



© 2022 CS³ Group – Todos los derechos reservados



Certificación/Conformidad con el ENS

Esquema Nacional de Seguridad (ENS)

Tipo de documento: Presentación

Autor del documento: CS³ Group (Pedro C. aka s4ur0n)

Documento: CS3-ENS_v3.pdf (TLP:GREEN)

Versión: 2.0

Categoría: CATÁLOGO DE SERVICIOS PARA PYMES

Fecha de elaboración: 04/05/2022

Nº de Páginas: 26

Spain





1. Esquema Nacional de Seguridad (ENS)

Certificación/Conformidad con el ENS

Certificación/Conformidad con el ENS

¿Qué es el Esquema Nacional de Seguridad (ENS)?

- En el ámbito de la **Administración Electrónica** española, el **Esquema Nacional de Seguridad (ENS)** tiene por objeto **establecer la política de seguridad en la utilización de medios electrónicos** y está constituido por **principios básicos y requisitos mínimos** que permitan una **protección adecuada** de la información.
- Dicho esquema se regula en **Real Decreto 311/2022, de 3 de mayo** (antes por el **R.D. 3/2010**, de 8 de enero, que ya fue establecido anteriormente en el artículo 42 de la **Ley 11/2007**, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicio Públicos, y que había sido modificado por el **Real Decreto 951/2015** para actualizarlo a la luz de la experiencia obtenida en su implantación, de la evolución de la tecnología y las ciberamenazas y del contexto regulatorio internacional y europeo).

Certificación/Conformidad con el ENS

¿Estoy **obligado** a su cumplimiento?

El ENS es aplicable a las entidades de derecho público **vinculadas o dependientes** de las **Administraciones Públicas**:

- Administración General del Estado.
- Administraciones de las Comunidades Autónomas.
- Entidades que integran la Administración Local.
- Entidades de derecho público vinculadas o dependientes de las mismas.

Certificación/Conformidad con el ENS

Vemos así que **los proveedores** de las **Administraciones Públicas**, con incidencia relevante en los servicios prestados por éstas en el ámbito del ENS, **podrían adoptar también la condición de sujeto obligado**, a todos los efectos.

Las organizaciones pertenecientes al **Sector Privado**, **estarían obligadas al cumplimiento del ENS**, en las mismas condiciones que las pertenecientes al Sector Público, dependiendo de estos casos (suelen ser notificadas dando un plazo de adaptación de aproximadamente 6 meses con un compromiso de cumplimiento):

- Si son sujetos obligados **al encontrarse vinculadas o dependientes** de las Administraciones Públicas.
- Si **proporcionan soluciones, o prestan servicios**, directamente a algún sujeto obligado por el ENS, ya sea una **Administración Pública** o cualquier otra **organización vinculada o dependiente**.

Certificación/Conformidad con el ENS

¿Cuáles son los **principios básicos** a los que hace referencia el ENS?

- La seguridad como un proceso integral.
- Gestión de la seguridad basada en los riesgos.
- Prevención, detección, respuesta y conservación.
- Existencia de líneas de defensa.
- Vigilancia continua.
- Reevaluación periódica.
- Diferenciación de responsabilidades.

Certificación/Conformidad con el ENS

¿Y los requisitos mínimos?

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos de seguridad y contratación de servicios de seguridad.
- Mínimo privilegio.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.

Certificación/Conformidad con el ENS

- Prevención ante otros sistemas de información interconectados.
- Registro de la actividad y detección de código dañino.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

Certificación/Conformidad con el ENS

¿Y las medidas de seguridad?

Las **(75) medidas de seguridad^(*) disponibles**, se encuentran organizadas en:

- Marco Organizativo (4)
- Marco Operacional (33)
- Medidas de protección (36)

^(*) Para la selección de las medidas de seguridad apropiadas de entre las contenidas en el ENS, siempre serán de acuerdo con las dimensiones de seguridad y sus niveles, y, para determinadas medidas de seguridad, de acuerdo con la categoría del sistema. <https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1073>

Certificación/Conformidad con el ENS

Disponemos de la Certificación **UNE-EN ISO/IEC 27001:20xx** ¿Es necesario hacer algo más o podemos cumplir con ello?

- Para satisfacer los citados principios básicos y requisitos mínimos del ENS, **se puede aplicar un modelo de tipo PCDA** para lo cual la normalización voluntaria ofrece herramientas como la norma ISO/IEC 27001:20xx
- Las organizaciones que se encuentren certificadas contra ISO/IEC 27001 **tienen una buena parte del camino recorrido** para lograr su conformidad con el ENS, toda vez que las medidas de protección que señala el ENS coinciden, en lo sustancial, con los controles que prevé la norma internacional.
- La norma **UNE-EN ISO/IEC 27002:20xx** es un conjunto de controles de seguridad para **sistemas de información genéricos**.

Certificación/Conformidad con el ENS

- Aunque muchas de las medidas de seguridad indicadas en el anexo II del ENS **coinciden con controles de UNE-EN ISO/IEC 27002:20xx**, el ENS es **más preciso** y establece un **sistema de protección proporcionado a la información y servicios** a proteger para racionalizar la implantación de medidas de seguridad y reducir la discrecionalidad.
- La norma **UNE-EN ISO/IEC 27002:20xx carece de esta proporcionalidad**, quedando a la mejor opinión del auditor que certifica la conformidad con la norma UNE-EN ISO/IEC 27001:20xx

Certificación/Conformidad con el ENS

Fase 1: Plan de Adecuación



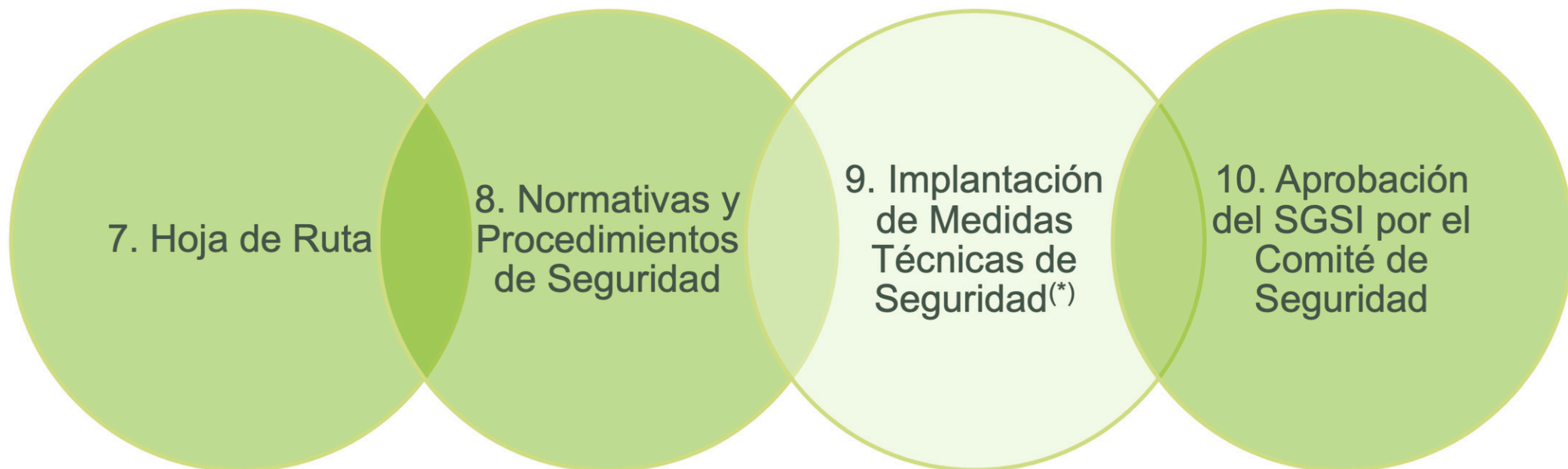
Certificación/Conformidad con el ENS

Con el **Plan de Adecuación** para la **Certificación/Conformidad** con el **ENS**, el Cliente tendrá todo lo que necesita (Política de Seguridad, Categorización de Sistemas, Análisis de Riesgos y Declaración de Aplicabilidad/Perfil de Cumplimiento).



Certificación/Conformidad con el ENS

Fase 2: Implementación de Seguridad



^(*) Supervisado y coordinado por CS³ Group.

Certificación/Conformidad con el ENS

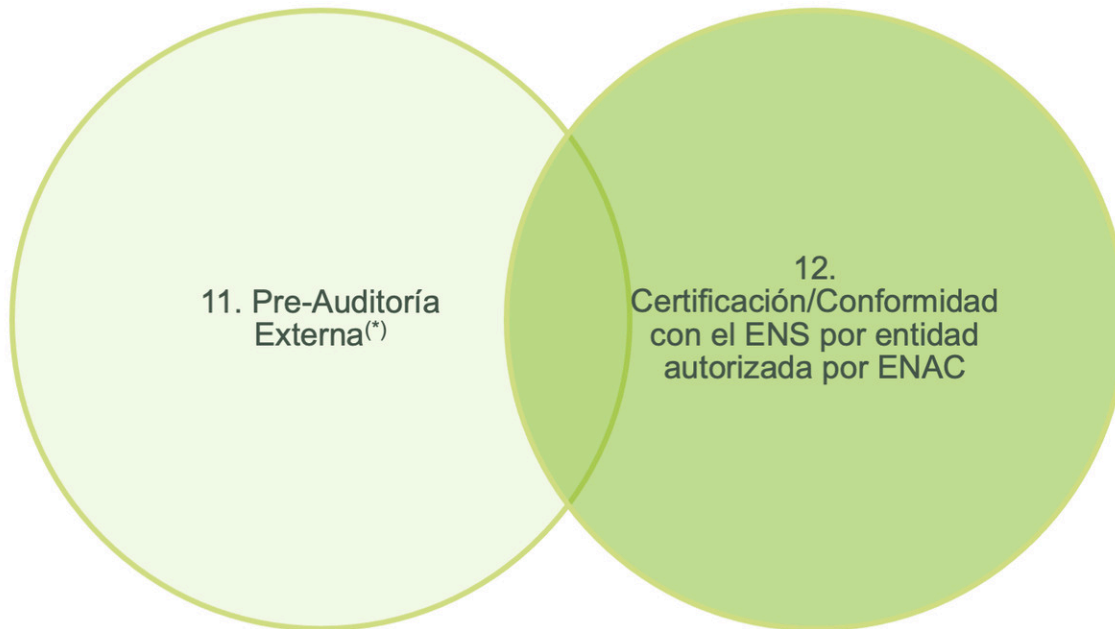
Una vez realizado el Plan de Adecuación, se pasará a la fase de **Implantación de la Seguridad**. Nuestro equipo de Consultores/Audidores en conjunto con los técnicos asignados en la organización, establecerán los siguientes puntos de control:

- **Hoja de Ruta:** Documentos a elaborar, medidas técnicas a implementar, establecimiento de prioridades.
- **Elaboración del Marco Normativo e Implantación de la Seguridad**
- **Aprobación del Sistema de Gestión de la Seguridad de la Información**

La Organización, comenzará a implementar bajo dichos criterios, todo aquello que sea necesario para poder alcanzar la Certificación/Conformidad con el ENS y **supervisadas por nuestro equipo de auditores**.

Certificación/Conformidad con el ENS

Fase 3: Certificación/Conformidad



(*) **OPCIONAL** con tercera empresa autorizada. Supervisado y coordinado por CS³ Group.

Certificación/Conformidad con el ENS

Se pasará entonces a la **Declaración/Certificación de Conformidad** con el **ENS**, donde nuestro equipo participará activamente en el proceso:

- La determinación de la conformidad de los sistemas de información del ámbito de aplicación del ENS con categorías **MEDIA o ALTA** se realizará mediante un procedimiento **de auditoría formal** que, con carácter ordinario, verifique el cumplimiento de los requerimientos contemplados en el ENS, al menos cada dos años.
- Para la determinación de la conformidad de los sistemas de información del ámbito de aplicación del ENS con **categoría BÁSICA** bastará con la ejecución de un **procedimiento de autoevaluación** que, con carácter ordinario, verifique el cumplimiento de los requerimientos contemplados en el ENS, al menos cada dos años. Nada impide que voluntariamente, se someta a una Auditoría formal de verificación de conformidad.

Certificación/Conformidad con el ENS

Con carácter extraordinario, tales auditorías, deberán realizarse **siempre que se produzcan modificaciones significativas** en el sistema considerado que pudieran repercutir en las medidas de seguridad que deban adoptarse.

Con **carácter opcional (no incluido en la oferta económica)**, se podrá requerir una **pre-auditoría** previa mediante una **tercera empresa**, que podrá ser elegida por el Cliente, o bien, emplear a uno de nuestros **partners (SIDERTIA SOLUTIONS <https://www.sidertia.com/>)** que emitirán un **informe objetivo, independiente** y con un **Plan de Acción** específico para poder solventar cualquier eventualidad detectada.

En ningún caso, la oferta comercial incluye el precio de la **Certificación/Conformidad con el ENS** de la entidad certificadora reconocida por ENAC, recomendando que dicha tarea específica sea realizada por **AENOR** (<https://www.aenor.com/certificacion/tecnologias-de-la-informacion/ens-esquema-nacional>)

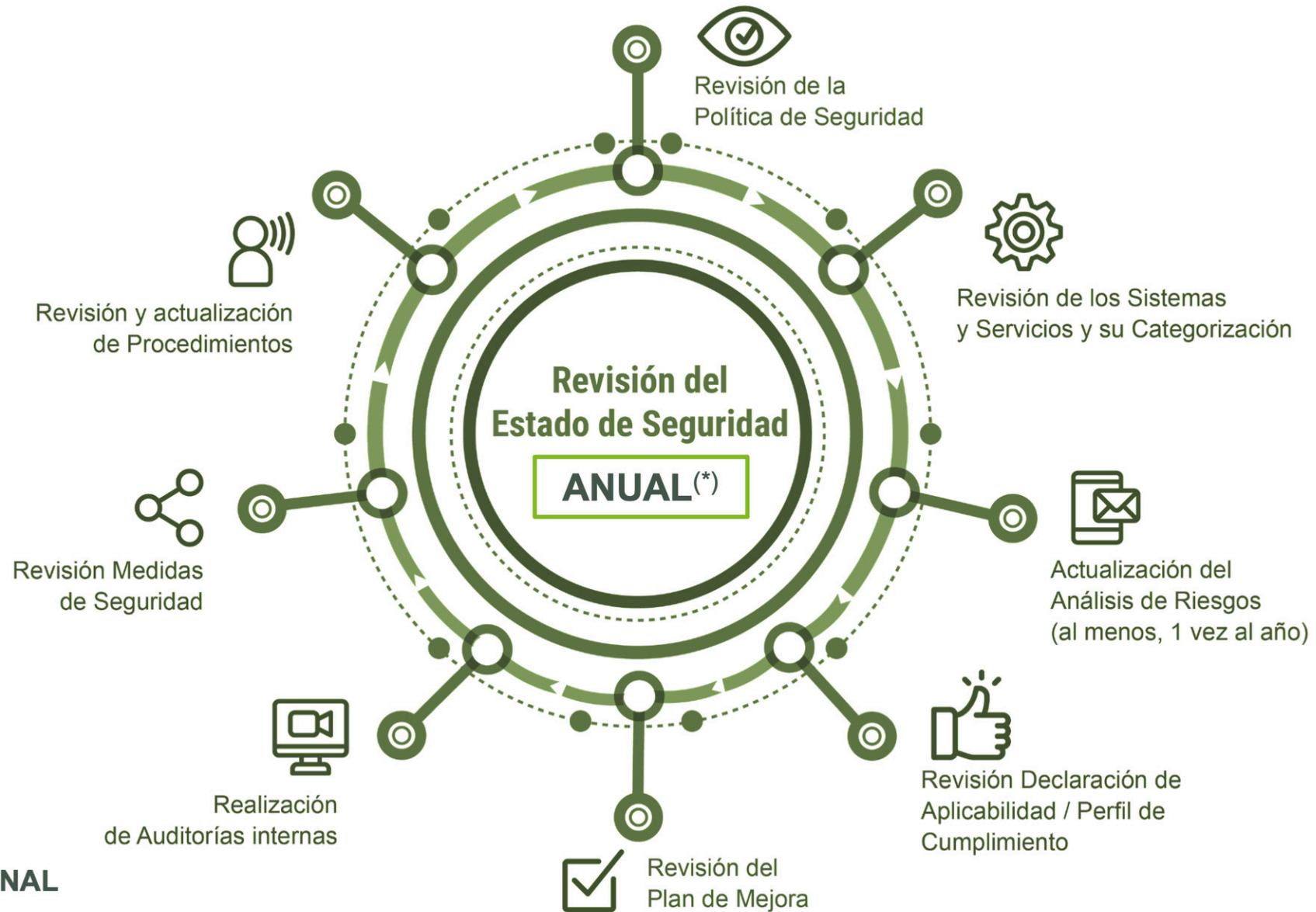
Certificación/Conformidad con el ENS



Opcionalmente y una vez obtenida la Certificación/Conformidad con el ENS, podrá ser contratado el **proceso de vigilancia y mejora continua**, donde nuestro equipo colaborará entre otras acciones en:

- Revisión de la Política de Seguridad de la Información.
- Revisión de la información y los servicios, y su categorización.
- Actualización del análisis de riesgos, al menos anualmente.
- Revisión de la Declaración de Aplicabilidad o del Perfil de Cumplimiento.
- Realización de auditorías internas.
- Revisión del Plan de Mejora.
- Revisión de las medidas de seguridad.
- Revisión y actualización de procedimientos.
- Revisión del Estado de Seguridad. INÉS.

Certificación/Conformidad con el ENS



(*) OPCIONAL



2. Condiciones económicas

Certificación/Conformidad con el ENS

Condiciones económicas

Para pertenecer a una **categoría de organización** se debe cumplir el límite de número de empleados y no superar la cifra volumen de negocio. Esta categorización se ha hecho siguiendo la **definición de PyME** de la Unión Europea.

Características de la organización	Número de empleados	Volumen de negocio
Micro	Menos de 10 empleados	Menos de 2 millones de EUR
Pequeña	De 11 a 50 empleados	Entre 2-10 millones de EUR
Mediana	De 51 a 250 empleados	Entre 10-50 millones de EUR
Grande	Más de 250 empleados	Más de 50 millones de EUR

Existen a veces, subvenciones para su implantación, en forma de concesión de ayudas. Podemos ayudarle a su gestión si es elegible para ellas (incluso para autónomos).

Condiciones económicas

Categoría: **BÁSICA**

Memoria técnica con la revisión completa de toda la documentación necesaria para solicitarla en caso de existir subvención aplicable para su implantación: **500 euros*** (no reembolsables o condicionado a la concesión).



CERTIFICACIÓN DE CONFORMIDAD CON EL



Esquema Nacional de Seguridad

Categoría **BÁSICA**

RD 3/2010

Micro
9.000 € *



CERTIFICACIÓN DE CONFORMIDAD CON EL



Esquema Nacional de Seguridad

Categoría **BÁSICA**

RD 3/2010

Pequeña
12.000 € *



CERTIFICACIÓN DE CONFORMIDAD CON EL



Esquema Nacional de Seguridad

Categoría **BÁSICA**

RD 3/2010

Mediana
18.000 € *



CERTIFICACIÓN DE CONFORMIDAD CON EL



Esquema Nacional de Seguridad

Categoría **BÁSICA**

RD 3/2010

Grande
21.000 € *

(*) Impuestos vigentes no incluidos.

Condiciones económicas

Categoría: **MEDIA**

Memoria técnica con la revisión completa de toda la documentación necesaria para solicitarla en caso de existir subvención aplicable para su implantación: **500 euros*** (no reembolsables o condicionado a la concesión).



CERTIFICACIÓN DE CONFORMIDAD CON EL



Esquema Nacional de Seguridad

Categoría MEDIA

RD 3/2010

Micro
12.000 € *



CERTIFICACIÓN DE CONFORMIDAD CON EL



Esquema Nacional de Seguridad

Categoría MEDIA

RD 3/2010

Pequeña
15.000 € *



CERTIFICACIÓN DE CONFORMIDAD CON EL



Esquema Nacional de Seguridad

Categoría MEDIA

RD 3/2010

Mediana
22.000 € *



CERTIFICACIÓN DE CONFORMIDAD CON EL



Esquema Nacional de Seguridad

Categoría MEDIA

RD 3/2010

Grande
25.000 € *

(*) Impuestos vigentes no incluidos.

Condiciones económicas

Categoría: **ALTA**

Memoria técnica con la revisión completa de toda la documentación necesaria para solicitarla en caso de existir subvención aplicable para su implantación: **500 euros*** (no reembolsables o condicionado a la concesión).



CERTIFICACIÓN DE CONFORMIDAD CON EL



Esquema Nacional de Seguridad

Categoría ALTA

RD 3/2010

**Micro
consultar**



CERTIFICACIÓN DE CONFORMIDAD CON EL



Esquema Nacional de Seguridad

Categoría ALTA

RD 3/2010

**Pequeña
consultar**



CERTIFICACIÓN DE CONFORMIDAD CON EL



Esquema Nacional de Seguridad

Categoría ALTA

RD 3/2010

**Mediana
consultar**



CERTIFICACIÓN DE CONFORMIDAD CON EL



Esquema Nacional de Seguridad

Categoría ALTA

RD 3/2010

**Grande
consultar**

(*) Impuestos vigentes no incluidos.



© 2022 CS³ GROUP. Todos los derechos reservados.

Todas las demás marcas comerciales, productos, servicios, logotipos, imágenes, etc. referenciados aquí son propiedad de sus respectivos dueños. La información presentada es exclusivamente con propósitos informativos y únicamente expresa la opinión del autor en el momento de su publicación. CS³ GROUP no puede garantizar la veracidad y licitud del contenido o información aquí presentada. CS³ GROUP ofrece TODO EL MATERIAL Y EL CONTENIDO DE ESTA PRESENTACION "COMO ESTÁ", SIN NINGUNA GARANTÍA EXPRESA O TÁCITA DE NINGÚN TIPO, INCLUYÉNDOSE SIN LIMITACIÓN LAS GARANTÍAS DE QUE EL PRODUCTO O SERVICIO SEA COMERCIALIZABLE, NO INFRACTORA DE LA PROPIEDAD INTELECTUAL DE NADIE, O IDÓNEA PARA UN DETERMINADO PROPÓSITO. CS³ GROUP NO TIENE NINGUNA OBLIGACIÓN DE PAGAR INDEMNIZACIÓN POR DAÑOS Y PERJUICIOS DE NINGÚN TIPO (INCLUYENDO, ENTRE OTRAS, LA PÉRDIDA DE GANANCIAS, PÉRDIDA DE EXPLOTACIÓN, PÉRDIDA DE INFORMACIONES) PRODUCIDOS POR EL USO O POR LA INCAPACIDAD DE USAR EL MATERIAL Y/O INFORMACION AQUÍ PRESENTADA.

