CECA MAGÁN
ABOGADOS

ESQUEMA NACIONAL DE SEGURIDAD

Real Decreto 311/2022 de 3 de mayo

13 de mayo de 2022

El pasado 5 de mayo de 2022 entró en vigor del Real Decreto 311/2022, de 3 de mayo de 2022, por el que se regula el Esquema Nacional de Seguridad.

El principal objetivo del Esquema Nacional de Seguridad (ENS) es **crear las condiciones necesarias de seguridad en el uso de los medios electrónicos**, a través de medidas que puedan garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, y que permitan el ejercicio de derechos, así como el cumplimiento de deberes a través de estos medios.

Con el ánimo de ofrecer la información más actualizada, recogemos en esta guía preguntas y respuestas a las principales dudas que se puedan tener, queriendo ser de la máxima utilidad práctica posible para sus potenciales lectores

#DerechoDePrivacidadalEstiloCeca

#EstiloCeca

1. ¿Por qué se ha implementado un nuevo Esquema Nacional de Seguridad?

Desde la entrada en vigor en 2010 del anterior Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica hasta ahora, **se han producido numerosos cambios** en España y en la Unión Europea en general, **que han incrementado y transformado los procesos de transformación tecnológica y digital de una manera notoria**.

Dicha situación ha originado un **nuevo escenario en materia de ciberseguridad**, en el cual se ha evidenciado que los sistemas de ciberseguridad están cada vez más expuestos a ciberataques, siendo prueba de ello el **gran aumento de ciberataques** que se ha venido produciendo, tanto en número como en sofisticación.

2. ¿Cuál es la principal finalidad del nuevo ENS?

La finalidad principal del ENS es la creación de las **condiciones necesarias de confianza** en el uso de los medios electrónicos, a través de medidas para garantizar:

- la seguridad de los sistemas
- los datos
- las comunicaciones
- y los servicios electrónicos

Por tanto, a través del nuevo RD 311/2022 se busca **adecuar el ENS al nuevo marco legal vigente, así como al contexto y a las necesidades actuales**, habiéndose procedido a una actualización de todos los principios básicos, así como de las medidas de seguridad.

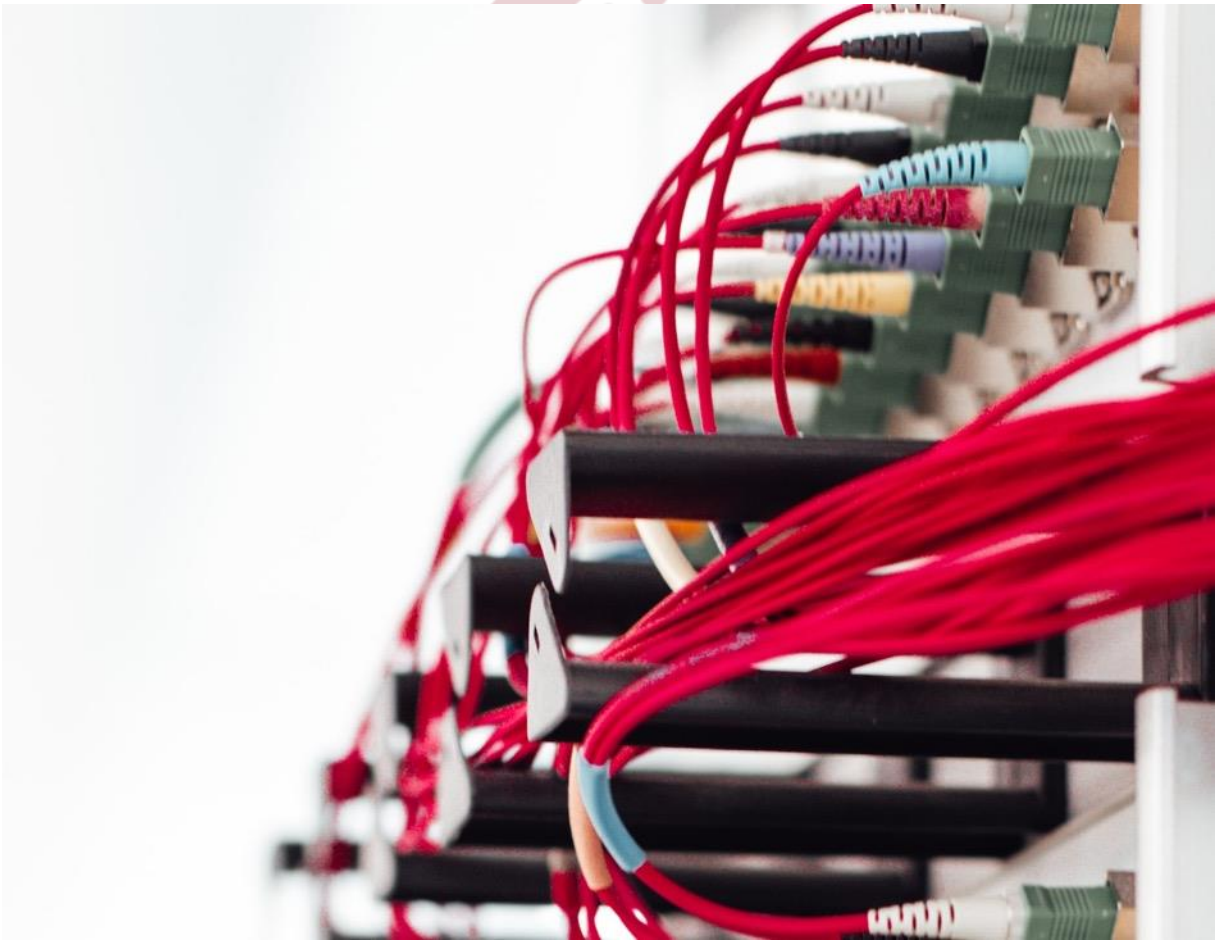
En definitiva, se facilita una mejor respuesta a las nuevas tendencias y/o necesidades en materia de ciberseguridad.

3. ¿Qué novedades supone el ENS desde un punto de vista técnico?

Desde un punto de vista técnico, cabe reseñar las siguientes novedades:

- Se permite una **adaptación al ENS más rápida y eficiente**, dado que se promueve la implementación de perfiles de cumplimiento, los cuales son una agrupación de medidas de seguridad que van directamente destinadas a una categoría concreta de seguridad.

- Respecto a las **medidas de seguridad, se han producido varias modificaciones sobre las mismas**, así como se ha intensificado la rigurosidad de estas. También se han **incluido otras nuevas**, como, por ejemplo, las relativas a servicios en la nube, interconexión de sistemas o dispositivos conectados a la red.



4. ¿Qué novedades supone el ENS por relación a la normativa protectora de datos de carácter personal?

De conformidad con el ENS, **cuando un sistema de información trate datos personales** le será de aplicación lo dispuesto en:

- El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)
- La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales,
- La Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales,

En estos supuestos, **el responsable o el encargado del tratamiento**, **asesorado por el Delegado de Protección de Datos**, realizarán un análisis de riesgos conforme al Reglamento General de Protección de Datos y, en los supuestos aplicables, una evaluación de impacto en la protección de datos, prevaleciendo **las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto,** en caso de resultar agravadas respecto de las previstas en el ENS.

5. ¿A quiénes les es de aplicación el ENS?

El ENS es de aplicación a:

Los sistemas de información de todo el SECTOR PÚBLICO, entendiendo por tal:

- La Administración General del Estado.
- Las Administraciones de las Comunidades Autónomas.
- Las Entidades que integran la Administración Local.
- El sector público institucional, es decir:
  - Cualesquiera organismos públicos y entidades de derecho público vinculados o dependientes de las Administraciones Públicas.
  - Las entidades de derecho privado vinculadas o dependientes de las Administraciones Públicas.
  - Las Universidades públicas.

Los sistemas de información de las entidades del SECTOR PRIVADO, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, **presten servicios o provean soluciones** a las entidades del sector público para el ejercicio por estas de **sus competencias y potestades administrativas.**

Los sistemas que tratan información clasificada.

6. ¿Dado que, a determinadas entidades del sector privado les es de aplicación el ENS en su relación contractual con el sector público, ¿deben contener algún tipo de previsión los pliegos de prescripciones administrativas o técnicas en este sentido?

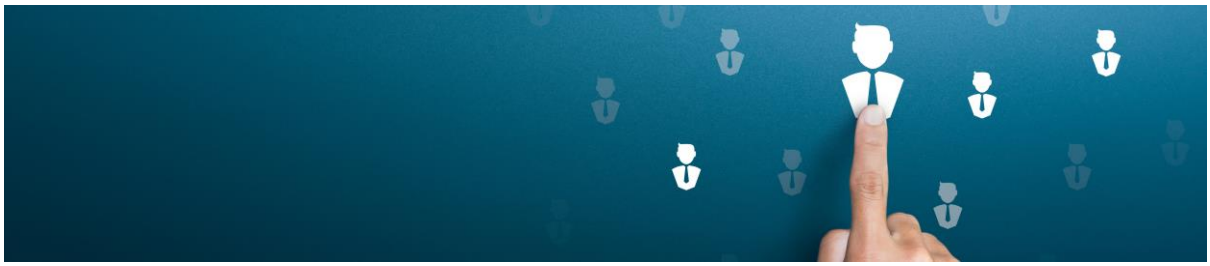
Sí, los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector público contemplarán **todos aquellos requisitos necesarios para asegurar la conformidad con el ENS** de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, **tales como la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS**.

Esta cautela se extenderá también a la cadena de suministro de dichos contratistas, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos.

7. ¿Cómo se determina la conformidad/cumplimiento con el Esquema Nacional de Seguridad?

Los sistemas de información comprendidos en la cuestión 5. deben ser objeto de un proceso para determinar su conformidad con el ENS. A tal efecto:

- los sistemas de categoría **MEDIA o ALTA precisarán de una auditoría para la certificación de su conformidad**,
- Los sistemas de **categoría BÁSICA solo requerirán de una autoevaluación para su** declaración de la conformidad.



8. ¿Qué roles/perfiles deben implementarse en el cumplimiento del ENS?

Se diferencian **cuatro** roles:

1. El responsable de información
2. El responsable del servicio
3. El responsable de la seguridad y
4. Se introduce la figura del responsable del sistema que, por norma general, **deberá ser distinto al responsable de la seguridad**

Además, se introduce la figura de la **Persona de Contacto (POC),** que deberá ser designada por las entidades jurídicas privadas que presten servicios dentro del alcance del ENS, actuando como responsable de seguridad de dicha organización.

9. ¿Deben contar las entidades a las que les es de aplicación el ENS con alguna Política?

Sí, los sujetos obligados, deben tener una **Política de Seguridad de la Información**.

Esta Política es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. A tal efecto, el instrumento que apruebe dicha política de seguridad deberá incluir, como mínimo, los siguientes extremos:
Los objetivos o misión de la organización.

- El marco regulatorio en el que se desarrollarán las actividades.
- Los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación.
- La estructura y composición del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad y la relación con otros elementos de la organización.
- Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.
- Los riesgos que se derivan del tratamiento de los datos personales. El análisis de riesgos en materia de protección de datos y, en su caso la evaluación de impacto en la misma, pase a formar parte integrante de la política de seguridad de la información.

Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente.

Además, el papel del **Delegado de Protección de Datos**, resulta esencial en todo el diseño y desarrollo de la política de seguridad de la información, debiendo tener pleno conocimiento de la misma y asesorar en su diseño e implantación, en virtud de las funciones que el Reglamento general de protección de datos le otorga expresamente.

10. ¿Puede el Responsable de Seguridad de la información ser a su vez Delegado de Protección de Datos?

No, existe una clara incompatibilidad entre ambas funciones.

El Informe 170/2018 de la Agencia Española de Proteccion de Datos ya recogía la incompatibilidad de ostentar ambos roles al entender que existen claras diferencias, tanto sustantivas como competenciales entre el ámbito de la seguridad de información y el de la protección de datos de carácter personal, y ello por que, no cabe duda de que la garantía de la seguridad de los datos personales adquiere una especial trascendencia en cuanto a su protección, pero sin que ésta se limite exclusivamente al ámbito de la seguridad de dicha información, en cuanto que la protección de datos personales tiene un ámbito mucho más extenso que abarca, a un conjunto de principios, derechos y obligaciones mucho más amplio que el de la seguridad.

11. ¿Deben realizarse Autorías de seguridad?

Los sujetos obligados serán objeto de una auditoría regular ordinaria, **al menos cada dos años,** que verifique el cumplimiento de los requerimientos del ENS.

Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en los sistemas de información, que puedan repercutir en las medidas de seguridad requeridas.

12. En caso de que se produzca un incidente de seguridad en el SECTOR PÚBLICO, ¿a quién deberá notificarse?

Al **Centro Criptológico Nacional Computer Emergency Response Team** (CCN-CERT).

13. Y en el caso de las entidades del SECTOR PRIVADO que prestan servicios al sector público?

En ese caso, deberá ser ante el **Centro de respuesta a incidentes de seguridad del Instituto Nacional de Ciberseguridad** (INCIBE-CERT).

14. ¿Cuál es el plazo para adecuarse al nuevo ENS?

Las entidades a las que les es de aplicación el ENS **tienen un plazo de dos años** desde la entrada en vigor del nuevo ENS, esto es hasta el 5 de mayo de 2024.

15. ¿Sigue siendo de aplicación el Real Decreto 3/2010, de 8 de enero por el que se regulaba anteriormente el ENS?

No, se deroga, así como cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en el nuevo RD 311/2022.

16. ¿Desde cuándo es aplicable el actual ENS?

Desde el día siguiente al de su publicación en el BOE, es decir, **desde el 5 de mayo de 2022.**

CECA MAGÁN
ABOGADOS

¿Podemos ayudarte?

Ingrid González

igonzalez@cecamagan.com

Sergio Santamaria

ssantamaria@cecamagan.com

Le recordamos, que todas las cuestiones del presente documento son de carácter informativo.

Para ampliar información y contratar nuestros servicios, por favor contacte con nuestros profesionales

info@cecamagan.com

CECA MAGÁN
ABOGADOS

#EstiloCeca

www.cecamagan.com

Contáctanos

(+34) 91 345 48 25

info@cecamagan.com

www.cecamagan.com

CHAMBERS EUROPE · The LEGAL 500 · Best Lawyers · LEADERS LEAGUE