta, como mínimo, a los siguientes aspectos:

- definición del sistema de gestión aplicable al contrato;
- asignación clara de funciones, responsabilidades y autoridades;
- planificación de la calidad del contrato, cuando proceda;
- control documental y trazabilidad de evidencias;
- gestión de riesgos y de cambios;
- gestión de la configuración del producto;
- control de suministradores y cadena de suministro;
- realización de revisiones, verificaciones, inspecciones o actividades de seguimiento que permitan demostrar conformidad frente a los requisitos contractuales.

Desde la perspectiva de esta guía, la ciberseguridad debe integrarse en estos elementos como parte de la gestión de riesgos, de la protección de la información, del control de la configuración, del tratamiento de incidentes y de la generación de evidencias objetivas de cumplimiento.

De este modo, la ciberseguridad deja de tratarse como una cuestión exclusivamente técnica y pasa a formar parte del funcionamiento normal del sistema de gestión y del aseguramiento contractual.

7.3.1. Despliegue de requisitos a subcontratistas

La organización debe garantizar que los requisitos de ciberdefensa y calidad no se diluyan en la cadena de suministro. Cuando un contrato de defensa invoca normas PECAL/AQAP, el suministrador principal es responsable de trasladar (“flow-down”) estas exigencias a sus proveedores críticos.

- **Evaluación de proveedores:** El Sistema de Calidad debe incluir criterios de selección que evalúen la madurez en ciberseguridad de los subcontratistas, especialmente si tienen acceso a información sensible o desarrollan software orientado al proyecto.

- **Cláusulas contractuales:** Es obligatorio incluir cláusulas de seguridad y calidad en los contratos de compra que obliguen al subcontratista a cumplir con los mismos estándares (ej. PECAL 2210 para software) que el suministrador principal.

- **Auditoría y control:** La organización debe realizar un seguimiento activo de sus proveedores, que puede incluir auditorías de segunda parte o la exigencia de evidencias objetivas de cumplimiento (certificaciones ENS, ISO 27001 o informes de pruebas de seguridad).

- **Trazabilidad de componentes:** Se debe asegurar que cualquier componente de terceros (hardware o software) integrado en el producto final cumple con los requisitos de integridad y procedencia exigidos en el contrato de defensa.

7.4. Caso particular del software entregable

Cuando el contrato incluya software orientado al proyecto o software entregable, deberá considerarse la aplicabilidad de la PECAL 2210 como suplemento a la PECAL 2110 o a la PECAL 2310.

En estos casos, la organización deberá prestar especial atención a:

- la gestión de requisitos del software;
- la trazabilidad entre requisitos, diseño, desarrollo, pruebas e incidencias;
- la gestión de la configuración del software;
- las revisiones y verificaciones a lo largo del ciclo de vida;
- el control de cambios;
- y la evidencia documental asociada al desarrollo y aceptación del software.

Por tanto, el software debe tratarse como un caso específico dentro del contrato, pero no como el único escenario contemplado por el marco PECAL.

7.5. Checklist de aplicabilidad e integración

El siguiente checklist puede utilizarse como herramienta de apoyo para determinar si un contrato o suministro requiere una integración específica de requisitos PECAL en el Sistema de Calidad de la organización.

- Si predominan las respuestas “No”, el contrato requerirá un análisis específico antes de considerar cubierto su cumplimiento por el sistema actual.
- Si predominan las respuestas “Parcial”, convendrá establecer un plan de adaptación documental, organizativa o de proceso.
- Si predominan las respuestas “Sí”, la organización dispondrá de una base razonable para integrar los requisitos del contrato en su Sistema de Calidad, sin perjuicio del análisis detallado de las cláusulas aplicables.

Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio
C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24
info@tedae.org
www.tedae.org

Pregunta de verificación	Sí	No	Parcial
¿El contrato pertenece al ámbito de defensa o a una cadena de suministro asociada a defensa?	☐	☐	☐
¿El contrato invoca expresamente una PECAL/AQAP o requisitos OTAN de calidad?	☐	☐	☐
¿La organización dispone de un Sistema de Calidad alineado con ISO 9001 o AS/EN 9100, según corresponda?	☐	☐	☐
¿Se requiere plan de calidad contractual o documento equivalente?	☐	☐	☐
¿Se han identificado los requisitos contractuales que afectan a riesgos, configuración, documentación, revisiones y evidencias?	☐	☐	☐
¿Se han analizado los impactos de ciberseguridad sobre producto, proceso, información y cadena de suministro?	☐	☐	☐
¿El contrato incluye software orientado al proyecto o software entregable?	☐	☐	☐
En caso afirmativo, ¿se ha evaluado la aplicabilidad de PECAL 2210 y de los controles específicos del ciclo de vida del software?	☐	☐	☐
¿Existen responsabilidades definidas para calidad, ingeniería, seguridad y gestión contractual?	☐	☐	☐
¿La organización puede generar evidencias objetivas de cumplimiento contractual y de control del producto o proceso?	☐	☐	☐
¿Se han trasladado formalmente los requisitos de calidad y ciberseguridad (PECAL/AQAP) a los subcontratistas y proveedores críticos del proyecto?	☐	☐	☐

Tabla 4. Checklist aplicabilidad integración PECAL

08 Formación y concienciación en ciberseguridad dentro del Sistema de Calidad

La integración de la ciberseguridad en los sistemas de gestión de la calidad no puede sostenerse únicamente sobre medidas técnicas o documentales. Requiere que las personas que intervienen en los procesos de la organización comprendan los riesgos, conozcan las obligaciones aplicables a su función y actúen de forma coherente con los principios, controles y procedimientos definidos en el sistema. En este sentido, la formación y la concienciación deben entenderse como un componente estructural del propio sistema de gestión, y no como una actividad aislada o puntual. Esta aproximación es coherente con el planteamiento general de la guía, que ya sitúa la formación entre los elementos que deben integrarse en la planificación, la trazabilidad, las auditorías y la mejora continua.

Además, marcos como ISO/IEC 27001, el Esquema Nacional de Seguridad (ENS) y los requisitos derivados de NIS2 exigen que las organizaciones dispongan de programas de formación y concienciación estructurados, continuos y medibles. En entornos de defensa, esta necesidad se refuerza cuando existen contratos, requisitos PECAL o exigencias específicas asociadas al desarrollo seguro, la protección de la información o la gestión de la cadena de suministro.

8.1. Principios del modelo de formación y concienciación

El modelo de formación y concienciación en ciberseguridad deberá regirse, como mínimo, por los siguientes principios:

- **Enfoque basado en riesgos:** los contenidos y colectivos prioritarios se definirán en función de la criticidad de los procesos, la sensibilidad de la información y la exposición al riesgo.
- **Adaptación al rol:** la formación deberá ajustarse a las responsabilidades de cada perfil, evitando enfoques homogéneos para toda la organización.
- **Continuidad en el tiempo:** la concienciación no deberá limitarse a acciones puntuales, sino mantenerse mediante refuerzos periódicos, campañas y actualizaciones.
- **Medición y evidencia:** la organización deberá conservar evidencias objetivas de las acciones realizadas y de su eficacia.

- Integración con el Sistema de Calidad: la formación deberá conectarse con competencias, auditorías, revisión por la dirección, tratamiento de riesgos y mejora continua.

8.2. Autoevaluación del nivel de preparación

Con carácter previo a la implantación o revisión del modelo de formación y concienciación, resulta conveniente que la organización realice una autoevaluación que le permita identificar su nivel de madurez. Este ejercicio no persigue una certificación formal, sino servir como herramienta de apoyo a la toma de decisiones, permitiendo detectar brechas, priorizar acciones y adaptar el modelo al grado real de madurez de la empresa.

La valoración de cada criterio podrá realizarse mediante una escala de cinco niveles:

- **0 – No iniciado:** el aspecto no ha sido abordado.
- **1 – Inicial:** existen iniciativas puntuales, no sistemáticas.
- **2 – En desarrollo:** el aspecto se encuentra parcialmente definido o en fase de implantación.
- **3 – Definido y operativo:** el aspecto está formalizado y se aplica de manera consistente.
- **4 – Consolidado y medido:** el aspecto está plenamente integrado y sujeto a seguimiento periódico.

Una vez completada la autoevaluación, el resultado agregado permitirá situar a la organización en una fase orientativa de madurez:

- Cuando la mayoría de los criterios se sitúen en los niveles 0 o 1, la organización estará en una fase inicial o exploratoria. En este caso, convendrá priorizar la definición de colectivos, contenidos básicos, responsabilidades mínimas y un plan inicial de formación.
- Cuando predominen valoraciones en el nivel 2, la organización podrá considerarse en fase intermedia. En este punto cobrará especial relevancia la estandarización de prácticas, la adaptación por rol, la creación de indicadores y la integración progresiva con el Sistema de Calidad.
- Cuando la mayoría de los criterios se sitúen en los niveles 3 o 4, la organización se encontrará en una fase avanzada, caracterizada por la integración sistemática del modelo en los procesos de calidad, la medición de su eficacia y la aplicación de mecanismos de revisión y mejora continua.

> **“LA INTEGRACIÓN DE LA CIBERSEGURIDAD REQUIERE QUE LAS PERSONAS QUE INTERVIENEN EN LOS PROCESOS DE LA ORGANIZACIÓN COMPRENDAN LOS RIESGOS, CONOZCAN LAS OBLIGACIONES Y ACTÚEN DE FORMA COHERENTE”**

Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio
C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24
info@tedae.org
www.tedae.org

Dimensión	Criterio de evaluación	0	1	2	3	4
Estrategia	La formación en ciberseguridad está alineada con los objetivos del Sistema de Calidad y con los riesgos de la organización.	☐	☐	☐	☐	☐
Liderazgo	La dirección participa, impulsa y revisa el modelo de formación y concienciación.	☐	☐	☐	☐	☐
Colectivos	Están identificados los colectivos destinatarios y sus necesidades específicas por rol.	☐	☐	☐	☐	☐
Contenidos	Existen contenidos mínimos definidos para cada perfil en función de sus responsabilidades.	☐	☐	☐	☐	☐
Implantación	Se ejecutan acciones periódicas de formación y concienciación, no solo sesiones puntuales.	☐	☐	☐	☐	☐
Evidencias	Se conservan registros, resultados y evidencias de las acciones realizadas.	☐	☐	☐	☐	☐
Indicadores	Existen indicadores para medir cobertura, eficacia y evolución del programa.	☐	☐	☐	☐	☐
Integración	El modelo está integrado con competencias, auditorías, riesgos y revisión por la dirección.	☐	☐	☐	☐	☐
Mejora continua	El programa se revisa y actualiza periódicamente en función de incidentes, auditorías y cambios normativos.	☐	☐	☐	☐	☐

Tabla 5. Checklist de autoevaluación del modelo de formación y concienciación

Una vez completada la autoevaluación, el resultado agregado permitirá situar a la organización en una fase orientativa de madurez:

- Cuando la mayoría de los criterios se sitúen en los niveles 0 o 1, la organización estará en una fase inicial o exploratoria. En este caso, convendrá priorizar la definición de colectivos, contenidos básicos, responsabilidades mínimas y un plan inicial de formación.
- Cuando predominen valoraciones en el nivel 2, la organización podrá considerarse en fase intermedia. En este punto cobrará especial relevancia la estandarización de prácticas, la adaptación por rol, la creación de indicadores y la integración progresiva con el Sistema de Calidad.
- Cuando la mayoría de los criterios se sitúen en los niveles 3 o 4, la organización se encontrará en una fase avanzada, caracterizada por la integración sistemática del modelo en los procesos de calidad, la medición de su eficacia y la aplicación de mecanismos de revisión y mejora continua.

8.3. Colectivos objetivo y contenidos mínimos por perfil

La formación y la concienciación deberán adaptarse, como mínimo, a los siguientes colectivos:

8.3.1. Alta dirección y responsables de contrato

Este colectivo toma decisiones sobre recursos, prioridades, riesgos, compromisos contractuales y cumplimiento. Su implicación resulta determinante para que la ciberseguridad no quede relegada exclusivamente al ámbito técnico.

Objetivo formativo.

Comprender el impacto organizativo, contractual y reputacional de los riesgos de ciberseguridad, así como su relación con la gobernanza, la supervisión y la revisión del sistema.

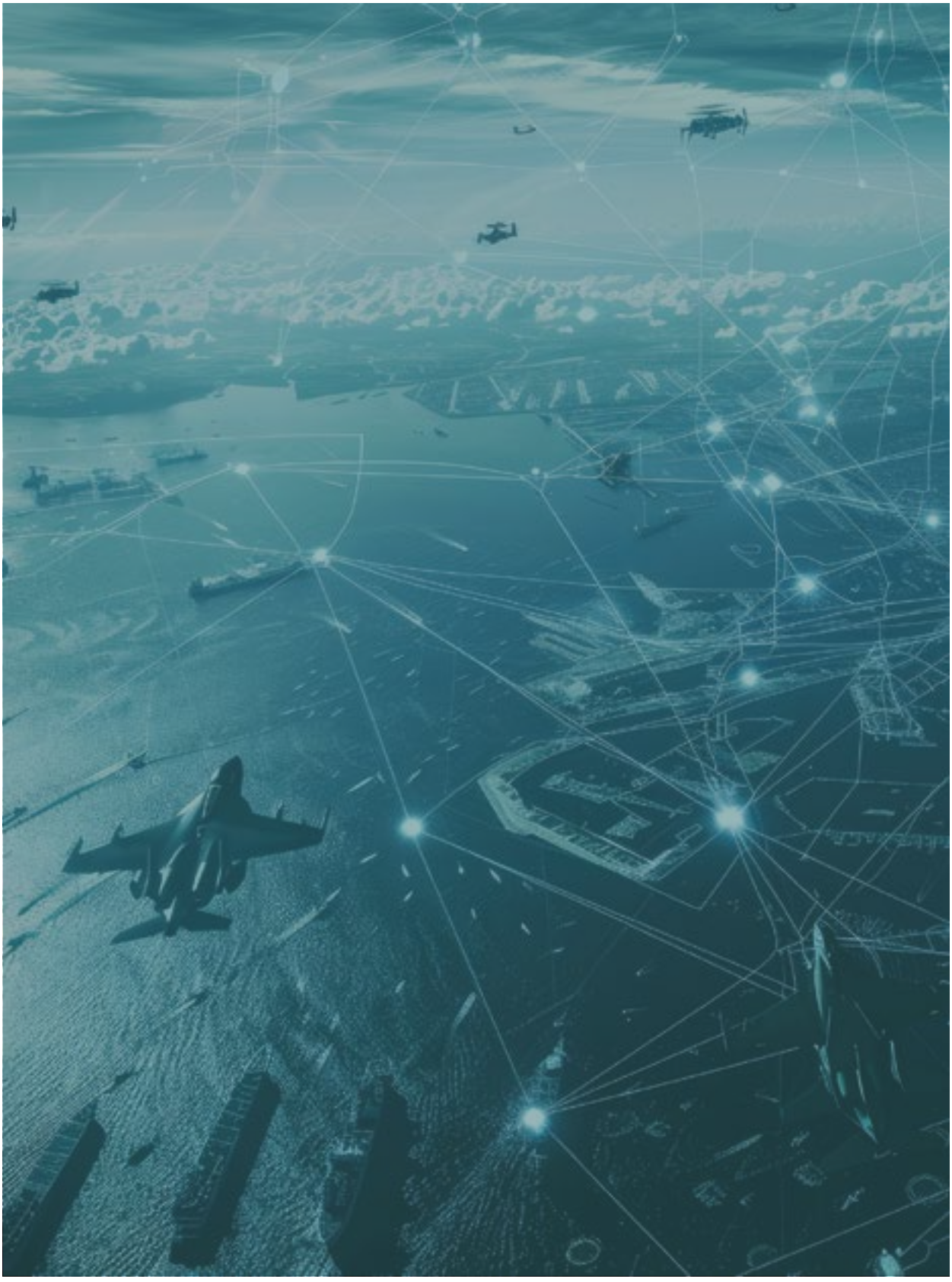
Contenidos mínimos.

- Principales riesgos de ciberseguridad y su impacto en la continuidad del negocio y en la calidad del producto o servicio.
- Obligaciones regulatorias y contractuales aplicables.
- Responsabilidades de liderazgo, asignación de recursos y seguimiento.
- Riesgos asociados a la cadena de suministro y a terceros.
- Lectura e interpretación de indicadores, hallazgos e incidencias relevantes.

Frecuencia orientativa.

Sesión inicial y actualización al menos anual, así como sesiones específicas ante cambios regulatorios, nuevos contratos críticos o incidentes relevantes.

Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio
C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24
info@tedae.org
www.tedae.org



Evidencias esperables.

- Matriz de Competencias y Polivalencia: Documento del Sistema de Calidad que vincule cada puesto de trabajo con el nivel de capacitación en ciberseguridad requerido y alcanzado.
- Evaluación de la eficacia: No basta con la asistencia; se debe incluir el resultado de cuestionarios técnicos o ejercicios prácticos que validen la adquisición de la competencia.
- Registros de asistencia, materiales utilizados, actas de revisión, evidencias de decisiones adoptadas y seguimiento de indicadores.

8.3.2. Usuarios internos operativos

Constituyen la primera línea de defensa frente a amenazas frecuentes como phishing, malware, fuga de información, errores de uso o incumplimiento de procedimientos.

Objetivo formativo.

Adoptar hábitos seguros de uso, reconocer incidentes o señales de alerta y actuar correctamente conforme a los procedimientos definidos.

Contenidos mínimos.

- Principios básicos de ciberseguridad y su relación con el trabajo diario.
- Gestión segura de contraseñas y uso de autenticación multifactor.
- Reconocimiento de phishing, ingeniería social y fraudes asociados.
- Clasificación y tratamiento de la información.
- Uso aceptable de los recursos TIC
- Procedimiento de notificación de incidentes o sospechas.

Frecuencia orientativa.

Formación inicial, refuerzo anual y campañas periódicas de concienciación.

Evidencias esperables.

- Matriz de Competencias y Polivalencia: Documento del Sistema de Calidad que vincule cada puesto de trabajo con el nivel de capacitación en ciberseguridad requerido y alcanzado.
- Evaluación de la eficacia: No basta con la asistencia; se debe incluir el resultado de cuestionarios técnicos o ejercicios prácticos que validen la adquisición de la competencia.
- Registros de asistencia, materiales utilizados, actas de revisión, evidencias de decisiones adoptadas y seguimiento de indicadores.

8.3.3. Equipos técnicos y de desarrollo

Su trabajo impacta directamente en la robustez técnica de las soluciones, la seguridad del desarrollo, la configuración de infraestructuras y la capacidad de prevención, detección y respuesta.

Objetivo formativo.

Aplicar de forma efectiva los principios de desarrollo seguro, administración segura, operación protegida y cumplimiento técnico de los requisitos de ciberseguridad.

Contenidos mínimos.

- Desarrollo seguro y desarrollo ciberseguro.
- Gestión de vulnerabilidades, hardening, control de cambios y configuración.
- Gestión de identidades y privilegios.
- Monitorización, trazabilidad y respuesta a incidentes.

Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio
C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24
info@tedae.org
www.tedae.org

- Requisitos normativos y contractuales aplicables al entorno técnico.
- Buenas prácticas en protección de repositorios, credenciales y entornos de integración y despliegue.
- Requisitos específicos asociados a desarrollo software cuando apliquen PECAL y AS/EN 9115.

Frecuencia orientativa.

Formación inicial por rol, actualización anual y refuerzo específico ante cambios tecnológicos, adopción de nuevas herramientas, nuevos requisitos o incidentes relevantes.

Evidencias esperables.

- Matriz de Competencias y Polivalencia: Documento del Sistema de Calidad que vincule cada puesto de trabajo con el nivel de capacitación en ciberseguridad requerido y alcanzado.
- Evaluación de la eficacia: No basta con la asistencia; se debe incluir el resultado de cuestionarios técnicos o ejercicios prácticos que validen la adquisición de la competencia.
- Registros de asistencia, materiales utilizados, actas de revisión, evidencias de decisiones adoptadas y seguimiento de indicadores.

8.3.4. Proveedores y terceros relevantes

Los terceros con acceso a sistemas, datos, entornos o procesos críticos amplían la superficie de exposición y deben ser gestionados como parte de la cadena de suministro.

Objetivo formativo.

Asegurar el conocimiento y cumplimiento de los requisitos mínimos de seguridad exigidos por la organización.

Contenidos mínimos.

- Políticas de seguridad que les resulten aplicables.
- Requisitos de acceso, confidencialidad y tratamiento de la información.
- Procedimientos de reporte y escalado de incidentes.
- Responsabilidades contractuales relacionadas con ciberseguridad.
- Requisitos específicos adicionales cuando participen en contratos o entornos de defensa.

Frecuencia orientativa.

Antes del inicio de la actividad y siempre que cambien las condiciones de acceso, el servicio prestado o los requisitos aplicables.

Evidencias esperables.

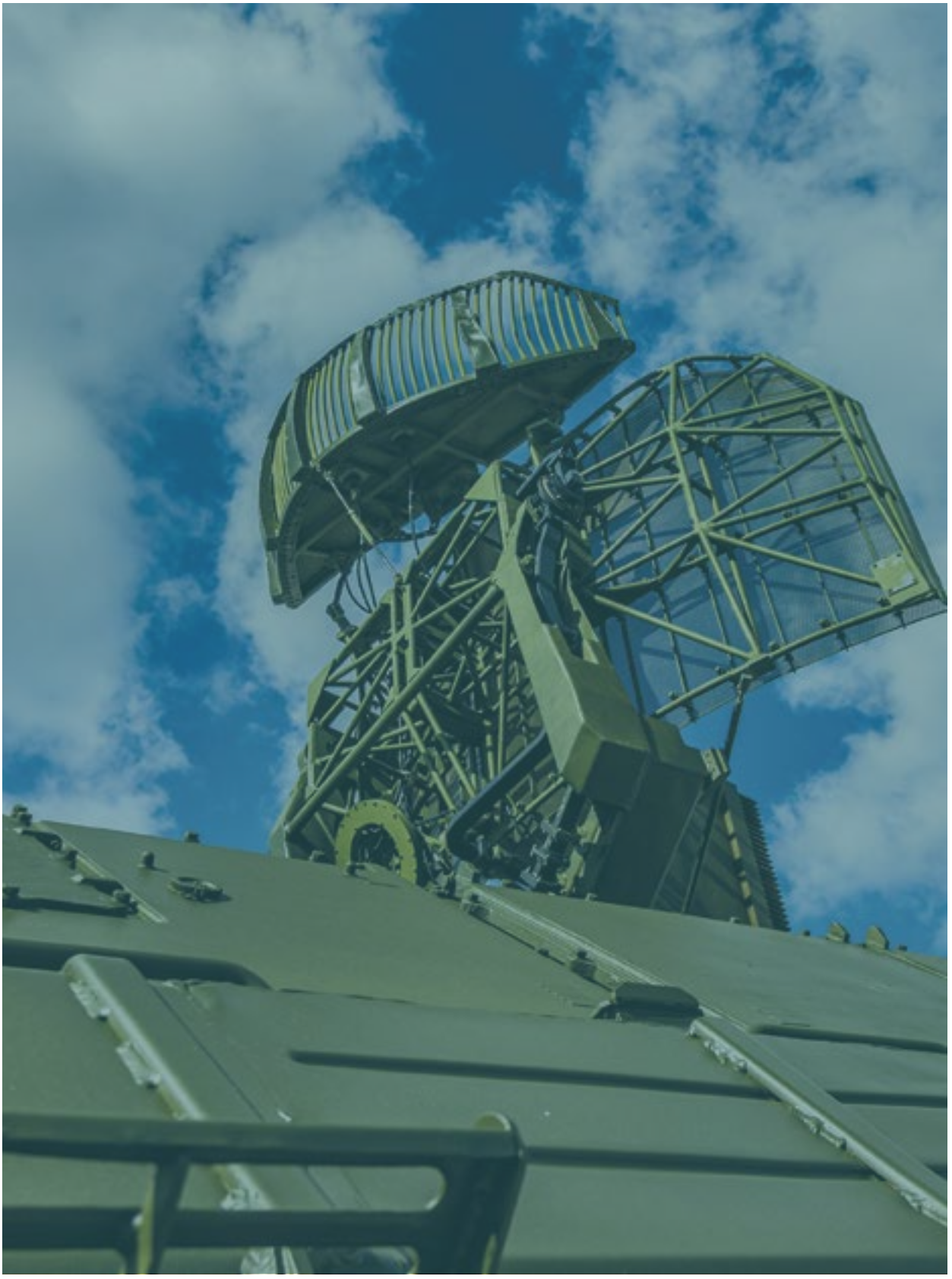
Aceptación formal de políticas, registros de formación o inducción, cláusulas contractuales, evidencias aportadas por el proveedor y controles de seguimiento.

8.3.5. Otras partes interesadas relevantes

Cuando proceda, la organización podrá incluir otros colectivos como auditores, responsables de procesos, personal temporal, organismos cliente u organismos contratantes que participen en comités, pruebas, ejercicios o actividades conjuntas. Su nivel de formación deberá definirse según su exposición al riesgo y su papel dentro del sistema.

8.4. Implantación del modelo de formación y concienciación

La implantación del modelo deberá abordarse de forma planificada, progresiva y coherente con el nivel de madurez de la organización. A tal efecto, se propone la siguiente estructura de implantación por niveles, con un enfoque progresivo utilizado para facilitar la toma de decisiones y adaptar el desplie-



Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio

C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24

info@tedae.org
www.tedae.org

gue al contexto real de la empresa.

La organización podrá complementar este modelo mediante acciones específicas como:

- formación inicial obligatoria;
- formación periódica;
- campañas de concienciación;
- simulaciones de phishing;
- ejercicios de respuesta a incidentes;
- sesiones específicas para proyectos o contratos críticos;

y canales de consulta o apoyo para resolución de dudas.

Nivel	Descripción	Alcance	Recursos necesarios	Beneficios esperados	Limitaciones
Inicial	Definición de colectivos, contenidos básicos y acciones formativas mínimas. Implantación de formación de acogida y campañas generales de concienciación.	Personal interno y perfiles con mayor exposición al riesgo.	Materiales base, responsable de coordinación, planificación mínima y registros de asistencia.	Cobertura básica, sensibilización inicial y generación de primeras evidencias.	Enfoque todavía general, escasa personalización y baja capacidad de medición.
Medio	Adaptación de contenidos por rol, campañas periódicas, simulaciones y definición de indicadores de seguimiento. Integración parcial con auditorías, competencias y revisión por la dirección.	Dirección, usuarios, técnicos, desarrollo y terceros relevantes.	Plan anual, contenidos segmentados, herramientas de e-learning o campañas, indicadores y validación por responsables de proceso.	Mayor coherencia, mejor adecuación al riesgo y evidencias más sólidas para auditorías.	Requiere coordinación interfuncional, mantenimiento de contenidos y seguimiento periódico.
Avanzado	Integración plena del modelo en el Sistema de Calidad y, cuando aplique, en SGSI, gestión de riesgos, auditorías y requisitos contractuales o PECAL. Revisión continua basada en indicadores, incidentes y lecciones aprendidas.	Toda la organización y terceros críticos.	Gobierno definido, indicadores consolidados, integración con sistemas de gestión, recursos formativos especializados y revisiones periódicas.	Modelo plenamente integrado, medible, auditable y alineado con la mejora continua.	Mayor complejidad organizativa y necesidad de recursos sostenidos.

Tabla 6. Propuesta de implantación del modelo de formación y concienciación

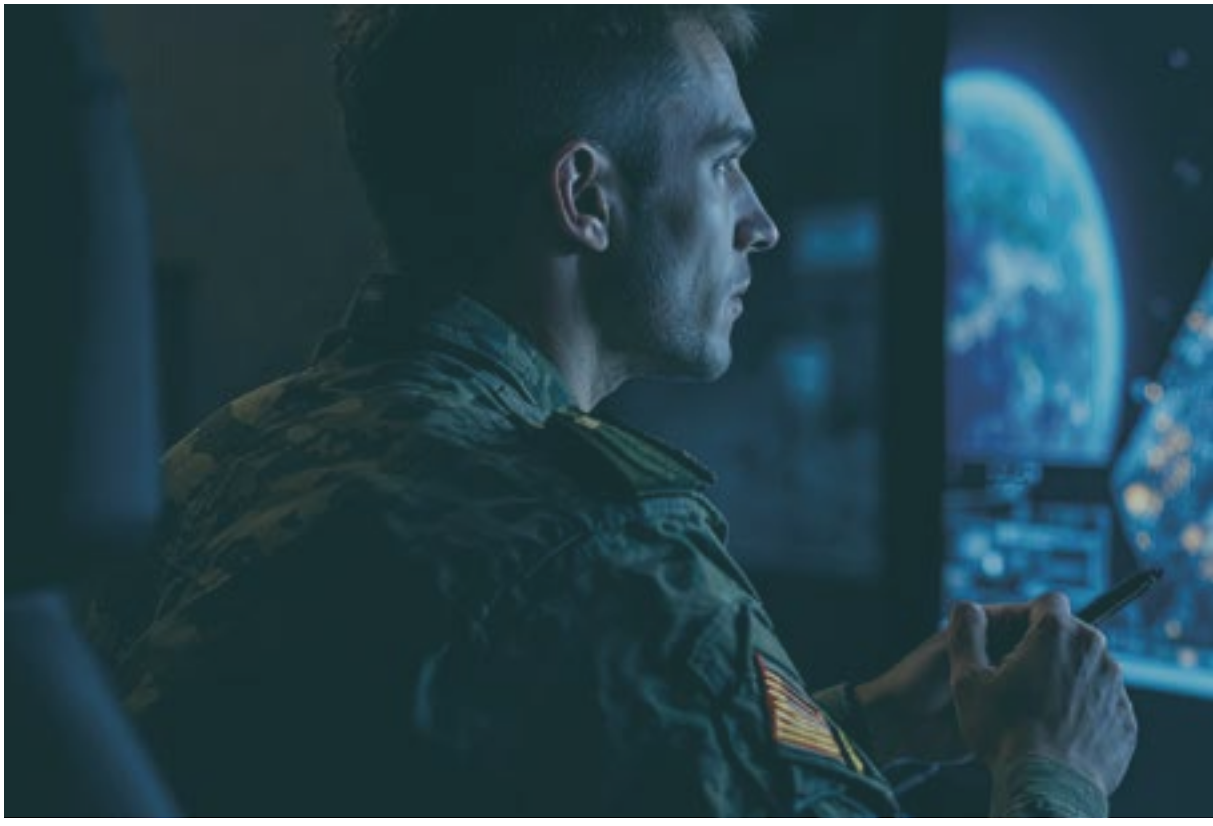
8.5. Evidencias, indicadores e integración con el Sistema de Calidad

Para que el modelo sea realmente parte del Sistema de Calidad, deberá quedar documentado, medido y sometido a revisión. Como mínimo, la organización debería conservar las siguientes evidencias:

- plan anual o planificación equivalente de formación y concienciación;
- identificación de colectivos y necesidades formativas;
- contenidos y materiales utilizados;
- registros de asistencia o participación;
- resultados de evaluaciones o verificaciones de aprovechamiento;
- resultados de campañas o simulaciones;
- acciones correctivas o de mejora derivadas de auditorías, incidentes o revisiones.

Asimismo, convendrá definir indicadores que permitan medir tanto la cobertura como la eficacia del modelo, por ejemplo:

- porcentaje de personal formado por colectivo;
- porcentaje de terceros críticos cubiertos;
- resultados de pruebas de conocimiento;
- tasa de clic o respuesta en campañas de phishing simulado;
- número de incidentes reportados por usuarios;
- número de desviaciones detectadas en auditorías relacionadas con falta de formación o concienciación;



- acciones de mejora abiertas y cerradas en relación con el programa.

La integración con el Sistema de Calidad deberá realizarse, como mínimo, a través de los siguientes procesos:

- gestión de competencias;
- análisis de riesgos;
- control documental;
- auditorías internas;
- revisión por la dirección;
- tratamiento de no conformidades y acciones correctivas;
- y, cuando aplique, integración con requisitos PECAL, contratos de defensa o sistemas complementarios como SGSI.

La existencia de un modelo único e integrado evita duplicidades, facilita la trazabilidad de evidencias y permite que la formación y la concienciación sean tratadas como un control verificable dentro del funcionamiento normal del sistema.

8.6. Revisión y mejora continua

El modelo de formación y concienciación deberá revisarse al menos una vez al año, y adicionalmente cuando se produzcan incidentes significativos, cambios regulatorios, nuevos contratos, incorporación de nuevas tecnologías o hallazgos relevantes en auditoría.

De este modo, la formación y la concienciación pasan a formar parte del ciclo de mejora continua del Sistema de Calidad y dejan de ser una actividad aislada.

09 Ejemplos de NO buenas prácticas y metodología para una buena práctica

9.1. Sistema de Calidad

NBP1. Falta de comprensión del contexto organizacional:

- No identificar cómo la ciberseguridad impacta en los procesos clave.
- Ignorar riesgos digitales en el análisis de contexto, lo que impide una integración efectiva.

Me1:

- Realizar un análisis estructurado del contexto interno y externo (DAFO, PESTEL).
- Incluir explícitamente los riesgos cibernéticos como parte del entorno digital.
- Documentar cómo la ciberseguridad impacta en los procesos clave del sistema de calidad.

NBP2. Desconocimiento de las partes interesadas:

- No considerar a los equipos de IT y ciberseguridad como partes interesadas clave.
- No evaluar sus necesidades ni expectativas en el sistema de gestión de calidad.

Me2:

- Identificar y mapear todas las partes interesadas relevantes (incluyendo IT, CISO, clientes con requisitos de seguridad).
- Usar herramientas como el análisis de las partes interesadas y entrevistas internas.
- Incorporar sus expectativas en los objetivos del sistema de gestión.

NBP3. Incumplimiento de requisitos legales:

- No incluir normativas de protección de datos (como GDPR) en el sistema de calidad.

- No documentar ni auditar controles de seguridad exigidos por clientes o reguladores.

Me3:

- Realizar un análisis de cumplimiento normativo (GDPR, ISO 27001, NIS2).
- Implementar un sistema de seguimiento de requisitos legales y contractuales.
- Auditar periódicamente el grado de cumplimiento exigido por clientes y reguladores.

NBP4. Falta de compromiso de la alta dirección:

- Delegar la ciberseguridad exclusivamente al área técnica sin alinearla con la estrategia de calidad.
- No asignar recursos para formación ni para medidas preventivas.

Me4:

- Incluir la ciberseguridad en la política de calidad y en los objetivos estratégicos.
- Establecer KPIs compartidos entre calidad y seguridad.
- Realizar sesiones de sensibilización para la dirección sobre riesgos digitales y su impacto en la calidad.

NBP5. Sistemas paralelos sin integración:

- Mantener sistemas de calidad y seguridad como estructuras independientes, duplicando esfuerzos y generando incoherencias.

Me5:

- Aplicar el enfoque de sistema único integrando procesos comunes: gestión de riesgos, auditorías, formación, documentación.
- Usar software de gestión que permita visualizar y coordinar ambos sistemas.

9.2. Nivel Técnico

NBP6. Apertura indiscriminada de puertos en firewall:

- Abrir puertos sin trazabilidad ni control, lo que debilita el perímetro de seguridad.

Me06:

- Aplicar políticas de firewall por defecto-denegado.
- Usar herramientas de escaneo de puertos y auditorías periódicas.
- Documentar y justificar cada excepción.

NBP7. Uso de VPN sin segmentación ni control de identidad:

- Las VPN tradicionales permiten acceso completo sin verificar identidad ni necesidad.

Me07:

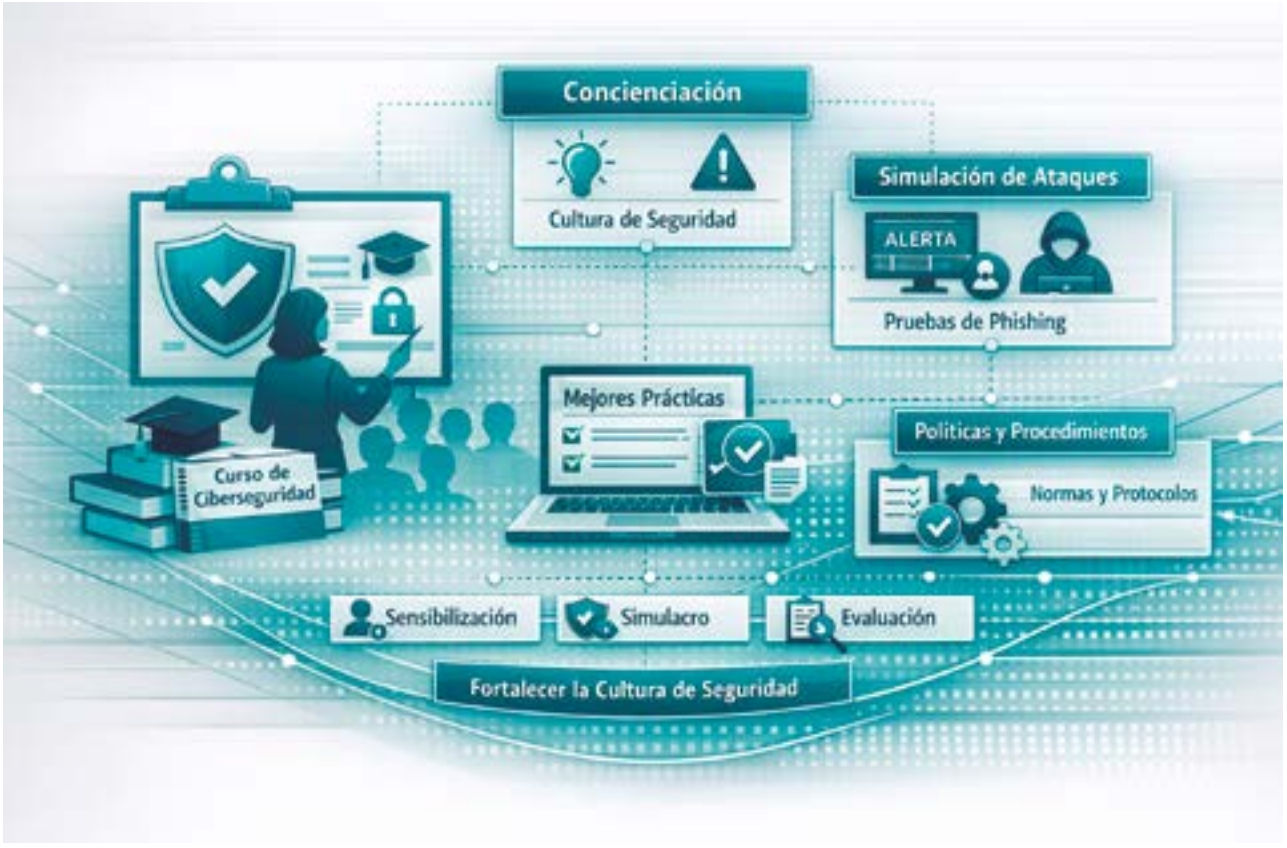
- Implementar Zero Trust Network Access (ZTNA).
- Autenticación multifactor (MFA) obligatoria.
- Segmentación de red por roles y funciones.

NBP8. Confianza en dispositivos sin validación:

- Se permite el acceso de dispositivos sin verificar su estado de seguridad.

Me08:

- Aplicar políticas de Bring Your Own Device (BYOD) con validación de seguridad.



- Uso de certificados digitales y control de acceso basado en dispositivos.
- Integración con soluciones de Endpoint Detection and Response (EDR).

NBP9. Tecnología obsoleta sin actualizaciones:

- Sistemas sin parches ni soporte que contienen vulnerabilidades conocidas.

Me09:

- Inventario de activos y clasificación por criticidad.
- Calendario de actualizaciones y parches.
- Uso de herramientas de gestión de vulnerabilidades.

NBP10. Falta de control en privilegios de usuario:

- Usuarios con permisos excesivos para tareas que no requieren ese nivel.

Me10:

- Aplicar el principio de mínimos privilegios.
- Revisiones periódicas de roles y accesos.
- Uso de Identity Governance and Administration (IGA).

NBP11. Ausencia de monitoreo continuo:

- No se registran ni analizan eventos de seguridad en tiempo real.

Me11:

- Implementar un sistema SIEM (Security Information and Event Management).
- Integrar con un SOC (Security Operations Center).
- Definir alertas y respuestas automatizadas.

NBP12. Formación insuficiente del personal:

Bajo índice de cumplimiento en cursos de concienciación.

Me12:

- Programas de formación continua y obligatoria.
- Simulacros de phishing y ciberejercicios.
- Indicadores de cumplimiento y refuerzo positivo.

NBP13. Análisis de seguridad manual o tardío en el código:

- Realizar revisiones de seguridad solo al finalizar el desarrollo o de forma manual, lo que permite la acumulación de vulnerabilidades críticas (como inyecciones SQL o desbordamientos de búfer) difíciles de corregir en fases avanzadas.

Me13: Implementación de herramientas SAST (Static Analysis Security Testing) automatizadas

- Integración en el Pipeline (DevSecOps): Configurar herramientas de análisis estático que escaneen el código fuente de forma automática en cada "commit" o "pull request".
- Definición de "Gatekeepers": Establecer umbrales de calidad donde el código con vulnerabilidades de criticidad "Alta" o "Crítica" bloquee automáticamente la integración hasta ser corregido.
- Selección de Reglas: Utilizar catálogos de debilidades estándar (como CWE o el Top 10 de OWASP) para parametrizar las herramientas según el lenguaje de programación utilizado.
- Generación de Evidencias: Utilizar los informes automáticos de la herramienta como evidencia objetiva para las auditorías del Sistema de Calidad y el cumplimiento de la PECAL 2210.

NBP14. Validación de seguridad basada exclusivamente en cumplimiento documental:

- Confiar en que poseer una certificación (ISO 27001 o ENS) garantiza la invulnerabilidad del sistema sin realizar pruebas técnicas reales de resistencia.

Me14: Integración de Pentesting y Auditorías Técnicas en el Ciclo de Mejora:

- Pruebas de Penetración (Pentesting): Programar ataques simulados periódicos sobre los sistemas críticos y productos finales para detectar vulnerabilidades que los escaneos automáticos omiten.
- Tratamiento como No Conformidad: Los hallazgos críticos de estas pruebas deben entrar en el flujo del Sistema de Calidad como "No Conformidades", activando el análisis de causa raíz y planes de acciones correctivas.

Referencias

- La OTAN y el desarrollo de capacidades para la ciberdefensa. (s. f.). otan.es. https://otan.es/blog/la-otan-y-el-desarrollo-de-capacidades-para-la-ciberdefensa
- Ciberseguridad: marco jurídico y operativo. (2021, 30 noviembre). Real Instituto Elcano. https://www.realinstitutoelcano.org/analisis/ciberseguridad-marco-juridico-y-operativo
- García Servert, R. C., & Iglesias Posada, L. (2022). La ciberdefensa en el ámbito de la OTAN. En www.acami.es.
- Reglamento (UE) 2024/2847 (Cyber Resilience Act). (2024). En https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R2847. Recuperado 10 de enero de 2026, de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R2847
- Guías - CCN-CERT. (s. f.). https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html

Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio
C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24
info@tedae.org
www.tedae.org

Acrónimos

- APT (Advanced Persistent Threat): Amenaza Avanzada Persistente. Ataques cibernéticos complejos y prolongados en el tiempo.
- CRA (Cyber Resilience Act): Ley de Ciberresiliencia de la UE.
- CVE (Common Vulnerabilities and Exposures): Lista de vulnerabilidades de seguridad informática conocidas públicamente.
- CWE (Common Weakness Enumeration): Sistema de categorías para debilidades de software y hardware.
- DAST (Dynamic Analysis Security Testing): Pruebas de seguridad de análisis dinámico (con la aplicación en ejecución).
- DGAM: Dirección General de Armamento y Material (ente regulador de las PECAL en España)
- ENS: Esquema Nacional de Seguridad (España).
- ITS: Instrucción Técnica de Seguridad.
- MCCE: Mando Conjunto del Ciberespacio (España).
- NIS2: Directiva (UE) 2022/2555 relativa a medidas para un elevado nivel común de ciberseguridad.
- PECAL/AQAP: Publicaciones Españolas de Calidad / Allied Quality Assurance Publications (OTAN).
- SAST (Static Analysis Security Testing): Pruebas de seguridad de análisis estático (análisis del código fuente).
- SBOM (Software Bill of Materials): Inventario formal de los componentes y dependencias de un software.
- SGSI: Sistema de Gestión de la Seguridad de la Información.
- SIEM (Security Information and Event Management): Gestión de información y eventos de seguridad.
- SOC (Security Operations Center): Centro de Operaciones de Seguridad.

Integración de la ciberdefensa

en los sistemas de calidad

TEDAE
Defensa, Seguridad, Aeronáutica y Espacio

info@tedae.org
www.tedae.org

Asociación Española de
Empresas Tecnológicas de
Defensa, Seguridad, Aeronáutica
y Espacio

C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24