



**AES**

ASOCIACIÓN ESPAÑOLA  
EMPRESAS DE SEGURIDAD

# GUÍA DE ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD





# Índice

<b>Introducción .....</b>	<b>5</b>
<b>Objeto .....</b>	<b>6</b>
<b>Área de Trabajo Ciberseguridad 2023 .....</b>	<b>9</b>
<b>Metodología AES.....</b>	<b>10</b>
<b>Comprobación de las medidas de seguridad existentes .....</b>	<b>12</b>
<b>Controles Categoría Básica .....</b>	<b>13</b>
<b>Implantar las medidas de seguridad necesarias .....</b>	<b>14</b>
<b>Elaborar el documento de Declaración de Aplicabilidad .....</b>	<b>15</b>
<b>Declaración de Aplicabilidad .....</b>	<b>17</b>
<b>Elaborar el documento de Declaración de Conformidad .....</b>	<b>19</b>



# Introducción

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, establece que el ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

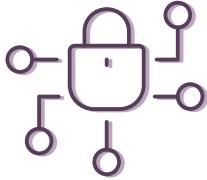
El ámbito de aplicación del citado Real Decreto contempla a los sistemas de información de las entidades del sector privado, cuando presten servicios o provean soluciones a entidades del sector público, extendiendo este ámbito de aplicación a la cadena de suministro de dichas entidades privadas.

La Asociación Española de empresas de Seguridad (AES) en su manifiesto 2020-2022 declaraba su compromiso con la seguridad de la sociedad.

"Una de las necesidades más básicas de la sociedad actual es la protección frente a las amenazas, en cualquiera de las formas en las que se produzcan. Sin las medidas de protección adecuadas, los ciudadanos que conforman la sociedad afrontan riesgos."

AES, teniendo en cuenta su compromiso con la seguridad de la sociedad y con el de aportar valor a sus asociados, y teniendo en cuenta que la mayoría de ellos son proveedores de soluciones y servicios a la administración pública o forman parte de la cadena de suministro de dichas soluciones y servicios, y por lo tanto se encuentran dentro del ámbito de aplicación, ha elaborado la presente guía con el objeto de ayudar a sus asociados en la tarea de lograr cumplir con los requisitos que establece el ENS para disponer de una Declaración de Conformidad para sus sistemas de categoría Básica.





Modelos de confianza cero



Prevención contra la fuga de información



Protección integral del puesto de trabajo remoto



Legislación vigente



Protección de la cadena de suministros



Servicios de prevención anti - ransomware



Seguridad de modelos colaborativos



# Área de Trabajo Ciberseguridad 2023

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

Elaboración de una Guía con el objeto de ayudar a sus asociados en la tarea de lograr cumplir con los requisitos que establece el ENS para disponer de una Declaración de Conformidad para sus sistemas de categoría Básica.

Dimensiones afectadas:

- ✓ **Disponibilidad**
- ✓ **Integridad**
- ✓ **Confidencialidad**
- ✓ **Autenticidad**
- ✓ **Trazabilidad**



# Metodología AES

Analizar las medidas de seguridad de las que dispone un sistema de información y determinar si cumple los requisitos que establece el ENS, consta de los siguientes pasos:

**Comprobación de las medidas de seguridad existentes**

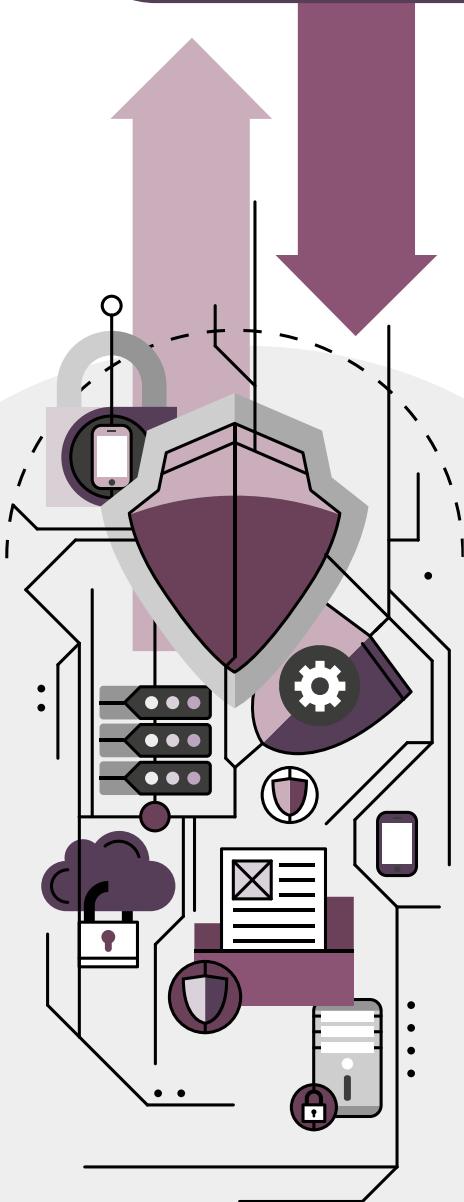
**Implantar las medidas de seguridad necesarias**

**Elaboración de la Declaración de Aplicabilidad**

**Elaboración de la Declaración de Conformidad**



# Comprobación de las medidas de seguridad existentes



## Políticas

Documento de alto nivel que establece los criterios y directrices a la hora de desarrollar los procedimientos técnicos y aplicar las medidas técnicas, estableciendo responsabilidades.

## Procedimientos

Documento que establece el modo específico de llevar a cabo una actividad o proceso.

## Contratos con terceras partes

## Medidas técnicas

Configuración específica del S.O., de las aplicaciones o de las comunicaciones. Hardware y/o software específico

## Controles Categoría Básica

Marco Operacional

32

Marco Organizativo

9

Medidas de Protección

26

Total

67

# Implantar las medidas de seguridad necesarias

Si alguna medida de seguridad de las contempladas no se encuentra implantada y es de aplicación al sistema de información objeto del análisis, deberá implantarse.

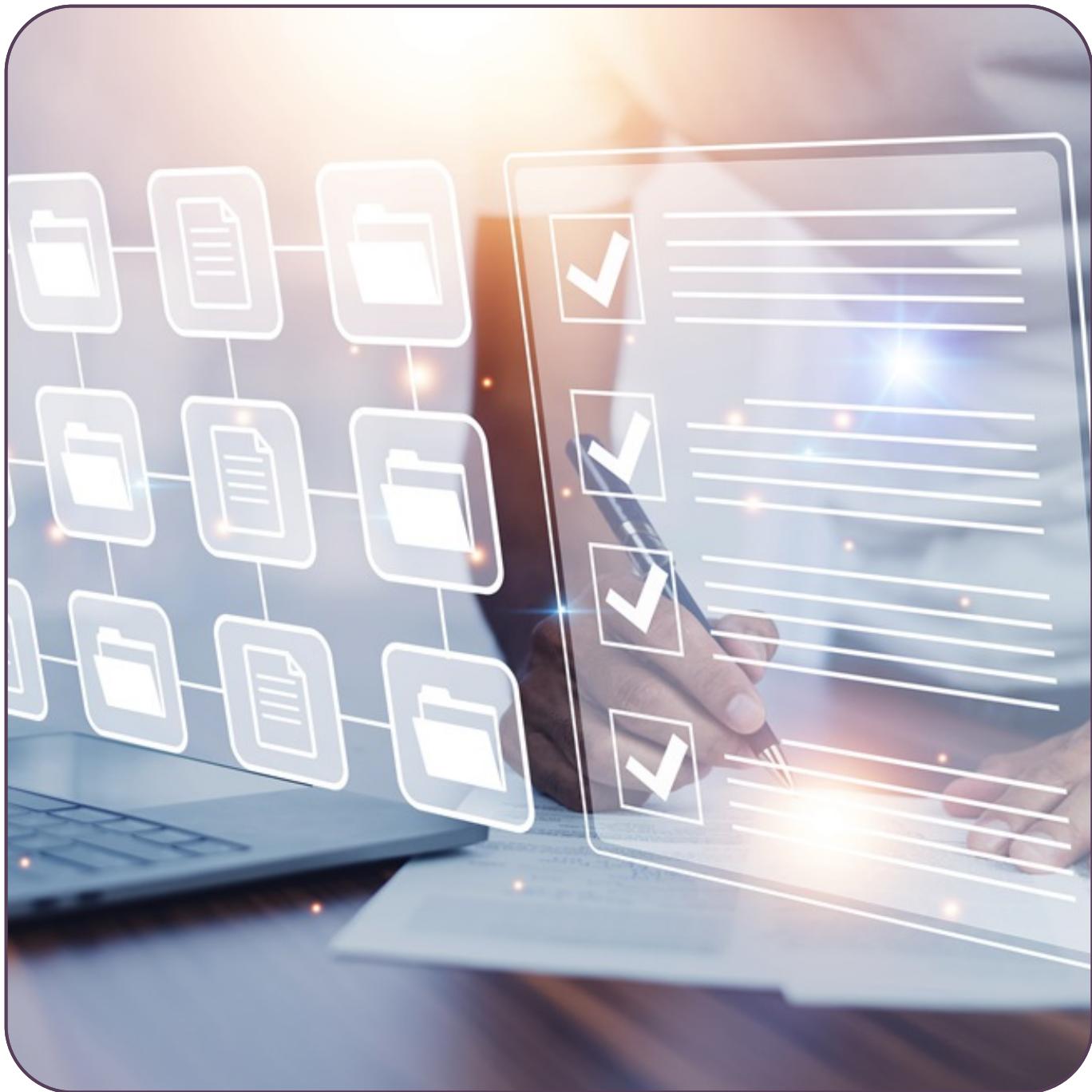


# Elaborar el documento de Declaración de Aplicabilidad

Se debe formalizar una Declaración de Aplicabilidad, firmada por el responsable de la seguridad de la empresa.

## Índice del documento de Declaración de Aplicabilidad

- Introducción
- Alcance
- Niveles de seguridad y categoría
- Análisis realizado
- Declaración de aplicabilidad
- Justificación de las medidas
- Medidas compensatorias
- Conformidad del responsable



# Declaración aplicabilidad

Para elaborar la declaración de aplicabilidad se recomienda utilizar

## **BP/14 Declaración de aplicabilidad – Buenas Practicas CCN-CERT**

<https://www.ccn-cert.cni.es/es/informes/informes-de-buenas-practicas-bp/3830-ccn-cert-bp-14-declaracion-de-aplicabilidad-ens/file>

## **Simulador de declaración de aplicabilidad CCN-CERT**

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6945-ccn-cert-bp-14-declaracion-de-aplicabilidad-ens-anexos/file.html>

Contemplará todas las medidas de seguridad aplicables, y si en algún caso se utilizaran medidas compensatorias, se justificará documentalmente que protegen, igual o mejor, que la medida a la que sustituyen de acuerdo a la establecido en la Guía CCN-STIC-819 "Medidas Compensatorias".





# Elaborar el documento de Declaración de Conformidad

Para poder elaborar el documento de Declaración de Conformidad es necesario haber realizado previamente:

- 🛡️ Una autoevaluación documentada
- 🛡️ La Declaración de Conformidad
- 🛡️ Un análisis y evaluación de la situación



El titular del órgano de dirección de la empresa aprobará una Declaración de Conformidad, cuya estructura y contenido se detallan en el Anexo A Guía de Seguridad de las TIC CCN-STIC 809.



# AES

ASOCIACIÓN ESPAÑOLA  
EMPRESAS DE SEGURIDAD

C/Alcalá, 99 2ºA - 28009 Madrid

Telf. 915 765 225

[www.aesseguridad.es](http://www.aesseguridad.es)

[aes@aesseguridad.es](mailto:aes@aesseguridad.es)

 @aes\_seguridad

 @aesseguridad2021

 Asociación Española de  
empresas de Seguridad