

2025



conetic
Confederación Española de Empresas de Tecnologías
de la Información, Comunicaciones y Electrónica

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD



ESTUDIO

SECTOR CIBERSEGURIDAD

EMPRESAS EN TERRITORIO ESPAÑOL

A fecha de **01/12/2025**

Resumen Ejecutivo

 **Financiado por
la Unión Europea**
NextGenerationEU



GOBIERNO
DE ESPAÑA

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO
DE TELECOMUNICACIONES
E INFRAESTRUCTURAS DIGITALES



Plan de
Recuperación,
Transformación
y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD



2025

ESTUDIO SECTOR CIBERSEGURIDAD

EMPRESAS
EN TERRITORIO ESPAÑOL

Estudio del sector de la ciberseguridad, empresas en territorio español 2025.

Resumen Ejecutivo

Índice

Metodología	03
Infografía «Datos clave del sector ciberseguridad»	04

Indicadores

1. Volumen de empleo	05
2. Estimación de fuerza laboral	06
3. Facturación	07
4. Demanda de personal formado	08
5. Información general sobre empresas	09
6. Mujeres en la ciberseguridad	11
7. Comparativa con otros países	12
8. Actividad de las empresas	13
9. Sujetos obligados de la NIS2	16
10. Entidades formadoras en ciberseguridad	18



Metodología

Recogida de datos
abril y mayo **2025**



- **Campaña telefónica**
- **Campaña de e-mailing**
- **Formulario web** de 40 preguntas por secciones

Contacto a empresas:



registradas en **Kit Consulting** y **Kit Digital**, asociadas de **CONETIC** y aquellas con relación **CPI** con **INCIBE**



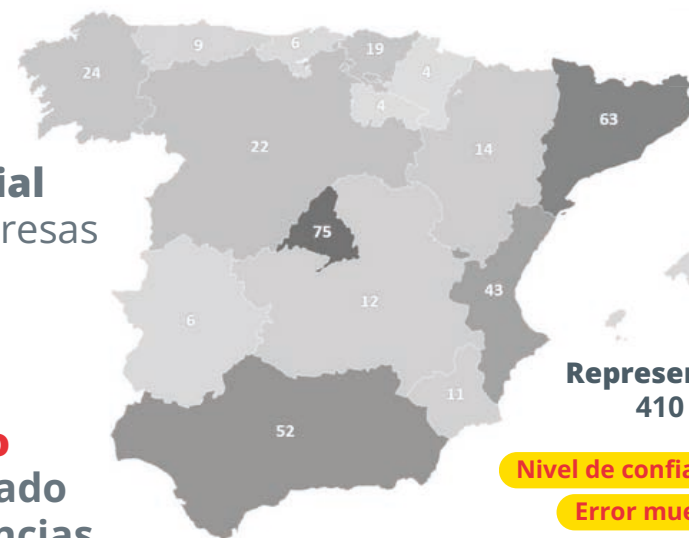
Concentración de empresas en grandes núcleos poblacionales



Base inicial
5639 empresas



Muestreo
estratificado
por **provincias**



Representatividad
410 respuestas

Nivel de confianza del 95%

Error muestral del 5%

Respuestas
recibidas

517



Respuestas
optimizadas

392

Soluciones y servicios seleccionados de la oferta registrada por las empresas en **Kit Consulting** y **Kit Digital**:

- Soluciones en Ciberseguridad
- Soluciones para las Comunicaciones Seguras
- Soluciones para un Puesto de Trabajo Seguro
- Servicio de Asesoramiento en Análisis de Datos (Avanzado)
- Servicio de Asesoramiento en Análisis de Datos (Básico)
- Servicio de Asesoramiento en Ciberseguridad (Avanzado)
- Servicio de Asesoramiento en Ciberseguridad (Básico)
- Servicio de Asesoramiento en Ciberseguridad (Preparación para Certificación)



Datos clave del sector ciberseguridad

1. Volumen de empleo actual



25,55% del **empleo TIC** es en **ciberseguridad**.

164.761
empleados

2024

- Las **empresas de ciberseguridad** (3.431) representan un **4,47%** del total **TIC** (76.828)
- **Volumen de empleo actual** de **164.761** empleados.

2. Facturación actual



4,65% de la **facturación TIC** es en **ciberseguridad**.

6.351
millones de €

2024

- **Empresas jóvenes** (403) facturan el **12%**.
- «**Emprendimiento INCIBE**» agrupa al **7%** de las **empresas de ciberseguridad** en España.

3. Estimación de fuerza laboral



14,25% de **crecimiento anual** en **ciberseguridad**.

282.157
empleados

2029

- **Previsión**, alcanzar **282.157 empleados** para 2029.
- **Modelo de predicción de la demanda:**
 - **Profesionales** formados
 - **Ataques** sufridos
 - **Incidentes** reportados
 - **PIB** nacional del sector
 - **Servicios de adaptación** a la NIS2 ofrecidos.

4. Demanda de personal formado



71,25% de **aumento** en el **mercado laboral** en ciberseguridad.

117.396
profesionales

2029

- **Previsión**, alcanzar **117.396 profesionales** en 2029.
- **Necesidad de incremento de la oferta formativa** pública y privada en un **76%**.
- **2025**, formación reglada (58%) y no reglada (42%).
- **Sistema formativo actual**, cubrirá el **24%** de la **demanda** 5.530 profesionales para 23.479 puestos.

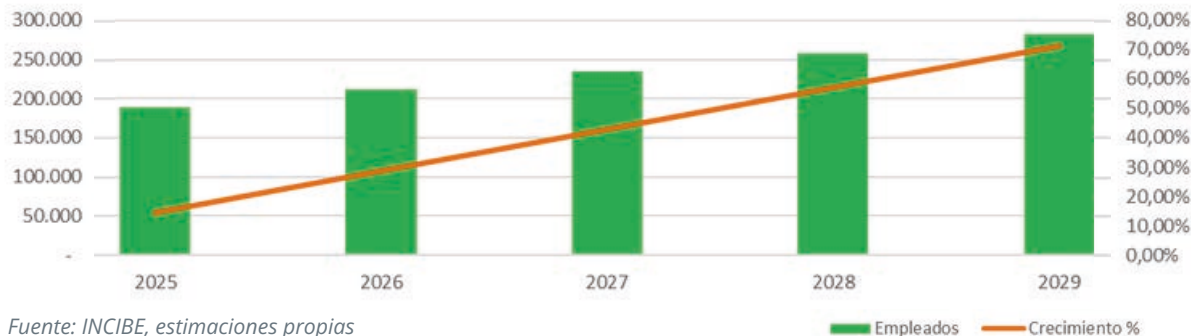
Estimaciones: con datos de las fuentes oficiales más recientes y los recabados *ad hoc* en el formulario del estudio.

Proyecciones: toman de referencia las estimaciones contrastables para 2024 y se proyectan hasta el 2029.



Volumen de empleo

Estimación de crecimiento de la fuerza laboral en el Sector Ciberseguridad
(en número de empleados)



PROCESO DE ESTIMACIÓN

La estimación en este estudio tuvo en cuenta las respuestas dadas por las empresas de la muestra y por otro la información proporcionada por el DIRCE (Directorio Central de Empresas) del INE (Instituto Nacional de Estadística) para el año 2023 en los «Indicadores del Sector de las Tecnologías de la Información y de las Comunicaciones (TIC)» publicados a fecha de julio de 2025.

El número total de empresas del Sector Ciberseguridad (3.431), se obtuvo escalando el porcentaje de respuesta obtenido en el formulario para la pregunta [35] ¿Está su empresa incluida en el Catálogo de empresas de ciberseguridad de INCIBE?, donde el 31% de las empresas de ciberseguridad dicen pertenecer al «Catálogo de empresas de ciberseguridad de INCIBE», dato contrastable a nivel nacional gracias a la información real propia sobre el número exacto de empresas que están registradas correctamente en este catálogo propio de INCIBE.

Añadido a esto, se estableció la cifra de empleados de media por intervalo según el tamaño de las empresas, escalándose a nivel nacional los resultados de respuesta a la pregunta [5] ¿Cuántos empleados tiene su empresa? del formulario y aplicando estas mismas medias por intervalo a los datos del Sector TIC y poder hacer la comparativa.

El crecimiento anual del 14,25% se corresponde a 23.479 nuevos puestos creados para el año 2025.

EMPLEO ACTUAL

164.761
empleados
en ciberseguridad



2024

14,25%
crecimiento
anual

Las **empresas de ciberseguridad (3.431)** representan un **4,47%** del total **TIC (76.828)**

El empleo actual en ciberseguridad representa el **25,55%** del **Sector TIC, 644.870 empleados.**

Modelo de estimación de la demanda de empleo

- ➖ **Profesionales** formados
- ➕ **Ataques** sufridos
- ➕ **Incidentes** reportados
- ➕ **PIB** nacional del sector
- ➕ **Servicios de adaptación** a la NIS2 ofrecidos.

Uso de **factores relacionados** con la empleabilidad en el **sector de la ciberseguridad** para realizar la predicción.

Contribución ponderada de cada factor a la demanda final en función de si su hipótesis es positiva o negativa.

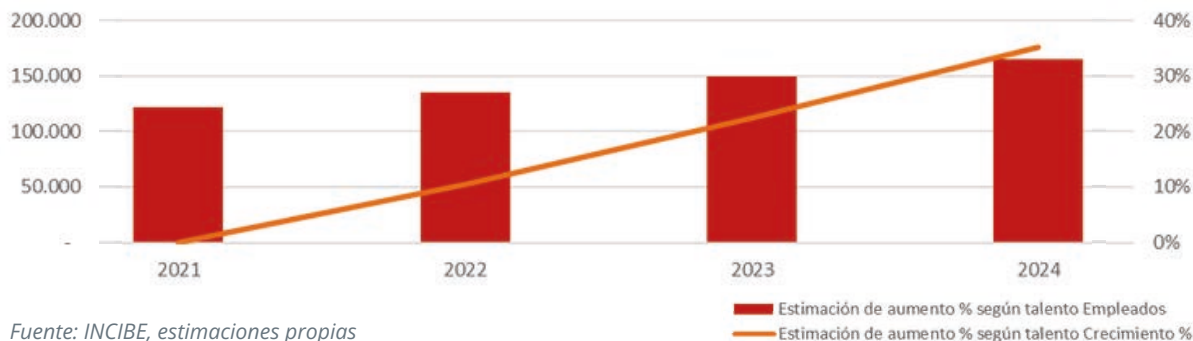
Hipótesis según su actuación en la estimación:

- ➕ Positivas, a mayor cantidad del factor, mayor demanda.
- ➖ Negativas, a menor cantidad del, menor demanda.



Estimación de fuerza laboral

Estimación de crecimiento de la fuerza laboral en el Sector Ciberseguridad
(en número de empleados)



COMPARATIVA CON ESTIMACIONES PREVIAS

Los datos obtenidos para la estimación del empleo en ciberseguridad son un 0,3% inferiores a las predicciones realizadas para este mismo año por el área de Talento del propio INCIBE en el informe, «Análisis y diagnóstico del talento de ciberseguridad en España, marzo de 2022» donde la cifra de fuerza laboral que se estimaba en los 165.256 puestos de empleados en 2024, tal y como aparece reflejado en la página 63 de dicho informe en la figura 27.

Dicho esto, la tendencia es igual en ambas predicciones, un crecimiento exponencial del número de trabajadores, indicativo de que el sector de la ciberseguridad está creciendo y va a continuar con esta tendencia en los próximos años.

Además, si se mantienen las proporciones que se observan actualmente en cuanto a la relación existente entre los sectores de la Ciberseguridad y el sector TIC, tanto para el número de empleados como de empresas, también se ven reflejados dichos incrementos para el año 2029.

En este sentido, se prevé que el número de empresas que conformen el sector de la ciberseguridad llegue a las 5.876 en 2029, un 4,47% de las 131.570 empresas del sector TIC para ese mismo año.

En lo relativo a empleo, si se mantiene que el 25,55% del empleo TIC es de ciberseguridad, el sector TIC llegará a 1.104.355 empleados y el sector ciberseguridad a los 282.157 estimados con el modelo.

EMPLEO FUTURO

282.157
empleados
en ciberseguridad



2029

+

71,25%
crecimiento
desde 2024

Las **empresas de ciberseguridad (5.876)** representan un **4,47%** del total **TIC (131.570)**

El empleo futuro en ciberseguridad representaría el **25,55%** del **Sector TIC, 1.104.355 empleados.**

Modelo de estimación de la demanda de empleo

Dando como válido el modelo de estimación del volumen de empleo actual, se extrapolaron las proporciones relativas al sector TIC y la ciberseguridad obteniendo con ello las cantidades de empresas y empleados para cada sector.

En comparación, la estimación de la demanda de empleo del informe previo de Talento (165.256 empleados en ciberseguridad para el 2024), representa un 0,3% más que la estimación del nuevo modelo (164.761 empleados para el 2024).

No obstante, el nuevo modelo aumenta el porcentaje de crecimiento anual.



Facturación

Estimación de la facturación en ciberseguridad en relación a la facturación TIC

Porcentaje (%)	Intervalo de facturación	Facturación media	Facturación total
96,70%	Menos de 2 mill.		132.205.339.000 €
2,60%	Entre 2 y 10 mill.		3.554.642.000 €
0,60%	Entre 10 y 50 mill.		820.302.000 €
0,10%	Más de 50 mill.		136.717.000 €
Porcentaje (%)	Total empresas	Facturación media	Facturación total
100,00%	76.828	1.779.520 €	136.717.000.000 €

Media de Métodos /* 1. Facturación x tamaño de empresa según su definición | 2. El % dedicado a ciberseguridad en la empresa | 3. Datos del INE (facturación x tamaño).

Facturación TIC	136.717.000.000 €	100%
Facturación TIC sin Ciber	130.365.894.859 €	95,35%
Facturación ciber dentro de TIC	6.351.105.141 €	4,65%
Empresas ciber dentro de TIC	3.431	4,47%
Diferencia medias Ciber vs TIC	71.574 €	Diferencia entre facturaciones medias Ciber vs TIC
Total empresas Ciber	3.431	Facturación total Ciber 6.351.105.141 €

Facturación
Sector TIC



Facturación
Sector Ciber



FACTURACIÓN ACTUAL

6.351
millones de €
en ciberseguridad



2024

=

4,65%
de lo facturado
en TIC

Las 403 **empresas jóvenes** (de menos de 5 años) facturaron el 12% del total de la ciberseguridad.

«Emprendimiento INCIBE» agrupa al **7%** de las **empresas de ciberseguridad en España**.

LA FACTURACIÓN DE CIBERSEGURIDAD EN RELACIÓN A LA FACTURACIÓN TIC

La facturación del sector de la Ciberseguridad en España en 2024 asciende a los 6.351.105.141 €, lo que representa un 4,65% del total facturado en el mismo periodo para todo el sector TIC.

El modelo de cálculo de la facturación utilizado, combinó tres métodos distintos, con la finalidad de realizar una mejor estimación de la realidad posible.

Dicho modelo, realiza la media de las facturaciones medias por empresa obtenidas de los resultados de cálculo obtenidos según: los datos *ad hoc* del propio formulario del estudio (respuesta a la pregunta [19] ¿Qué porcentaje del volumen de negocio de su empresa es debido a la realización de actividades de ciberseguridad?), y los datos de otras fuentes representativas oficiales y actualizadas (Definición de facturación por tamaño de empresa según la Real Academia Española y facturación asociada a cada tamaño de empresa según el Instituto Nacional de Estadística).

Como resultado de la aplicación del modelo, se obtuvo que con el 4,47% de las empresas de todo el sector TIC, la ciberseguridad factura un 4,65% del total. Es decir, la ciberseguridad, con un porcentaje menor de empresas que el porcentaje facturado, factura más que otros sectores dentro de las TIC. Esto es visible en la diferencia entre las facturaciones medias, donde la facturación media de las empresas de ciberseguridad es 71.574€ superior a la facturación media de todas las empresas TIC.

Modelo de cálculo de la facturación

Se realizó una media de los resultados obtenidos a través de 3 métodos para una mejor aproximación a la realidad.

- 1 Facturación asociada al **tamaño de empresa según su definición (RAE)**.
- 2 Facturación en función del **% del negocio dedicado a ciberseguridad**.
- 3 Facturación según los **datos del INE respecto a la facturación por tamaño de empresa**.

La media de las 3 facturaciones por empresas se tomó como la facturación media final del modelo.



Demanda de personal formado

Tipología de formación	Nº de formaciones	Plazas (Media)	Éxito de la formación (%)	Total profesionales (graduados)	Total de profesionales (matriculados)
 Total de Formaciones	240	32	72%	5.530	7.680
Diferencia entre Reglada y No Reglada	43%	-	-	42%	43%
 Formación reglada	138	32	72%	3.180	4.416
 Formación no reglada	102	32	72%	2.350	3.264

CÁLCULO DE LA DEMANDA FORMATIVA EN CIBERSEGURIDAD Y LA OFERTA ACTUAL

A la hora de realizar los cálculos de la oferta formativa actual en ciberseguridad, se tomaron como referencia los registros de formaciones en los «Catálogos de Formación en Ciberseguridad de INCIBE», los cuales recopilan todas las formaciones existentes actualmente a nivel nacional en el campo de la ciberseguridad, diferenciando a las mismas según su tipología y naturaleza.

Así pues, se encontraron un total de 240 formaciones activas en España en 2025, de las cuales 138 son impartidas de forma reglada (58%) y 102 de forma no reglada (42%).

A la hora de calcular tanto el número de plazas ofrecidas, como el porcentaje de alumnos matriculados y graduados, se utilizaron las estimaciones del área de Talento del propio INCIBE, en el informe «Análisis y diagnóstico del talento de ciberseguridad en España, marzo de 2022», donde se establece una media de 32 plazas disponibles por formación y una tasa de éxito de finalización del 72%, todo ello independientemente de la naturaleza o tipología que tenga la misma.

Aplicado estas proporciones en los cálculos, se obtuvo el número total de alumnos matriculados (7.680) y graduados (5.530) y su división por tipología y naturaleza de la formación, dato que si asociamos a la demanda de empleo estimada previamente de 23.476 nuevos puestos para 2025, nos da una cobertura del 24% de las plazas con 5.530 profesionales para 23.479 puestos a cubrir.

FORMACIÓN NECESARIA

117.396

profesionales
en ciberseguridad



2029

+

71,25%

aumento del
mercado laboral

Se prevé un **aumento del 71,25% en el mercado laboral de ciberseguridad** para 2029.

Se **necesitarán 117.396 nuevos profesionales** en ciberseguridad para 2029.

Modelo de cálculo de la **demanda formativa**

La **formación actual en ciberseguridad (2025)** es **reglada en un 58% y no reglada en un 42%.**

Sabiendo esto, el modelo utilizó los **registros de todas las tipologías de formaciones** nacionales en ciberseguridad y su porcentaje de graduados para calcular el número total de nuevos profesionales.

El **sistema formativo actual cubrirá el 24% de la demanda**, con **5.530 nuevos profesionales para 23.479 nuevos puestos** a cubrir en 2025.

Estos datos indican la **necesidad de un incremento de la oferta formativa**, tanto público como privada en un **76%.**



Información general sobre empresas

➤ Participación en iniciativas públicas:

Del total de empresas partícipes, **el 91% está presente en el Kit Digital y el 59% en Kit Consulting.**
El nivel de satisfacción con ambas iniciativas es **alto en un 30%** **medio en un 46%** y **bajo en un 24%.**



red.es

➤ Localización y expansión geográfica:

Un **10%** tiene presencia internacional



Mayor presencia:

Latinoamérica, Europa y América del Norte



Menor presencia:

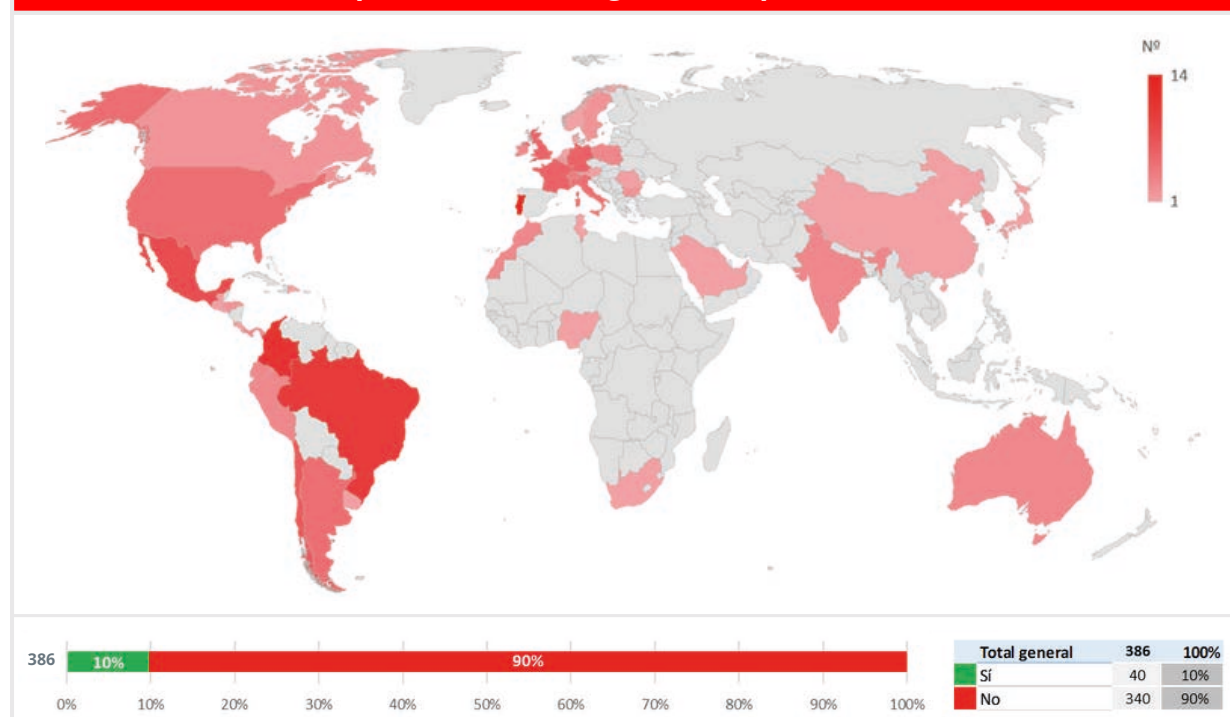
África, Asia y Oceanía.

PRESENCIA DE LAS EMPRESAS DE CIBERSEGURIDAD ESPAÑOLAS A NIVEL INTERNACIONAL

A nivel internacional, las empresas españolas están presentes en países localizados fuera de España en el 10% de los casos.

Dentro de las empresas presentes internacionalmente, se puede ver que por la tipología de países del listado indicado por las empresas en el mapa de la derecha, el sector de la ciberseguridad español está muy globalizado.

Presencia de las empresas de ciberseguridad españolas a nivel internacional



No obstante, esta presencia no es homogénea para todos los países, por lo que se destacan áreas concretas que agrupan una mayor cantidad de presencia empresarial.

Las zonas de mayor presencia se localizan en Latinoamérica y Europa, especialmente en los países de Portugal, Colombia, Alemania, Brasil y Chile.

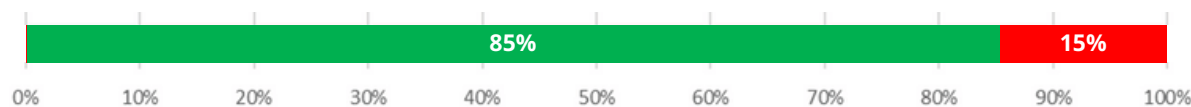
En el caso opuesto, también se pueden destacar áreas donde directamente no existe presencia empresarial o esta es muy reducida. Estas zonas se localizan en África y Asia donde se tienen pocos registros de empresas en los países de: Marruecos, Nigeria, Sudáfrica, Emiratos Árabes Unidos, India, China, Corea del Sur y Australia.



Información general sobre empresas

➤ Perfiles profesionales:

El perfil más común, observado es **«Gobernanza, Estrategia y Gestión»** con un 25% de la tasa de respuesta de la muestra. El **85% cuenta con al menos un profesional especializado en algún ámbito de la ciberseguridad.**



Total	374	100%
Tienen algún perfil de profesional ciber	327	85%
Ningún perfil	59	15%

PERFILES PROFESIONALES EN CIBERSEGURIDAD Y AGRUPACIÓN POR ÁMBITOS

Se realizó una agrupación de los perfiles profesionales por ámbitos en función de la relación y similitud existente entre los perfiles indicados por las empresas.

- La agrupación más común con el 25% de la tasa de respuesta fue la «Gobernanza, Estrategia y Gestión», con un total de 2.328 perfiles entre los que se incluyen: CISO (344), Responsable de Cumplimiento (571), Auditor de Ciberseguridad (663) y Gestor de Riesgos de Ciberseguridad (750).
- La segunda agrupación de ámbitos más común, «Operaciones y respuesta» cuenta con el 23% de la tasa de respuesta y 2.101 perfiles como: Personal de Respuesta Ante Incidentes (1.298), Forense Digital (317) y Penetration Tester (486).
- La tercera agrupación de ámbitos, «Diseño e implementación técnica» cuenta con el 20% de la tasa de respuesta y 1.875 perfiles asociados, entre los que destacan: Arquitecto de Ciberseguridad (480) e Implementador de Ciberseguridad (1.395).
- La cuarta agrupación más común, serían «Otro/s», con el 16% de las respuestas y 1.446 perfiles de muy diversa naturaleza según la información aportada por las empresas y con la que no se puede extraer una pertenencia a ninguna de las demás agrupaciones de ámbitos.
- La quinta agrupación, está representada bajo el nombre «Análisis, inteligencia y auditoría», la cual representa al 12% de la muestra con 1.108 perfiles: Analista de Ciberinteligencia (531) e Investigador de Ciberseguridad (577).
- La última de las agrupaciones, «Concienciación y formación», representa al 4% de la muestra estudiada con 377 perfiles asociados a Educadores y Formadores en Ciberseguridad (377).

➤ Certificaciones en ciberseguridad:

El **44% de las empresas cuenta con al menos una certificación** vinculada con la **ciberseguridad.**



Las respuestas de las empresas en cuanto al número y tipo de certificaciones más común:

ENS 21 %, ISO 27001 25 %, ENS e ISO27001 a la vez 26%.



Mujeres en la ciberseguridad

➤ Mujeres en las empresas de ciberseguridad:

En España, la **diferencia entre hombres y mujeres** empleados es de **60 puntos porcentuales** por motivos de género (2024).

De un total de **71.035 empleados, encuestados**, se obtuvo que un **80% de ellos son hombres**

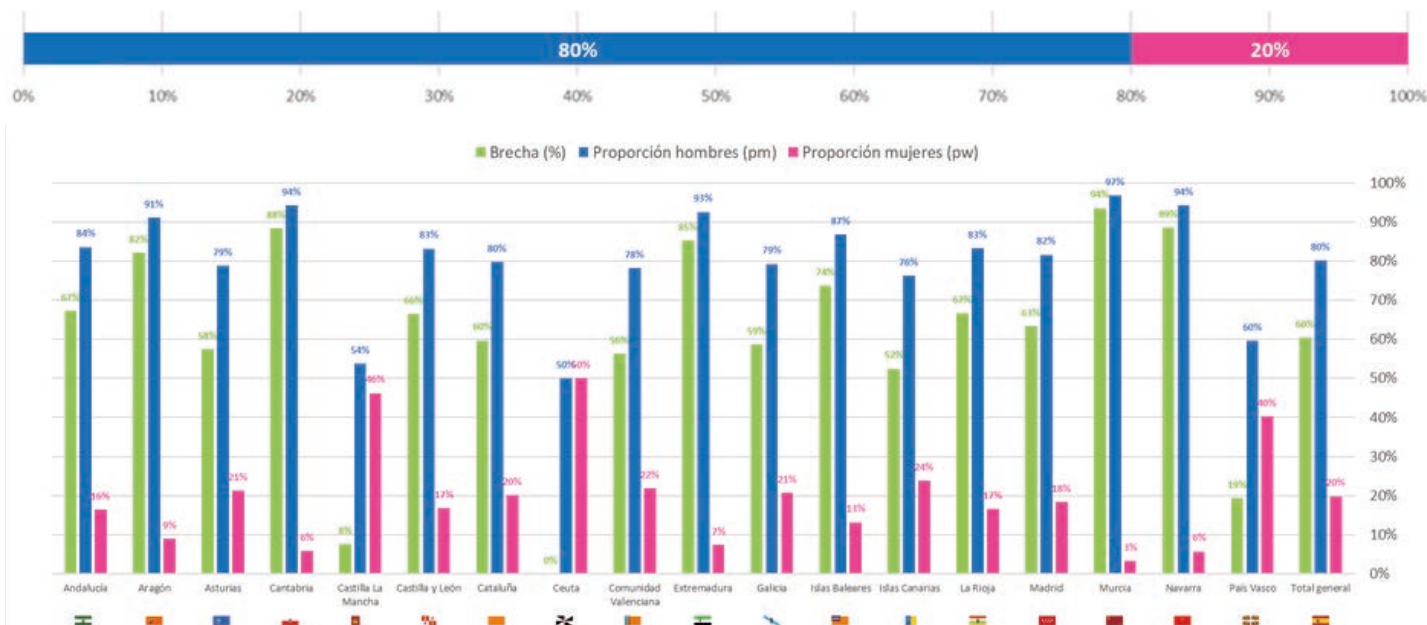


♀ **20%**

La **inclusión actual** (2024) de las mujeres del **sector de la ciberseguridad (20%)**, es superior al dato registrado para el sector TIC (19,57%) en el año 2024 según Eurostat.



Estimación de la brecha de género entre mujeres y hombres empleados en ciberseguridad



Método de cálculo para la brecha de género

La brecha de género fue calculada como la **diferencia porcentual entre el número de hombres y mujeres** que indicaron las empresas como respuesta a la pregunta [6] ¿Cuál es el número de mujeres que componen su plantilla?

Vinculado a este proceso, también se la **media nacional** de mujeres por empresa de de ciberseguridad, establecida en **36 mujeres/empresa**.

A nivel de comunidades autónomas: destaca el **País Vasco** por tener una **mayor inclusión** y **Extremadura** por tener la **menor inclusión** de las mujeres en las empresas.



Comparativa con otros países

➤ Comparativa en ciberseguridad de España con otros países (facturación):

España aporta más del 12% de la facturación europea en ciberseguridad, lo que supone un **2,8% a nivel mundial**.

FACTURACIÓN DE LAS EMPRESAS DE CIBERSEGURIDAD A NIVEL MUNDIAL (COMPARATIVA POR ZONAS)

A la hora de establecer una comparativa por zonas geográficas que permitiera saber la posición que ocupa España en el ámbito mundial para la ciberseguridad con el resto de potencias y países, se recurrió a la facturación como dato indicativo de dicha realidad.

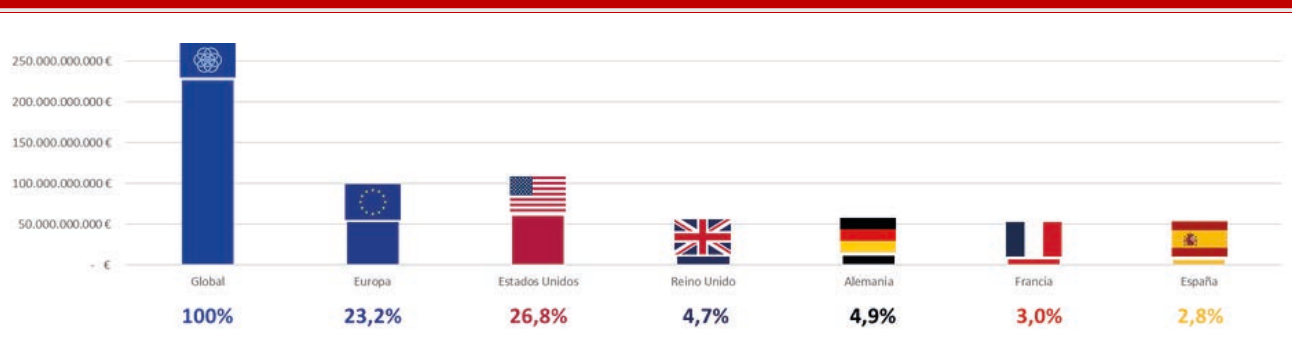
La elección de la facturación y no otra magnitud vino derivada de la dificultad de encontrar un dato de medición que fuera común entre todas las zonas geográficas y que a su vez fuese bastante representativo del progreso en ciberseguridad que tienen las mismas.

Así las cosas, se consultaron fuentes como el ICEX (España, Exportación e Inversiones) para obtener los datos para las principales potencias sobre las que establecer la comparativa. No obstante, en algunas ocasiones, estas magnitudes de facturación se encontraban en dólares y no euros, por lo que se procedió a convertir la cifra para todas las zonas a comparar en las dos monedas.

Dicho esto, la selección de zonas se basó en la importancia que representan dentro del sector y la cercanía y características comunes con respecto a España. Fruto de esta comparativa, España representa el 12% de la facturación de todos los países europeos y un 2,8 % de toda la facturación de los países a nivel global.

Zona geográfica	% Mercado	US\$M	Millones de €
 Global (Total)	100%	\$ 245.621.200.000	225.971.504.000€
 Europa	23,20%	\$ 56.963.383.150	52.406.312.498€
 Estados Unidos	26,80%	\$ 65.831.500.000	60.564.980.000€
 Reino Unido	4,70%	\$ 11.576.700.000	10.650.564.000€
 Alemania	4,90%	\$ 11.993.000.000	11.033.560.000€
 Francia	3,00%	\$ 7.260.600.000	6.679.752.000€
 España	2,80%	\$ 6.903.375.153	6.351.105.141€

Comparativa de facturaciones en ciberseguridad por zonas geográficas a nivel mundial





Actividad de las empresas



➤ Oferta de productos y servicios:

El **80 %** de las empresas de la muestra ofrece al menos un servicio tipo TIC.

Se han detectado **zonas con el 100 % de las empresas ofertando este tipo de servicios.**

CC.AA: Cantabria, Extremadura, Islas Baleares, Islas Canarias, La Rioja, Navarra, y el País Vasco.

➤ Porcentaje de negocio dedicado a la ciberseguridad:

Un **44,44%** dedica más del 25 % del negocio a ciberseguridad.
Mayor especialización en País Vasco e Islas Baleares.

Mayor porcentaje dedicado a ciberseguridad en las **asociadas a CONETIC**



OFERTA DE PRODUCTOS Y PORCENTAJE DEL NEGOCIO DEDICADO A LA CIBERSEGURIDAD

Si bien el 80% de las empresas encuestadas dice ofrecer al menos un servicio de tipo TIC, en algunas zonas geográficas la oferta de estos servicios es superior y especialmente alta, dado que el 100% de las empresas oferta al menos un servicio de estas características. Dentro de las zonas con esta oferta superior se encuentran las comunidades autónomas de: Cantabria, Extremadura, Islas Baleares, Islas Canarias, La Rioja, Navarra, y el País Vasco.

Respecto al porcentaje del negocio que tienen las empresas dedicadas a la ciberseguridad, este es superior al 25% en el 44,44% de los casos aunque en algunas zonas como el País Vasco e Islas Baleares este se incrementa. Añadido a esto, también se observó un mayor porcentaje en las empresas asociadas a CONETIC.

➤ Innovación y desarrollo:

Un **26%** de las empresas dicen tener un producto pendiente de ser lanzado al mercado.

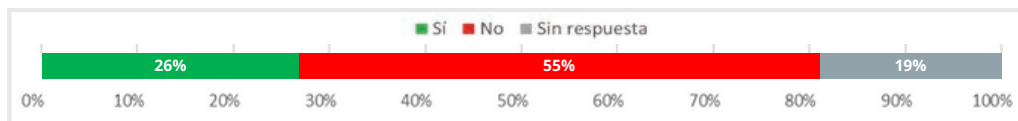


INNOVACIÓN Y DESARROLLO EN CIBERSEGURIDAD

El 26% de las empresas encuestadas tienen un producto pendiente de lanzar al mercado, mientras que el 19% desconoce si lo va a lanzar o no y el 55% niega tener intención de hacerlo.

La comunidad autónoma más propicia para el lanzamiento es Cantabria con un 67% de las empresas con una actividad lista para ello.

Por el lado contrario, en La Rioja, ninguna de las empresas tiene previsión de lanzar actividades al mercado.





Actividad de las empresas

► Actividades representativas de negocio y ámbitos de actuación:

Un 69 % enfoca su actividad a la formación/consultoría, un 25 % a la fabricación.
«Protección (PR)» es la agrupación de ámbitos más común (26 %).

Seguridad de los Datos PR.DS
ámbito más común (6%)



ACTIVIDADES REPRESENTATIVAS

En cuanto a las actividades representativas y ámbitos de actuación, las empresas españolas están más enfocadas en ofrecer conocimientos técnicos que en la aplicación práctica de dichos conocimientos.

Esto es debido a que las actividades relacionadas con los conocimientos técnicos como la consultoría y formación (1. Proveedores de Servicios de Ciberseguridad Gestionada y SOC (23%), 4. Consultores de Ciberseguridad (28%) y 5. Proveedores de Servicios de Formación en Ciberseguridad (18%)), tienen un porcentaje del 69% de representatividad, superior al de las actividades enfocadas a la fabricación y de índole más práctica (2. Fabricantes y Suministradores de Productos de Ciberseguridad Propios (7%) y 3. Desarrolladores e Integradores de Productos de Ciberseguridad de Terceros (19%)), que cuentan con un 25% de representatividad.

ÁMBITOS DE ACTUACIÓN

En lo relativo a los ámbitos de actuación, se realizaron agrupaciones de diversos ámbitos de manera individualizada en función de la aplicabilidad de los mismos en ciberseguridad.

Así pues, se obtuvieron las agrupaciones relativas a: Protección (PR), Respuesta (RS), Gobierno (GV), Identificación (ID), Detección (DE), Recuperación (RC).

Si bien la agrupación de ámbitos más común es la «Protección (PR)» con un 26% de la tasa de respuesta, a nivel de ámbitos individuales los tres más representados son «Seguridad de los Datos PR.DS» dentro de la «Protección (PR)» con un 6,3% de la aportación de su grupo, «Gestión de Incidentes RS.MA» dentro de «Respuesta (RS)» con un 5,8% dentro de su grupo y en tercer lugar «Evaluación de Riesgos ID.RA» con un 5,5% de aportación dentro del grupo «Identificación (ID)».

Más allá de estos tres primeros puestos de representatividad por ámbitos individualizados, el resto de datos muestran una gran diversidad y una distribución porcentual bastante homogénea donde la representatividad del resto de ámbitos individualizados oscila entre el 3% y el 6%.

Ámbitos de actuación agrupados en función de su aplicabilidad en ciberseguridad			
T	100%	100%	Ámbitos individualizados:
PR	26%	5%	Resiliencia de la Infraestructura Tecnológica PR.IR
		5%	Seguridad de la Plataforma PR.PS
		6%	Seguridad de los Datos PR.DS
		5%	Concienciación y Formación PR.AT
		5%	Gestión de Identidad, Autenticación y Control de Acceso PR.AA
RS	20%	5%	Mitigación de Incidentes RS.MI
		5%	Informes y Comunicación sobre Respuesta a Incidentes RS.CO
		5%	Análisis de Incidentes RS.AN
		6%	Gestión de Incidentes RS.MA
GV	16%	3%	Gestión de Riesgos en la Cadena de Suministro de Ciberseguridad GV.SC
		3%	Supervisión GV.OV
		3%	Política GV.PO
		3%	Roles, Responsabilidades y Autoridades GV.RR
ID	14%	4%	Estrategia de Gestión de Riesgos GV.RM
		4%	Mejora ID.IM
		6%	Evaluación de Riesgos ID.RA
DE	10%	5%	Gestión de Activos ID.AM
		5%	Análisis de Eventos Adversos DE.AE
RC	9%	6%	Monitoreo Continuo DE.CM
		4%	Comunicación para la Recuperación de Incidentes RC.CO
-	4%	5%	Ejecución del Plan de Recuperación de Incidentes RC.RP
		4%	Ningun ámbito



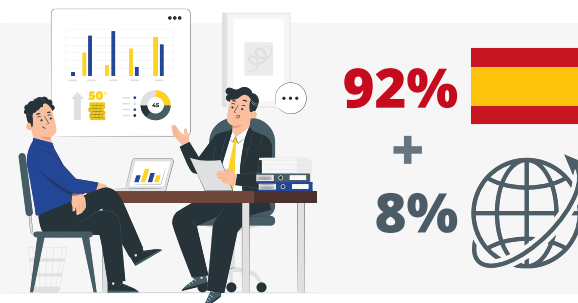
Actividad de las empresas

Facturación y orientación del negocio

El 92% factura en España (nivel local, regional o nacional).

Un 8% recibe ingresos internacionales (tanto a nivel europeo como más allá).

Sectores principales: Admin. Pública 19%, Fabricación 14% y Alimentación 8%.



FACTURACIÓN, ORIENTACIÓN Y PROVEEDORES

La facturación de las empresas de ciberseguridad españolas se agrupa principalmente dentro de territorio español, sobre todo a nivel local (36%). No obstante, más allá de España, se corresponde con un 8% repartido homogéneamente entre el ámbito europeo (4%) y el internacional (4%).

Dentro de los sectores a donde se dirigen las empresas, la Administración pública es la que mayor porcentaje ocupa (19%), aunque también existen algunos sectores críticos de la NI2 y otros sectores estratégicos nacionales donde la presencia indicada es nula, como el sector químico y sanitario.

Los proveedores de servicios de las empresas son muy diversos y de entre las tipologías observadas, las más comunes son: «Protección del endpoint, EDR, antivirus» (9%), «Protección de las comunicaciones, VPN» (8%) y «Seguridad en redes y sistemas, seguridad web» (7%).

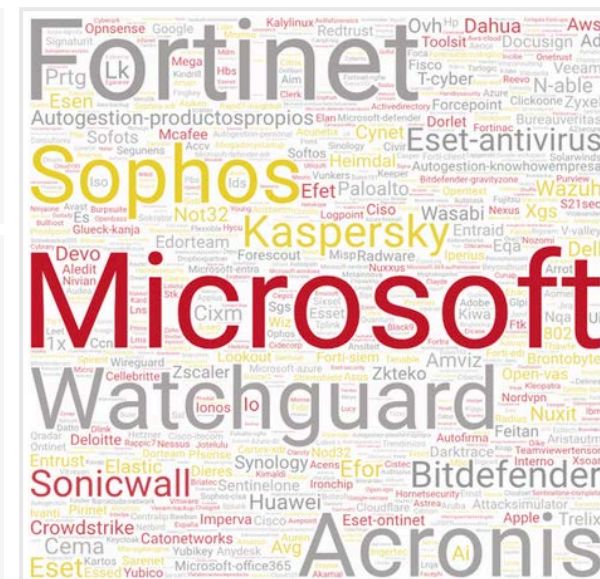
Proveedores:

Gran diversidad de servicios ofrecidos.

«Protección del endpoint, EDR, antivirus» (9%)

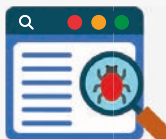
«Protección de las comunicaciones, VPN» (8%)

«Seguridad en redes y sistemas, seguridad web» (7%)





Sujetos obligados de la NIS2



► Nivel de conocimiento y preparación ante NIS2:

Un **49%** dice conocer la normativa. De estas, un **28%** afirma que estará obligada, un **44%** lo desconoce y un **28%** no prevé serlo.

El 55% cuenta con al menos un servicio de adaptación.

Los más ofrecidos: «**Servicios de gestión de riesgos y planificación de ciberseguridad**» (22%) y «**Operaciones de ciberseguridad (SOC) o servicios de seguridad gestionada**» (20%).

CONOCIMIENTO Y PREPARACIÓN DE LAS EMPRESAS ANTE LA NIS2

A nivel nacional, un 28% de las empresas se consideran sujetos obligados por la directiva NIS2, un porcentaje inferior al de aquellas empresas que dicen estar en conocimiento de la misma (49%).

Por otro lado, otro 28% de las empresas encuestadas dice que no serán sujetos obligados, lo que puede estar relacionado con la falta de conocimiento, pero solo en parte puesto que dentro del porcentaje de respuestas de las empresas que sí están en conocimiento de lo que es la Directiva NIS2, el 44% faltante se corresponde a las empresas que no dieron respuesta por no interesarles o desconocer si van a ser afectadas.

Como preparación ante la directiva, el 55% de las empresas encuestadas afirma ofrecer al menos un servicio de adaptación para la NIS2. Dentro de estos servicios ofrecidos, la representatividad de cada uno se divide en: «Servicios de gestión de riesgos y planificación de ciberseguridad» (22%), «Auditorías de ciberseguridad» (17%), «Operaciones de ciberseguridad SOC» (20%), «Servicios de gestión de incidentes» (18%), «Servicios de continuidad de negocio» (18%) y Otros servicios (4%).

► Incidentes de ciberseguridad sufridos:

El 15% de las empresas dice haber sufrido al menos un incidente en algún momento.

► Apoyo en incidentes:

Un 81% de las empresas presta apoyo a sus clientes tras el suceso.





Sujetos obligados de la NIS2

➤ Procesos y mecanismos de notificación:

Un **85% conoce el proceso** de notificación de incidentes y un **73%, quiere saber más** independientemente del nivel de conocimiento.

➤ Participación en el Catálogo de Ciberseguridad:

Un **31% de las empresas participa**.

El **69% que no pertenece, tiene interés** por hacerlo.

➤ INCIBE-CERT y 017:



El **52%** de las empresas **conoce al menos uno de los dos servicios** de INCIBE.

- Conocimiento de INCIBE-CERT ligeramente superior al 017.
- Un **12%** de la muestra tiene un **acuerdo NDA con INCIBE**.
- El **65% de las empresas** que **reciben avisos**, lo hace **a través del servicio de «Alerta Temprana»**.

NOTIFICACIÓN DE INCIDENTES Y SERVICIOS DE INCIBE ASOCIADOS

A nivel nacional, el 85% de las empresas conoce el proceso de notificación de incidentes de ciberseguridad, mientras que el 15% restante lo desconoce.

- No obstante, dentro de las empresas que conocen el proceso, un 63% tiene interés por contar con más información y un 22% dice no necesitarla.
- En el caso de las empresas que desconocen el proceso, un 10% tiene interés por saber sobre él y un 5% quiere seguir sin conocerlo.

Asociado al proceso de notificación de incidentes de ciberseguridad, el 52% de las empresas encuestadas dice conocer al menos uno de los servicios INCIBE-CERT o 017 de INCIBE. Sin embargo, dentro de estas, el nivel de conocimiento del servicio de INCIBE-CERT (54%) es ligeramente superior al de la Línea de Ayuda 017 (46%).

En lo que respecta a los acuerdos NDA con INCIBE-CERT (Acuerdos de Confidencialidad), un 12% de la muestra afirma contar con uno, mientras que un 88% dice carecer del mismo. En relación con esto, destaca que un 72% pese a carecer del acuerdo, demuestra interés por recibir información para conseguir uno.

Vinculado al conocimiento del sistema de avisos de vulnerabilidades, a nivel nacional un 65% de las empresas conoce lo que es un servicio de aviso de vulnerabilidades, mientras que un 35% lo desconoce. Además, dentro de la agrupación de empresas que conocen el servicio, un 65% afirma recibir estos avisos a través del servicio de «Alerta Temprana» de INCIBE y un 35% a través de otros proveedores externos que se encargan de enviarles los avisos.

En cuanto al «Catálogo de Ciberseguridad» de INCIBE, el 31% de las empresas dice formar parte de él y, de las que no lo hacen, el 69% tiene interés por hacerlo.



Entidades formadoras en ciberseguridad

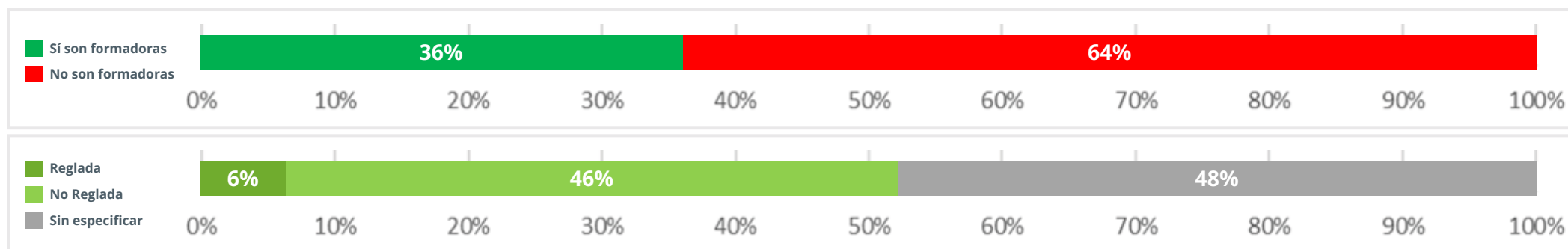


➤ Empresas como formadoras:

Un 64% de las empresas no son formadoras en ciberseguridad frente al 36% que sí.

➤ Tipo de formaciones:

Un 6% regladas.
Un 46% no regladas.



ENTIDADES FORMADORAS Y TIPOLOGÍA DE FORMACIÓN

A nivel nacional, el 36% de las empresas se consideran como entidades formadoras en ciberseguridad mientras que un 64% no.

Reduciendo la muestra a las empresas que si se consideran formadoras, un 6% indica que el tipo de formación que ofrecen es de tipo reglada, un 46% que su formación es no reglada y un 48% no sabrían especificar el tipo de formación que ofrecen.

A nivel geográfico por comunidades autónomas, se observa un mayor número de entidades formadoras en La Rioja (100%), Navarra (75%) y País Vasco (63%), mientras que las zonas con menor cantidad de entidades formadoras están localizadas en Ceuta (0%), Murcia (18%) y Comunidad Valenciana (19%).

➤ Conocimiento del Catálogo de formación: El 80% de la muestra quiere integrarse.



CATÁLOGO DE FORMACIÓN

A nivel nacional, el conocimiento del catálogo de entidades formadoras es del 28%. Sin embargo, un 80% de las empresas tiene interés por formar parte.



Entidades formadoras en ciberseguridad

➤ Modalidades formativas:

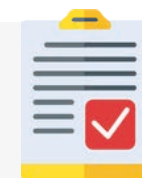
Regladas: tienden a ser formaciones **presenciales** y con **prácticas obligatorias**.

No regladas: generalmente en formato **online** y con **prácticas voluntarias**.



➤ Requisitos de acceso:

Las **formaciones no regladas** requieren de **certificación de acceso en mayor medida** que las regladas.



Total de entidades con registro de información sobre formaciones regladas			8	100%
Total de formaciones sobre las que se tiene registro de su duración			9	100%
De 2 o más horas			8	89%
Entre 1 y 2 horas			0	0%
De 1 o menos horas			1	11%
Total de prácticas asociadas a las formaciones			9	100%
Prácticas Obligatorias			6	67%
Prácticas No Obligatorias			3	33%
Total de modalidades de formaciones			14	100%
Con modalidad Presencial			7	50%
Con modalidad Semipresencial			4	29%
Con modalidad Online			3	21%
Total de certificaciones de acceso para formaciones			0	
Total de enlaces a contenidos de formaciones			2	

Total de entidades con registro de información sobre formaciones NO regladas			66	100%
Total de formaciones sobre las que se tiene registro de su duración			89	100%
De 2 o más horas			80	90%
Entre 1 y 2 horas			8	9%
De 1 o menos horas			1	1%
Total de prácticas asociadas a las formaciones			89	100%
Prácticas Obligatorias			31	35%
Prácticas No Obligatorias			58	65%
Total de modalidades de formaciones			179	100%
Con modalidad Presencial			58	32%
Con modalidad Semipresencial			46	26%
Con modalidad Online			75	42%
Total de certificaciones de acceso para formaciones			21	
Total de enlaces a contenidos de formaciones			27	

CARACTERÍSTICAS DE LAS FORMACIONES DE CIBERSEGURIDAD IMPARTIDAS

Se registraron mayor número de formaciones que entidades formadoras y de estas más de tipo no reglado. Esto, es debido a que una misma entidad puede tener más de una formación con tipologías distintas y que las formaciones regladas necesitan de cumplir con más requisitos para ser consideradas como tal.

No obstante, se obtuvo que independientemente de su tipología, ambos tipos de formación tienden a contar con una duración de 2 o más horas (89-90%). En cuanto a las diferencias observadas, las formaciones regladas (50%) tienen un porcentaje de presencialidad superior a las no regladas (32%). Por otro lado, la semipresencialidad entre ambas es bastante pareja (26-29%). En cuanto a las prácticas, su obligatoriedad es superior en las regladas (67%) que en las no regladas (35%) y en el caso de los requisitos de acceso, estos son más exigentes para las formaciones no regladas que para las regladas dadas las certificaciones de acceso.

2025



conetic
Confederación Española de Empresas de Tecnologías
de la Información, Comunicaciones y Electrónica

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD



ESTUDIO SECTOR CIBERSEGURIDAD

EMPRESAS EN TERRITORIO ESPAÑOL

A fecha de **01/12/2025**

Resumen Ejecutivo

 Financiado por
la Unión Europea
NextGenerationEU



GOBIERNO
DE ESPAÑA

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO
DE TELECOMUNICACIONES
E INFRAESTRUCTURAS DIGITALES



Plan de
Recuperación,
Transformación
y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

