CIBERSEGURIDAD Y RD 43/2021

Nuevas obligaciones en ciberseguridad para empresas esenciales

edorteam

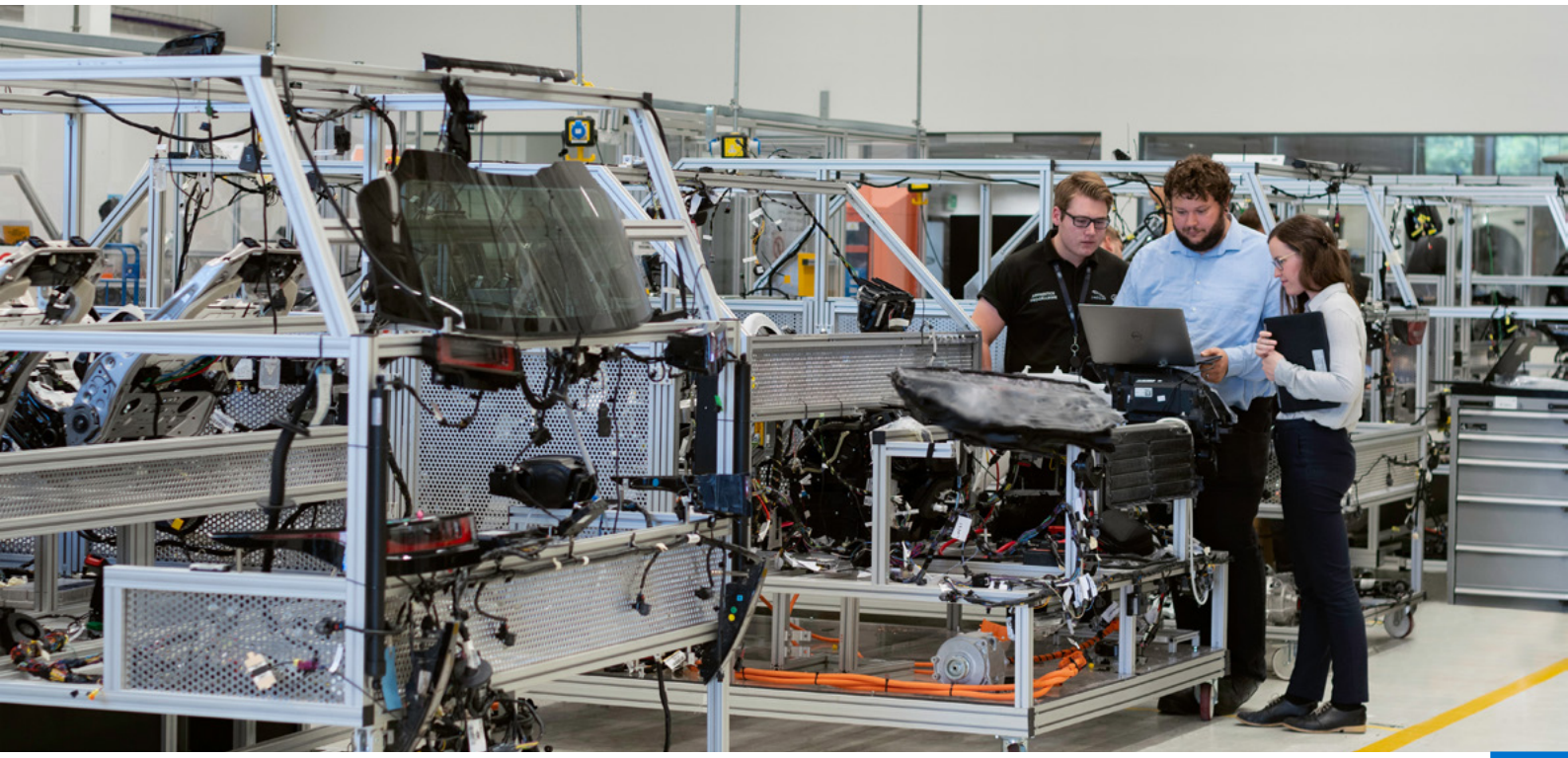
Llegan importantes cambios con el Real Decreto 43/2021

La ciberseguridad, esencial en 2021

En vigor el Real Decreto 43/2021, un antes y un después para la ciberseguridad de muchas empresas

El 27 de enero entró en vigor el Real Decreto 43/2021 por el que se desarrolla el Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

La aprobación de esta normativa supone un hito para la ciberseguridad de las empresas porque establece **importantes cambios para un gran número de éstas**: Operadores de Servicios Esenciales y Proveedores de Servicios Digitales.



¿Por qué se aprueba esta normativa?

Con este Real Decreto se quiere acabar con las políticas de ciberseguridad insuficientes que todavía encontramos en muchas empresas, y está motivado por el **crecimiento exponencial de los ciberataques** durante el último año, aprovechando la situación pandémica y el auge del teletrabajo y el comercio electrónico.

Dicho de otra manera, la normativa quiere impulsar iniciativas para que las empresas de servicios esenciales **alcancen un nivel de ciberseguridad adecuado**. Se considera que empresas de servicios esenciales como energéticas, salud, gestión de residuos o alimentación, deben **reducir al máximo sus riesgos** de sufrir una ciberincidencia que paralice su actividad laboral.

✓

Estos cambios deben llevarse a cabo en unos plazos de tiempo muy breves y tienen un alto impacto en la gobernanza de la ciberseguridad de las empresas.

¿Por qué supone un antes y un después?

Si tu empresa ya disponía de una **política de ciberseguridad rigurosa**, será mucho más fácil adaptarte a la nueva normativa. Por el contrario, si la ciberseguridad en tu empresa siempre ha sido un tema secundario, hay mucho trabajo por delante:

- Afecta a un **gran número de empresas**: los Operadores de Servicios Esenciales y los Proveedores de Servicios Digitales. En la siguiente página hablamos más en detalle.
- Obliga a estas empresas a **designar o contratar un nuevo cargo profesional**: el Responsable de Seguridad de la Información, un perfil con altas exigencias técnicas.
- El profesional designado para el cargo debe desarrollar un plan de ciberseguridad para su empresa y presentar ante las autoridades la **Declaración de Aplicabilidad**.
- Se establece un **plazo de tiempo muy limitado** para cumplir con estas obligaciones: una primera fecha límite en abril y una segunda en julio.

¿Qué empresas están obligadas a cumplir el RD 43/2021?

Conforme a lo establecido en el artículo 2 del RD 43/2021, las organizaciones obligadas se dividen en dos grandes grupos:

1. **Operadores de Servicios Esenciales**, es decir, empresas que pertenecen a sectores denominados como **Infraestructura Crítica** por La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016 (conocida como Directiva NIS).

   Los sectores de Infraestructura Crítica proporcionan los servicios necesarios para el mantenimiento de las **funciones sociales básicas**: salud, seguridad, bienestar social y económico de los ciudadanos, o eficaz funcionamiento de las instituciones del Estado y las Administraciones Públicas.

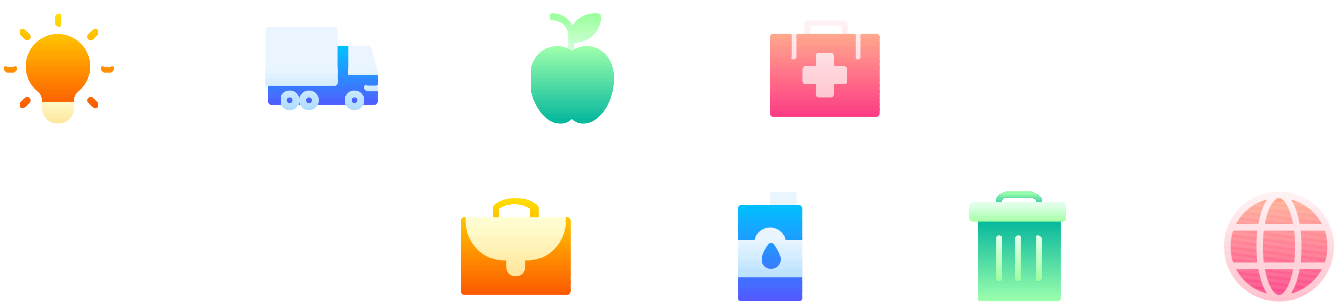
   En la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, se establecen cuáles son estos sectores de actividad:

   - » **Administración**
   - » **Agua**
   - » **Alimentación**
   - » **Energía**
   - » **Espacio Exterior**
   - » **Industria Nuclear**
   - » **Industria Química**
   - » **Instalaciones de Investigación**
   - » **Sanidad**
   - » **Sistema Financiero y Tributario**
   - » **Tecnologías de la Información y las Comunicaciones (TIC)**
   - » **Transporte**

2. **Proveedores de Servicios Digitales**, específicamente:

   - » **Mercados en línea** (plataformas de venta de productos y/o servicios de terceros)
   - » **Motores de búsqueda en línea**
   - » **Servicios en la nube**

   Dentro de este segundo grupo, están exentas las pequeñas empresas o microempresas (menos de 50 trabajadores o menos de 10 millones de euros de facturación anual).



¿Cuáles son las obligaciones derivadas del RD 43/2021?

1

Designar al Responsable de Seguridad de la Información o CISO *(Chief Information Security Officer)*

Esta figura puede ser una persona, entidad u órgano colegiado, y se nombrará ante el Ministerio correspondiente (según sector de la empresa) como máximo el **27 de abril de 2021**.

Ejercerá como punto de contacto con la autoridad competente y supervisará que la empresa cumple con los requisitos de ciberseguridad establecidos.

2

Elaborar la Declaración de Aplicabilidad

Conforme a lo establecido en el artículo 6 del RD 43/2021, el CISO debe realizar un documento denominado Declaración de Aplicabilidad de las **medidas de seguridad** de la empresa.

A grandes rasgos, debe incluir:

- Análisis del **estado actual** de la ciberseguridad de la empresa con el fin de identificar carencias y riesgos.
- Reflejar las **deficiencias** detectadas y cómo se pretenden solucionar.
- Desarrollar un plan de seguimiento para **verificar** que estas deficiencias se acaben subsanando.
- Establecer **planes** para la detección, gestión, recuperación y aseguramiento de la continuidad de las operaciones en caso de ciberincidente.

3

Firmar y presentar la Declaración de Aplicabilidad

La Declaración de Aplicabilidad debe ser firmada por el CISO y aprobada por la empresa. Finalmente, se presentará ante la autoridad competente como muy tarde el **27 de julio de 2021**.

Además, la Declaración de Aplicabilidad será **revisable** como mínimo cada 3 años.

¿Qué otras funciones realiza un CISO?

Desempeñará las funciones recogidas en el artículo 7 del RD 43/2021:

- **Prevenir y reducir** al máximo los efectos de ciberincidencias que pudieran producirse.
- **Supervisar** y desarrollar la aplicación de las políticas de seguridad, normativas y procedimientos, así como llevar a cabo controles periódicos de seguridad.
- **Promover y velar** por unas buenas prácticas en ciberseguridad dentro de la empresa.
- **Remitir a la autoridad competente**, a través del CSIRT de referencia y sin dilación indebida, las notificaciones de incidentes que tengan efectos perturbadores en la prestación de servicios esenciales.
- Actuar como punto de **contacto con la autoridad competente** en materia de supervisión de los requisitos de seguridad de las redes y sistemas de información.
- Actuar como punto de contacto especializado para la coordinación de la **gestión de los incidentes** con el CSIRT de referencia.

¿Quién debería ser el CISO de la empresa?

Por la naturaleza y complejidad de sus funciones, recomendamos que el CISO de tu empresa sea un **profesional técnico con conocimientos especializados en seguridad informática**, a poder ser contratado específicamente para este cargo o, en todo caso, promocionado tras recibir la formación complementaria que pueda necesitar.

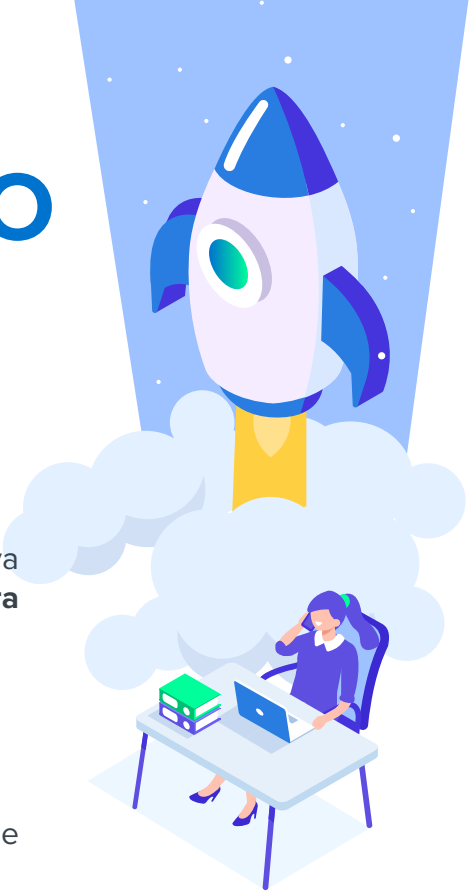
El perfil profesional debería contar con estas capacidades:

- **Conocimientos informáticos avanzados**, a poder ser con titulación universitaria en Ingeniería Informática o similar.
- Conocimientos especializados y experiencia en materia de **ciberseguridad** desde los puntos de vista organizativo, técnico y jurídico.
- Capacidad para participar en todas las cuestiones relativas a la seguridad, manteniendo una **comunicación** real y efectiva con la dirección de la empresa.
- Capacidad de **independencia** con respecto a los responsables de las redes y los sistemas de información de la empresa.

Edorteam, un valioso apoyo para tu CISO

Con nuestro Plan CISO Asesor, acompañamos a tu empresa en su adaptación al RD 43/2021

La figura del CISO requiere de altas capacidades y conlleva importantes responsabilidades. **Confía en Edorteam para guiar y acompañar** al futuro CISO de tu empresa:



Análisis de situación

- Analizamos el estado actual de la ciberseguridad de la empresa.
- Identificamos posibles riesgos y amenazas.
- Asesoramos a la dirección para designar al CISO de la empresa.

Definición de objetivos

- Trabajamos codo con codo con el CISO en la elaboración de un Plan de Ciberseguridad para la empresa.
- Definimos los objetivos estratégicos a alcanzar en materia de ciberseguridad y cómo solucionarlos.

Acciones de mejora

- En caso de necesitar soluciones software para mejorar la ciberseguridad de la empresa, nos encargamos de su implantación en todos los equipos informáticos.
- Formamos en su uso a tus profesionales, promoviendo unas buenas prácticas en ciberseguridad.

Apoyo y seguimiento

- Asesoramos a tu CISO en la presentación de la Declaración de Aplicabilidad.
- Supervisamos la eficacia de las medidas aplicadas.
- Mantendremos contacto directo para resolver incidentes técnicos o de seguridad digital.

✓

En Edorteam cuentas a la vez con un departamento legal y un departamento informático especialista en soluciones de ciberseguridad.

✓

El servicio es integral: no solo identificamos las mejoras a realizar, también nos encargamos de su implantación en la empresa.

✓

En el sector desde 1992, una sólida experiencia y conocimiento especializado nos avalan.

¿Empezamos?

Adapta tu empresa a la nueva normativa

Contáctanos en
www.edorteam.com

edorteam
DESDE 1992

Madrid
C/ Isabel Colbrand 6, 5º
28050 Madrid
91 344 69 10

Lleida
Avenida Madrid 38, 2º-2ª
25002 Lleida
973 248 601

info@edorteam.com

www.edorteam.com