CIBERSANIDAD:

UN ANÁLISIS EUROPEO DE LA CIBERSEGURIDAD SANITARIA

relyens

GRUPO MUTUALISTA EUROPEO
SEGUROS Y GESTIÓN DE RIESGOS

La **Sociedad Española de Electromedicina e Ingeniería Clínica** (SEEIC) es una entidad profesional de carácter científico técnico y sin ánimo de lucro. SEEIC agrupa a profesionales que desempeñan funciones técnicas y de gestión del equipamiento electromédico, desempeñando un papel crucial tanto en el ámbito público como el sector privado.

La SEEIC se posiciona como interlocutor clave ante la administración sanitaria, priorizando la defensa del interés general y la salud pública. Su enfoque principal está en garantizar la seguridad del paciente mediante el correcto uso y mantenimiento de la Tecnología Sanitaria, promoviendo estándares de calidad y buenas prácticas en electromedicina e ingeniería clínica.

La **Sociedad Española de Informática de la Salud** (SEIS) ha sido, desde su fundación, un pilar fundamental en el impulso de la tecnología dentro del ámbito sanitario español. Su misión principal es promover la innovación tecnológica en la salud, enfocándose en la eficiencia, seguridad y calidad del sistema de salud a través de la digitalización. Uno de los principales compromisos de la SEIS es garantizar la seguridad de la información en el sector sanitario.

Dado que los sistemas de salud manejan grandes volúmenes de datos personales y confidenciales, como los historiales médicos y la información de los pacientes, la ciberseguridad se ha convertido en una prioridad fundamental para la SEIS. La organización ha trabajado de forma constante en la implementación de normativas, buenas prácticas y estándares para garantizar que la información médica se maneje de manera segura, cumpliendo con las regulaciones legales y protegiendo la privacidad de los ciudadanos.

En **Relyens** somos mucho más que un simple asegurador, somos un gestor de riesgos. Controlar, prevenir los riesgos y asegurarlos, es nuestro compromiso para proteger eficazmente a los actores sanitarios y territoriales en Europa. A su lado, actuamos e innovamos para garantizar un servicio de interés general, cada vez más seguro para todos.

Anticipar hoy
para proteger mañana.

ÍNDICE

01 LA COLABORACIÓN COMO PUNTO DE ENCUENTRO Y ANÁLISIS

Philippe PAUL

Director ejecutivo de Relyens en España

En el actual entorno de digitalización, cada vez se prestan más servicios al ciudadano que implican de, una forma u otra, la utilización de sistemas de información y comunicaciones. El sector sanitario no es ajeno a esta revolución digital que se refleja tanto en las nuevas tecnologías hospitalarias como en la prestación de servicios online, incluso, en la asistencia remota para tratamientos médicos.

Para que estos procesos se puedan asentar con éxito y seguir evolucionando, es clave garantizar la confianza en la prestación de los servicios, de forma que quede asegurada la continuidad de la atención sanitaria, la confidencialidad e integridad de la información, así como la trazabilidad y autenticación de los procesos.

Los centros sanitarios se han convertido en objetivos principales para los delincuentes debido a la magnitud del impacto potencial en los sistemas y datos, y a los beneficios que se pueden obtener al monetizar esta situación. De hecho, hoy en día, los datos de salud son considerados el nuevo “oro negro” y la crisis del Covid vivida, ha acentuado el problema.

Hoy en día, ninguna infraestructura sanitaria, independientemente de su tamaño o especialidad, es segura y, por ende, esto pone en juego la seguridad de los pacientes. Un ciberataque o el mal funcionamiento de los sistemas pueden tener consecuencias graves, desde la interrupción del servicio hasta la falta de acceso a los datos críticos de los pacientes, con el consiguiente riesgo de errores médicos o la pérdida de oportunidades vitales de tratamiento.

Los responsables de las instituciones sanitarias son muy conscientes de las normativas y regulaciones relativas a la protección de sus sistemas y están luchando por conciliar esta tarea con la ecuación presupuestaria y operativa.

Con este estudio, hemos querido evaluar el nivel de madurez de las instituciones sanitarias con respecto a este riesgo cibernético, cada vez más presente, y abordar la gobernanza del riesgo dentro de la institución, cruzando la visión de diferentes perfiles implicados en las tecnologías sanitarias como: Responsables de Tecnologías de la Información, Responsables de Ciberseguridad y Responsables de Electromedicina.

Aunque en el presente informe se exponen y analizan los datos de España, se ha realizado el estudio también en Francia, Italia y Alemania, de forma que podamos situar los resultados de nuestro país en un contexto europeo, obteniendo diferentes visiones enriquecedoras que nos ayudan a impulsar la mejora conjunta en los países en los que Relyens está presente.

Este estudio ha sido posible gracias a un **trabajo profundamente colaborativo**. En el marco de la colaboración con los actores sanitarios, Relyens, como Gestor de riesgos sanitarios y en concreto, los riesgos de la ciberseguridad, ha promovido este estudio, coordinando las diferentes fases y realizando desde el análisis hasta el resultado final.

Pero, para conseguir unos datos representativos, es clave disponer de la **participación de los responsables directos en los centros sanitarios**, y por ello, se ha contado con la colaboración de los roles vinculados a los riesgos de la ciberseguridad, CIO's o Responsables de Tecnologías de la Información, CISO's o Responsables de Seguridad de la información o Ciberseguridad, y los Responsables de Electromedicina.

En España, la participación de estos profesionales se ha conseguido gracias a la gran implicación de dos principales asociaciones en el sector sanitario, la **Sociedad Española de Informática de la Salud (SEIS) y la Sociedad Española de Electromedicina e Ingeniería Clínica (SEEIC)**, a quienes desde aquí, aprovechamos para felicitar y agradecer su aportación en la calidad de las respuestas y la garantía del conocimiento práctico en las cuestiones planteadas.

La ciberseguridad en la sanidad es un desafío creciente que requiere de una respuesta conjunta. En Relyens estamos firmemente comprometidos con la protección de las instituciones sanitarias ante estos riesgos y seguiremos trabajando mano a mano con todos los actores de este ecosistema para garantizar que la seguridad, tanto de los datos como de los pacientes, sea siempre una prioridad. La colaboración entre profesionales es, sin duda, el camino para construir una ciberseguridad sólida y sostenible en el sector sanitario.

D. Antonio Manuel OJEDA

Presidente de SEEIC

Desde la Sociedad Española de Electromedicina e Ingeniería Clínica (SEEIC), reconocemos que la ciberseguridad ha ganado una relevancia crucial en la seguridad de los dispositivos y sistemas médicos en los últimos años. Es un aspecto de vital importancia tanto para la seguridad del paciente y sus datos, como para garantizar la continuidad de los servicios esenciales proporcionados por las diversas tecnologías sanitarias.

Nuestro objetivo principal es velar por el interés general y la salud de la sociedad en su conjunto, poniendo especial énfasis en la seguridad del paciente. Esto implica armonizar la actividad clínica y asistencial con el uso seguro y un mantenimiento adecuado de la tecnología sanitaria. Para lograr este propósito, es crucial implementar buenas prácticas y fomentar un cambio de paradigma en las responsabilidades y relaciones entre los diferentes actores involucrados.

La ciberseguridad se concibe como un proceso en capas y una práctica continua que involucra a diversos perfiles profesionales dentro del ámbito sanitario. Se requiere una colaboración multidisciplinar entre centros asistenciales, fabricantes, proveedores y profesionales de la Electromedicina e Ingeniería Clínica, así como de los servicios TIC.

Las normativas actuales se centran en la identificación y mitigación de riesgos, proporcionando directrices sobre los aspectos que deben ser evaluados y cómo realizar dicha evaluación. Con base en estas evaluaciones, se implementan las medidas de seguridad adecuadas, adaptadas a la gravedad y probabilidad de cada riesgo identificado, siempre teniendo en cuenta el factor humano.

Es fundamental realizar evaluaciones de riesgo continuas a lo largo de todo el ciclo de vida del producto sanitario, tanto por parte de los centros sanitarios como por los proveedores y fabricantes. En este sentido, la SEEIC promueve un cambio de mentalidad respecto a la inversión en seguridad, enfatizando tanto los recursos técnicos como la formación especializada del personal.

Como entidad de cohesión y representación de los profesionales dedicados a la gestión, desarrollo y mantenimiento de los equipos y sistemas electromédicos, la SEEIC aboga por fortalecer estas prácticas para asegurar un entorno seguro y eficiente en el ámbito de la salud.

D. Luciano SÁEZ

Presidente de SEIS

La Sociedad Española de Informática de la Salud (SEIS) ha decidido implicarse en el presente estudio europeo "CiberSanidad: Un análisis Europeo de la Ciberseguridad Sanitaria", motivada por el compromiso de fortalecer la seguridad y la protección de datos en el sector sanitario. En un contexto en el que la digitalización avanza rápidamente, proteger los sistemas e infraestructuras críticas de salud es una prioridad que requiere tanto el esfuerzo de entidades públicas como el conocimiento técnico del sector privado.

Nuestra sociedad ha liderado diversas iniciativas en este campo, destacando el Foro de Seguridad y Protección de Datos de Salud, el cual durante sus más de dos décadas de existencia se ha consolidado como un espacio de referencia para el diálogo y la colaboración entre autoridades de protección de datos, organismos de ciberseguridad y el sector sanitario. Este foro simboliza el poder de la colaboración público-privada para construir una respuesta sólida y coordinada frente a las amenazas cibernéticas.

Además, el Índice SEIS, uno de los pilares claves de la sociedad y de publicación anual, proporciona indicadores esenciales que permiten evaluar la madurez en ciberseguridad de las instituciones sanitarias. Entre los principales indicadores se encuentran la inversión en ciberseguridad, la capacidad de respuesta ante incidentes, la resiliencia de las infraestructuras y la confidencialidad de los datos de los pacientes. Este índice permite identificar áreas de mejora y fomenta el desarrollo de buenas prácticas en seguridad, elementos que son indispensables para asegurar una continuidad asistencial segura y confiable. Sin duda, el presente estudio colaborativo a nivel nacional y europeo en el que han participado más de 50 profesionales con distintas responsabilidades (Directores Generales, CISO, CIO y Responsable de Electromedicina) complementa y fortalece los indicadores en materia de ciberseguridad del Índice SEIS, proporcionando una visión amplia y detallada sobre las necesidades y retos específicos en Europa.

Nuestra colaboración con Relyens se basa en esta visión compartida de crear un entorno sanitario seguro, donde la ciberseguridad sea una prioridad estratégica no solo para proteger los datos, sino también para garantizar la continuidad y calidad de la atención sanitaria. Estamos convencidos de que esta alianza representa un paso importante hacia un modelo de gestión de riesgos en salud más sólido y resiliente, que beneficiará tanto a los profesionales como a los ciudadanos europeos, impulsando una cultura de seguridad que se adapte a los desafíos digitales de nuestro tiempo.

PROPUESTA METODOLÓGICA

02

02 PROPUESTA METODOLÓGICA

OBJETIVOS

Los **objetivos** del proyecto se concretan en:

1. **Comprender y medir** el valor de la ciberseguridad en el sector sanitario, tanto público como privado en el contexto europeo (España, Francia, Italia y Alemania).
2. **Analizar la madurez** de la gestión del riesgo cibernético hospitalario y su vinculación con los objetivos corporativos.
3. **Evaluar la coordinación** entre los diferentes responsables en la gestión del riesgo cibernético con el fin de favorecer el diálogo entre las distintas funciones y aumentar la conciencia interna y la alineación entre los diferentes perfiles participantes.
4. Recoger las principales **preocupaciones y expectativas** de futuro de los profesionales del sector respecto a la ciberseguridad.

Para ello, estructuraremos el estudio en las siguientes áreas de análisis de forma general:

1. Sensibilidad respecto a la ciberseguridad.
2. Gobernanza, organización de la seguridad y responsabilidades involucradas.
3. Aspectos económicos, presupuestos y alineación con los objetivos corporativos.
4. Medidas implementadas para la gestión de riesgos.
5. Perspectivas sobre la evolución de los riesgos ciber y las necesidades del sector.

METODOLOGÍA

En cuanto a la metodología empleada en el estudio, se ha adoptado un **doble enfoque: un estudio cualitativo, basado en entrevistas dirigidas, y un estudio cuantitativo**, recogiendo la información a través de encuestas online. Para ambos casos, se parte de una segmentación de los participantes atendiendo al país participante y su rol en la organización.

Los datos obtenidos, entre 2022 y 2023, se analizan con técnicas adecuadas para extraer las correlaciones entre las diferentes variables y obtener los **resultados y conclusiones del informe**.

	PASO 1 - CUALITATIVO	PASO 2 - CUANTITATIVO
OBJETIVO	**Comprender en profundidad** la dinámica y los procesos de influencia con respecto a las cuestiones de ciberseguridad en los centros sanitarios. Definir en profundidad el nivel de concienciación y el valor del riesgo de ciberseguridad.	**Recopilar** datos **estadísticamente sólidos y representativos** capaces de medir cuál es el nivel de conocimiento y sensibilidad relacionados con el riesgo de ciberseguridad.
METODOLOGÍA	**Entrevistas en profundidad en línea**	**CAWI** (Entrevista web asistida por ordenador)
MUESTRA 	**48 participantes** (Directores Generales de Hospitales – CIO de Servicios de Salud y Hospitales – Responsable de Ciberseguridad - Responsable de Electromedicina de cada país)	**115 participantes** (CIO de Servicios de Salud y Hospitales – Responsable de Ciberseguridad – Responsable de Electromedicina de cada país)

Ilustración 1. Metodología del estudio

Respecto a los perfiles participantes, el estudio se ha centrado en los siguientes roles:

1. Director General.

Es el principal responsable de la toma de decisiones en los centros sanitarios, pero no desempeña un papel operativo en la ciberseguridad. Involucrado en las decisiones de inversión, pero no en aspectos técnicos y compras concretas de ciberseguridad y TI.

2. CIO de Servicios de Salud y Hospitales.

Responsable de todos los procesos relacionados con los dispositivos informáticos y la gestión de la información. Normalmente tiene una alta coordinación con el CISO y con el Director General. En ocasiones, asume el rol del CISO dentro de sus funciones.

3. CISO. Responsable de Ciberseguridad.

Coordina la política de ciberseguridad y trabaja en estrecha colaboración con el CIO. En ocasiones, depende jerárquicamente de él. Realiza tareas de supervisión e identificación de necesidades en torno a la seguridad de la infraestructura informática y la protección de los datos del hospital.

4. Responsable de Electromedicina.

Responsable de la gestión y operación de los dispositivos médicos: planificación de adquisiciones, calibración, mantenimiento, etc. Sus responsabilidades incluyen la operatividad y la seguridad de los dispositivos médicos (instrumentos de imagen, radioterapia, medicina nuclear, unidad quirúrgica...). Es un perfil que hasta ahora no ha estado muy involucrado en las responsabilidades de la ciberseguridad, sin embargo, ésta impacta directamente en sus responsabilidades (disponibilidad de los equipos).

Propuesta cualitativa

El estudio cualitativo ayudará a comprender las dinámicas y los procesos de influencia con respecto a los problemas de ciberseguridad dentro de las instalaciones sanitarias y a profundizar en el nivel de conciencia y el valor del riesgo de ciberseguridad. Se ha basado en una serie de entrevistas de 60 minutos a diferentes perfiles seleccionados entre los roles participantes en el estudio.

Con estas entrevistas, se ha pretendido obtener un mejor conocimiento de las necesidades de cada perfil y opiniones a través de un discurso abierto con el entrevistador.

Se realizaron un total de 48 entrevistas de una hora de duración distribuidas entre diferentes roles de los centros sanitarios: Director General, CIO, CISO y Responsables de Electromedicina.

ENCUESTADO	Nº	TITULARIDAD		Nº CAMAS			
		PRIV	PUB	250-499	500-999	1000-1499	>1500
Dir. General	2		2		1		1
CIO	2		2				2
CISO	5		5		1		4
Resp. Electr.	4	1	3		2		2

ENCUESTADO	Nº	TITULARIDAD		Nº CAMAS			
		PRIV	PUB	250-499	500-999	1000-1499	>1500
Dir. General	2		2		2		1
CIO	4	1	3		2	1	1
CISO	2	1	1		1	1	
Resp. Electr.	3		3		2	1	

ENCUESTADO	Nº	TITULARIDAD		Nº CAMAS			
		PRIV	PUB	250-499	500-999	1000-1499	>1500
Dir. General	3	2	1		2		
CIO	4	2	2		4		
CISO	4	2	2		2		2
Resp. Electr.	2		2		2		

ENCUESTADO	Nº	TITULARIDAD PRIV	TITULARIDAD PUB	Nº CAMAS 250-499	Nº CAMAS 500-999	Nº CAMAS 1000-1499	Nº CAMAS >1500
Dir. General	3	1	2		2		1
CIO	4			2	1		1
CISO	-	-	-	-	-	-	-
Resp. Electr.	4	1	3		3	1	

Ilustración 2. Distribución entrevistas responsables sector sanitario

La representación de los roles y el sector público y privado es bastante equilibrada en los datos obtenidos en España, sin embargo, en los otros países participantes se ha conseguido mayor colaboración del sector público que del privado. De cualquier modo, el reparto de perfiles es adecuado para el objeto de las entrevistas.

Las entrevistas se centraron en recoger información sobre los siguientes temas:

- Percepción del riesgo de ciberseguridad en el sector sanitario.
- Principales preocupaciones de los responsables respecto a los riesgos de ciberseguridad.
- Coordinación interna y los procesos de decisión respecto a la ciberseguridad.
- Principales proyectos y desafíos respecto a la ciberseguridad.

Ilustración 3. Participación sector sanitario España

Los resultados de estas entrevistas se tuvieron en cuenta para el diseño de la encuesta utilizada en la parte cuantitativa del estudio.

Propuesta cuantitativa

El estudio cuantitativo recoge la información de un grupo más amplio de participantes para medir el nivel de desarrollo y sensibilidad relacionados con el riesgo de ciberseguridad. Se ha realizado mediante una encuesta en línea orientada a los diferentes perfiles participantes.

Para el lanzamiento y promoción de las encuestas en España ha sido clave la participación de las asociaciones SEIS y SEEIC. A través de estas organizaciones, se ha garantizado el acceso a perfiles cualificados y representativos de la realidad de los hospitales en nuestro país.

	TOTAL	CIO	CISO	RESP. ELECTROM.
ITALIA	23	10	5	8
ESPAÑA	30	4	9	17
ALEMANIA	30	9	6	15
FRANCIA	32	8	10	14
TOTAL	**115**	**31**	**30**	**54**

Ilustración 4. Participación por países y roles

Respecto a los centros sanitarios participantes, vemos un alto porcentaje del sector público, que se ha mostrado más abierto a participar en la encuesta enviada. En concreto en España, el sector público representa un 73% de las respuestas, frente al 27% que representa al sector privado, asumiendo que el 10% son centros concertados que, aunque trabajan para el sector público, son de titularidad privada.

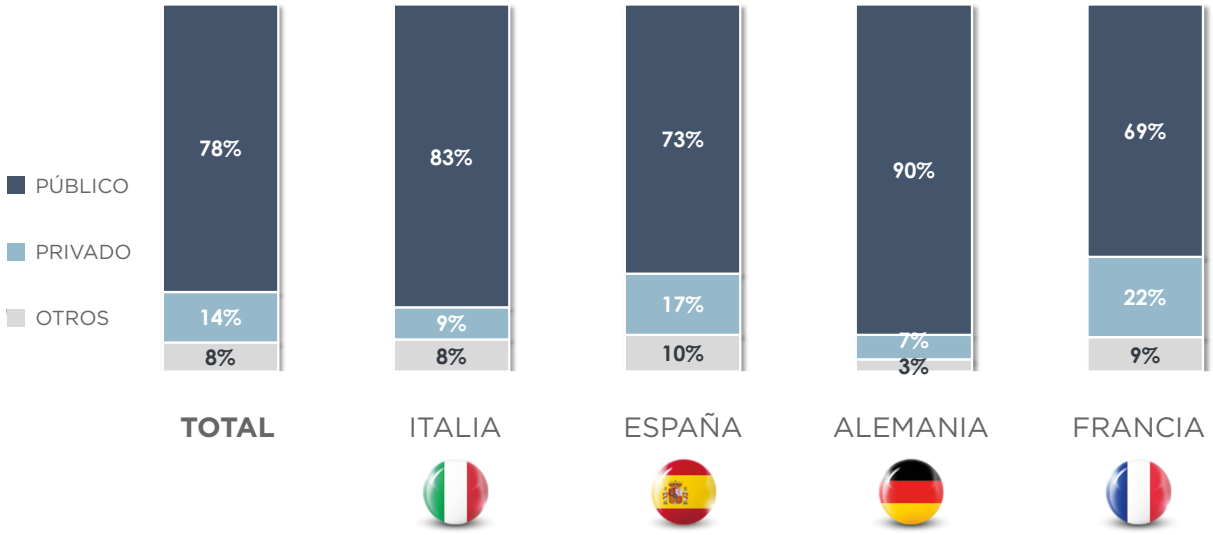


Ilustración 5. Titularidad centros participantes

El perfil técnico de los hospitales participantes, mayoritariamente Hospitales Universitarios y Hospitales Generales, garantiza el conocimiento de los profesionales de los riesgos ciber. Estos establecimientos, al tener una alta base tecnológica en sus servicios, se encuentran más expuestos a los ciberincidentes y sus equipos, en general, cuentan con mayor sensibilidad y medios ante los riesgos de ciberseguridad.

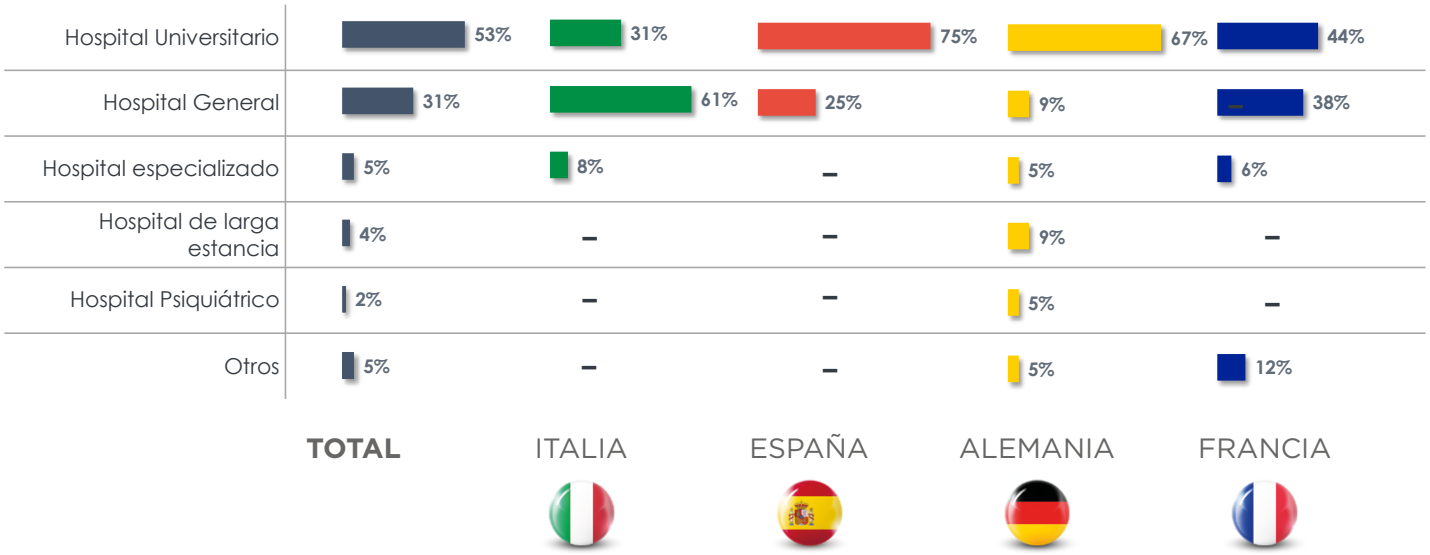


Ilustración 6. Tipos de hospitales participantes

Si analizamos los centros participantes desde el punto de vista de su pertenencia o no a un grupo sanitario, vemos que España destaca en esta característica con un 73% de centros pertenecientes a un Grupo con el que comparten estrategias e incluso tecnologías de ciberseguridad. El 73% de los hospitales participantes pertenecen al sector público y este agrupa los centros de cada Comunidad Autónoma (CCAA).

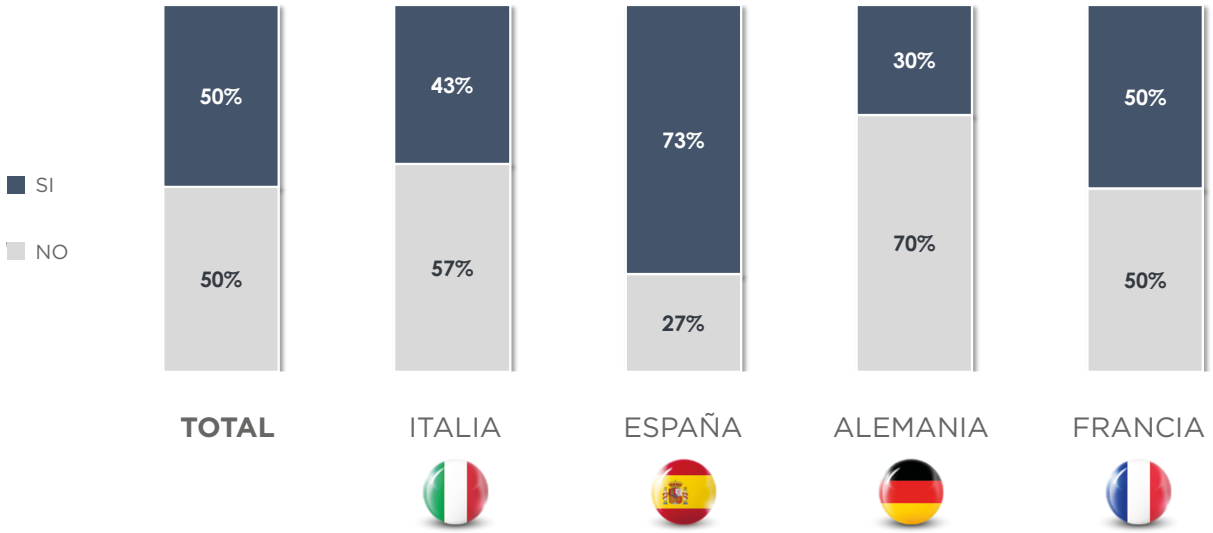


Ilustración 7. Pertenencia a un Grupo hospitalario

Respecto al número de camas de los centros participantes, en general, se trata de centros de un tamaño medio o grande.

El tamaño de los hospitales en España varía mucho, desde los pequeños hospitales comarcales, con menos de 100 camas, hasta los grandes Hospitales Universitarios, con más de 1.000 camas. Sin embargo, el tamaño de un hospital mediano en España es de alrededor de 500 camas, siendo el más común en nuestro país (Hospital de área). Vemos que en el caso de España la muestra recoge una representación de los diferentes tipos de hospitales.

El tamaño de los hospitales en Alemania también varía mucho, en el mismo rango de hospitales comarcales de 100 camas hasta los hospitales universitarios con más de 1.000 camas. Sin embargo, el tamaño medio de 378 camas es el más común, algo por debajo del tamaño en España. En el caso de Alemania ha participado un mayor número de hospitales grandes, más representados que los de menor tamaño.

En Italia, el tamaño por camas se distribuye de una forma similar a Alemania y España, con una media de 367 camas. Destaca la representación de este tipo de hospitales (300-500 camas) y los hospitales grandes, en detrimento de los de menor tamaño.

En el caso de Francia, el tamaño medio de los hospitales se sitúa en el mismo rango de 300-500 camas con 350 camas de media por hospital.

Podemos concluir que la muestra de hospitales es representativa de la realidad de los países, incluyendo hospitales de gran tamaño con mayor dependencia de la tecnología y, por lo tanto, mayor exposición a incidentes de ciberseguridad.

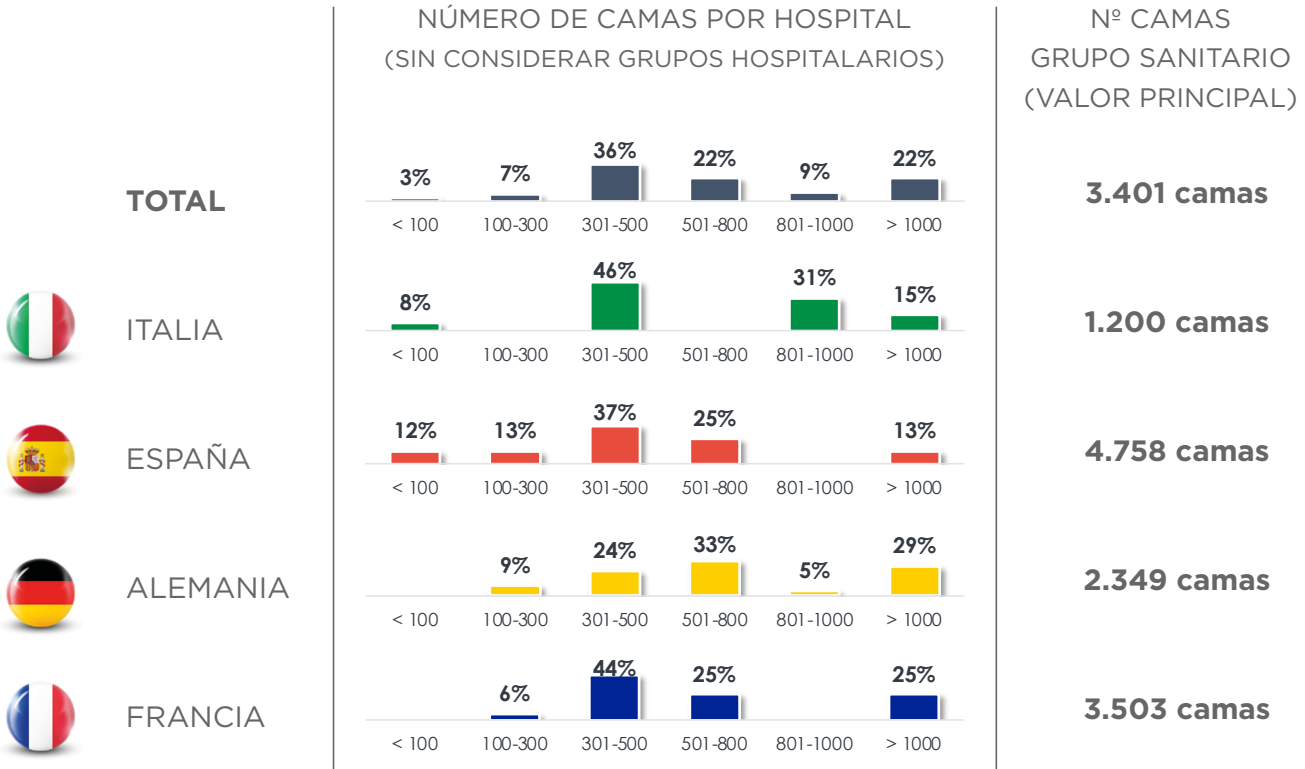


Ilustración 8. Tamaño de hospitales participantes según número de camas

INFORME EJECUTIVO

03

03 INFORME EJECUTIVO

LA VISIÓN DEL SECTOR Y SUS NECESIDADES EN UN FUTURO PRÓXIMO

La sanidad, sector clave en nuestra sociedad, está inmersa en un proceso de digitalización acelerado que permite una mayor eficiencia y mejores servicios al ciudadano. Vemos en nuestro día a día avances como, equipos cada vez más sofisticados, asistencia sanitaria en remoto (incluyendo operaciones de alta complejidad) y sistemas de información interconectados que ofrecen mayor movilidad al ciudadano y más control sobre su historial clínico. Sin embargo, esta situación, lejos de frenarse, no ha hecho más que empezar. La incorporación de la IA para el diagnóstico y la telemedicina, por ejemplo, abren nuevos campos en la atención sanitaria que están por explorar.

Todos estos avances y la gran inversión que requieren, sin embargo, necesitan de garantías que aseguren la disponibilidad y resiliencia de los servicios, y la confidencialidad e integridad de los datos sanitarios de los ciudadanos. Y este es el papel de la ciberseguridad en este contexto: vigilar que las nuevas tecnologías sean resilientes ante ataques e incidentes y los datos estén protegidos ante usos inadecuados.

En este contexto, hemos querido analizar junto con los principales actores en el entorno de la ciberseguridad sanitaria, algunos aspectos clave para conocer el punto de partida actual. De este modo, podremos diseñar planes de mejora adecuados que alineen los avances tecnológicos con su protección ciber. Para ello, hemos llevado a cabo este estudio con una doble aproximación: una prospección cualitativa en base a entrevistas con perfiles relevantes, y un análisis cuantitativo basado en encuestas preparadas para los diferentes participantes.

Objetivos del estudio

- Comprender el valor de la ciberseguridad del sector sanitario en el contexto europeo.
- Evaluar la coordinación entre los diferentes responsables en la gestión del riesgo ciber.
- Analizar la madurez de la gestión del riesgo cibernético hospitalario y su vinculación con los objetivos corporativos.
- Recoger las principales preocupaciones y expectativas de futuro de los profesionales del sector respecto a la ciberseguridad.

Principales conclusiones de la situación de la ciberseguridad en el sector sanitario

Percepción de la ciberseguridad

El incremento del ciberriesgo se refleja en un aumento de la concienciación sobre los problemas que genera en los centros sanitarios. **Desde la dirección hasta los responsables de las diferentes áreas técnicas y médicas, tienen una clara conciencia de la necesidad de incluir la ciberseguridad en la gestión de los riesgos de la organización.**

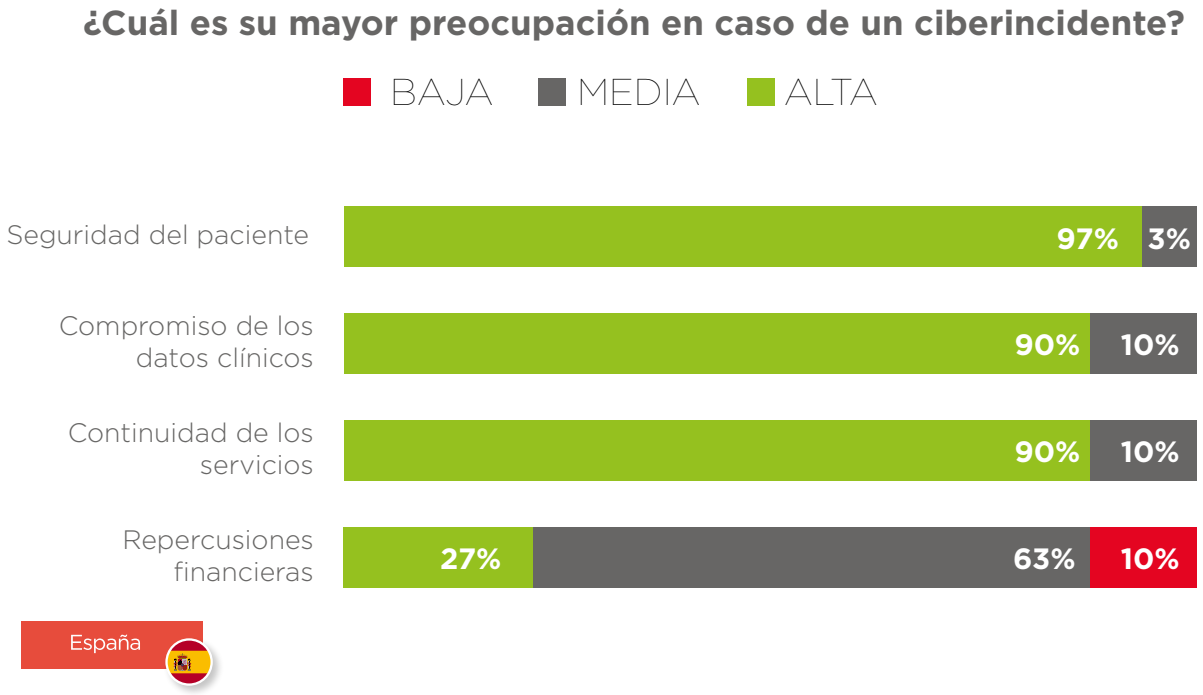
Los principales riesgos percibidos sobre el servicio sanitario son la **seguridad del paciente y la continuidad del servicio médico, la confidencialidad de los datos sanitarios** y el **impacto financiero**. Estas preocupaciones se comparten tanto entre los diferentes perfiles profesionales, como entre los diferentes países participantes.

En un futuro próximo, además de un **incremento y especialización de los ataques actuales** (principalmente robo de datos y ransomware) se anticipan nuevos temas a gestionar en el ámbito de la ciberseguridad, como los riesgos derivados de la **telemedicina**, de la **cadena de suministro** y del aumento de **conexiones externas** para el intercambio de información y prestación de servicios.

Este aumento de la sensibilización respecto al riesgo ciber se refleja directamente en las inversiones en ciberseguridad. Estas deben ser **acordes con los objetivos del negocio**, apoyando la digitalización de los servicios sanitarios.

En general, los centros sanitarios tienen en consideración las necesidades de los servicios prestados para las inversiones en ciberseguridad y la definición de los presupuestos. Cada vez más, los hospitales cuentan con presupuestos propios e independientes de las áreas de TI, sin embargo, **aún se detecta dependencia de los presupuestos de ciber de los presupuestos para TI**. Un mayor nivel de ciberseguridad necesita de presupuestos propios, como se observa en los centros con mayor madurez en la gestión de los riesgos ciber.

De cara a los próximos retos sobre la ciberseguridad que el sector tendrá que afrontar, la financiación de los proyectos de ciberseguridad es una preocupación de los centros sanitarios, en particular para proyectos específicos y desarrollo de nuevas tecnologías. **La ayuda de las Administraciones Públicas (AAPP) se revela como pieza clave para poder financiar los retos a los que se enfrenta el sector.**



Organización y Responsabilidades en la ciberseguridad

La ciberseguridad no puede enfocarse como una actividad exclusivamente tecnológica. Como se ha dicho, su objetivo es conseguir que los servicios sanitarios se presten con garantías de resiliencia y seguridad de los datos, por lo que deben alinearse con la estrategia sanitaria y adaptarse a los objetivos y proyectos de los hospitales.

Para ello, necesita no solo tecnología, sino que ésta se defina y se gestione de forma coordinada entre las diferentes partes implicadas y siempre con la prestación del servicio sanitario como meta final de sus actividades.

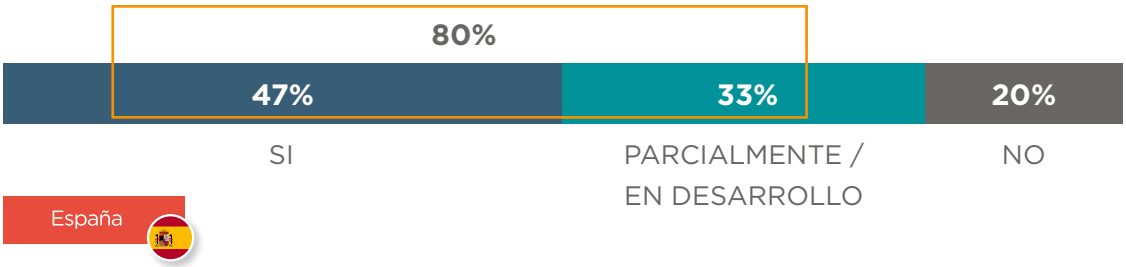
La **gestión de la ciberseguridad** incluye procesos orientados a proteger (tareas de prevención) y a reaccionar en caso de un ciberataque (gestión de incidentes).

Ambas etapas deben estar **coordinadas con las necesidades del negocio** y, por lo tanto, deben intervenir los diferentes roles involucrados según su responsabilidad.

La madurez en la gestión de la ciberseguridad se refleja en la **participación y coordinación de los comités de ciberseguridad**. Si bien la mayoría de las instituciones cuentan con estos comités, es esencial fortalecer su rol y composición. La incorporación de áreas técnicas como la electromedicina, aporta una visión más holística de los riesgos y facilita la toma de decisiones estratégicas en materia de ciberseguridad. Sin embargo, se detecta que estos comités están mayoritariamente compuestos por responsables de sistemas, responsables de ciberseguridad y de la dirección de los centros sanitarios.

Por otro lado, las funciones del propio comité deben evolucionar a gestionar todo el ciclo de vida de la ciberseguridad, más allá de proyectos técnicos y de respuesta a incidentes. **La involucración en las decisiones estratégicas permite un correcto análisis de los riesgos** para los servicios y la optimización de las inversiones.

¿Está la ciberseguridad vinculada a los objetivos de negocio?



Atendiendo a los resultados del estudio, **la figura del CISO o Responsable de ciberseguridad se afianza en los centros sanitarios**. Sin embargo, este rol aún no está suficientemente reconocido en la estructura sanitaria, puesto que en muchas ocasiones **continúa dependiendo del CIO o responsable de los sistemas de información**, tanto con una dependencia funcional como presupuestaria.

Por otro lado, si bien existe una **creciente concienciación sobre los riesgos cibernéticos en el ámbito de la electromedicina, la participación activa** de los responsables de esta área en la gestión de la ciberseguridad **aún es limitada**. Es fundamental potenciar su rol en la integración de medidas de seguridad desde las primeras fases del ciclo de vida de los equipos médicos, especialmente durante el proceso de adquisición. De esta manera, se garantizará la incorporación de requisitos técnicos y de mantenimiento de la ciberseguridad que minimicen la exposición a amenazas. Esta estrategia permitirá optimizar la resiliencia de los sistemas médicos y proteger la información sensible de los pacientes.

La gestión de la ciberseguridad

Los niveles de madurez en ciberseguridad presentan variaciones significativas entre los países participantes. **En España**, aunque se han establecido procedimientos y se cuenta con el apoyo de la Administración Pública (principalmente en el sector público), **los sistemas de ciberseguridad se encuentran en una fase de desarrollo.**

Es necesario avanzar en la consolidación de **modelos de gestión integrados** y en la **formación especializada**, concretamente en áreas críticas como la **respuesta a incidentes y los planes de continuidad**. Más allá de estos aspectos, podemos destacar lo siguiente:

- La realización de **análisis de riesgos** está generalizada para la selección de las medidas de seguridad a implantar y mayoritariamente, se contratan a empresas externas.
- Aunque se realizan actividades de **formación** en ciberseguridad, no están adaptadas a los diferentes perfiles técnicos y directivos, ni mantenidas de forma periódica.
- Respecto a las **medidas de protección tecnológicas**, los sistemas de backup y control de la red son los más extendidos en los centros sanitarios, aunque se van implantado otras medidas para el control de la IoMT, segmentación de red, control de accesos etc.

El sistema sanitario español está avanzando significativamente en la mejora de su postura sobre la ciberseguridad. El esfuerzo realizado para exigir certificaciones a los proveedores de soluciones de seguridad, puede ser un factor clave para elevar los estándares de protección y asegurar la implementación de tecnologías robustas.

El papel de los seguros ciber

La adopción de seguros ciber es incipiente, con una **baja penetración en el mercado**. En general, se reconoce la protección desde el punto de vista financiero, pero se considera que el seguro ciber tiene escaso impacto en la prevención de los ataques, no jugando un papel activo en este aspecto.

Los hospitales que cuentan con dichas pólizas (un 10% de los participantes en España) consideran que el seguro ciber tiene un **enfoque predominantemente reactivo y genérico** y no satisface las necesidades específicas del sector. Los centros asegurados consideran **positiva** la oportunidad de realizar una **evaluación de los riesgos ciber**

y obtener una serie de **recomendaciones** para mejorar los niveles de protección por parte de la compañía aseguradora. También se reconoce la utilidad de la **compensación de daños** en caso de materializarse un incidente, aunque se demanda un papel más proactivo en la gestión de los riesgos.

Al mismo tiempo, entre los centros que no cuentan con pólizas ciber, se detecta bastante **desconocimiento** por parte de los responsables técnicos de las posibilidades de estos productos del seguro, percibiéndolos como un gasto y no como una palanca para mejorar la madurez de la ciberseguridad.

¿Está su organización cubierta por una póliza de ciberseguro?

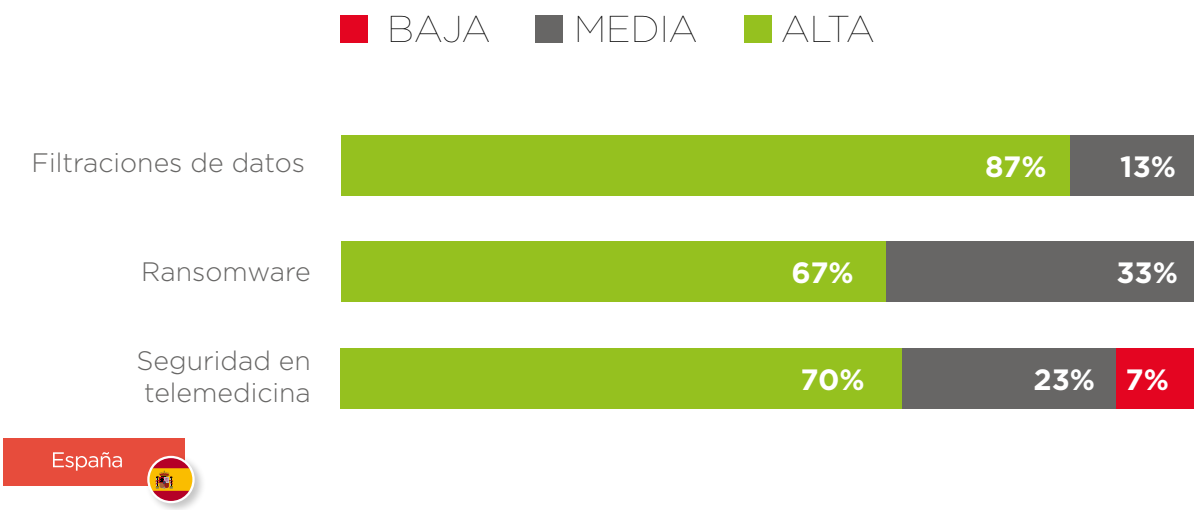
El futuro próximo: necesidades para la ciberseguridad

Como tarea clave en la gestión de la ciberseguridad, además de gestionar los riesgos inmediatos, se deben anticipar las amenazas que se esperan para los próximos años derivadas de los cambios tecnológicos y la evolución de los ataques.

El sector sanitario considera que las **principales amenazas que se mantendrán en un futuro próximo son el ransomware y el robo de datos**. Además de estas amenazas, se esperan nuevos riesgos derivados de nuevas actividades como la **telemedicina**.

Para afrontar los desafíos de la ciberseguridad con éxito, los centros sanitarios han presentado sus principales necesidades y demandas. Cabe destacar las carencias de recursos económicos y humanos; pero otros aspectos como la coordinación entre diferentes actores y el desarrollo normativo son también puntos clave a destacar.

¿Cuáles son sus principales preocupaciones en materia de ciberseguridad para los próximos años?



Implicación activa de las Administraciones Públicas

Las Administraciones Públicas (AAPP) juegan un papel esencial en el fortalecimiento de la ciberseguridad en el sector sanitario. Como destacan los participantes de este estudio, es imprescindible un compromiso firme y estructurado a múltiples niveles. No obstante, cualquier acción en ciberseguridad debe basarse en un análisis exhaustivo de la situación y de las necesidades específicas del sector, con el fin de desarrollar una **Estrategia Nacional de Ciberseguridad para el Sector Sanitario**. Esta estrategia debe proporcionar coherencia y establecer las bases de una intervención coordinada y exhaustiva, asegurando una protección efectiva y sostenible del ecosistema sanitario.

- **Apoyo Económico:** La asignación de presupuestos específicos para ciberseguridad permitirá a los centros sanitarios invertir en tecnologías, herramientas y personal especializado.
- **Desarrollo Normativo:** La Unión Europea implusa la normativa en ciberseguridad, contando además con regulación especifica en España. Sin embargo, el desarrollo de estándares de aplicación específica al sector sanitario, facilitaría la madurez de los sistemas de ciberseguridad.

- **Soporte Técnico:** Las AAPP pueden ofrecer soporte técnico especializado a través de la creación de centros de ciberseguridad o la colaboración con entidades expertas.
- **Cooperación Interinstitucional:** Fomentar la colaboración entre diferentes actores del sector sanitario, así como con otras instituciones públicas y privadas, permitirá compartir conocimientos, experiencias y recursos.

Gobierno de la ciberseguridad en los centros sanitarios

La ciberseguridad debe pasar a formar parte de la gestión de los centros sanitarios con entidad propia, como un facilitador indispensable de la prestación de servicios sanitarios. Por lo tanto, la estrategia de ciberseguridad debe estar alineada con la estrategia corporativa, concretándose en unos presupuestos propios que permitan el desarrollo de sus proyectos con garantías.

Esto significa una evolución de la cultura y conocimiento de la ciberseguridad a todos los niveles de los centros sanitarios.

En el área del gobierno de la ciberseguridad, también se resalta la necesidad de avanzar en los órganos de gobierno:

- El **comité de ciberseguridad** debe evolucionar hacia un órgano gestor y coordinador de la ciberseguridad y no solo ser el responsable en tareas de respuesta ante incidentes.
- La figura del **CISO** o **Responsable de Ciberseguridad** debe contar con la responsabilidad y posición del organigrama que le permita desarrollar sus funciones con garantías e independencia, una vez acordadas con la dirección del centro.

Formación continua y concienciación

La ciberseguridad debe convertirse en parte de la cultura organizacional de los centros sanitarios. Puesto que los riesgos ciber van evolucionando conforme lo hace la tecnología, es necesario crear esta cultura de la formación continua entre todas las partes implicadas. Para ello, es necesario:

- **Programas de Formación Continua:** Implementación de programas de formación adaptados a los diferentes perfiles profesionales, con especial atención a la formación del personal vinculado a las áreas tecnológicas.

- **Campañas de Concienciación:** Desarrollo de campañas informativas para sensibilizar a todos los empleados sobre los riesgos cibernéticos y las buenas prácticas de seguridad.

Implementación de Medidas Tecnológicas:

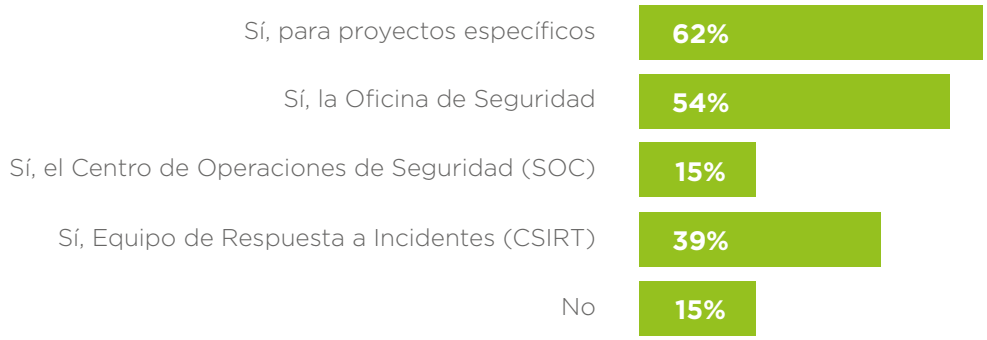
La inversión en tecnologías de seguridad es fundamental para proteger los sistemas y datos de los centros sanitarios. Entre las medidas más importantes destacan:

- **Sistemas de Detección y Prevención de Intrusiones (IDS/IPS):** Para identificar y bloquear ataques cibernéticos.
- **Soluciones de Seguridad de la Información y Gestión de Eventos de Seguridad (SIEM):** Para monitorizar y analizar la actividad de la red en busca de anomalías.
- **Cifrado de Datos:** Para proteger la confidencialidad de la información.
- **Gestión de Identidades y Accesos (IAM):** Para controlar el acceso a los sistemas y datos.

Recursos Humanos: La necesidad de expertos especializados en ciberseguridad sanitaria

Los centros sanitarios necesitan contar con equipos de expertos en ciberseguridad con conocimientos específicos del sector. Actualmente, este es uno de los mayores retos, ya que es difícil encontrar técnicos en ciberseguridad debido a la alta demanda del mercado en prácticamente todos los sectores. Los centros sanitarios tratan de solventar esta situación con subcontrataciones a terceros de sus proyectos de ciberseguridad, pero consideran que es imprescindible una plantilla estable para las tareas recurrentes dentro de sus instalaciones.

¿Subcontrata servicios de ciberseguridad?



España

En particular, cabe destacar la necesidad de contar con equipos de respuesta a incidentes especializados. Estos equipos requieren de una alta capacidad técnica y conocimiento de los procesos sanitarios, de forma que se pueda gestionar un incidente en un contexto de alta presión para la recuperación del servicio. En este aspecto, se reclama la colaboración de las AAPP como agente capaz de preparar estos equipos especializados y dar un servicio clave para el sector.

En conclusión, la ciberseguridad en el sector sanitario es un desafío complejo que requiere una acción coordinada y sostenida por parte de todos los actores involucrados. La inversión en tecnología, la formación del personal, la mejora de la coordinación interna y el apoyo de las Administraciones Públicas son elementos clave para garantizar la seguridad de los sistemas sanitarios y proteger la información de los pacientes.

RESULTADOS CUALITATIVOS

04

04 RESULTADOS CUALITATIVOS

A través de una serie de entrevistas dirigidas, se ha analizado la apreciación del riesgo ciber en el sector sanitario, las preocupaciones en el sector, qué medios tienen disponibles para gestionar esos riesgos y qué medidas demandan para mejorar sus perfiles de ciberseguridad.

LA PERCEPCIÓN DE LA CIBERSEGURIDAD EN EL SECTOR SANITARIO

Sensibilización al riesgo ciber

En general, todo el equipo directivo de los centros entrevistados se muestra sensibilizado con los riesgos de ciberseguridad. Los riesgos cibernéticos afectan directamente a las operaciones sanitarias, por lo que se ha convertido en una preocupación en alza para la dirección de los centros.

Los órganos de dirección del sector sanitario hacen referencia a la presencia en los medios de comunicación de los problemas derivados de la ciberseguridad, los ataques a los centros sanitarios y la opinión pública en general como reflejo de la importancia de estos riesgos para la sociedad.

Los responsables de los centros sanitarios destacan la dependencia creciente de la prestación sanitaria de la digitalización de los servicios de salud. Esto implica que un incidente de ciberseguridad tenga un alto impacto, tanto sobre el hospital por sus repercusiones económicas y reputacionales, como sobre los los ciudadanos, por la degradación del servicio prestado.

NOTICIAS

El creciente aumento de los ataques en instalaciones sanitarias y en agencias e instituciones gubernamentales

ATAQUES

La mayoría de los centros sanitarios han experimentado algún ataque de ciberseguridad con mayor o menor impacto en sus servicios sanitarios

OPINIÓN PÚBLICA

Existe un creciente interés en la opinión pública sobre esta materia

USO DE TECNOLOGÍA

El aumento de la dependencia de los servicios sanitarios de la tecnología, imprescindible para prestar servicios más eficaces para la salud pública

IMPACTO REPUTACIONAL

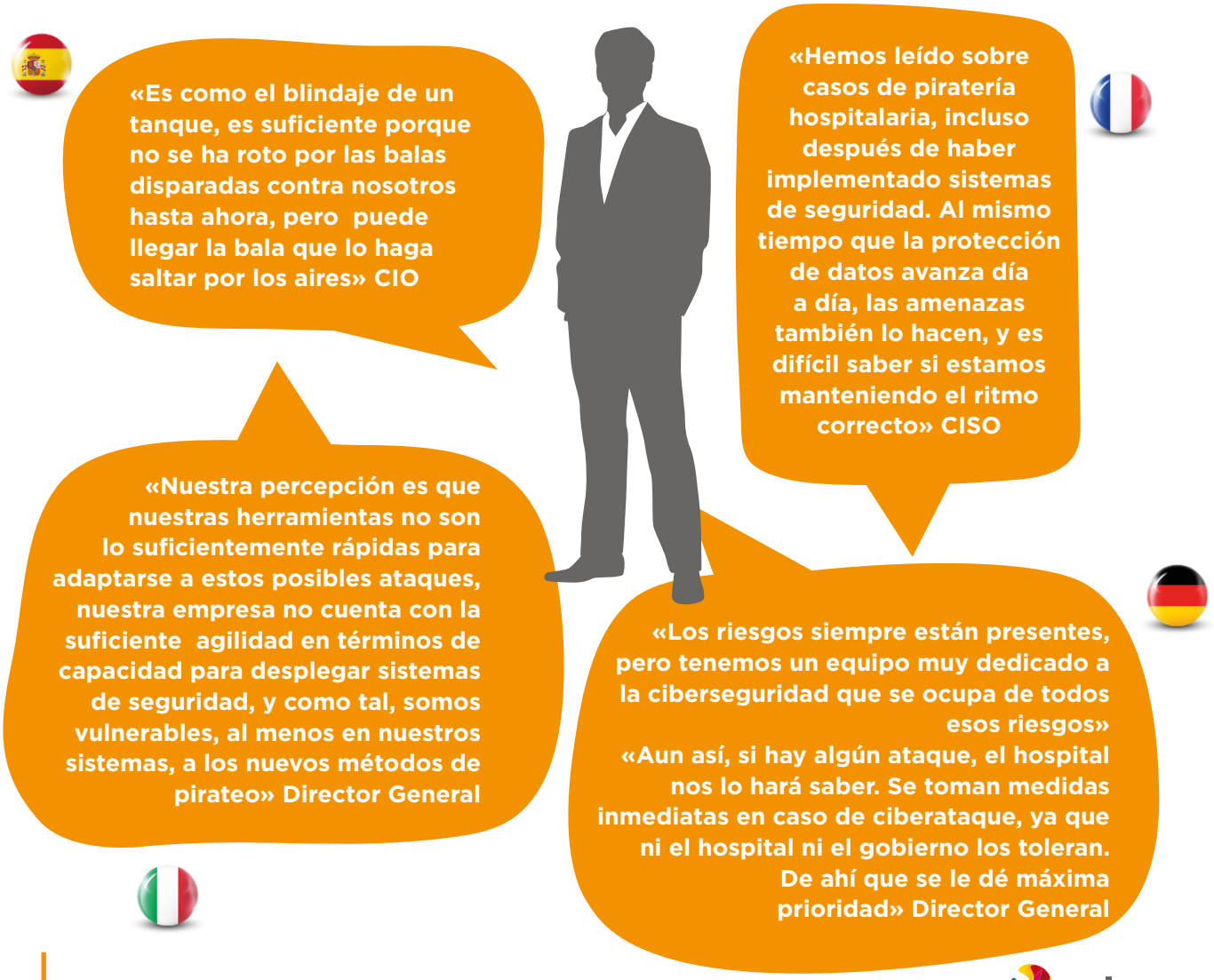
Preocupación por el impacto de la imagen del centro sanitario en caso de verse afectado por un ciberataque

En general, atendiendo a los resultados de las entrevistas, **el nivel de sensibilización es alto**, aunque se detectan diferencias en cómo se aprecian las vulnerabilidades y la situación de exposición a los riesgos de los centros sanitarios en los distintos países.

Mientras que España, Francia e Italia tienen una percepción de alta vulnerabilidad en sus centros sanitarios derivada de la conciencia del riesgo, los centros sanitarios en Alemania tienen una mejor percepción de su preparación ante los riesgos de ciberseguridad.

Los responsables de ciberseguridad tienen conciencia de que el proceso de protección es continuo y desigual. El análisis del riesgo y la aplicación de medidas de ciberseguridad es una actividad reciente y existe un temor generalizado a avanzar a un ritmo más lento que la propia evolución de los ataques. El grado de preocupación en Alemania es menor, ya que consideran que tienen una conciencia establecida de gestión de riesgos y que cuentan con el apoyo del Gobierno alemán.

EN SUS PALABRAS:



Riesgos percibidos e incidentes en los centros sanitarios

Los centros sanitarios se encuentran en el punto de mira de los ciberdelincuentes. La información confidencial que albergan, como historiales médicos y datos personales, los convierte en un objetivo atractivo para ataques que pueden tener graves consecuencias, tanto para los pacientes como para las instituciones. Esta realidad es la base de las preocupaciones de los profesionales y así se han recogido en las diferentes entrevistas.

Los riesgos principales percibidos por los entrevistados se agrupan en 4 áreas:

1. **Seguridad del paciente.** La interrupción del servicio sanitario, además de consecuencias económicas para el centro, podría tener un impacto decisivo en la seguridad del paciente.

   Los hospitales dependen de sistemas informáticos y equipamiento médico para mantener las funciones vitales de los pacientes. Un ataque que involucre a estos sistemas provoca riesgos para la seguridad del paciente por la indisponibilidad del equipamiento electromédico o por alterar el tratamiento programado al paciente. Otros servicios, como la gestión de citas, laboratorio o pruebas médicas también podrían verse afectados retrasando la atención al paciente con consecuencias para su salud.

«Tenemos respiradores, escáneres... tenemos infinidad de equipos médicos conectados a la red corporativa, pero también hay elementos industriales como cámaras, biometría, sondas de temperatura, monitorización de CO2, muchos sensores. El riesgo hoy es que la industria no pensó en la ciberseguridad en los equipos médicos»
Director General - España

«Lo que más nos preocupa es la imposibilidad de garantizar la continuidad asistencial de los pacientes. Gestionamos pacientes bastante críticos desde el punto de vista de la continuidad asistencial. Es el aspecto que más repercutiría en la estructura»
Responsable Electromedicina - Italia

2. **Violación de la privacidad.** Los ciberataques pueden comprometer la confidencialidad de los datos médicos. Si los sistemas se ven afectados, los atacantes podrían acceder a historiales clínicos, diagnósticos, tratamientos y otra información de carácter personal. Esto no solo viola la privacidad del paciente, sino que también podría utilizarse para realizar chantajes o fraudes.

«El riesgo que observo es el secuestro de datos de pacientes que puedan ser revelados y, publicados o, manipulados o hacer cualquier tipo de uso fraudulento.»
CIO – España

«Creo que el principal problema son los ransomwares por dos motivos. La primera preocupación es la pérdida de datos, la segunda preocupación, que tiene menor impacto financiero, pero es más importante desde el punto de vista de la información, es la fuga de datos. Hoy en día, los datos sanitarios se venden a precios muy altos en el mercado negro.»
CISO - Francia

3. **Impacto financiero.** Además de las pérdidas derivadas de la interrupción del servicio, su recuperación y la imposibilidad de prestar los servicios sanitarios, hay que añadir las sanciones y repercusiones legales derivadas de los incidentes. Cuando se ven afectados datos personales, se pueden derivar sanciones debidas a la legislación de protección de datos personales, además de demandas de los pacientes afectados. Además, si el hospital tiene compromisos contractuales o afecta a terceros, pudiera enfrentarse a sanciones e indemnizaciones por dichos incumplimientos.

«La encriptación de la información. En este caso el hospital se queda sin información y para recuperar los datos hay que pagar el rescate.»
Director General - España

«La seguridad del paciente es nuestra preocupación porque toda la información de nuestros pacientes es confidencial. El impacto financiero, la reputación y las sanciones gubernamentales serán las consecuencias.»
Responsable Electromedicina - Alemania

4. **Impacto reputacional.** Un ciberataque puede afectar a la confianza de los pacientes en el hospital. Si se divulga públicamente que los datos han sido comprometidos o que los servicios se han visto afectados, la reputación del hospital sufrirá. Esto podría llevar a una disminución de pacientes y, en última instancia, afectar la calidad de la atención.

«Consecuencias de imagen, la reputación de nuestro hospital; sin saber si ponemos en compromiso a otro establecimiento a causa de nuestro phishing. Eso para mí es una preocupación, así que pusimos una seguridad en el correo electrónico más fuerte.»
CISO - Francia

Cuando se ha tratado de recoger información sobre los incidentes detectados y/o sufridos por los centros sanitarios, se comprueba que es un asunto muy sensible para los entrevistados, y en muchas ocasiones, han preferido no comentar nada sobre incidentes propios.

Todos los centros participantes han sufrido intentos de ataque, aunque no siempre tuvieron éxito. Se comparte como idea común que los ataques se van incrementado y es clave estar preparados para limitar el impacto en caso de que consigan afectar al centro sanitario.

Los canales utilizados para acceder a los sistemas que se han declarado en las diferentes conversaciones han sido el email, a través de campañas de phishing, y a través de equipos conectados a la red explotando alguna vulnerabilidad.

RESPONSABILIDADES EN LA GESTIÓN DE LA CIBERSEGURIDAD

Para conseguir una gestión adecuada de la ciberseguridad, es necesario establecer un proceso orientado a proteger (tareas de prevención) y a reaccionar en caso de un ciberataque (gestión de incidentes).

Ambas etapas deben estar coordinadas con las necesidades del negocio y, por lo tanto, deben intervenir los diferentes roles involucrados según su responsabilidad. Si se analiza la posición de cada rol respecto a su capacidad de decisión en ciberseguridad y su implicación operativa, en una primera aproximación, según describen los responsables, podemos considerar la siguiente distribución de responsabilidades.

Ilustración 9. Responsabilidades respecto a la ciberseguridad

Como podemos observar en la gráfica anterior, se representan las posiciones relativas de los diferentes roles respecto a la toma de decisiones y su aplicación operativa. Como figura de mayor responsabilidad, **el Director General será el último responsable de las decisiones económicas de asignación de presupuestos y aprobación de políticas de ciberseguridad.**

El Responsable de Electromedicina, a pesar de las repercusiones de los incidentes de ciberseguridad en la disponibilidad de los dispositivos médicos, tiene **menor capacidad de decisión sobre las medidas a tomar y una baja capacidad en la operación.**

Respecto a las figuras del CIO y el CISO encontramos más disparidad en las respuestas. Aunque el **CISO es quien tiene mayor responsabilidad en la operación de las medidas de ciberseguridad, en muchas ocasiones el CIO tiene mayor nivel de decisión** ya que es habitual una dependencia jerárquica entre ellos. Por lo tanto, encontramos que los presupuestos de ciberseguridad están incluidos en muchas ocasiones en los presupuestos de TI. En países como Italia, las responsabilidades del CISO son asumidas directamente por el CIO como parte de la gestión de los sistemas de información y operativos.

LA MADUREZ DE LA CIBERSEGURIDAD EN LOS DIFERENTES PAÍSES

La madurez en ciberseguridad se refiere al estado de desarrollo y eficacia de las medidas de seguridad que una organización ha implementado para proteger sus activos digitales. Una organización con un alto nivel de madurez en ciberseguridad será capaz de:

1. **Gobernar la seguridad:** la organización tendrá un marco de gobierno de seguridad que define las responsabilidades, los procesos y las políticas para la gestión de la ciberseguridad.

2. **Identificar y prevenir amenazas:** La organización tendrá una comprensión clara de los riesgos a los que se enfrenta y habrá implementado medidas para prevenir o mitigar el impacto de un ataque.

3. **Detectar y responder a incidentes:** La organización tendrá sistemas y procesos para detectar rápidamente los incidentes de seguridad y responder a ellos de manera eficaz.

4. **Recuperarse de un ataque:** La organización tendrá un plan de recuperación de desastres para minimizar el impacto de un ataque y restaurar sus sistemas a su estado normal lo más rápido posible.

Existen diferentes modelos para medir la madurez en ciberseguridad, pero generalmente se basan en cinco niveles:

- **L1 Inicial:** La organización tiene una conciencia limitada de los riesgos de seguridad y no ha implementado medidas formales de seguridad.

- **L2 Reactivo:** La organización reacciona a los incidentes de seguridad después de que ocurren. Pueden aplicar medidas de ciberseguridad, pero no de una forma planificada y analizada.

- **L3 Proactivo:** La organización ha implementado medidas de seguridad de una forma procedimentada para prevenir los incidentes de seguridad analizando los riesgos y estableciendo responsabilidades.

- **L4 Gestionado:** La organización tiene un enfoque sistemático para la gestión de la ciberseguridad, incluyendo métricas que permiten analizar la eficiencia de las medidas aplicadas.

- **L5 Optimizado:** La organización tiene un programa de ciberseguridad maduro que es continuamente mejorado y forma parte de las prácticas de la organización.

Aunque distinguimos 5 niveles en la valoración de la madurez, la mejora de la ciberseguridad no suele ser lineal. De hecho, el nivel de mejora más significativo lo encontramos entre el L2 y el L3, cuando se analizan formalmente los riesgos, se definen los procesos y se establece un proceso de mejora. Aunque en el L1 hay ciertas medidas de seguridad, no se suele hablar de un nivel aceptable de mejora, ya que las medidas son insuficientes y al no estar los procesos adecuadamente implantados, la ciberseguridad depende mucho de la cualificación y desempeño del personal, siendo muy complicado detectar la situación real de riesgo y la aplicación de mejoras.

El segundo incremento significativo lo encontramos entre el nivel L3 y L4 con la incorporación de las métricas de eficiencia de los controles, ya que mejora el nivel de seguimiento y la toma de decisiones. El nivel L5 generalmente se considera la institucionalización de la gestión de la ciberseguridad, incorporándose a las prácticas habituales de la organización. Esto se consigue con el tiempo según se va aplicando el sistema de mejora y la cultura general de ciberseguridad, obteniendo cada vez un mejor control, aunque habitualmente el salto no es tan elevado como entre los niveles anteriores.

La madurez en ciberseguridad es un proceso continuo que requiere una inversión constante de tiempo y recursos. Sin embargo, los beneficios de una buena madurez en ciberseguridad son significativos, ya que puede ayudar a proteger a la organización de las amenazas cibernéticas, reducir el impacto de un ataque y aumentar la confianza de los clientes y socios.

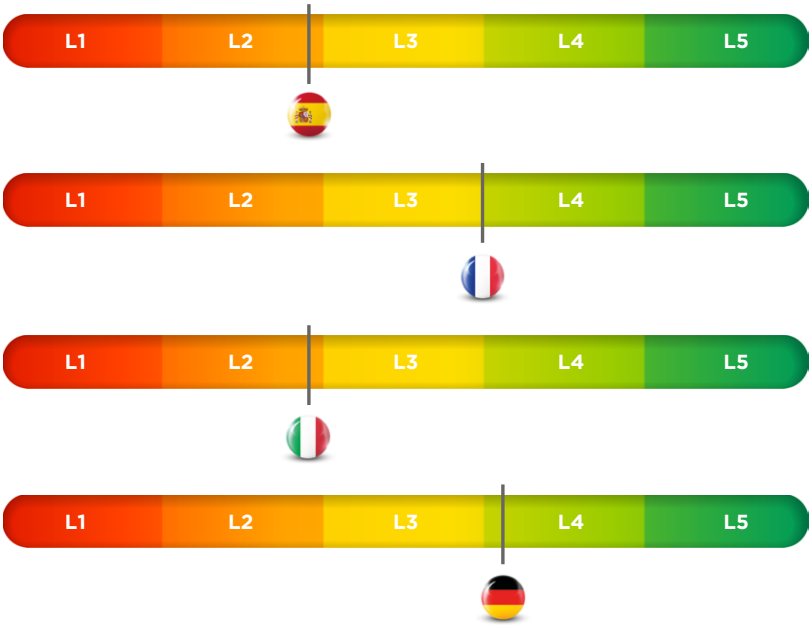
Considerando lo anterior, se ha conversado con los participantes en el estudio sobre sus modelos de ciberseguridad y la madurez que cuentan sus centros.

Los centros que evalúan su nivel de madurez en los ratios más bajos o iniciales, en general, alegan, bien falta de presupuestos para la inversión en ciberseguridad, o bien el hecho que los riesgos de ciberseguridad son una preocupación reciente en las organizaciones, por lo que todavía los proyectos no han alcanzado un nivel de madurez adecuado. En realidad, ambas razones suelen estar ligadas, ya que **es necesaria una correcta apreciación del riesgo para establecer presupuestos suficientes para su gestión.**

En el otro extremo de madurez, encontramos centros sanitarios donde se han establecidos procesos de análisis de riesgo ciber desde hace más años, contando con

mayores recursos y mayor sensibilidad hacia la ciberseguridad.

Como comparativa general, basándonos en las declaraciones de los participantes, podemos distinguir diferencias en la apreciación de la madurez de la ciberseguridad por los responsables. Mientras España e Italia se auto-definen entre el nivel L2-L3, Francia declara encontrarse entre los niveles L3-L4 y Alemania se percibe en un nivel más maduro, llegando hasta niveles de madurez claramente identificados en L4[1].



Un dato que debemos tener en cuenta en la interpretación del nivel de madurez es el perfil de los participantes. Si revisamos la titularidad y el tamaño de los hospitales participantes, España e Italia han obtenido respuestas tanto del sector público como del privado y con un tamaño de hospital entre mediano y pequeño. Sin embargo, Alemania y Francia cuentan con hospitales participantes de mayor tamaño y mayoritariamente del sector público.

[1]Estos datos se refieren a las declaraciones de los participantes en la muestra cualitativa, no representan a cada país ni son estadísticamente relevantes.

Se puede interpretar que los hospitales de mayor tamaño se ven más afectados por los riesgos de ciberseguridad al ser, en general, más dependientes de la tecnología. Asimismo, el sector público está más sujeto a regulaciones y fondos públicos que facilitan la implantación de medidas de seguridad. Cuando coinciden ambas características, se puede esperar, como vemos, que el nivel de madurez esté en diferentes puntos de desarrollo.

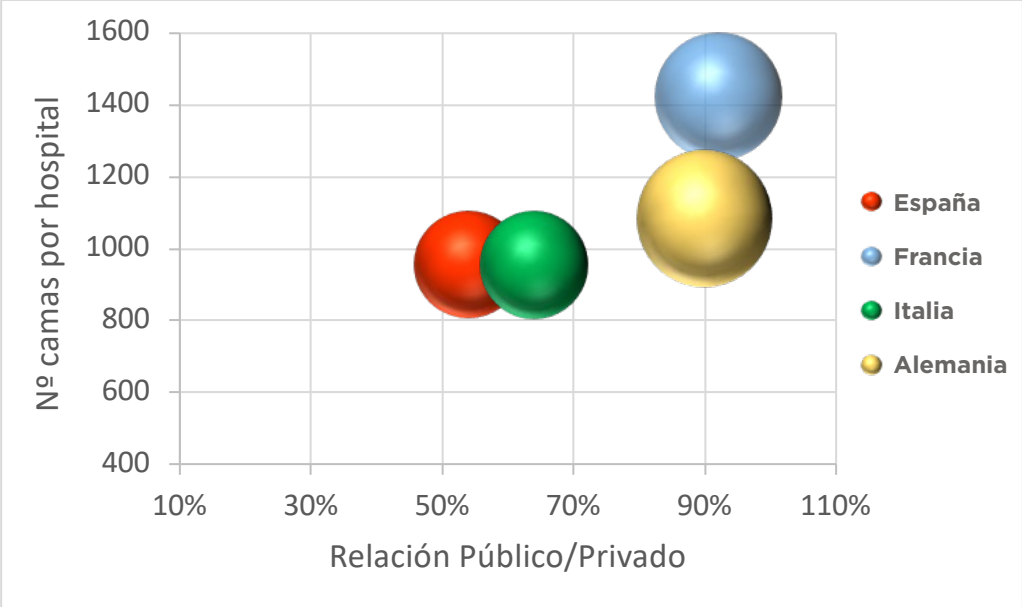


Ilustración 10. Titularidad y Nº camas de las entidades participantes y su relación con la apreciación de la madurez de la ciberseguridad

Si analizamos los niveles de madurez percibida considerando 5 características básicas de los sistemas de gestión de ciberseguridad podemos recoger las siguientes características:

Estructura de ciberseguridad y equipos dedicados

En los centros con menores niveles de madurez declaran una falta de estructura organizativa dedicada a la ciberseguridad. Tan solo los centros con altos niveles consideran que cuentan con la organización y equipos humanos necesarios para la gestión de los riesgos ciber. Esto se explica porque al tener sistemas de gestión basados

en análisis de riesgos, un mayor número de procedimientos y medidas técnicas de ciberseguridad, se requiere personal especializado y permanente para abordar estas tareas con garantías.

Los centros con menor nivel de madurez suelen delegar las tareas de ciberseguridad en el personal de TI, no siempre con la suficiente formación en ciberseguridad, o en equipos externos subcontratados ad-hoc para proyectos concretos. En este caso, es el responsable de TI quien desarrolla las tareas de ciberseguridad con muy poca participación de perfiles responsables de los equipos de electromedicina.

Sin embargo, en **los centros más maduros sí declaran tener un equipo dedicado a la ciberseguridad, coordinando sus actividades con los responsables TI de electromedicina.**

Presupuesto específico en ciberseguridad

Al igual que en el punto anterior, **un mayor nivel de ciberseguridad necesita de presupuestos propios** que permitan asignar personal, gestionar los riesgos y planificar las inversiones para las medidas derivadas del análisis de los riesgos.

Los centros con menor nivel de madurez no cuentan con presupuesto específico para ciberseguridad, incorporándose en los presupuestos de TI, por lo que se dificultan las inversiones estructurales, primando las adquisiciones necesarias para resolver situaciones de riesgo más inminente o tras sufrir algún incidente de ciberseguridad.

Los centros con mejor madurez sí cuentan con presupuestos específicos, involucrando a la dirección y a los responsables de todas las áreas afectadas.

Análisis de riesgos

La realización de un análisis de riesgos formal es una tarea clave y obligada en cualquier sistema de gestión de ciberseguridad y, por lo tanto, obligatoria a partir de niveles L3 de madurez. Hasta ese momento, normalmente las medidas de seguridad se seleccionan por una evaluación informal de los riesgos cubriendo las situaciones más críticas detectadas.

Tal y como declaran los responsables, en general **se apoyan en empresas externas para realizar este análisis de riesgos y en ocasiones, esperan el apoyo de las Administraciones Públicas.**

En los centros con altos niveles de madurez, se realizan análisis de riesgos periódicamente, al menos anualmente. En estos análisis se incluyen auditorías tanto internas como de terceras partes.

Formación y concienciación del personal

La formación y concienciación del personal es una tarea que se aborda normalmente desde las primeras etapas, ya que un nivel de formación y concienciación básica no requiere un gran presupuesto y **es una de las medidas fundamentales a tomar.**

Sin embargo, la formación, como otras medidas de seguridad, no siempre se implementa ajustada a las necesidades de cada perfil y evaluando los resultados e impacto en el riesgo. Los mismos responsables detectan debilidades como falta de frecuencia adecuada de la formación o no estar focalizada en las necesidades reales del sector sanitario.

Por el contrario, sistemas de formación más maduros, son capaces de solventar los problemas anteriores, creando programas anuales de formación ajustados a las necesidades de los diferentes roles y teniendo en cuenta las amenazas detectadas en el entorno.

Medidas de protección

En los centros donde se evalúan con niveles más bajos de ciberseguridad, declaran tener **medidas básicas de seguridad, principalmente medidas de control perimetral, antimalware, back-up y de control de tráfico en la red.**

Sin embargo, en los centros con **altos niveles de madurez se han instalado medidas alineadas con su análisis de riesgos**, cubriendo las áreas de riesgo detectadas e incorporando medidas como el análisis de tráfico inteligente, auditorías, adopción de estándares de ciberseguridad o equipos de respuesta a incidentes.

Aunque las medidas adoptadas por los centros con menores niveles de ciberseguridad son adecuadas, al no contar con un sistema de gestión, no se garantiza la mejora y la adaptación a los cambios del negocio y el entorno.

EL PAPEL DE LAS PÓLIZAS DE LOS SEGUROS CIBER

Las pólizas de seguros ante incidentes ciber se van abriendo camino en el sector sanitario, sin embargo, analizando las respuestas de los participantes, se detecta disparidad en su implantación, en las prestaciones y coberturas y en las expectativas que despiertan en el sector sanitario.

Por un lado, encontramos centros sanitarios que declaran tener pólizas de ciberriesgos, pero por otro lado, otros participantes no conocen las coberturas que proveen estos seguros o el rol que pueden jugar en caso de un ciberataque.

Los participantes creen que las principales debilidades de las pólizas actuales se centran en dos aspectos:

- **Falta de especificidad para el sector sanitario**, con un diseño generalista y apenas incluyendo peculiaridades del sector.
- **Una posición reactiva de compensación económica** y, en su caso, acompañamiento durante el incidente, pero no un acompañamiento preventivo para evitar los incidentes.

¿ESTÁ SU ORGANIZACIÓN CUBIERTA POR UN CIBERSEGURO? ¿QUÉ TIPO DE SEGURO? ¿QUÉ ASPECTOS CUBRE LA PÓLIZA DE SEGURO?

«Tenemos un seguro general que también cubre esta situación... debido a los crecientes riesgos y también para una mayor concienciación del tipo de riesgos que se pueden correr en este ámbito, también estamos estudiando con nuestro gabinete jurídico si mejorar la cobertura de nuestro seguro».
Responsable Electromedicina - Italia

«¡No! No estamos cubiertos por una póliza porque es difícil cumplir los criterios mínimos que exigen las compañías para ofrecer una póliza razonable».
CIO - España

«Todavía no tenemos. Pero creo que deberíamos proponerlo a la Dirección porque la frecuencia con la que podrían ocurrir aumentará inevitablemente en los próximos años».
Responsable Electromedicina - Italia

Entre las respuestas de los participantes, vemos que pocos hospitales consideran una póliza de ciberriesgo en este momento y la mayoría de los que cuentan con una póliza, son coberturas sobre los daños del equipamiento informático, no específicamente ante un ciber ataque.

Cabe pensar que las **pólizas de ciberriesgo deben evolucionar hacia un acompañamiento en la gestión del riesgo y la respuesta a incidentes**, considerando las necesidades respecto a la disponibilidad de los sistemas y la confidencialidad de la información que necesita el sector.

Este acompañamiento en la mejora se aplica a cualquier nivel de madurez de los hospitales. En una etapa más inicial, el propio estudio de viabilidad de la póliza ayuda a detectar las áreas más críticas de mejora (aquellas que determinan la asegurabilidad del centro). En esta etapa se demandan, además de apoyo en las auditorías iniciales y actividades de prevención, acompañamiento para responder a los incidentes, tanto para responder desde el punto de vista técnico como para dar soporte legal ante posibles sanciones o responsabilidad civil ante terceros.

Para aquellos centros con unos niveles mayores de madurez, **el ciber seguro puede ser un impulsor para la mejora del riesgo**, aportando información de las amenazas detectadas en el sector, mejores prácticas, selección de tecnologías, etc.

¿CREE QUE LOS SEGUROS PUEDE DESEMPEÑAR UN PAPEL CLAVE EN LA REDUCCIÓN DE LOS RIESGOS CIBERNÉTICOS? ¿CÓMO?

«Creo que sí, sin duda. En el aspecto económico... pero si las aseguradoras aportaran los conocimientos de profesionales expertos para intentar resolver el problema, creo que sería un gran servicio».
Director General - España

«Creo que el seguro puede decir, si aplicas estas políticas de seguridad puedo darte un porcentaje de descuento en la prima del seguro, indicaciones y sugerencias para mejorar la seguridad de toda la empresa».
CIO - Italia

«El seguro de ciberriesgo es interesante para tener un diagnóstico externo sobre la exposición al riesgo, y asistencia para reducirlo. El seguro en el aspecto económico puede tener un coste en función de la exposición al nivel de riesgo».
CIO - Francia

LAS NECESIDADES DE LOS HOSPITALES RESPECTO A LA CIBERSEGURIDAD

En las entrevistas realizadas con los responsables de los centros sanitarios se han detectado una serie de necesidades respecto a la ciberseguridad que podrían agruparse en cuatro grandes áreas.

Institucionales

Se demanda una **mayor implicación y colaboración de las administraciones públicas** para ayudar a los centros sanitarios en el gobierno de la ciberseguridad. Esta involucración debe desarrollarse con las inversiones necesarias, pero también con un desarrollo normativo que apoye a los centros sanitarios en la gestión de los riesgos ciber.

Actualmente se detecta falta de **desarrollo normativo** a nivel nacional de las nuevas normativas europeas en materia de ciberseguridad. Además de trasponer cuanto antes y de forma clara las regulaciones europeas, el sector sanitario, por sus especifidades, necesita de guías o interpretaciones específicas de las normas transversales, de forma que se aborden correctamente las áreas de riesgo del sector.

En el campo de las inversiones, se debe considerar el gap inicial de inversión en ciberseguridad y las necesidades continuas de actualización de sistemas y de personal cualificado. Esto requiere el **apoyo de las instituciones, considerando estas inversiones dentro de los presupuestos asignados a la sanidad.**

Por último, hay que señalar la necesidad de la **cooperación entre los diferentes actores** involucrados: sector público y privado sanitario, organismos públicos de ciberseguridad, entidades privadas, etc. La coordinación en la detección de amenazas, respuestas y planes conjuntos es fundamental.

Financieras

Los riesgos de ciberseguridad tienen un peso específico en los servicios sanitarios, por lo que deben tener su asignación presupuestaria específica en las organizaciones. Actualmente, estos presupuestos están incluidos en muchas ocasiones en los presupuestos TI o tecnológicos. Sin embargo, en lugar de una dependencia, es necesaria una **coordinación entre los desarrollos de digitalización y la ciberseguridad, contando cada área con su asignación presupuestaria específica que permita el desarrollo de los proyectos con autonomía.**

«La ciberseguridad no se trata de informática o tecnología, la ciberseguridad es salud»

CISO - España

Culturales

La formación en ciberseguridad debe convertirse en un requisito para todos los perfiles de los centros sanitarios, de forma que se convierta en parte de su cultura en sus tareas laborales.

La formación debe estar definida según las necesidades de cada rol, desde la dirección hasta el personal sanitario o de servicios y debe ser actualizada y reforzada periódicamente. Todo el personal debe contar con guías y procedimientos donde se describan las normas de ciberseguridad para su consulta en caso necesario.

«Los empleados deben ser conscientes del riesgo cibernético y formarse contra ciberdelitos, ser capaces de reconocer y responder a las amenazas cibernéticas».
CISO - Francia

«La falta de competencias digitales es una cuestión muy relevante, especialmente con las generaciones mayores. Tenemos que trabajar en ello».
Ingeniero de Electromedicina - Italia

Estructurales

Los hospitales deben establecer condiciones operacionales y técnicas adecuadas para cubrir las necesidades de ciberseguridad de sus sistemas. Esto pasa desde contar con un equipo técnico formado trabajando en local, hasta el diseño de redes, accesos, etc., incorporando criterios de protección.

Las medidas de seguridad de los equipos médicos merecen una atención especial, ya que es un ámbito donde todavía queda mucho por hacer respecto a la protección de sus conexiones. Añadido a esto, los riesgos de ciberseguridad se multiplican debido a la incorporación de la telemedicina y el incremento de las tecnologías digitales en el tratamiento y diagnóstico médico.

«Telemedicina, servicios en la nube, block chain... La ciberseguridad es más difícil cada día»
Director General - Alemania

«Necesitamos contar con expertos que conozcan las dificultades de operar en el sector sanitario... Considerando también que utilizaremos cada vez más procesos de telemedicina »
Ingeniero de Electromedicina - Italia

ESPAÑA: ASPECTOS CLAVE

Visión global de la situación de los centros

Percepción del riesgo ciber

Los ataques a centros sanitarios ocurridos en los últimos años, y concretamente en el periodo próximo al estudio, ha aumentado de forma muy importante la **percepción del riesgo ciber** entre los responsables participantes en las encuestas. En esta concienciación han tenido peso no sólo los ataques conocidos por saltar a los medios, sino también el aumento de los gestionados internamente que no se han conocido públicamente.

«Los riesgos cibernéticos que ya hemos visto en otros hospitales podrían causar colapso operativo, así que desde mi punto de vista como Director Médico de un hospital eso significa ciberseguridad como una preocupación».
Director General

¿Qué hay de los otros países participantes? El nivel alto en la percepción del riesgo es común en los 4 países debido al aumento de ciberincidentes y el impacto que producen. Esta situación es homogénea en el territorio europeo.

Percepción de la vulnerabilidad

Respecto a la **percepción de la vulnerabilidad** de las infraestructuras frente a los ciberataques, cabe destacar el esfuerzo que se está realizando por analizar los niveles de vulnerabilidad de las instalaciones y establecer un marco para su control. En este aumento de la percepción de la vulnerabilidad de las instalaciones cabe destacar el esfuerzo de los hospitales privados.

«El nivel de atención es muy alto, creo que los hospitales se dan cuenta de la situación actual y empiezan a gestionar el riesgo con sistemas centralizados para disminuir el acceso al sistema, pero los riesgos siempre están presentes».
CIO

¿Qué hay de los otros países participantes? Sobre la percepción de cuan vulnerables son los centros sanitarios, se detectan diferencias de apreciación. Mientras que España e **Italia** muestran ambos países niveles elevados en cuanto a su preocupación por la vulnerabilidad de los centros sanitarios, en **Francia** desciende este nivel a moderado porque consideran que se están empezando a tomar medidas al respecto. Solo **Alemania** considera que la vulnerabilidad es baja porque cuentan con regulaciones que ayudan a proteger los centros sanitarios.

Organización de la ciberseguridad

Si analizamos los **niveles de organización respecto a la ciberseguridad**, cabe destacar que en España existe esencialmente un **equilibrio** entre instalaciones **privadas y públicas**, no apreciándose diferencias reseñables.

En general, el sistema sanitario español **trabaja con rapidez en la mejora de la organización** de la ciberseguridad, destacando:

- Evaluación de riesgos, apoyándose en proveedores externos.
- Protección de la ciberseguridad.
- Atención a las certificaciones en la selección de proveedores.

Por el contrario, hay otros aspectos como la **formación y concienciación de los empleados**, proceso completo de la **gestión de riesgos y los planes de continuidad** que necesitan de **mayor desarrollo**.

La **necesidad de personal especializado en ciberseguridad** en la plantilla de los centros sanitarios es una demanda en la que coinciden ampliamente todos los participantes tanto para poder implementar las medidas de ciberseguridad como para poder responder adecuadamente en caso de un ciberincidente. Esta necesidad está presente en todas las áreas tecnológicas, tanto en TI como en los sistemas electromédicos.

¿Qué hay de los otros países participantes?

En **Italia** se refleja una mayor diferencia entre el sector público y el privado. Los centros públicos parecen encontrarse en un estado más embrionario debido a dificultades presupuestarias y de cooperación con el sistema sanitario público. Los centros privados, sin embargo, pueden superar mejor estas limitaciones debido a que cuentan con mayor presupuesto y más agilidad en las relaciones con los proveedores.

En **Francia** la situación es más heterogénea, encontrando diferentes niveles de madurez respecto a la organización. La falta de medios económicos y de personal de ciberseguridad son las necesidades más repetidas, aunque los centros que han sido capaces de solventar estas dificultades se muestran más evolucionados respecto a la ciberseguridad.

Alemania manifiesta un buen nivel organizativo según los centros participantes. Se ha hecho un esfuerzo en materia de formación en ciberseguridad y en la asignación de presupuestos ligados a los proyectos tecnológicos. Además, las directrices establecidas por la Administración han facilitado el proceso de aseguramiento.

Seguros ante incidentes de ciberseguridad

Respecto a la **penetración de las pólizas de ciberriesgo** en el sector sanitario, la opinión es desigual según el rol del participante. Mientras que en los puestos de dirección los seguros son mejor valorados, en los niveles técnicos no se considera tan relevante contar con un seguro de ciberseguridad.

Del total de participantes en España, tan solo un centro tenía una póliza específicamente de ciberseguridad y otros 4 habían integrado alguna cobertura dentro de pólizas de protección tecnológica.

En general, se considera **positiva** la oportunidad de realizar una **evaluación de los riesgos ciber** y obtener una serie de **recomendaciones** para mejorar los niveles de protección por parte de la compañía aseguradora. También se reconoce la utilidad de la **compensación de daños** en caso de materializarse un incidente.

Por el contrario, los participantes opinan que el seguro ciber tiene **escaso impacto en la prevención** de los ataques, no jugando un papel activo en este aspecto. Echan de menos una **mayor participación de las compañías aseguradoras** en la gestión de los riesgos de ciberseguridad detectados.

¿Qué hay de los otros países participantes?

Apreciamos una situación similar en todos los países con una baja penetración de las pólizas de ciberriesgo en el sector sanitario. Está bien valorada la ayuda técnica en caso de ciberincidente y la cobertura de daños y pérdidas, pero los requisitos de ciberseguridad o legales suponen una barrera de entrada. En **Italia**, en general, se incluyen en otras pólizas alguna de las coberturas de riesgos ciber, pero los encuestados no cuentan con pólizas expresamente de ciberriesgo, siendo un producto bastante desconocido. En **Francia**, hay un mayor conocimiento de este producto, pero poca penetración. Las pólizas contratadas, como en el caso anterior, cubren solo algunos aspectos de los riesgos en TI, aunque ya se va estudiando la opción de contratar pólizas expresamente de ciberriesgo. Por último, en **Alemania**, ser repite la poca implantación del seguro y el desconocimiento de este por el personal más técnico (TI, electromedicina).

«Las aseguradoras son empresas especializadas, ¿verdad? Pueden realizar auditorías y pueden asesorarte sobre las herramientas y todo lo demás».

Director General

«¡Yo no lo veo así! En mi opinión, no desempeñan un papel clave en la reducción de los riesgos cibernéticos».

Responsable Electromedicina

Implicación de los roles participantes

Si consideramos la implicación en la ciberseguridad de los diferentes roles, según los resultados de las entrevistas en España, los **Directores Gerentes y los CISO son los roles más involucrados**, mientras que los **CIO y Responsables de Electromedicina son los profesionales menos involucrados** en las funciones de ciberseguridad.

Esto indica que las funciones del CISO están cada vez mejor definidas y reconocidas dentro de las organizaciones, pero es necesario incidir en la coordinación interna en la detección de riesgos y aplicación de medidas.

Director General

Los Directores Generales asumen las **tareas presupuestarias**, asignando presupuestos específicos para ciberseguridad que cada vez más son gestionados por profesionales dedicados a esta materia (CISO).

La dirección general es responsable de la toma de decisiones en la **contratación de las pólizas de seguros** para cubrir los riesgos ciber, valorando la colaboración de las compañías aseguradoras en el análisis de riesgo y la propuesta de mejoras.

Como **necesidades** detectadas señalan:

- Aumentar el presupuesto específico relacionado con la ciberseguridad.
- Equipo interno de expertos especializados en ciberseguridad.
- Regulaciones de ciberseguridad.
- Inversiones públicas.
- Equipos (interno o externo) para intervenir en caso de ataque.

¿Qué hay de los otros países participantes?

En todos los países es la Gerencia la responsable tanto de aprobar los presupuestos como de contratar un seguro ciber. Respecto a las necesidades, coinciden con las destacadas en España, aunque **Alemania** incide más en la necesidad de una cultura de ciberseguridad y **Francia** destaca la necesidad de implementar más medidas técnicas en los sistemas.

CISO – Responsable de Ciberseguridad

El CISO o Responsable de Ciberseguridad es quien **propone las necesidades** respecto a la ciberseguridad y **presenta los presupuestos** a la dirección del centro. En ocasiones, este presupuesto es parte del presupuesto de TI, pero es habitual que el CISO se responsabilice de esta partida presupuestaria.

El CISO también **participa en el proceso de contratación del seguro**. Participa en la definición de las coberturas necesarias, evaluación de los servicios ofrecidos por la compañía aseguradora y proporciona la información necesaria para la evaluación del riesgo.

La principal necesidad mencionada por los CISO, se refiere a la posibilidad de **crear un equipo interno de expertos especializados en ciberseguridad**. La falta de personal especializado en el mercado es un freno para la aplicación y mantenimiento de medidas de seguridad en los centros sanitarios.

¿Qué hay de los otros países participantes?

Los roles del CISO son prácticamente similares en todos los países participantes. Solo señalar que en **Italia** no está claramente definido este rol CISO, siendo asumido por el responsable de TI (CIO). Como necesidades, todos coinciden en la necesidad de contar con un equipo interno experto en ciberseguridad que sea capaz de implementar y gestionar las medidas aprobadas y responder en caso de incidente. **Alemania** añade, al igual que la dirección general, la necesidad de extender la cultura de la ciberseguridad en las organizaciones.

CIO – Responsable de TI

El CIO, bien porque los presupuestos de ciberseguridad están dentro de los sistemas de información o porque deben coordinarse los proyectos de ambas áreas, **participa en los presupuestos relacionados con la ciberseguridad** en colaboración con el CISO.

En el caso de que el centro sanitario cuente con un responsable de ciberseguridad, la implicación del CIO en estas tareas se limita a la **coordinación con el CISO** para el desarrollo de los proyectos, el despliegue de soluciones en los sistemas, etc.

Respecto al **seguro ciber,** en general los CIO están **menos involucrados** en la contratación de un seguro de ciberseguridad y muestran menos interés en las mejoras técnicas derivadas del proceso de contratación del seguro. Consideran que el papel principal del seguro es la cobertura financiera/legal, no la mejora técnica.

Como principales **necesidades** mencionan la creación de **un equipo interno de expertos en ciberseguridad especializados**, capaces de gestionar la ciberseguridad no sólo en el departamento de informática, sino en todos los departamentos del hospital.

¿Qué hay de los otros países participantes?

Tal y como se ha dicho anteriormente, en **Italia** añaden a las tareas comunes de este rol, las responsabilidades en ciberseguridad. Las funciones, por otro lado, son comunes en todos los países. Respecto a las necesidades detectadas, coinciden con España y los CISO en la necesidad de contar con personal experto en plantilla. **Francia**, por su parte, añade la necesidad de la publicación de Guías y Normativas específicas de ciberseguridad para el sector sanitario y ayudas públicas e **Italia** insiste en la formación en general de toda la plantilla.

Responsable de Electromedicina

Los **Responsables de Electromedicina son los menos involucrados** en las decisiones de ciberseguridad. Sin embargo, puesto que la disponibilidad de los equipos médicos es una de las prioridades de sus funciones, consideran que sus actividades se pueden ver afectadas por los ciberataques. Por lo tanto, los Ingenieros de Electromedicina están poco implicados en las decisiones respecto a la ciberseguridad, pero demandan coordinación en el centro sanitario para incorporar sus necesidades en la estrategia de ciberseguridad del centro sanitario.

Respecto a los seguros de ciberseguridad, son los profesionales **menos concienciados** de su necesidad de contratación, no valorando el papel que desempeñan en la reducción de los riesgos cibernéticos.

Los Responsables de Electromedicina, como necesidades específicas, mencionan las siguientes:

- Establecer las **medidas de seguridad** necesarias para garantizar la continuidad del servicio, la seguridad de los datos sanitarios y la protección frente a ciberataques.

- Establecer **procesos de coordinación interna** con electromedicina para considerar las necesidades de ciberseguridad de una forma integral.
- Incorporar **personal experto en ciberseguridad** en su área hospitalaria.

¿Qué hay de los otros países participantes?

La menor involucración en presupuestos y gestión de la ciberseguridad, es común en todos los países participantes. Tampoco es habitual que este perfil se involucre en las decisiones del seguro ciber.

Respecto a las necesidades detectadas, todos coinciden en la necesidad de mejorar las medidas de ciberseguridad de los equipos médicos. **Italia** y **Francia** demandan además regulación en ciberseguridad para el sector sanitario y mayores presupuestos. Además, **Francia** coincide con España en la necesidad de formación en ciberseguridad del personal responsable de los equipos médicos.

RESULTADOS CUANTITATIVOS

05

05 RESULTADOS CUANTITATIVOS

La segunda parte del estudio se ha basado en los datos recogidos a través de una encuesta online enviada a representantes de los diferentes perfiles en los países objeto de estudio.

A través de las preguntas realizadas se analizan varios aspectos de la ciberseguridad en los centros sanitarios. El objetivo es establecer cómo perciben los riesgos de ciberseguridad, qué presupuestos se asignan a su gestión, cómo se organizan los centros sanitarios para afrontar estos retos y qué medidas de seguridad se consideran prioritarias para elevar los perfiles de madurez en la prevención y respuesta de los incidentes ciber.

SENSIBILIZACIÓN RESPECTO A LA CIBERSEGURIDAD EN LA SANIDAD

La ciberseguridad es una preocupación en los centros sanitarios que se ha ido elevando en los últimos años desde los perfiles más técnicos vinculados a las áreas TI hasta las gerencias médicas y la dirección de los centros sanitarios.

Esta concienciación viene derivada de la evidencia de que, en un entorno cada vez más digital, los incidentes de ciberseguridad afectan gravemente a la atención al paciente, a la confidencialidad de los datos sanitarios e, incluso, a la seguridad del paciente. En resumen, **la ciberseguridad no es tan sólo un problema técnico, sino del propio servicio de salud.**

¿Cómo afecta la ciberseguridad a las organizaciones sanitarias?

Cuando se pregunta a los centros sanitarios si han tenido algún incidente de ciberseguridad significativo, al menos la mitad de ellos declaran haber sufrido un ataque en sus establecimientos. Cabe destacar que **la mayoría de ellos han sido en los últimos 3 años**, lo que es coherente con el aumento de ataques en el sector sanitario tras la pandemia por el coronavirus Covid 19.

En España, se ve claramente como los ataques se han ido incrementando en los tres últimos años, identificando más de la mitad de los ataques en el periodo más cercano a la realización de la encuesta. Por el contrario, en **Italia** parece haberse reducido el nivel de incidencia en el último año, y en **Alemania**, a pesar de haberse reducido el nivel de ataques en los últimos 3 años, el perfil de incremento es similar al español.

Francia, es el país de los participantes donde menos hospitales declaran haber sufrido un incidente, más de la mitad no se han visto afectados de forma significativa. Sin embargo, también se detecta un incremento en los últimos meses antes de la realización de esta encuesta.

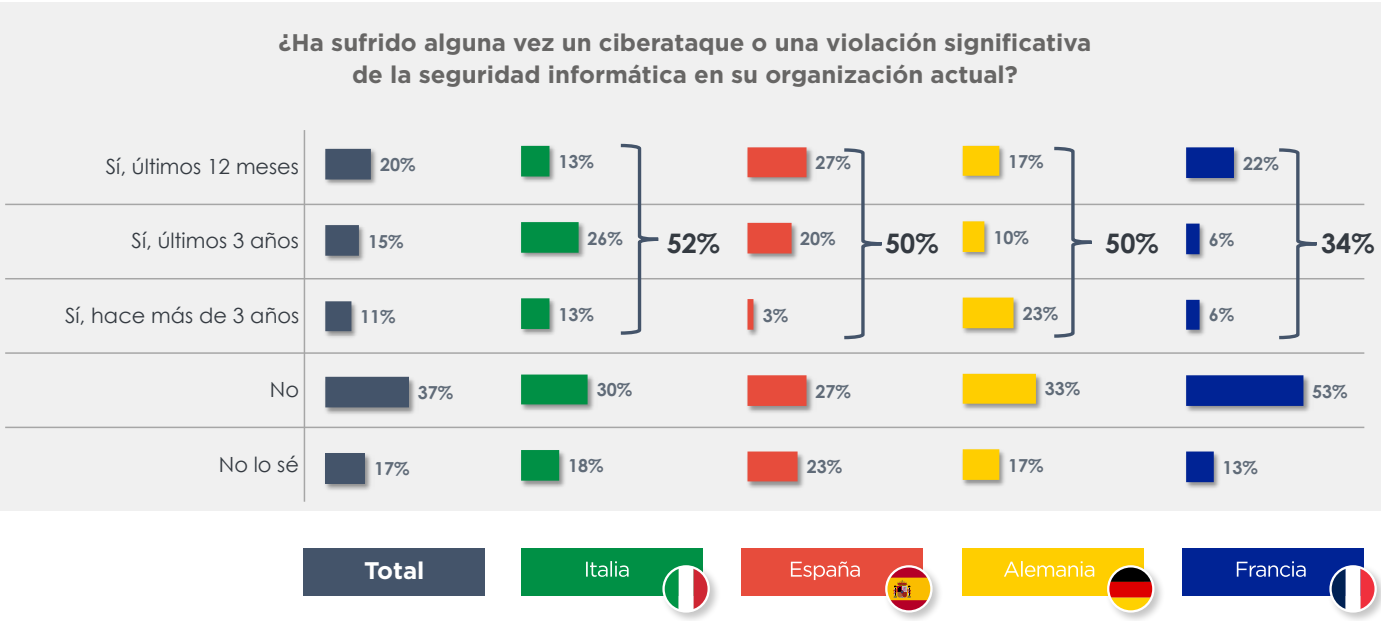


Ilustración 11. Ciberataques en centros sanitarios

Los ciberincidentes provocan diferentes impactos sobre los centros sanitarios. Respecto al nivel de preocupación declarado por los participantes, podemos ver **bastante similitud en todos los países**.

La **seguridad del paciente, el compromiso de los datos clínicos y la continuidad del servicio** son los impactos que generan **mayor preocupación** en los centros sanitarios.

Las **repercusiones financieras y reputacionales, la tensión del personal y las sanciones** estarían dentro de un nivel medio en la preocupación del sector, con algunas diferencias entre los países, como la mayor preocupación por el impacto reputacional en Alemania.

Ilustración 12. Principales impactos de la ciberseguridad sobre el sector sanitario. Países

Si analizamos el nivel de preocupación de los diferentes perfiles profesionales por las consecuencias y los incidentes de ciberseguridad, vemos que se mantienen los mismos resultados que los obtenidos por países, por lo que podemos establecer que **hay un acuerdo en el sector sanitario sobre los principales impactos derivados de un ciber ataque**. Además hay una conciencia clara de otros impactos, también relevantes, pero considerados con una relevancia intermedia en comparación con la seguridad de paciente, la seguridad de los datos y la continuidad del servicio.

Ilustración 13. Principales impactos de la ciberseguridad sobre el sector sanitario. Responsables

Principales preocupaciones respecto a la ciberseguridad en el futuro próximo

Ante la pregunta de qué impactos de la ciberseguridad preocupan en el futuro próximo a los centros sanitarios, vemos que se mantienen en las dos primeras posiciones la **pérdida de confidencialidad de los datos y el ransomware**.

Los datos personales son un activo valioso tanto para el hospital como para los ciberdelincuentes. Para el hospital, la pérdida de confidencialidad puede provocar un

fuerte impacto reputacional, sanciones y litigios por responsabilidad civil, ya que se ven afectados los derechos de los ciudadanos.

El ransomware es un tipo de ataque en el que se está detectando una evolución en el entorno de los atacantes. Por un lado, se van **profesionalizando grupos de ciberdelincuentes** en las diferentes herramientas necesarias para ejecutar un ransomware, lo que facilita este tipo de ataques por grupos menos 'profesionales', aumentando la incidencia. Por otro lado, ante la mejora de las medidas de seguridad de los centros sanitarios, también se están detectando **ataques dirigidos**, con un estudio previo de los sistemas del hospital, lo que hace más complicada una defensa eficaz.

En paralelo a estos dos tipos de ataque vemos cómo preocupan en mayor o menor medida **incidentes relacionados con las conexiones en el sistema sanitario**: la telemedicina, el teletrabajo y las conexiones entre diferentes centros y organismos del propio sistema sanitario. Esto viene derivado de la apertura de los hospitales como centro de atención sanitaria. El entorno físico del hospital se amplía al domicilio del paciente, a otros organismos de diagnóstico o especialización e incluso a la asistencia remota de expertos en disciplinas concretas. Esto implica una mayor conectividad y un mayor riesgo en la gestión de los datos de salud.

Por otro lado, la digitalización conlleva una mayor dependencia de proveedores, tanto para los propios sistemas TI como para los servicios sanitarios. No solo los aplicativos de los sistemas pueden introducir riesgos y errores en la prestación de los servicios, sino que proveedores especializados prestan servicios dentro del propio hospital, conectados a las redes digitales del centro. Esto, como estamos viendo, introduce nuevos **riesgos de la cadena de suministro** que ya se revelan como una preocupación en el sector.

Como en el caso anterior, el perfil de preocupación por estos riesgos que se adivinan en un futuro próximo, se reproduce si los presentamos según el perfil profesional. Por lo tanto, vemos que **el sector comparte las preocupaciones venideras en ciberseguridad**.

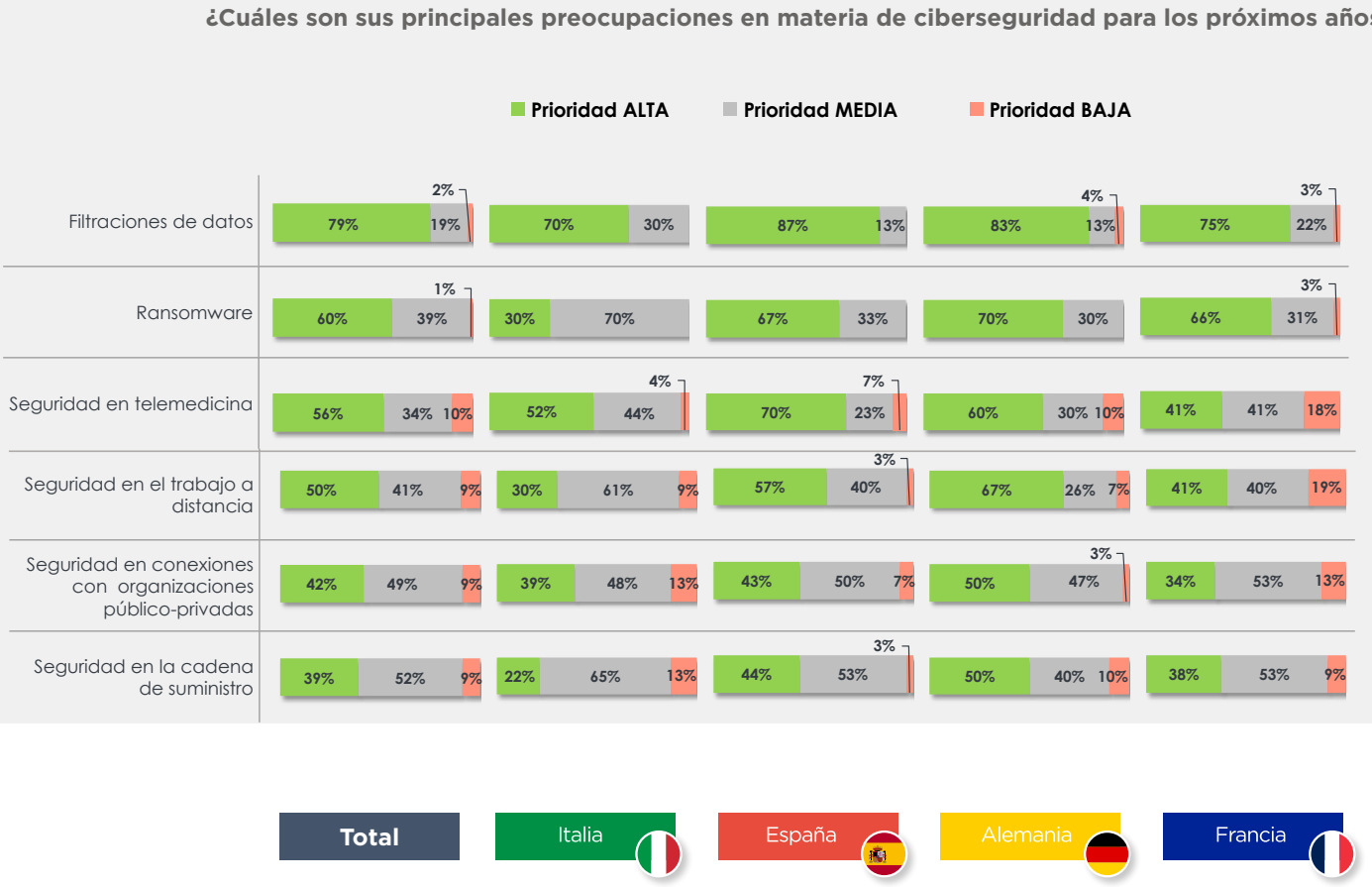


Ilustración 14. Tendencia del impacto de la ciberseguridad. Países

Ilustración 15. Tendencia del impacto de la ciberseguridad. Responsables

Áreas de desarrollo de la ciberseguridad prioritarias

A la vista de los riesgos percibidos y los principales retos que se esperan en un futuro próximo, se consulta sobre las áreas en las que los centros sanitarios invertirían prioritariamente. Como se puede ver, todos los temas recogidos en la encuesta están en la lista de prioridades del sector, haciendo complicada una priorización y exigiendo un abordaje en paralelo en diferentes líneas de acción.

La **seguridad de los datos** es el **área de inversión prioritaria** en todos los países. Sin embargo, encontramos diferencias en las prioridades de otros grupos de proyectos.

España, excepto en la temática referida a los requisitos de certificación de productos sanitarios, donde la prioridad está situada en la media europea, destaca la priorización en la inversión en la seguridad de la telemedicina, el desarrollo de normativa sobre ciberseguridad y la seguridad de los dispositivos médicos. Además, surge la necesidad de invertir en la seguridad del uso de IA en el entorno sanitario, asignándole una prioridad muy por encima de la media europea.

Ilustración 16. Áreas de inversión en ciberseguridad. Países

Si analizamos los resultados por los diferentes perfiles profesionales participantes, vemos como la seguridad de los datos sigue siendo la principal preocupación y área para la priorización de inversiones.

Además, podemos observar cómo **los Ingenieros de Electromedicina destacan por encima de la media en sus necesidades de inversión** en las áreas relacionadas con los dispositivos médicos, como son la certificación de productos sanitarios, la telemedicina y los equipos médicos portátiles implantados en el paciente. Además, este grupo de profesionales destaca sobre el resto de perfiles en la necesidad de inversión en la seguridad de la IA, normalmente vinculada a áreas médicas o de análisis de datos obtenidos en pruebas médicas.

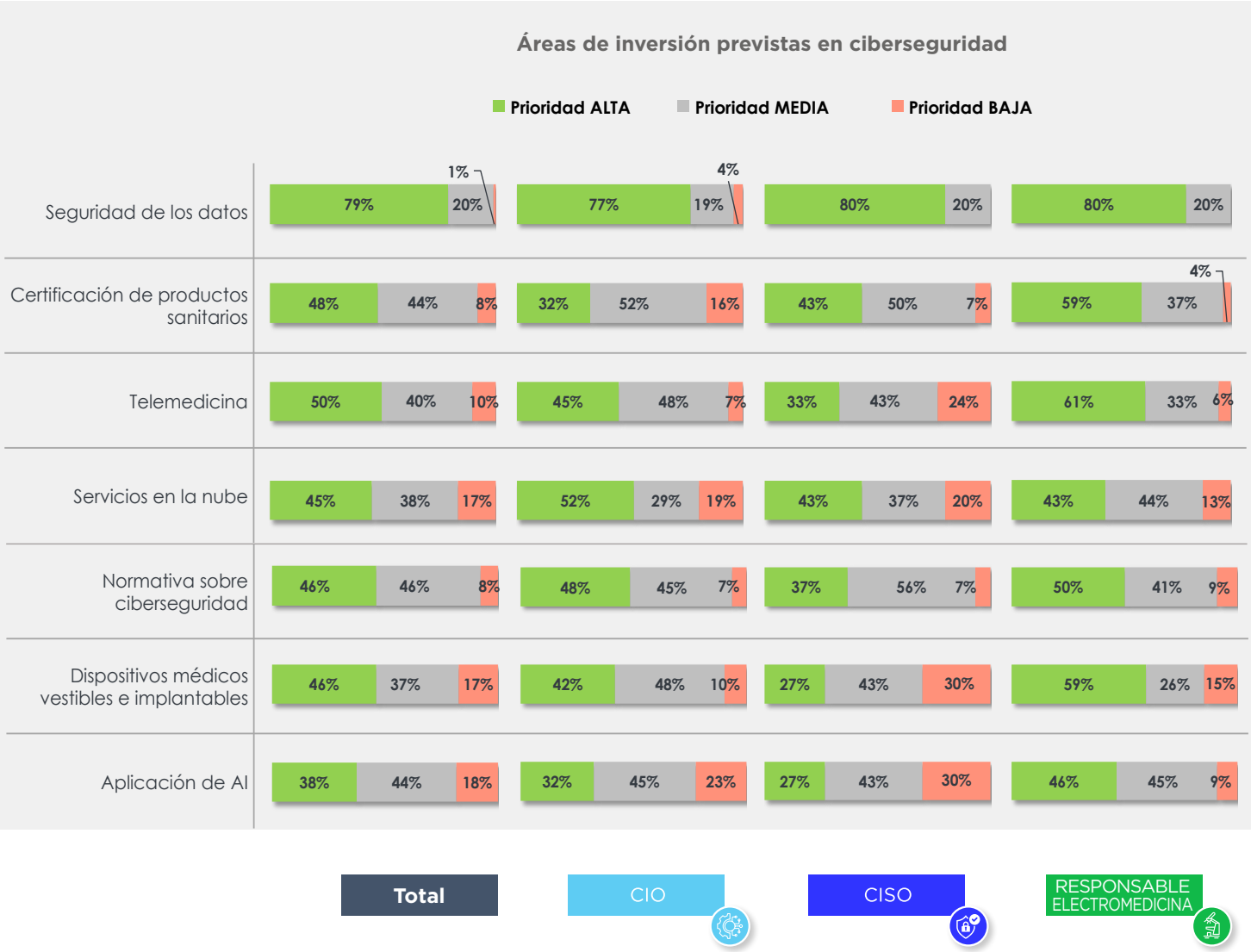


Ilustración 17. Áreas de inversión en ciberseguridad. Responsables

ESTRUCTURA DE LA ORGANIZACIÓN DE LA CIBERSEGURIDAD

En la gestión de la ciberseguridad, además de las medidas técnicas y procedimentales concretas que hay que aplicar, es importante establecer una colaboración eficaz entre las partes implicadas en la evaluación de los riesgos y en la necesidad de protección ante incidentes ciber.

Normalmente, esto se hace a través de comités específicos de ciberseguridad, pero como elementos indispensables cabe destacar:

- **Establecimiento de responsabilidades** en materia de ciberseguridad según perfil profesional.
- **Conocimiento** de cada perfil del impacto de la ciberseguridad y las medidas necesarias según sus responsabilidades.
- **Canales de comunicación** establecidos entre los diferentes responsables para gestionar la ciberseguridad en todo su proceso.

En los centros sanitarios, la ciberseguridad no es sólo responsabilidad del CISO. Esta figura será quien desarrolle el análisis de riesgos, proponga las medidas a desplegar y gestione la ciberseguridad de la operativa del hospital. Sin embargo, otras figuras deben estar involucradas en la gestión de la ciberseguridad.

En este estudio se ha evaluado la organización establecida entre los CISO, CIO y Responsables de Electromedicina. Aunque podríamos haber incorporado otros roles como la Dirección General, los Responsables de Infraestructuras hospitalarias o los Responsables de Protección de Datos (DPO), se ha centrado el estudio en los tres primeros. Consideramos que en el estado actual de madurez de la ciberseguridad en el sector sanitario, es suficiente con esta aproximación, dejando para futuros análisis un alcance más amplio.

El CIO es el Responsable de los Sistemas de Información y gestiona la operativa de la red y las tecnologías conectadas. Por lo tanto, debe trabajar directamente con el CISO, ya que las medidas definidas deben implementarse en su área de responsabilidad.

El Responsable de Electromedicina es una figura que, aunque parezca no estar directamente involucrada, **es la máxima responsable de la disponibilidad y la correcta operación de los equipos electromédicos**. Por lo tanto, los efectos de un incidente repercuten directamente en su campo de trabajo y deben ser partícipes de las necesidades de protección y operación segura de estos equipos. Por otro lado, también tienen responsabilidad en la **planificación de compras y mantenimientos**, momentos importantes en el ciclo de vida de los equipos en los que se deben incorporar criterios de ciberseguridad.

Identificación de responsabilidades respecto a la ciberseguridad

Como podemos ver en la imagen siguiente, en general, **los centros sanitarios no han alcanzado niveles adecuados de madurez en la identificación de responsabilidades**. Globalmente, tan solo un 49% de las organizaciones las han identificado en las áreas tecnológicas, con menos de un tercio que lo han hecho en toda la organización.

En España, aunque mejora el porcentaje de los centros que declaran no haber identificado sus responsabilidades en ningún área, vemos que hay un alto grado de definición en áreas tecnológicas con una menor identificación en otras áreas del centro sanitario.

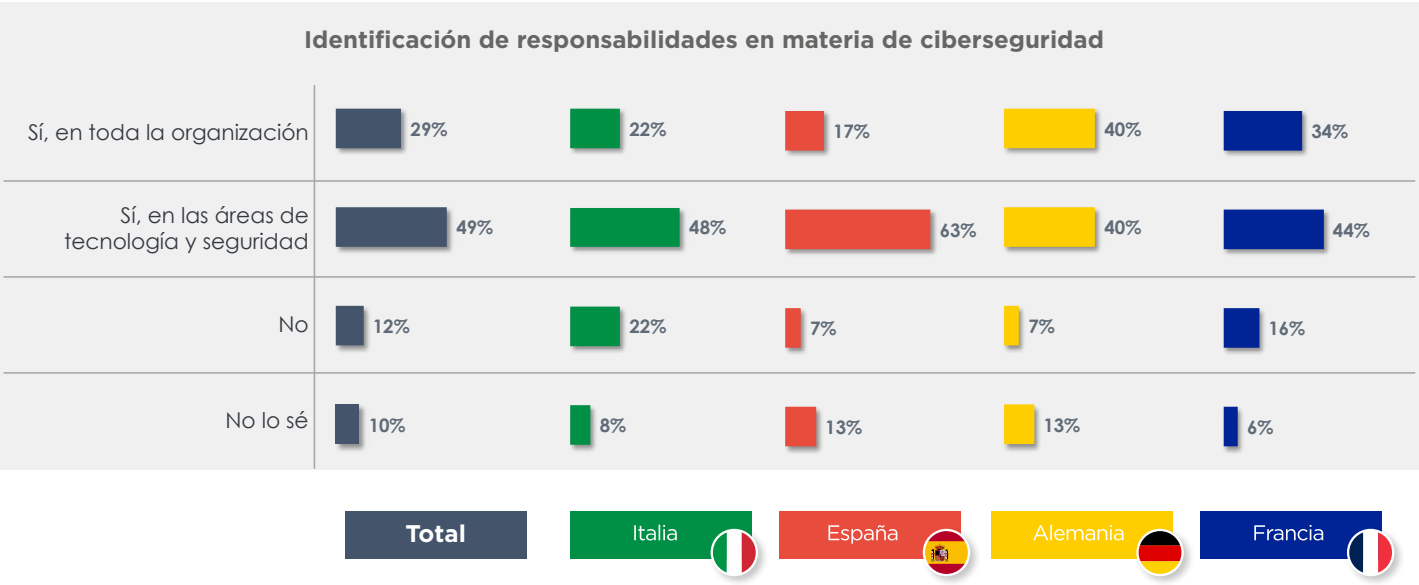


Ilustración 18. Identificación de responsabilidades

Si analizamos la misma pregunta respecto a los diferentes perfiles encuestados, vemos una respuesta bastante homogénea. Todos los perfiles coinciden en que, mayoritariamente, se definen responsabilidades en las áreas técnicas y en un menor grado en el resto de la organización. Cabría pensar que quizás no se conozca desde las funciones técnicas las responsabilidades en otras funciones organizativas, pero aún en este caso, nos indicaría una **deficiente coordinación en las organizaciones sanitarias en la definición de responsabilidades**.

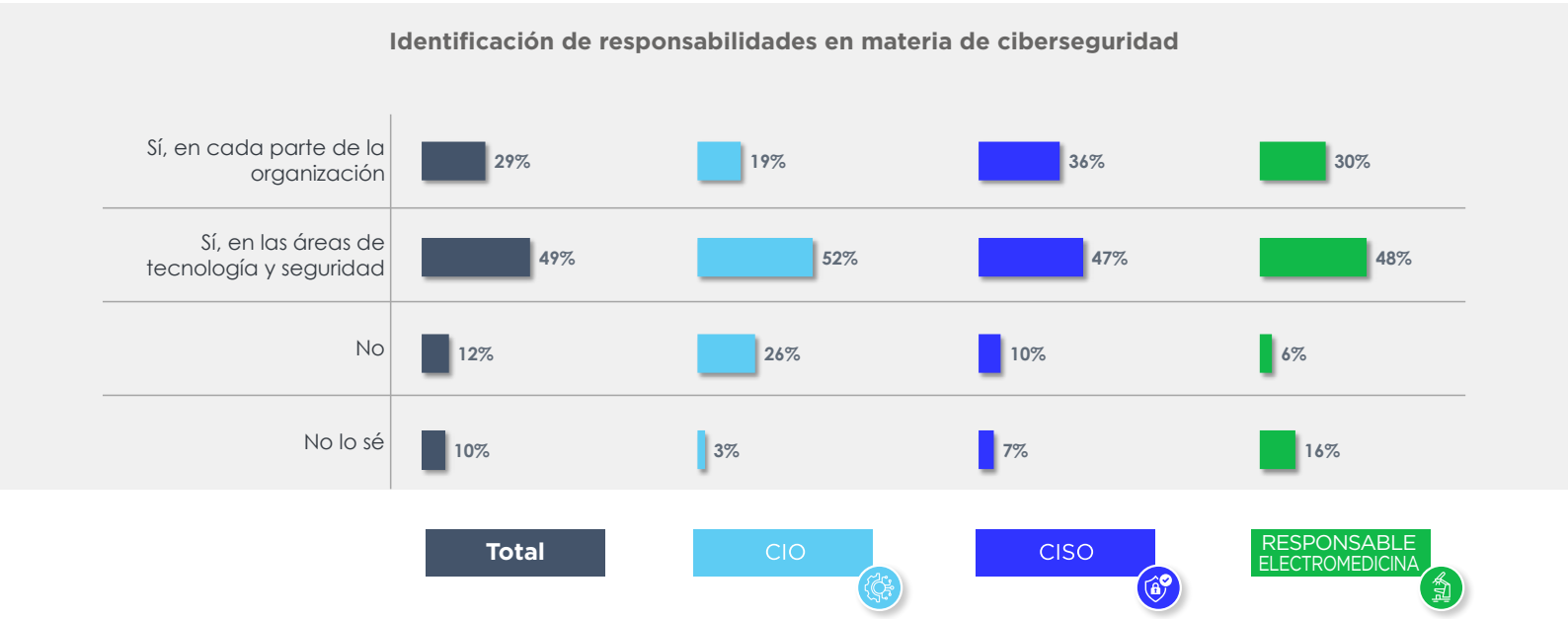


Ilustración 19. Identificación de responsabilidades por perfiles

Relación entre los responsables de los centros sanitarios respecto a la ciberseguridad

Un dato que permite ilustrar la madurez en la organización de la ciberseguridad es la línea de reporte tanto del CISO como del Responsable de Electromedicina. El CISO debería tener su propia área de competencia, independiente del CIO o responsable tecnológico, ya que son tareas diferenciadas, con sus propias responsabilidades y, en ocasiones, pueden entrar en conflicto (puesta en operación de soluciones vs controles de seguridad testados).

Como podemos apreciar en las siguientes ilustraciones, casi un 70% de los participantes en España manifiesta que **el CISO depende jerárquicamente del CIO**. En estos casos, el presupuesto de ciberseguridad estará incluido en los presupuestos TI y posiblemente los proyectos ciber no tengan suficiente visibilidad a nivel de la dirección del centro sanitario.

Estos datos destacan sobre **Italia**, donde también se reporta mayoritariamente al CISO, pero sobre todo respecto a **Alemania** y **Francia**, donde los Responsables de Ciberseguridad si reportan mayoritariamente al Director General del centro sanitario.

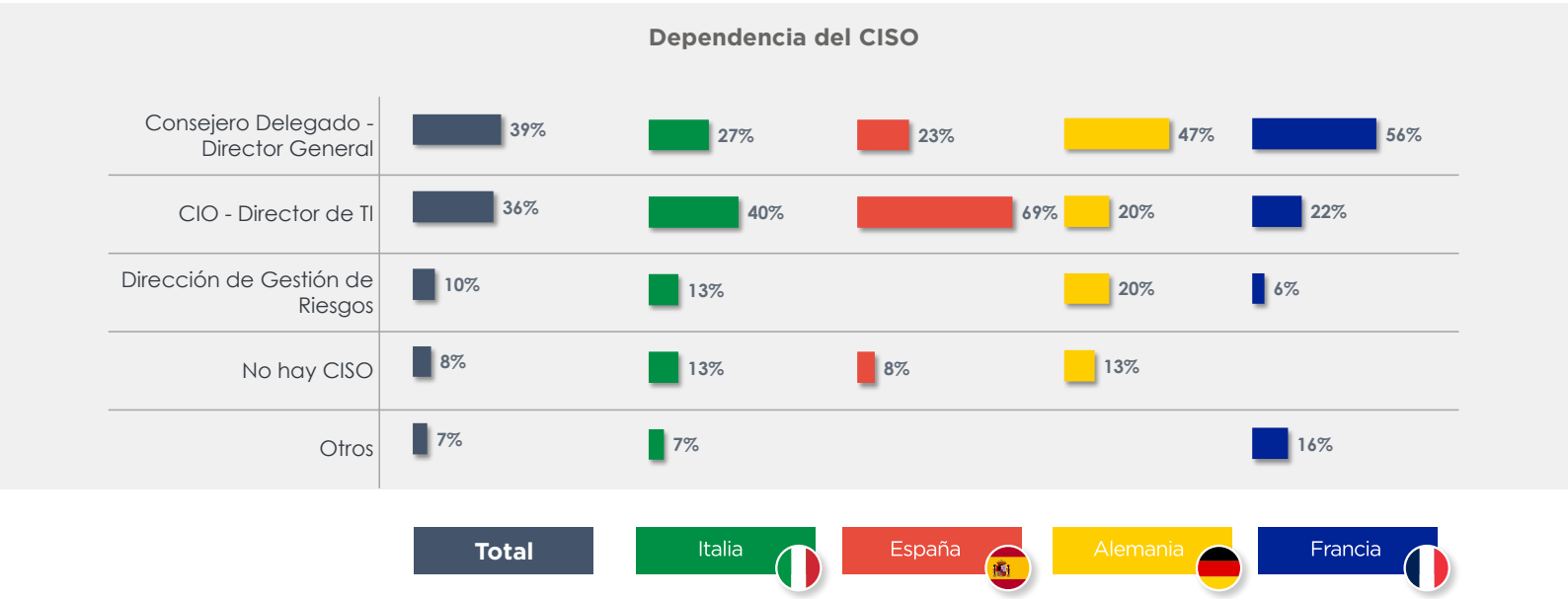


Ilustración 20. Reporte del CISO

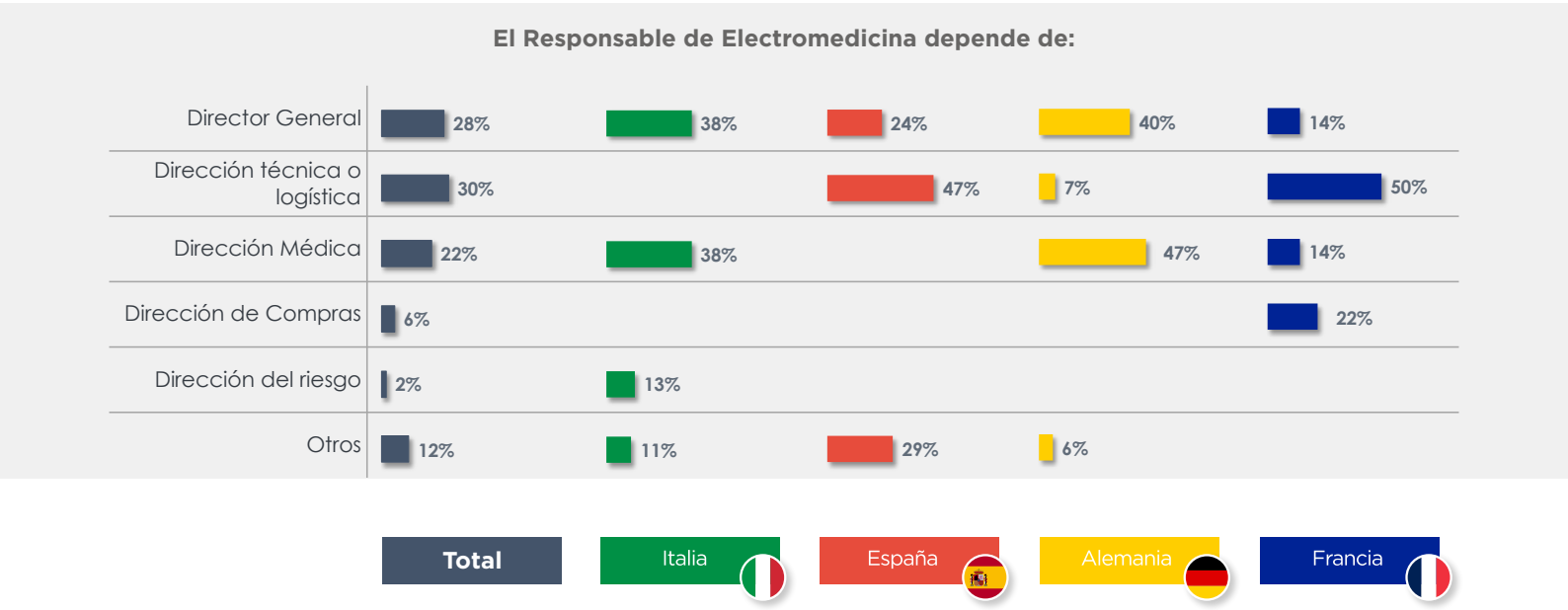


Ilustración 21. Reporte del Responsable de Electromedicina

Los **Responsables de Electromedicina** no dependen jerárquicamente de las áreas tecnológicas de TI, sino de las áreas de tecnología y dirección médica. Esto hace que tradicionalmente hayan estado **más ligados a objetivos de asistencia sanitaria** y aún se detecte esta **falta de coordinación respecto a la seguridad** de la conectividad de los equipos.

Analizando de forma global las diferentes responsabilidades del hospital relacionadas de algún modo con la ciberseguridad, vemos como la más **destacada la coordinación con los Responsables de Protección de Datos o DPO**. Esto es coherente con la preocupación mostrada anteriormente de forma general sobre la seguridad de los datos personales y las exigencias legales al respecto recogidas en el Reglamento Europeo de protección de datos. Podemos observar una estrecha relación, en particular entre el CIO, el CISO y el DPO, por encima de los Ingenieros de Electromedicina. Sin embargo, estos últimos destacan en su coordinación con el CIO o Director de TI, necesaria para la conectividad de los equipos a las redes.

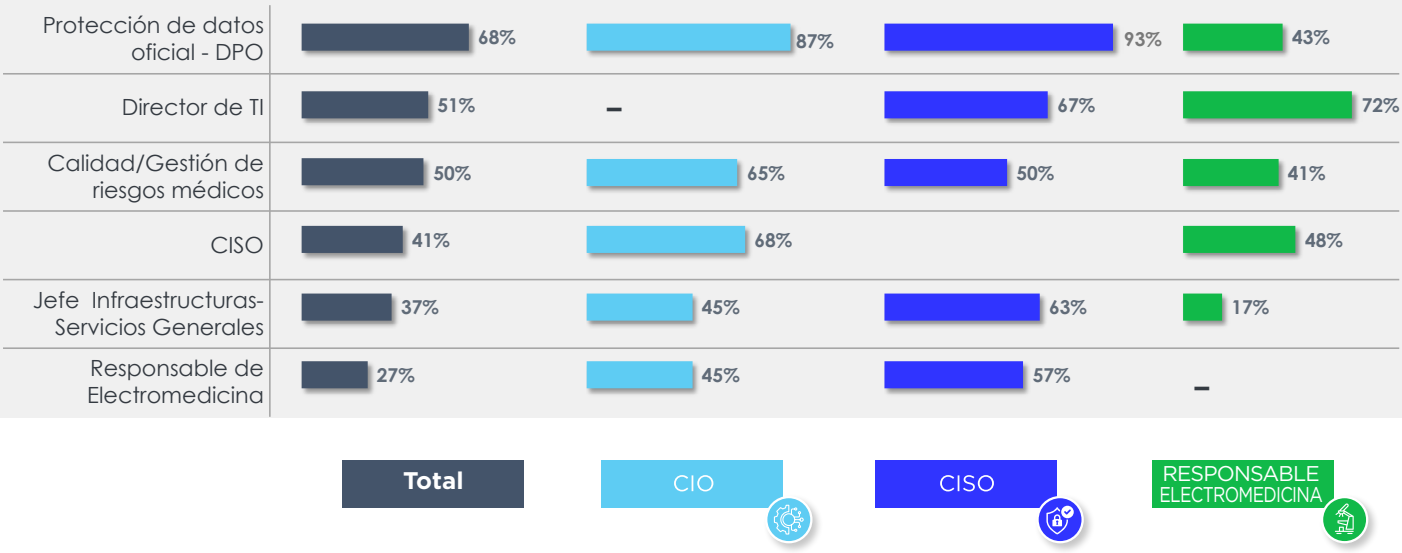


Ilustración 22. Coordinación en ciberseguridad

Cuando hablamos de coordinación entre funciones en materia de ciberseguridad, es clave analizar la **participación en los comités de ciberseguridad**, donde se analizan los proyectos en la materia y se gestiona la respuesta a los ciberincidentes.

Del análisis de los datos por países, vemos que España está en la media de los responsables que participan en dichos comités, pero destaca por el bajo número de respuestas que declaran no contar con un comité de ciberseguridad. Esto quiere decir que, si bien no todos los perfiles participan en el grado necesario, sí que es un **órgano de gobierno de la ciberseguridad que está muy implantado en nuestro sistema sanitario**.

Además, podemos observar cómo estos comités son **organismos permanentes, con reuniones periódicas, y no solo equipos de respuesta y coordinación en momentos de crisis**. España es el país con mayor porcentaje de comités de ciberseguridad con funciones periódicas, por encima incluso de países como **Francia** donde hay una mayor integración de profesionales en los comités de ciberseguridad, pero una menor asignación de responsabilidades permanentes.

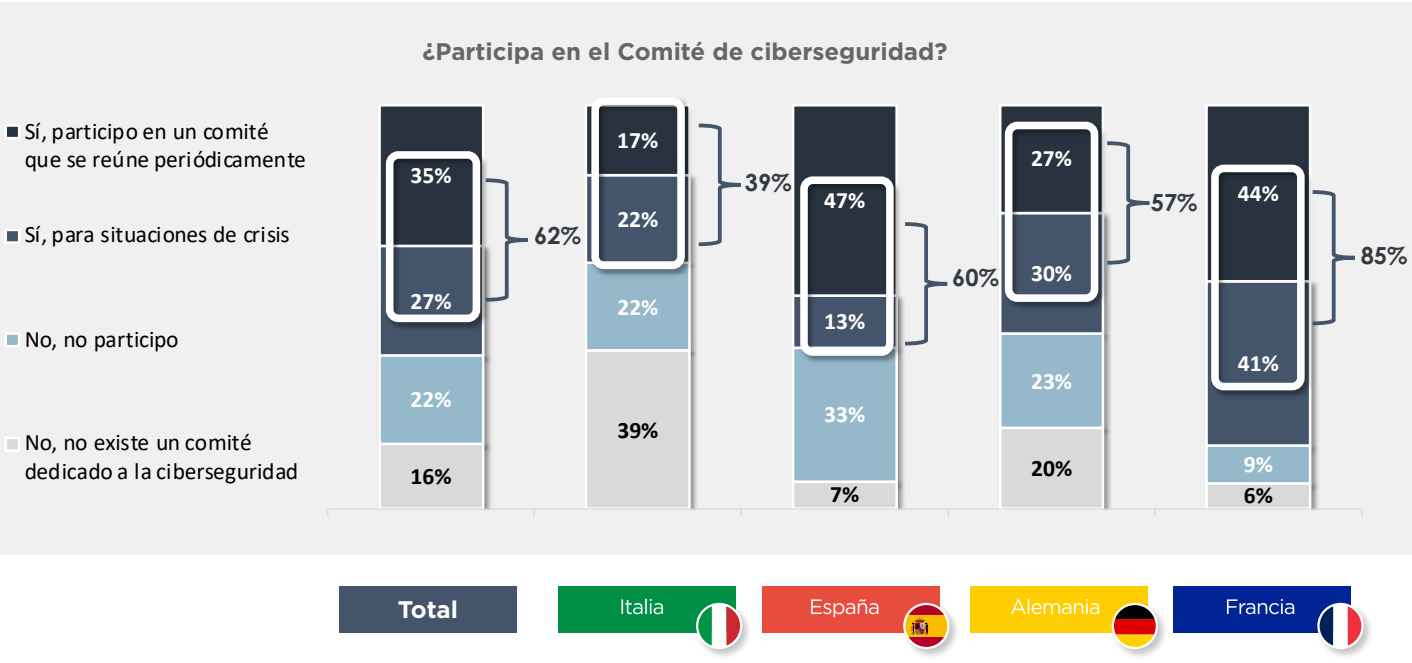


Ilustración 23. Participación en comités de ciberseguridad. Países

Si analizamos la participación por perfiles, como cabe esperar, el **CISO es el responsable con una mayor participación e implicación en los comités**. Sin embargo, vemos que **es necesario desarrollar la participación de los Ingenieros de Electromedicina**, figura que menos participa y cuando lo hace, se trata, en general, de dar respuesta a situaciones de crisis y no de planificación de la ciberseguridad.

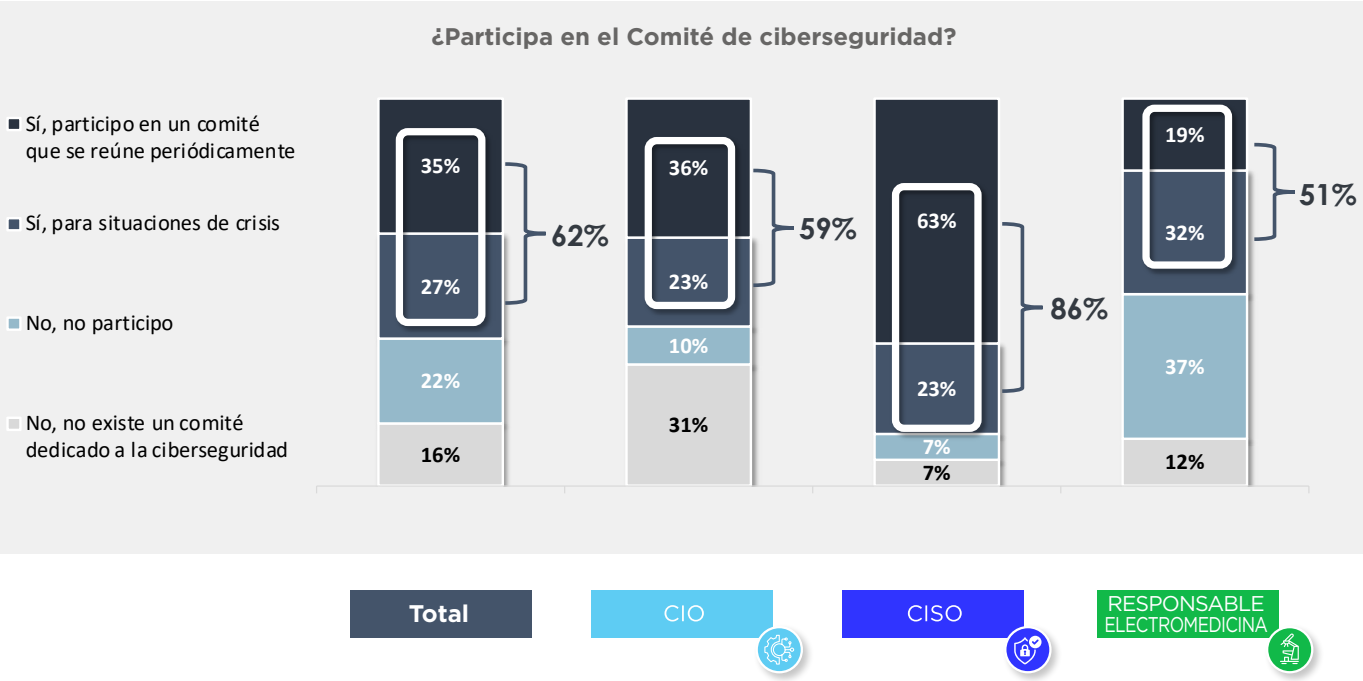


Ilustración 24. Participación en comités de ciberseguridad. Responsables

Análisis de riesgos de ciberseguridad

La base de cualquier estrategia de ciberseguridad debe establecerse sobre un **análisis de riesgos cibernéticos** que determine las áreas más críticas donde mejorar y priorizar las inversiones. Vemos que, en general, es una **práctica que se realiza en la gran mayoría de los centros sanitarios** (alrededor del 90%), y mayoritariamente se realizan de **forma periódica**.

Podemos destacar en este punto, la realización de **análisis de riesgos** en España, donde está **por encima de la media europea** con una diferencia importante (70%).

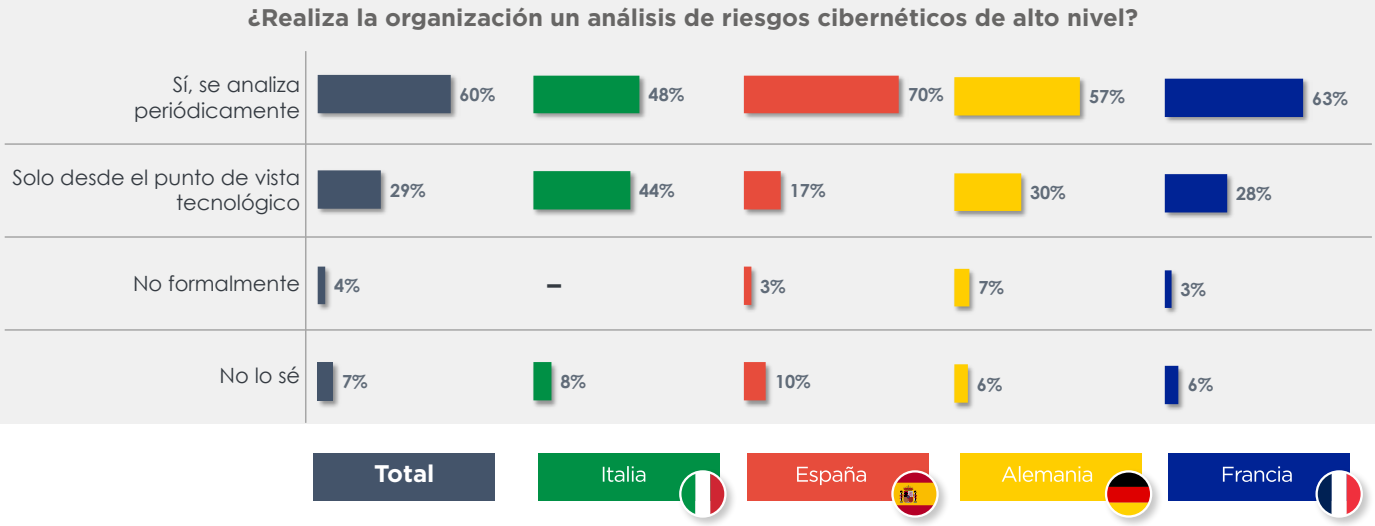


Ilustración 25. Análisis de riesgos de ciberseguridad. Países

Si nos aproximamos desde la perspectiva de los diferentes perfiles profesionales, vemos cómo hay un alto nivel de conocimiento del proceso de análisis de riesgos por parte de los CISO (normalmente figura responsable de su desarrollo).

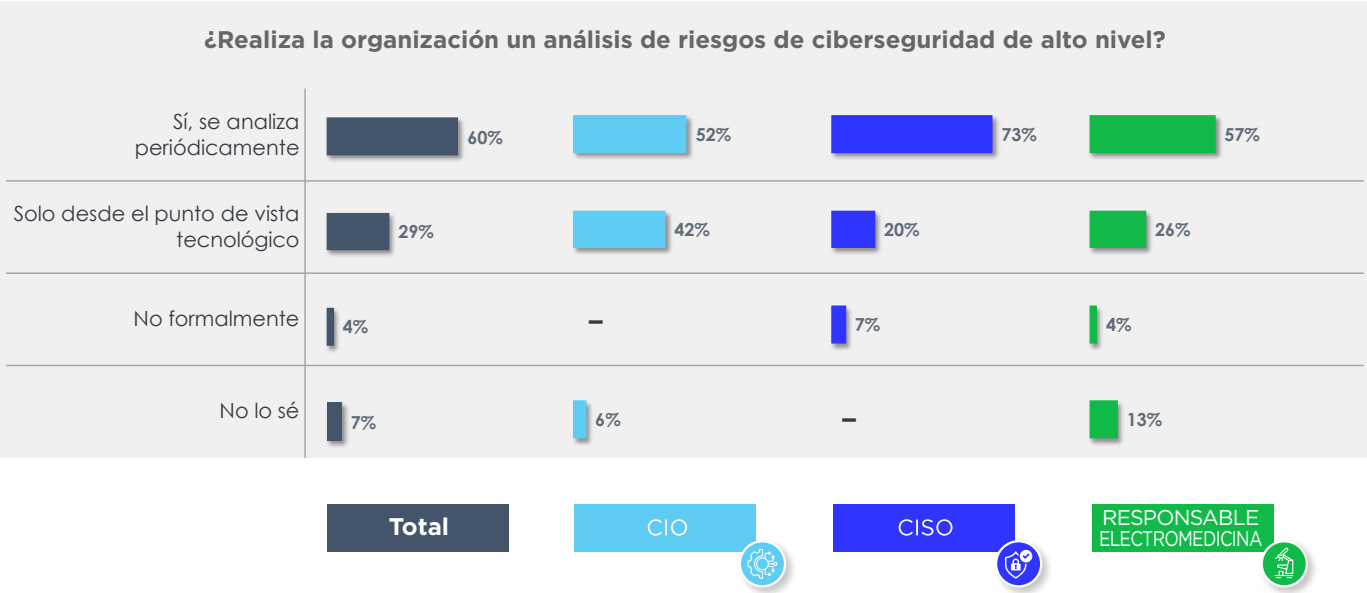


Ilustración 26. Análisis de riesgos de ciberseguridad. Responsables

La **gestión de los riesgos** además de un análisis de riesgos, requiere de un **sistema de gestión**, que establezca responsabilidades, revisiones periódicas, medición o evaluación de la eficacia de las medidas de seguridad, etc. Alrededor de **un 60% de los centros declaran contar con un Sistema de Gestión**, sin embargo, el nivel de madurez aún no es muy avanzado, ya que solo el 20% de media está certificado. España está por encima de la media en este aspecto con un 27% de los sistemas certificados dentro de la muestra participante.

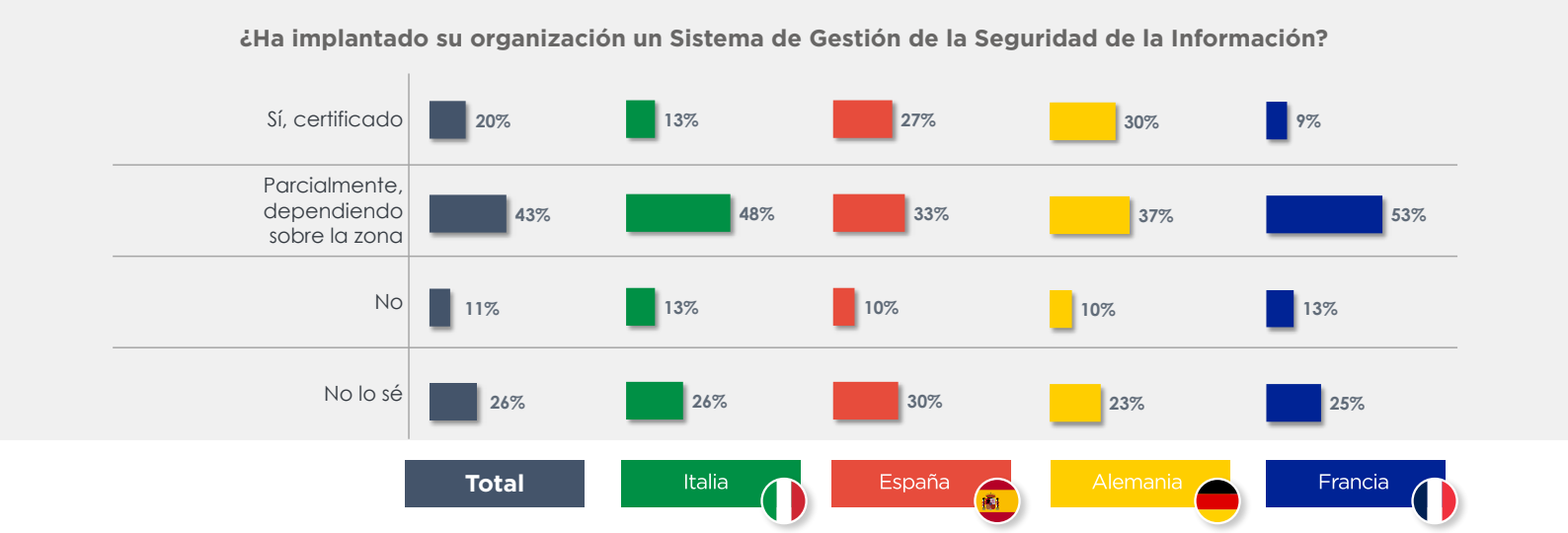


Ilustración 27. Sistemas de Gestión de la ciberseguridad. Países

Viendo las respuestas por perfil profesional, vemos que las respuestas positivas en los sistemas certificados destacan entre los CISO. Esto es debido a que un sistema de gestión requiere de esta figura para su funcionamiento, mientras que los sistemas sobre áreas más acotadas o aún en desarrollo pueden estar estableciendo su organización, comenzando por tareas más técnicas.

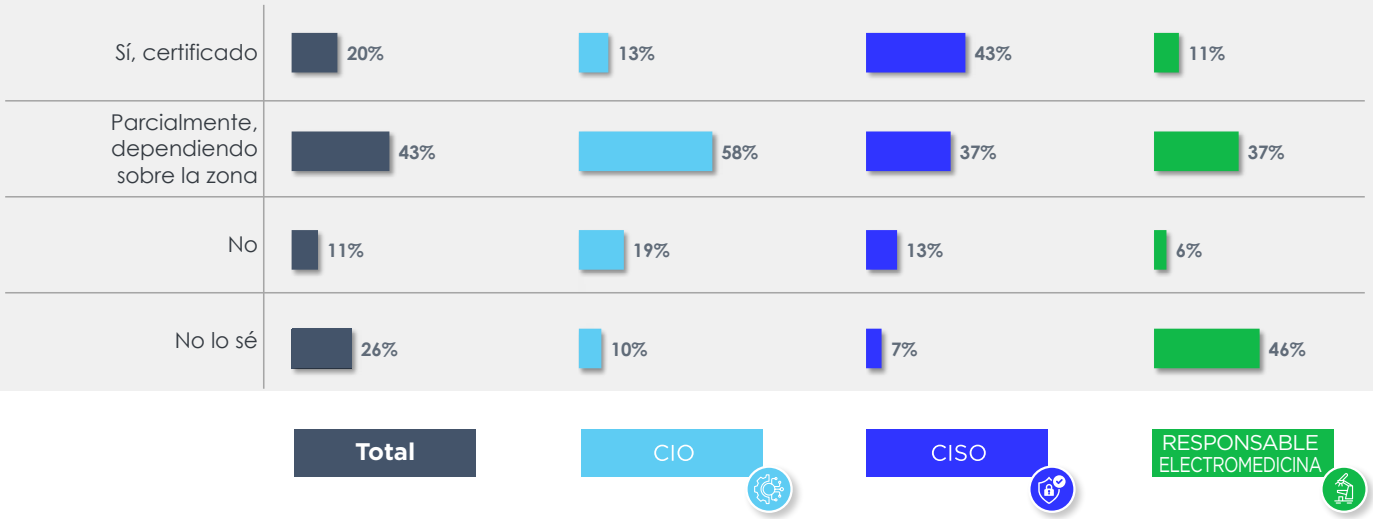


Ilustración 28. Sistemas de Gestión de la ciberseguridad. Responsables

ASPECTOS ECONÓMICOS DE LA CIBERSEGURIDAD

La ciberseguridad, a pesar de ser una garante de la continuidad de los servicios sanitarios, necesita de sus propios presupuestos e inversión para proteger de las amenazas del entorno cibernético de forma eficaz. Es importante, a la hora de establecer esos presupuestos, que estén alineados con las necesidades de los planes de desarrollo digital y tecnológico de los centros sanitarios, es decir, con los objetivos globales de la organización. En el siguiente apartado veremos cómo tratan los centros sanitarios estos aspectos económicos del ciberriesgo.

Vinculación de la ciberseguridad a los objetivos de negocio

Ante la pregunta de si **los objetivos establecidos respecto a la ciberseguridad están alineados con los objetivos del centro sanitario**, vemos que la respuesta es afirmativa **en un 80% de los hospitales**. En esta cifra incluimos tanto las respuestas positivas como las parcialmente positivas. Cabe destacar que en España la mayoría de los centros sanitarios tienen correctamente establecidos los presupuestos en función de las necesidades del servicio, frente a otros países donde esta alineación es parcial o está en desarrollo (**Alemania** e **Italia**).

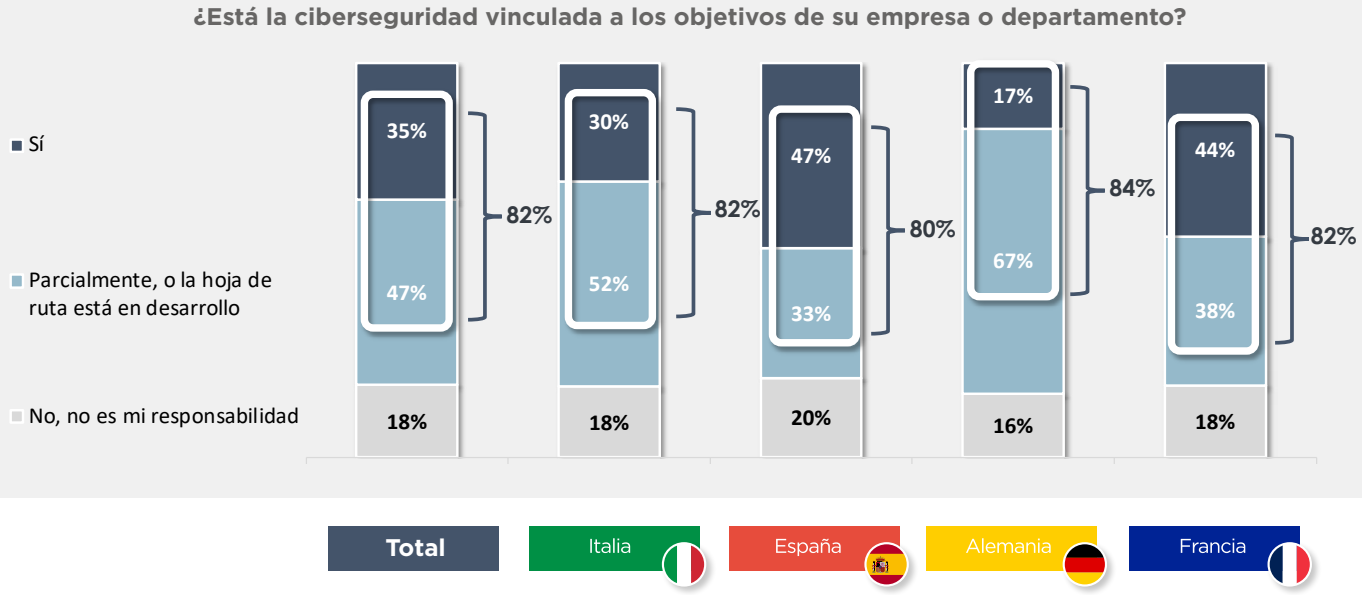


Ilustración 29. Objetivos de negocio y ciberseguridad. Países

Si vemos las respuestas por perfiles profesionales, destaca claramente la respuesta de los CISO frente a otros perfiles, ya que su responsabilidad es precisamente la gestión de los presupuestos de ciberseguridad. Es su función, en colaboración con otros implicados, garantizar que dichos presupuestos apoyen los procesos del hospital.

Cabe destacar las respuestas de los Responsables de Electromedicina, donde hay una menor vinculación entre sus objetivos y la ciberseguridad. Aunque sus funciones estén más vinculadas a aspectos del servicio asistencial, se deberían tener en cuenta las necesidades en ciberseguridad siempre que hay tecnología conectada implicada.

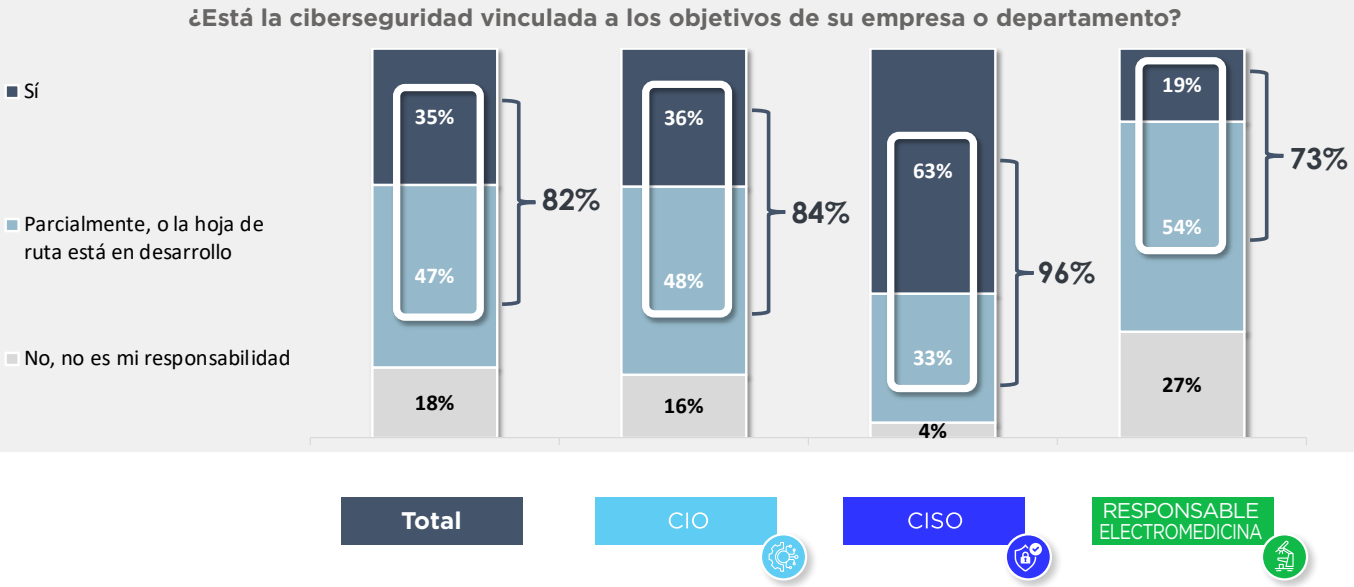


Ilustración 30. Objetivos de negocio y ciberseguridad. Responsables

Presupuestos de ciberseguridad en los centros sanitarios

Un indicador de la independencia de las funciones del CISO en los centros sanitarios es la existencia de un presupuesto expreso para ciberseguridad gestionado directamente por el responsable de seguridad de la información.

Vemos que, mayoritariamente, sí que **existe un presupuesto asignado a los proyectos de ciberseguridad, sin embargo, podemos ver como en muchas ocasiones ese presupuesto no depende del CISO**, sino que está integrado en otra área, normalmente la de Sistemas de la Información. Esto está en línea con los datos del apartado sobre la estructura de la información, donde se reflejaba la dependencia funcional entre el CISO y el CIO.

Ilustración 31. Presupuesto de ciberseguridad. Países

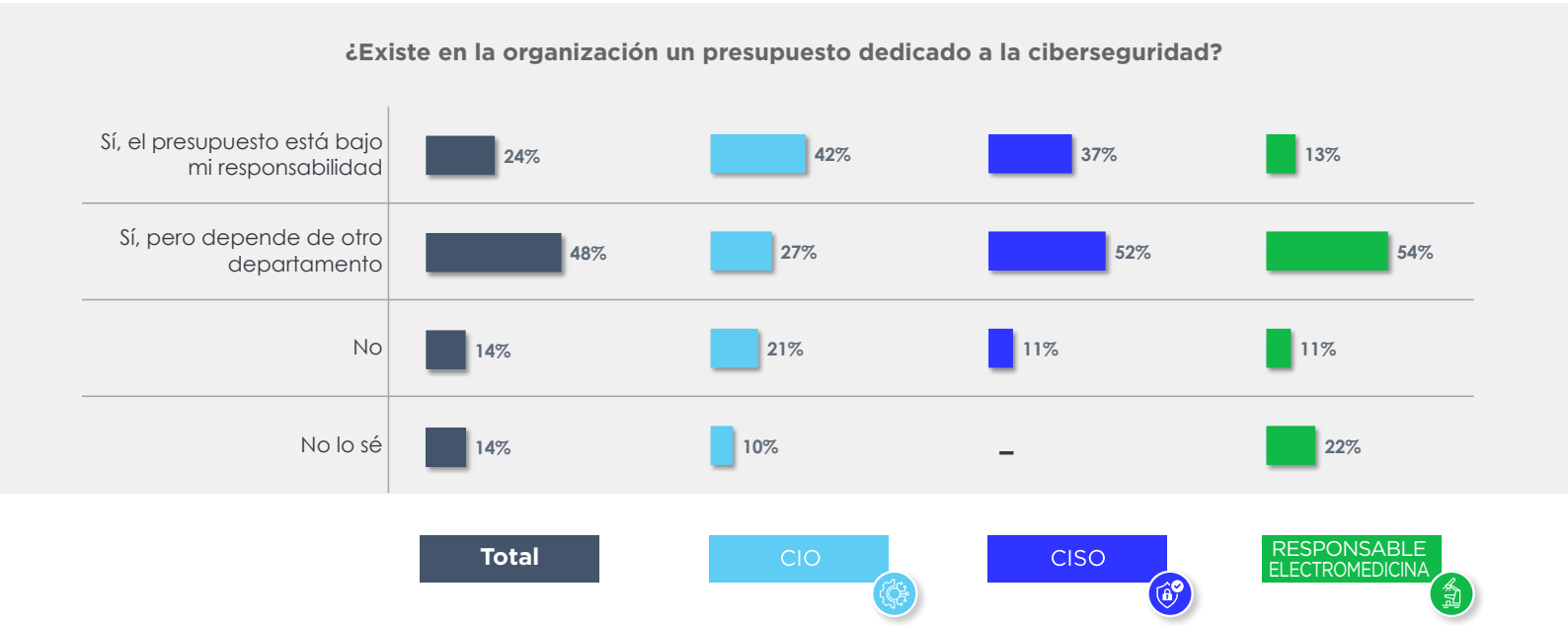


Ilustración 32. Presupuesto de ciberseguridad. Responsables

Colaboración de las Administraciones Públicas

Una de las demandas más habituales en el sector sanitario es la necesidad de contar con la colaboración de la Administración Pública en materia de ciberseguridad. Actualmente, alrededor de **un tercio de los proyectos cuentan con ayudas públicas**, tanto proyectos específicos como presupuestos anuales de seguridad. En España, las ayudas públicas están por debajo de la media europea, destacando **Italia** como el país que más apoya los presupuestos de ciberseguridad del sector sanitario.

Ilustración 33. Presupuestos subvencionados de ciberseguridad. Países

El apoyo de **la Administración Pública** no solo se materializa con ayudas económicas, sino que también **puede ofrecer servicios relacionados con las operaciones de ciberseguridad** (gestión de incidentes, auditoria, formación, etc). La Administración Pública española está alineada con la media europea en cuanto a la prestación de servicios de ciberseguridad, si bien estos servicios se prestan por diferentes organizaciones dependiendo de la estructura de competencias de cada país. Tanto en España como en **Francia**, la administración central proporciona servicios a todas las entidades encuestadas, complementando los servicios por entidades regionales y europeas.

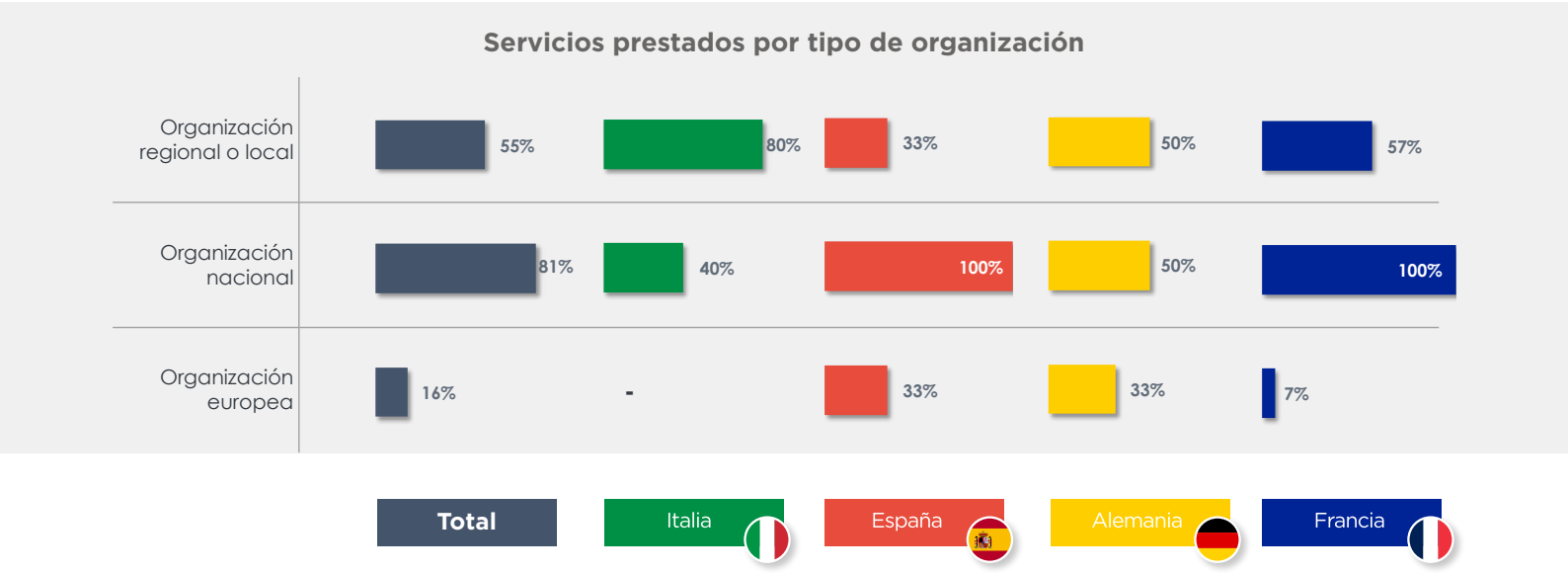


Ilustración 34. Servicios públicos de ciberseguridad

Sobre el tipo de servicios ofertados por las AAPP, hay cierta variedad en los diferentes países. **España cuenta con una variada oferta de apoyos: herramientas de ciberseguridad, intercambio de IoC, formación en ciberseguridad, gestión de vulnerabilidades, etc**, estando por encima de la media de los servicios ofertados por otras administraciones europeas.

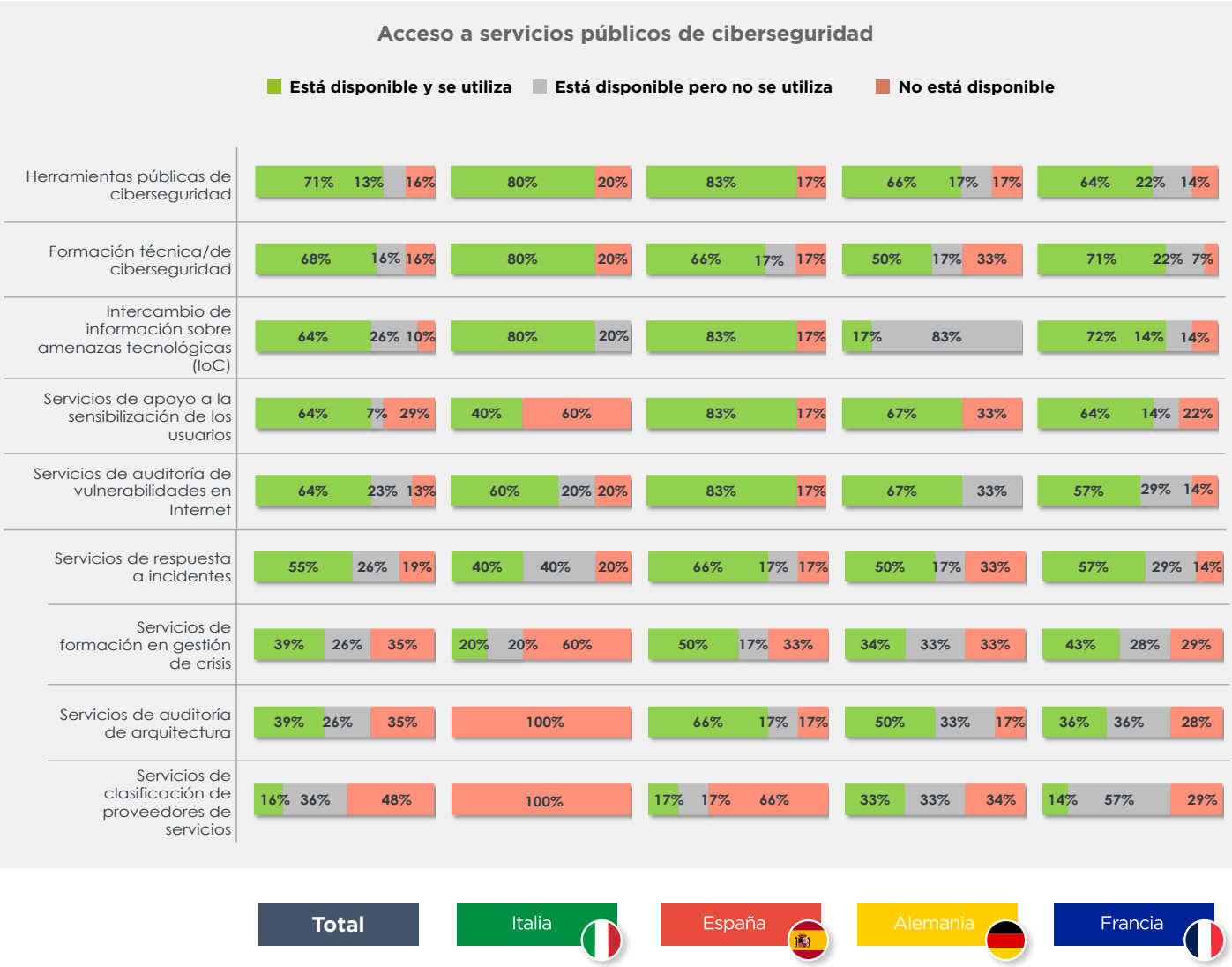


Ilustración 35. Tipos de servicios públicos de ciberseguridad. Países

En general, las necesidades del sector sanitario son amplias y demandan a la Administración Pública una gran variedad de servicios, desde la formación, al apoyo para la securización de las redes hasta la asistencia para la respuesta a incidentes y análisis de vulnerabilidades.

Entre los participantes que declaran no tener acceso a servicios de las Administraciones Públicas, consideran que servicios como la **evaluación de proveedores, la formación específica en gestión de crisis y el apoyo para la sensibilización de los usuarios, serían los servicios más valorados**. Otros, como la gestión de incidentes y las herramientas de ciberseguridad públicas, también están dentro de las demandas de los centros sanitarios.

Ilustración 36. Demanda de servicios de ciberseguridad. Países

LA GESTIÓN DE LA CIBERSEGURIDAD

Para finalizar el análisis de la ciberseguridad en el sector sanitario, se han revisado las prácticas implantadas en las organizaciones para gestionar los riesgos ciber. Las medidas analizadas comprenden tanto aspectos organizativos (políticas, personal, etc.) como medidas técnicas de prevención y reacción a los incidentes.

Políticas de ciberseguridad y cumplimiento

Las políticas de ciberseguridad se consideran el punto de partida de cualquier proyecto de ciberseguridad. La organización debe establecer sus objetivos, prioridades y recursos. Además, establecerá el marco en el que los proyectos se desarrollarán, alineados con los objetivos de negocio.

La política de ciberseguridad es un documento que emana de la dirección, que es quien debe aprobarla y asegurarse que se divulga por toda la organización, de forma que se aplique en los proyectos corporativos.

Los profesionales consultados declaran en **un alto porcentaje que cuentan con políticas de seguridad en diferente grado de aplicación**. En torno a un 33% de los países participantes tienen políticas totalmente desarrolladas con un porcentaje algo mayor (38%) donde están en proceso de aplicación. Es decir, es un tipo de medida que aun debe madurar y desarrollarse.

Sin embargo, en España el 50% de los participantes declara tener políticas ya implantadas y un 33% políticas en desarrollo. **Esto indica un grado de madurez mayor que el promedio europeo.**

¿Existe una política de ciberseguridad/seguridad de la información en su organización?

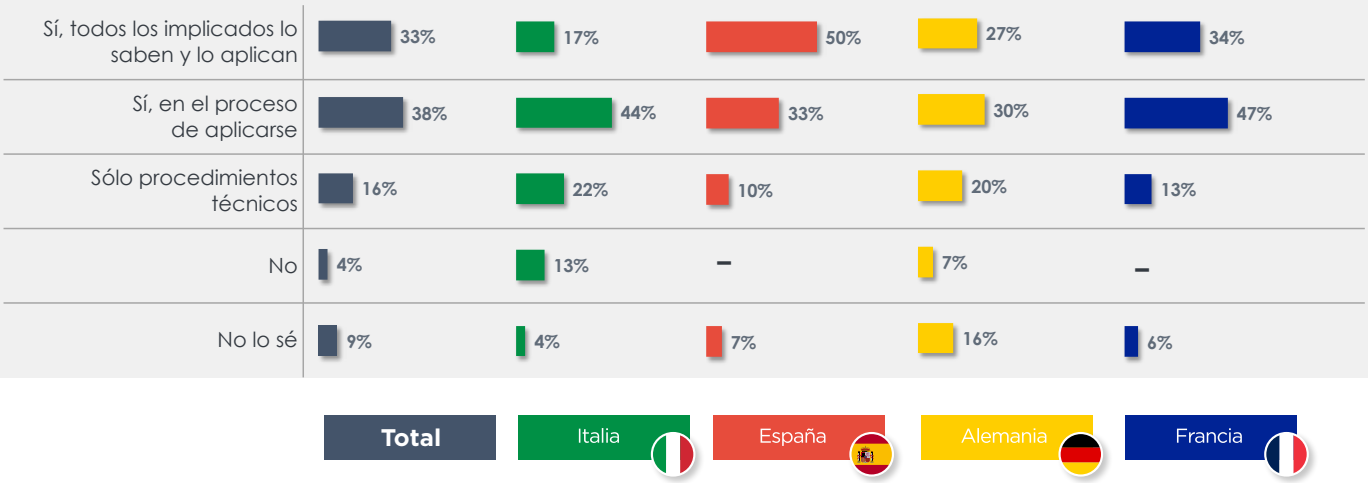


Ilustración 37. Políticas de ciberseguridad. Países

Si analizamos por perfil profesional, vemos claramente un **mayor conocimiento por la figura del CISO, responsable a cargo del desarrollo y difusión de las políticas**. En aquellos centros donde las políticas están en desarrollo, son los CIOs los que detectan esta situación. Esto es indicador de un estado de desarrollo menor del sistema, donde posiblemente no se haya llegado a la etapa de definir la figura del CISO como responsable de la seguridad.

Los Responsables de Electromedicina presentan un perfil más disperso en el conocimiento de las políticas de ciberseguridad, reflejo del nivel de madurez del centro en la integración de todos los participantes en la gestión de la ciberseguridad.

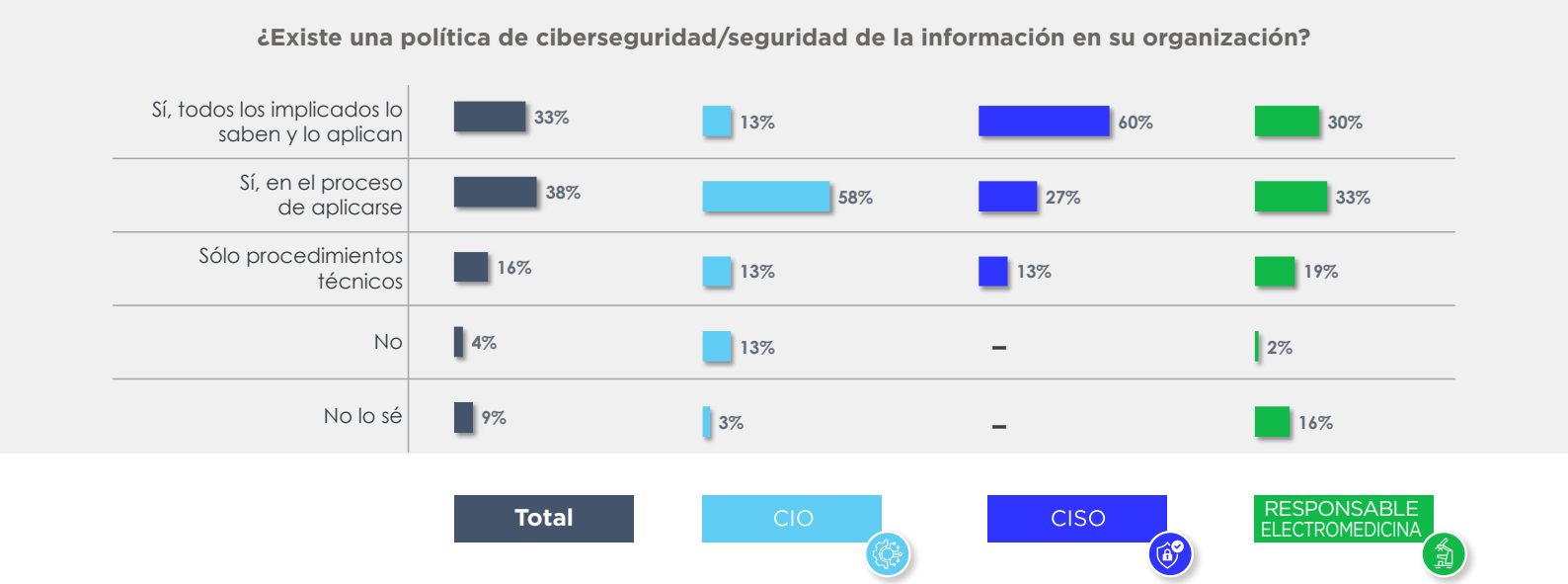


Ilustración 38. Políticas de ciberseguridad. Responsables

La ciberseguidad es cada vez un campo más regulado, particularmente desde organismos europeos, aunque también nacionales. Para asegurar el cumplimiento, es necesario establecer procesos que identifiquen estas regulaciones, determinen las acciones a tomar para su cumplimiento y vigilen su aplicación en la compañía. Ejemplo de esto es el Reglamente de Protección de Datos Personales, que si bien no es estrictamente una regulación sobre ciberseguridad, está fuertemente vinculado por la sensibilidad de los datos sanitarios y el mandato de seguridad que exige dicho reglamento.

Todos los participantes declaran cumplir con los requisitos legales en sus organizaciones, bien totalmente o en proceso de aplicación. El hecho de que los incumplimientos legales puedan tener consecuencias sancionadoras, o incluso penales, normalmente es un acelerador de la aplicación de las medidas en todos los organismos.

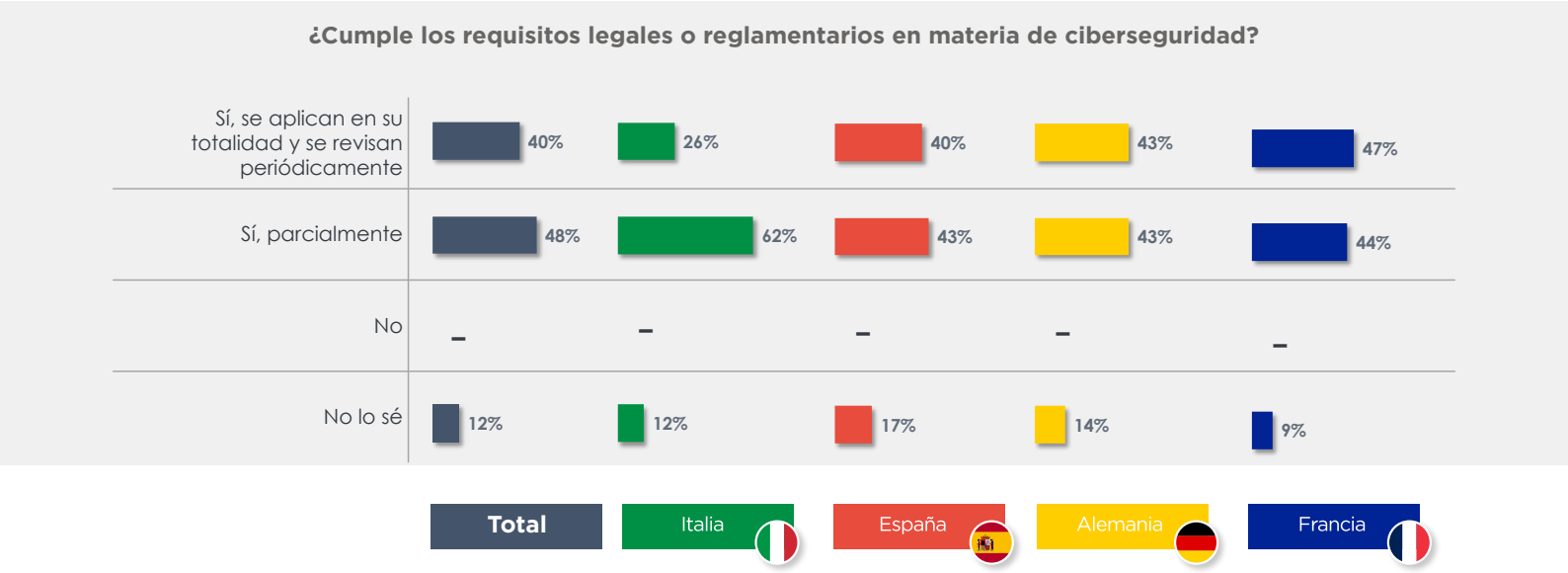


Ilustración 39. Cumplimiento medidas legales y reglamentarias. Países

Si consultamos el cumplimiento legal por perfiles profesionales, vemos que la respuesta sigue manteniendo un alto grado de cumplimiento. Como en el caso de las políticas, es el CISO quien declara mayor cumplimento legal, sistemas más maduros, y el CIO quien declara mayores casos de sistemas en desarrollo. Los Responsables de Electromedicina, aunque tienen un nivel mayor de desconocimiento sobre el cumplimiento de requisitos legales, también presentan un buen grado de conocimiento de la situación de desarrollo en esta materia (alrededor del 77%).

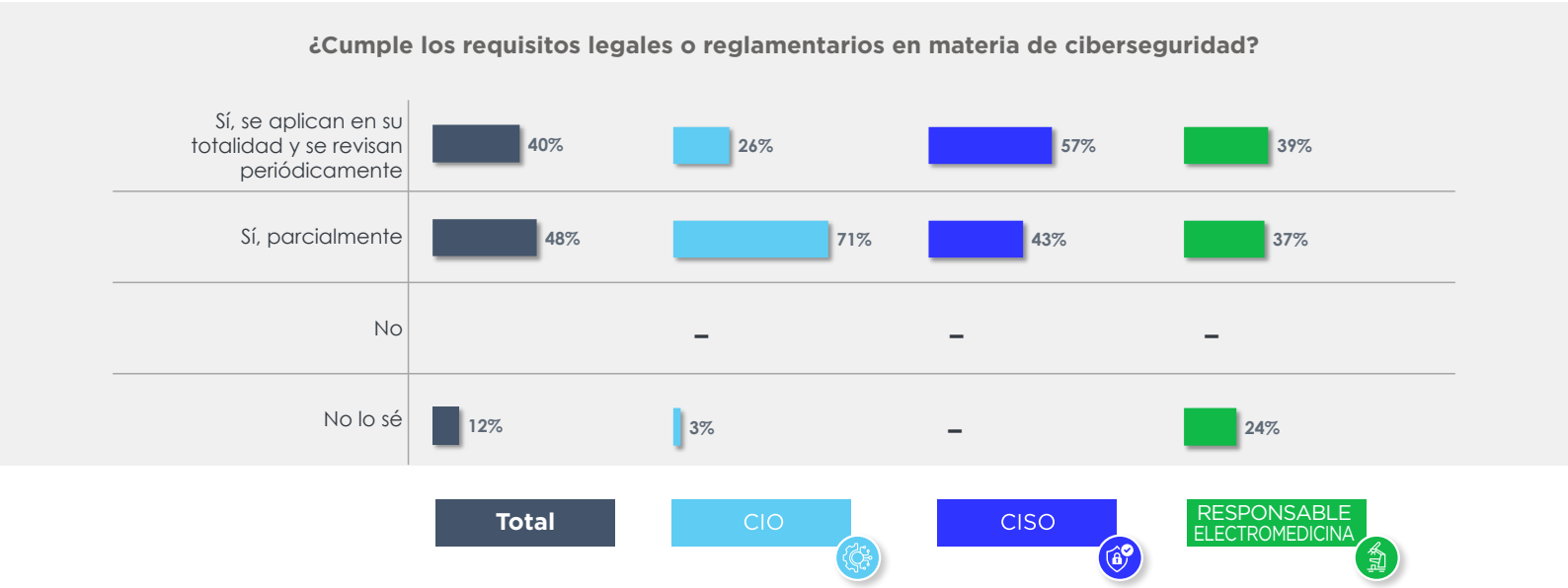


Ilustración 40. Cumplimiento medidas legales y reglamentarias. Responsables

Los RRHH y el conocimiento sobre ciberseguridad

Aunque los procesos médicos cada vez están mas interconectados y digitalizados, detrás de cada proceso y tratamiento están los profesionales sanitarios y técnicos en sus diferentes funciones. Es clave que todo el personal, en función de sus responsabilidades, cuente con los conocimientos necesarios y actualizados para mantener la ciberseguridad. Los usuarios tendrán que recibir la formación necesaria para hacer un uso seguro de los sistemas, aplicaciones y tecnologías; los técnicos de equipos médicos tendrán que conocer los riesgos de sus equipos y cómo securizarlos y el personal técnico debe tener la cualificación adecuada para el manejo y configuración de los sistemas.

Para ello, **el centro sanitario debe tener unos planes de formación y concienciación y, en su caso, apoyarse en personal externo para tareas donde se requiera una cualificación específica.**

De promedio, poco más del 60% reconoce tener campañas de concienciación y formación para el personal. España, con un 63% se ajusta a esta media, sin embargo, **Francia** está por encima del resto de países con un 72%. Aquí vemos un **área de mejora clara en el sector sanitario** y la primera capa de protección frente a un ciberincidente.

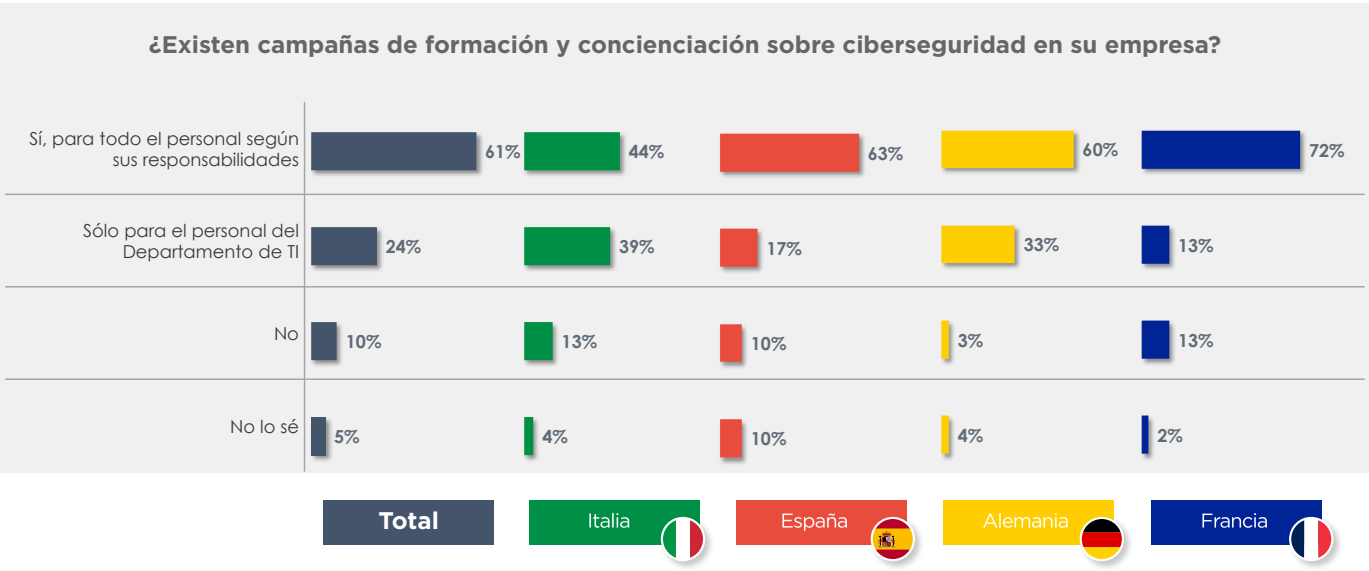


Ilustración 41. Campañas de concienciación en ciberseguridad. Países

Seleccionando las respuestas por perfiles profesionales, podemos concluir que los porcentajes están muy equilibrados entre ellos, con el porcentaje menor en **los Ingenieros de Electromedicina: es el grupo que menos percibe que existan campañas de concienciación a los usuarios.**

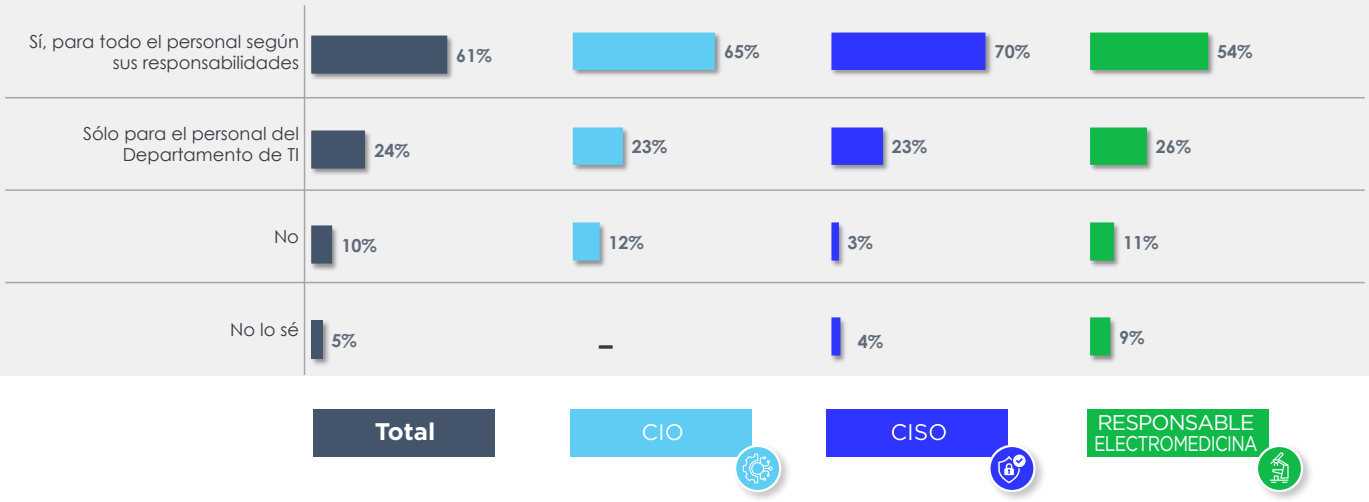


Ilustración 42. Campañas de concienciación en ciberseguridad. Responsables

Si analizamos la cualificación en ciberseguridad del personal técnico de los centros sanitarios, vemos como **España está muy por encima de la media en incluir personal experto dedicado a la ciberseguridad** frente a otros países donde tan solo se abordan las tareas diarias o cuenta con conocimientos básicos. Mantener estos equipos es, en ocasiones, un reto por la demanda que hay en el sector de la ciberseguridad, por lo que merece el desarrollo de políticas específicas para mantener los equipos y desarrollar el talento en esta área.

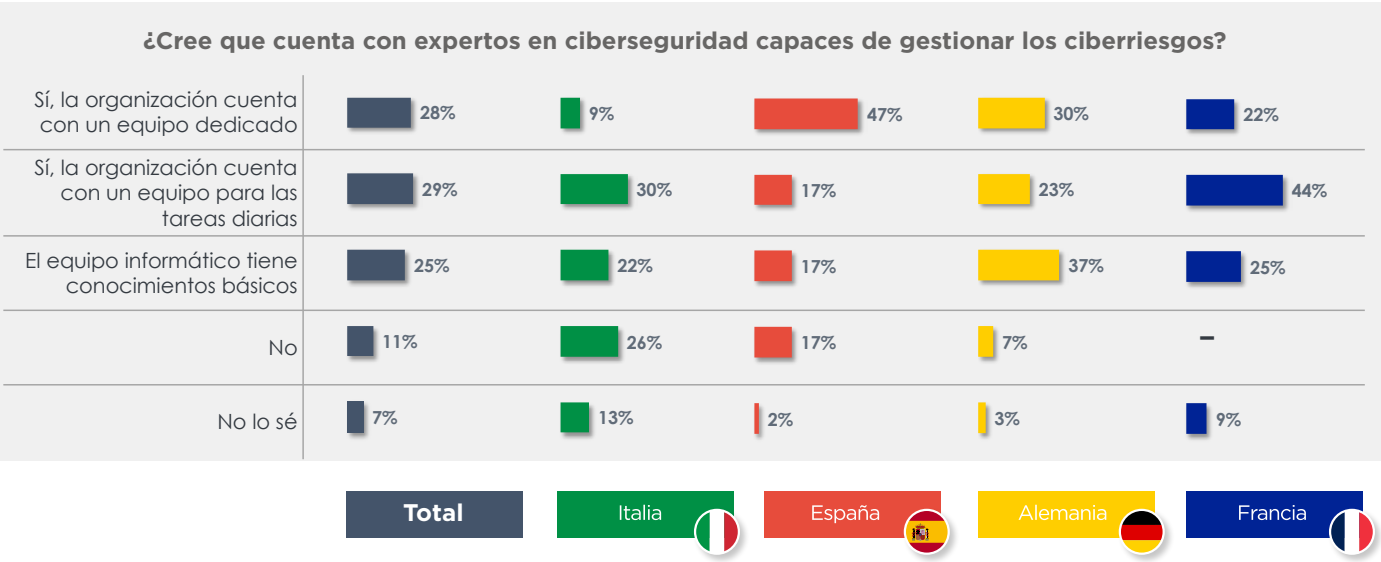


Ilustración 43. Expertos en ciberseguridad en sanidad. Países

Respecto a los perfiles profesionales, aunque **el CISO es el profesional que dice contar con un equipo dedicado a la ciberseguridad en un porcentaje mayor,** vemos que tan solo un 43% tienen un equipo dedicado. Un 33% más tienen personal para abordar las tareas diarias, pero en un contexto tan cambiante y en desarrollo, hay dificultades para planificar y desarrollar nuevos proyectos con garantías.

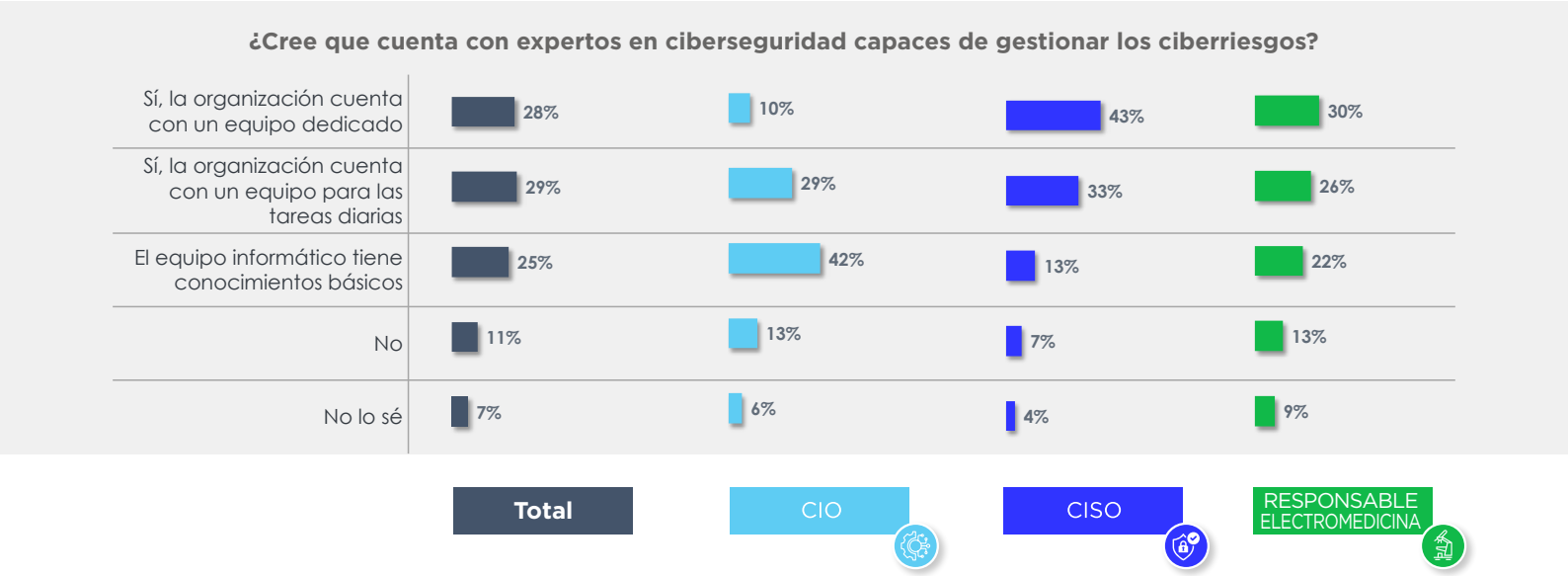


Ilustración 44. Expertos en ciberseguridad en sanidad. Responsables

Parte de las carencias del equipo interno, sobre todo para tareas de planificación y proyectos específicos, se puede cubrir con personal externo de empresas especializadas. España se apoya en este modelo en un alto porcentaje, muy por encima de la media europea. Por ejemplo, más de la **mitad de los encuestados cuentan con una Oficina de ciberseguridad externa**, frente al 18% del conjunto de los 4 países analizados.

El tercer servicio contratado en España en orden de relevancia es el equipo de respuesta a incidentes. Este equipo es habitual que sea externo por la alta especialización y su intervención limitada a los incidentes. Cabe pensar que quien no tenga contratado este servicio, es más por no tenerlo previsto y/o presupuestado que por no ser necesario. De hecho, tanto la activación como la coordinación con estos equipos debe estar incluida en los planes de gestión de incidentes.

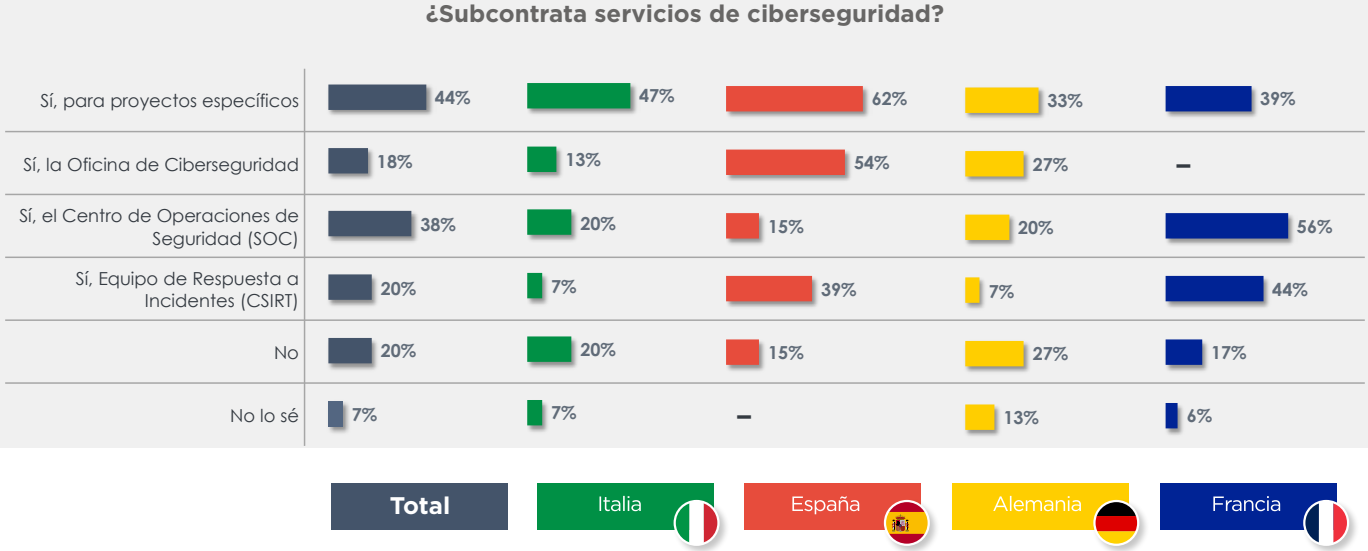


Ilustración 45. Subcontratación de servicios de ciberseguridad. Países

La seguridad en los procesos de compras

En ciberseguridad se dice muy a menudo que la seguridad empieza en el diseño. Muchas veces, esto se refleja en el proceso de definición de los proyectos y en la gestión de las compras. **Si se incluyen criterios de seguridad en los requisitos de contratación, la prevención y mitigación de los riesgos será más fácil de conseguir.**

Vemos a través de las respuestas que **los criterios de ciberseguridad se van incorporando en los proyectos de ámbito informático, pero aún no se han establecido en otras áreas**. Cabe destacar el área médica y OT, donde se gestionan los proyectos de compra de equipos conectados a los sistemas y, muchas veces, con importantes vulnerabilidades. Este es un área importante de mejora y vemos cómo a nivel europeo se van a exigir requisitos de seguridad para todos los equipos conectados. En cualquier caso, es un criterio que debe incluirse y exigirse siempre que sea necesario.

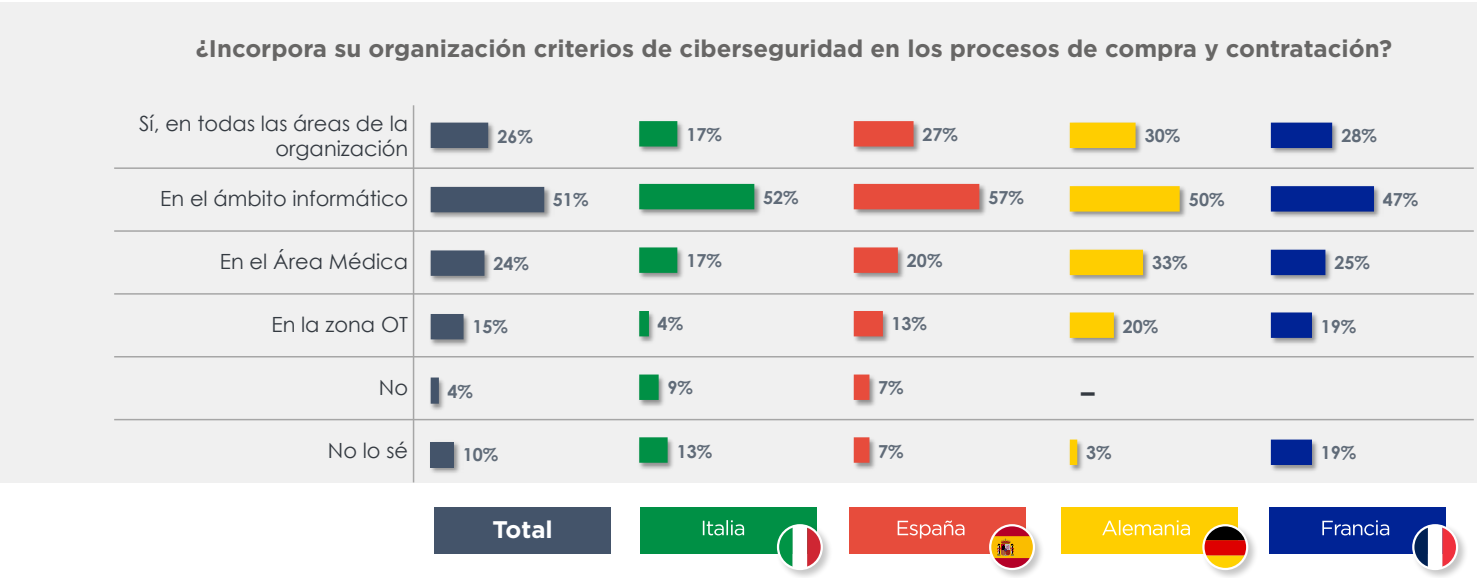


Ilustración 46. Ciberseguridad en los procesos de compra. Países

El perfil que explicábamos con la gráfica anterior se muestra también en la encuesta por perfiles profesionales. Es el ámbito informático, tanto por el CISO como por el CIO, donde más se tienen en cuenta criterios de ciberseguridad en la adquisición de equipos y servicios con más del 60% de los encuestados. Sin embargo, en el área de electromedicina estos criterios no están tan implantados, con un 24% en el área médica.

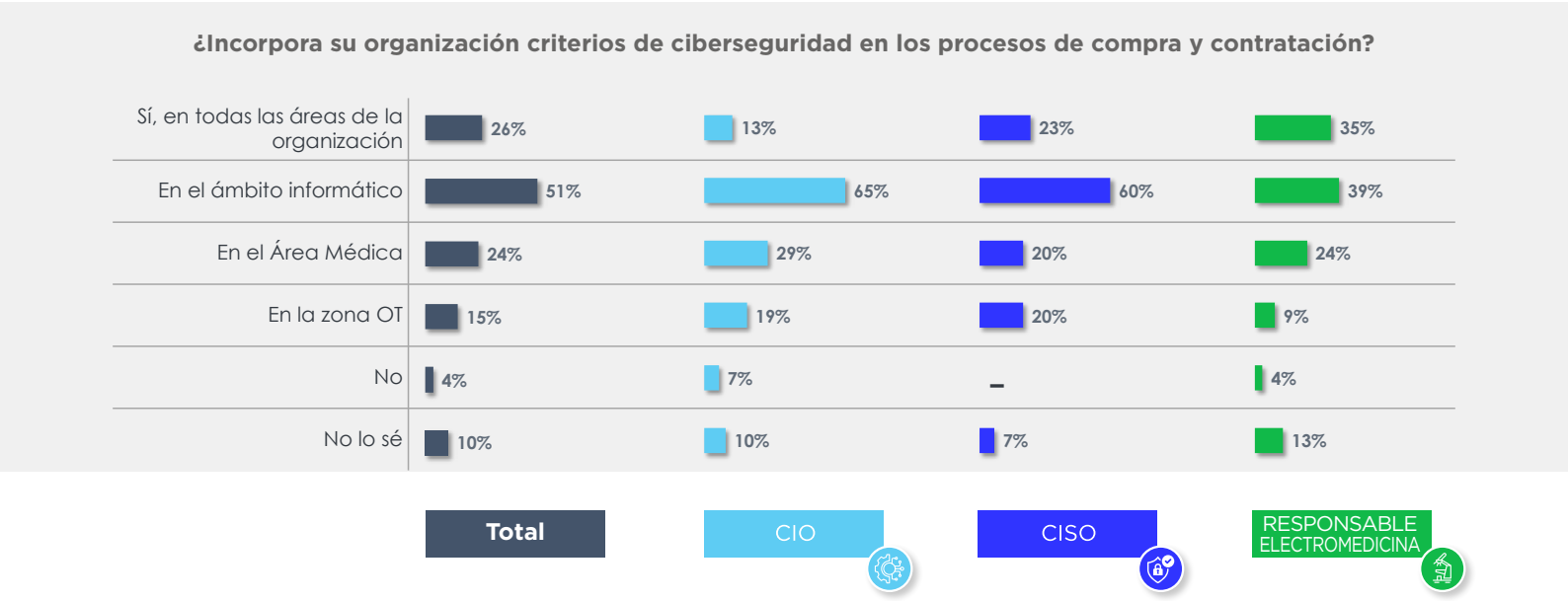


Ilustración 47. Ciberseguridad en los procesos de compra. Responsables

Uno de los canales de entrada de las amenazas de ciberseguridad que cada vez se ve con más fuerza es la cadena de suministro: los incidentes derivados de un tercero que presta servicios o productos al centro sanitario. Es importante analizar este riesgo y gestionarlo de forma adecuada, sobre todo para aquellos servicios más críticos.

Si consideramos los centros que supervisan la ciberseguridad de los proveedores de forma global y los que lo aplican a los servicios críticos vemos que, de media, un 77% de los hospitales tienen algún tipo de supervisión. Este perfil de cumplimiento se mantiene si analizamos los datos por perfiles profesionales: la mayoría de las medidas se aplican por requisitos legales.

En general, los requisitos legales tienen un gran peso en esas medidas, principalmente los derivados de la aplicación del Reglamento General de Protección de Datos que exige unos requisitos básicos para las contrataciones de servicios y productos vinculados con los datos personales. Este es un punto de partida, pero es un **área para avanzar en los procesos de análisis y control a la vista del incremento de incidentes y a la gravedad de sus consecuencias.**

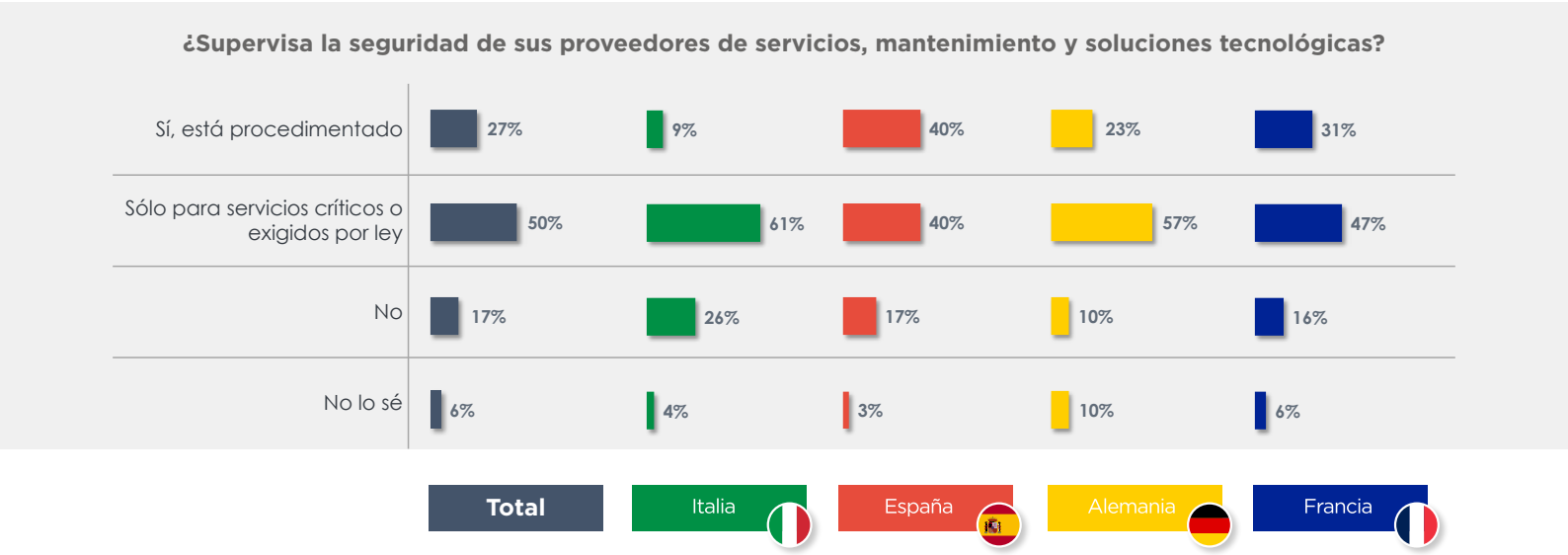


Ilustración 48. Ciberseguridad de proveedores. Países

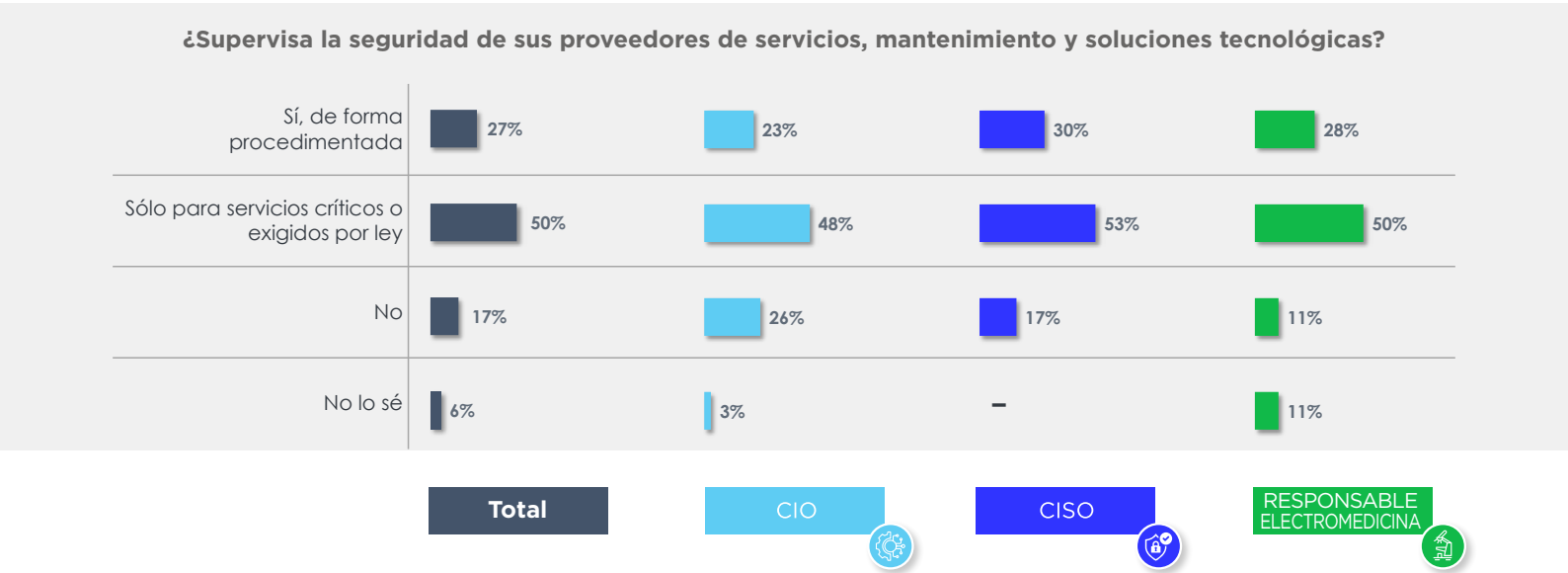


Ilustración 49. Ciberseguridad de proveedores. Responsables

Medidas tecnológicas

Por último, haremos un recorrido por las medidas de seguridad para la prevención y la gestión de los incidentes de ciberseguridad. No se pretende un análisis exhaustivo según un modelo de madurez o normativa, pero sí conocer la aplicación de aquellas medidas más implantadas y necesarias en el sector sanitario.

Conocimiento de los sistemas: el Inventario

En un proceso de gestión del riesgo, debemos seguir una secuencia que responde a la siguiente lógica: lo que no se conoce, no se mide; lo que no se mide, no se gestiona y lo que no se gestiona, se degrada. Aplicando esto a la gestión de la ciberseguridad, veremos que una de las primeras acciones que hay que llevar a cabo para aplicar medidas de seguridad es tener un inventario de los equipos conectados, las aplicaciones y software desplegado. A partir de aquí, se podrán tomar medidas para analizar sus vulnerabilidades, configuración, etc.

Vemos que tan **sólo el 40% de los centros sanitarios declara tener un inventario completo y actualizado**. Un porcentaje similar declara tener un inventario, pero desactualizado e incompleto, por lo que resta eficacia en la gestión del riesgo.

Aunque este perfil de respuesta es similar cuando analizamos los datos por los diferentes responsables, vemos como el CIO evalúa en mayor medida su inventario como incompleto (61%) y los Responsables de Electromedicina tienen sistemas algo más maduros, con inventarios actualizados (52%).

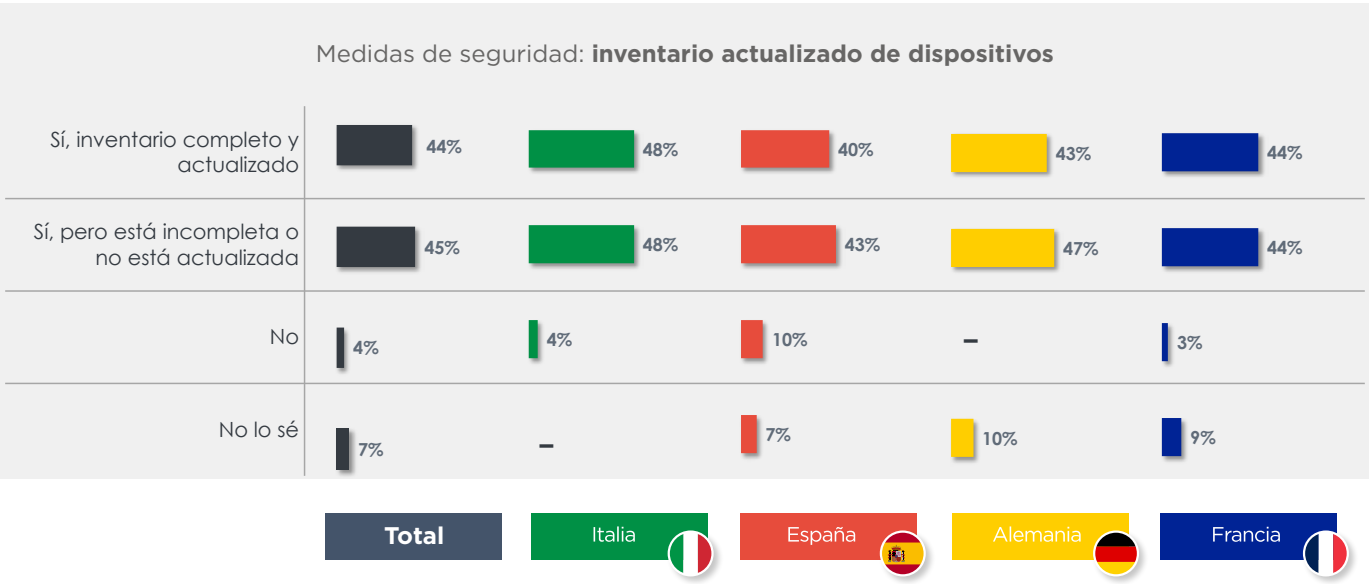


Ilustración 50. Medidas de seguridad: Inventario de equipos. Países

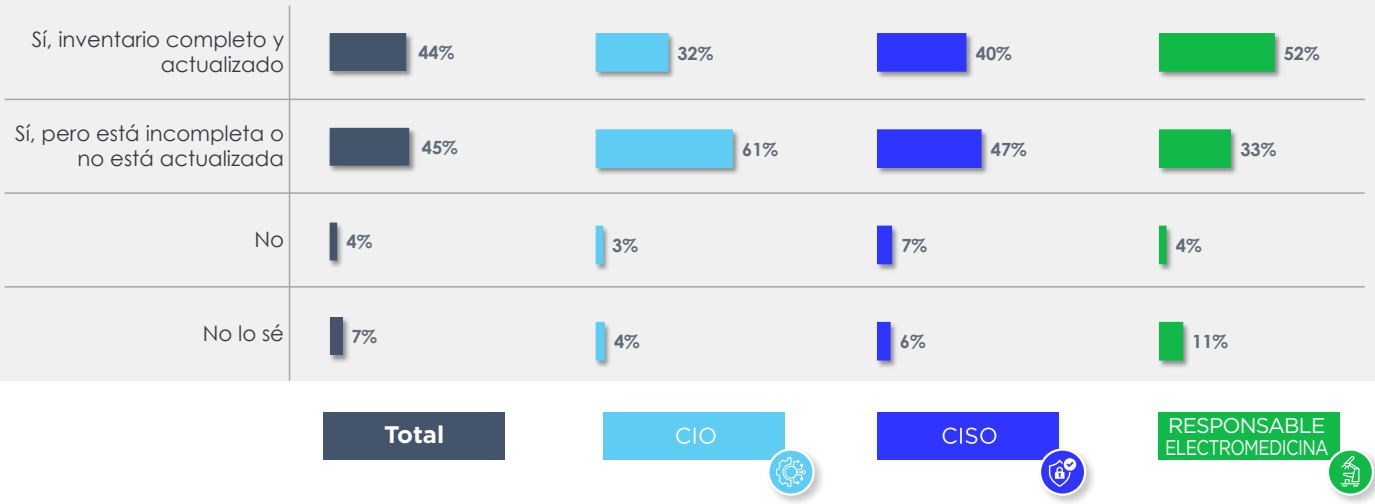


Ilustración 51. Medidas de seguridad: Inventario de equipos. Responsables

Seguridad de los datos

Los datos de los centros de salud son datos muy sensibles y relevantes para la prestación del servicio. Además, están especialmente protegidos por la legislación, por lo que es imprescindible aplicar medidas que garanticen su seguridad.

Las medidas por las que se ha consultado en relación con la seguridad de los datos son las siguientes:

- **Gestión de identidades y accesos.** Es la medida de mayor implantación, con más del 80% de los hospitales que declara aplicarla y es utilizada por todos los perfiles profesionales consultados.
- **Sistemas de cifrado.** Esta medida está implantada en la mitad de los centros sanitarios, cifrando la información más sensible.
- **Prevención de la pérdida de datos (DPL).** Medida con menor implantación, alrededor de un 45%.

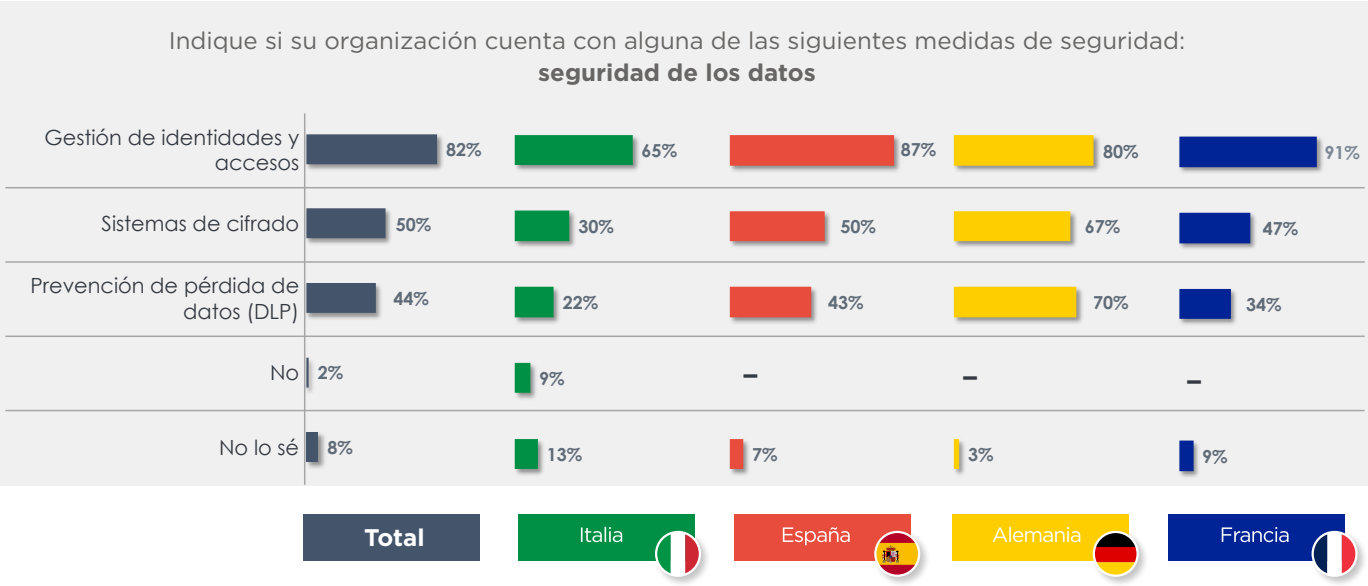


Ilustración 52. Medidas de seguridad: Seguridad de los datos. Países

Indique si su organización cuenta con alguna de las siguientes medidas de seguridad:
seguridad de los datos

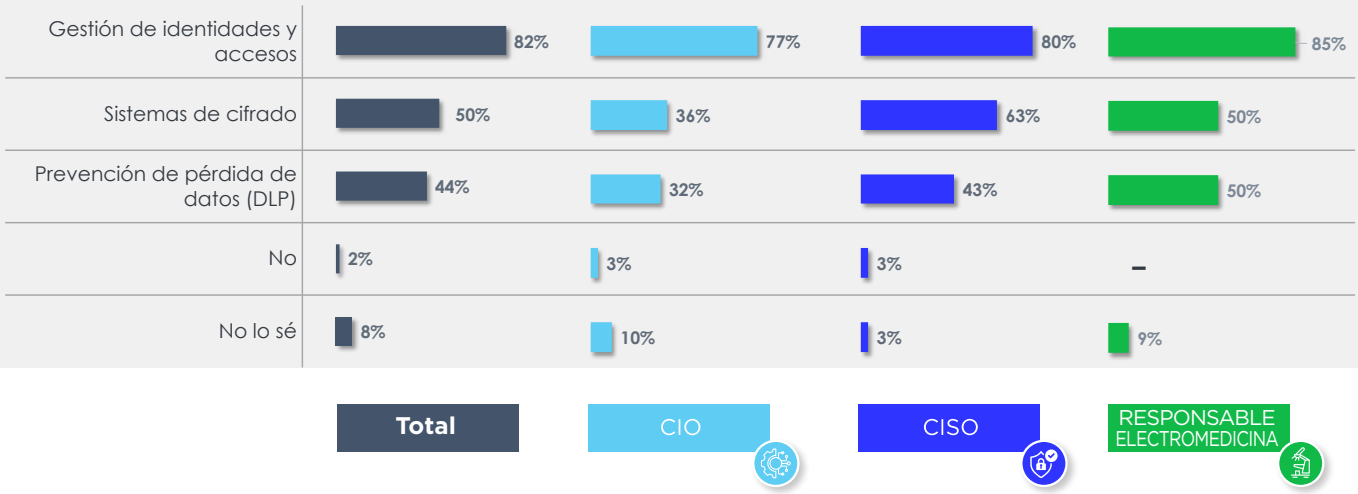


Ilustración 53. Medidas de seguridad: Seguridad de los datos. Responsables

Seguridad de las redes

La seguridad de las redes se garantiza con un grupo variado de herramientas, actuando sobre diferentes aspectos y, dentro de lo posible, actuando de forma coordinada.

Las dos medidas más extendidas son las **aplicaciones antimalware y las políticas de seguridad y segmentación de red**, implantadas en el 70% de los centros encuestados en nuestro país. En segundo nivel tenemos otro grupo de medidas con un 50% de aplicación: **NAC, gestión de vulnerabilidades, análisis de tráfico y seguridad perimetral.** En ultimo término, aunque a un nivel similar de aplicación, tenemos las soluciones de EDR.

La responsabilidad de la gestión de esas soluciones corresponde habitualmente a CISO y en su defecto al CIO. Sin embargo, también el responsable de electromedicina muestra un buen conocimiento de las medidas implementadas ya que afectan en mayor o menor medida a las redes de conexión de los equipos médicos.

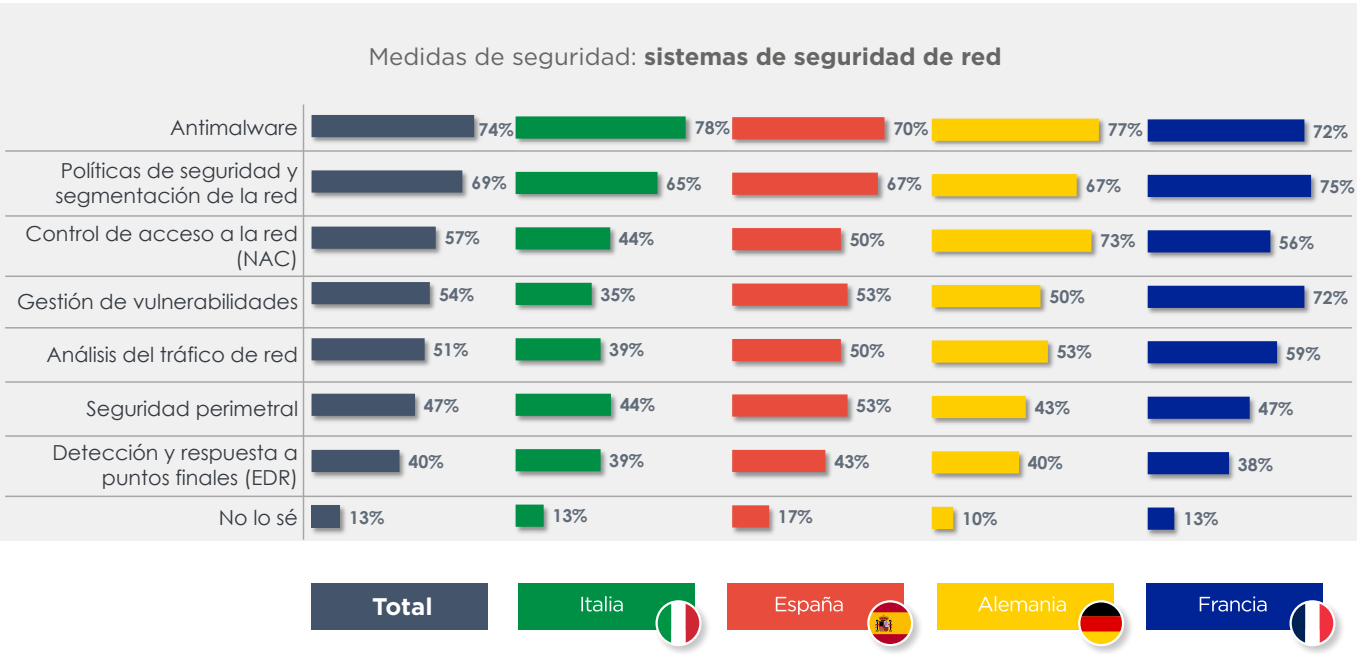


Ilustración 54. Medidas de seguridad: Seguridad de las redes. Países

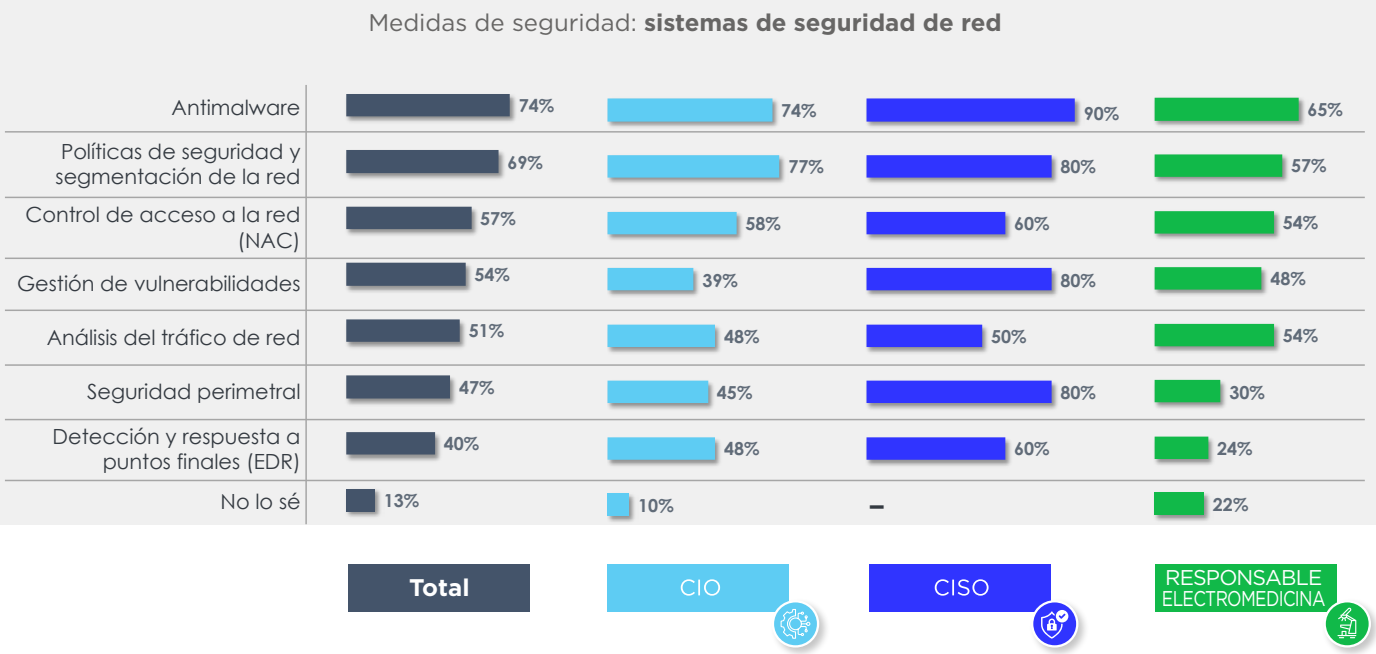


Ilustración 55. Medidas de seguridad: Seguridad de las redes. Responsables

Seguridad de equipos médicos

Los equipos médicos son parte de la OT de los centros sanitarios que cuenta con sus propias características. En particular, son **equipos con dificultades para la actualización de su software, con conexiones remotas para su control y que afectan directamente al servicio sanitario.**

Las medidas que se aplican son comunes al resto de la red, pero como se aprecia, los sistemas antimalware bajan su aplicación y cobra relevancia el control de los accesos remotos, normalmente de los proveedores de mantenimiento.

Vemos como en este tipo de equipos, los Responsables de Electromedicina muestran un mayor conocimiento de las medidas aplicadas, ya que la gestión de estos equipos recae normalmente bajo su responsabilidad.

Medidas de seguridad: **sistemas de seguridad de dispositivos médicos**

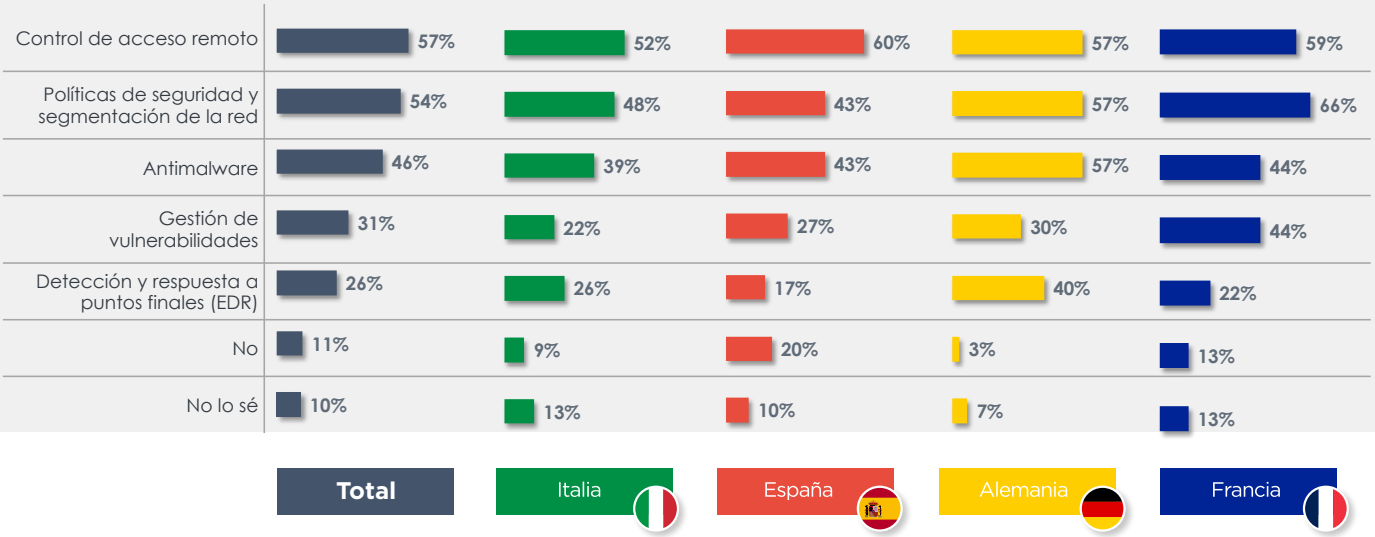


Ilustración 56. Medidas de seguridad: Seguridad de los dispositivos médicos. Países

Medidas de seguridad: **sistemas de seguridad de dispositivos médicos**

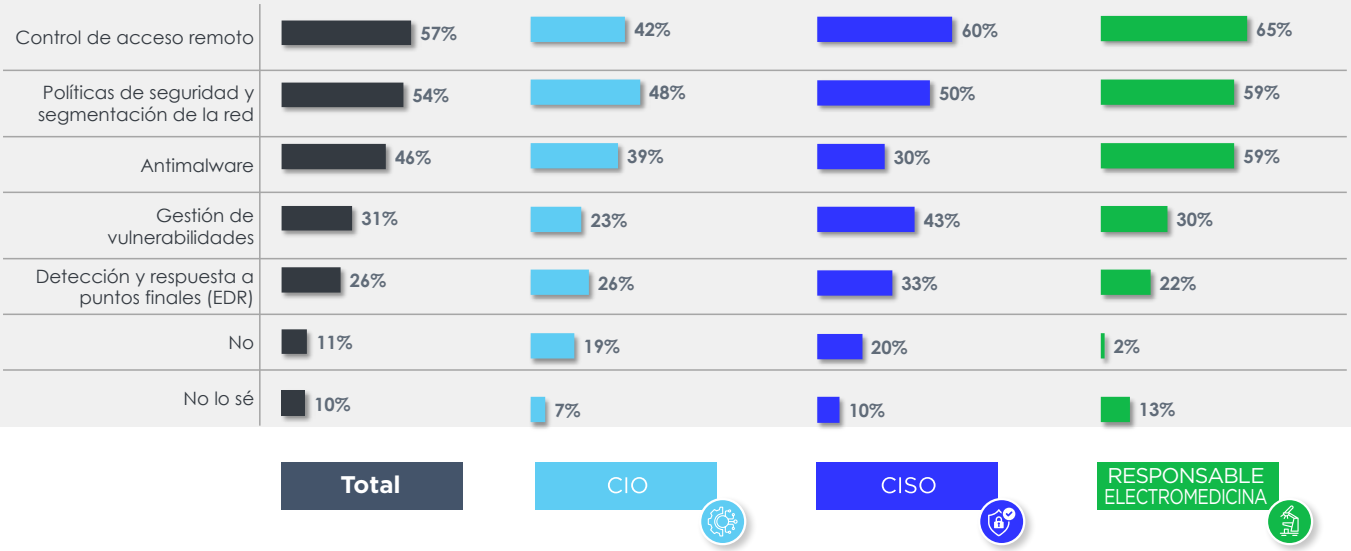


Ilustración 57. Medidas de seguridad: Seguridad de los dispositivos médicos. Responsables

Seguridad del correo electrónico

El correo electrónico es una herramienta transversal en las organizaciones que se ha convertido en un canal de comunicación interna y externa casi prioritario. Sin embargo, se ha convertido también en una puerta de entrada para los ciber atacantes, principalmente con técnicas de ingeniería social tratando de manipular a los usuarios para que les den acceso a través de malware, robo de credenciales, etc.

Además de las campañas de concienciación y formación para que los usuarios puedan distinguir los correos ilícitos y no caer en campañas de phishing, es necesario implantar herramientas de seguridad que detecten estos intentos de intrusión.

Las principales soluciones de ciberseguridad implantadas son el antimalware para el correo y los filtros antispam. España se sitúa en la media europea, aunque todos los países tienen cifras similares de implantación (alrededor del 80%).

Los sistemas antiphising y el establecimiento de políticas de uso del correo, se sitúan justo por debajo de las anteriores, en aproximadamente la mitad de las organizaciones. Concretamente **en España, los sistemas antiphising tan solo se declaran implantados por un 40% de las organizaciones**, mientras que está por encima de la media en la definición de políticas y buenas prácticas (70%).

Medidas de seguridad: **seguridad del correo electrónico**

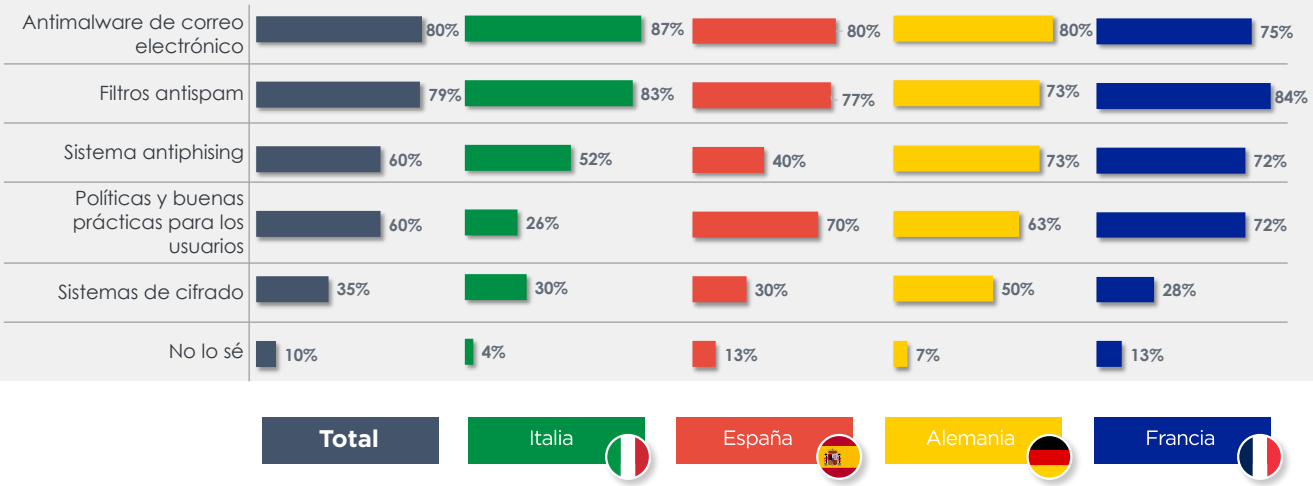


Ilustración 58. Medidas de seguridad: Seguridad del correo electrónico. Países

Copias de seguridad

Los sistemas de copia de seguridad son un pilar fundamental de la protección de los datos sanitarios. Ante un ataque de ransomware, es imprescindible contar con una copia completa y protegida que permita restaurar los sistemas. En caso contrario, la organización tendrá dificultades para recuperar la información, sufriendo mayor presión en caso de chantaje por el atacante.

Estas copias deben incluir, además de la información de los pacientes y de gestión del centro sanitario, los datos de restauración de los sistemas que permitan una recuperación lo más rápida posible.

Una dificultad añadida en el sector sanitario es la velocidad a la que se actualizan los datos, que hace necesaria la realización de copias con una alta frecuencia teniendo los sistemas de copia conectados a las redes. En esta situación se aumenta el riesgo de que las propias copias estén comprometidas, por lo que es necesario proteger los sistemas de backup y conservar copias desconectadas regularmente.

Vemos que las copias de seguridad, en general, se realizan con suficiente frecuencia (diaria-semanal-mensual), aunque su aplicación es desigual en los diferentes países. **España se sitúa por encima de la media europea** con el 83% de los establecimientos sanitarios que realizan copias de calidad en sus sistemas de información.

Sin embargo, tan solo la mitad de los centros cuentan con copias fuera de los locales físicamente y un porcentaje menor cuenta con copias desconectadas de la red. La tendencia que se está viendo en el sector es llevar copias a la nube, de forma que se cumplan los requisitos de distancia física y de desconexión de los sistemas.

La **realización de pruebas de las copias** es fundamental para garantizar que las copias son operativas. Debido al volumen de datos y complejidad de los sistemas, no es una medida de fácil implantación, pero es necesario definir una estrategia que garantice que las copias permitan recuperar la operación de los sistemas de información. Podemos ver que **esta medida es prácticamente inexistente en la mayoría de las organizaciones encuestadas, por lo que aquí habría un área de mejora importante.**

Indique si su organización cuenta con alguna de las siguientes medidas de seguridad: **sistemas de copia de seguridad**

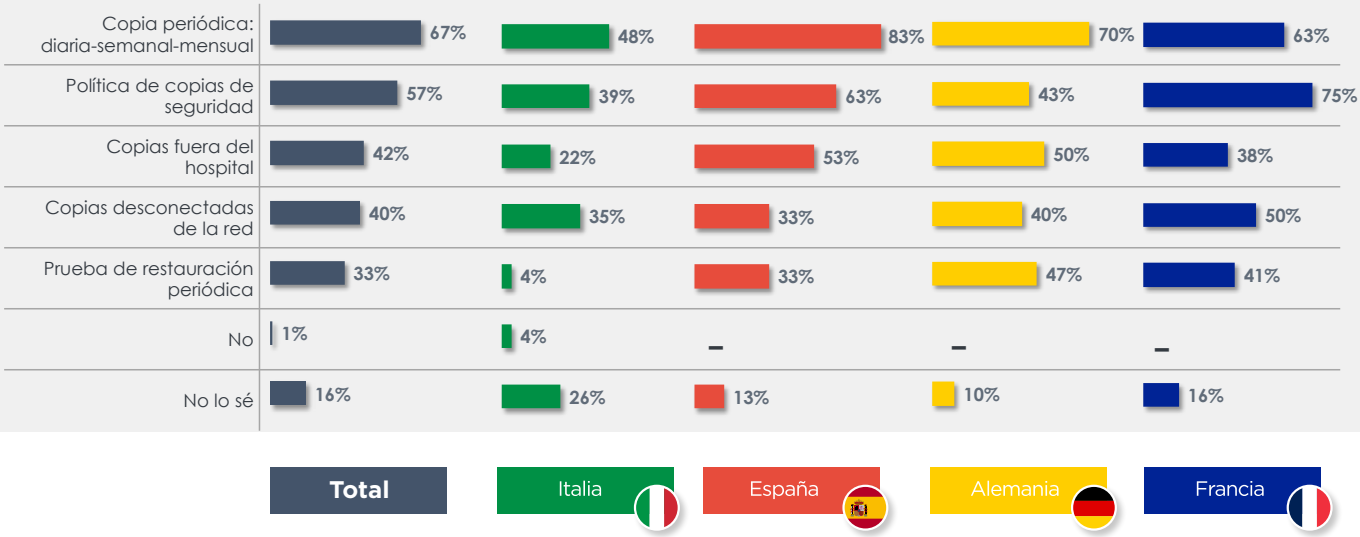


Ilustración 59. Medidas de seguridad: Copias de seguridad. Países

Si analizamos la realización de copias de seguridad desde la perspectiva de los diferentes profesionales encuestados, vemos que el perfil de respuesta se mantiene respecto a la gráfica de los países. El CISO y el CIO son los profesionales que mayor conocimiento tienen de la aplicación de estas medidas, como corresponde a sus responsabilidades. **Los Responsables de Electromedicina están por debajo en el conocimiento o aplicación de las medidas de copias de seguridad**. Esto puede indicar una falta de participación en la definición de la estrategia de copias de seguridad, aunque la información manejada por los equipos médicos debería considerarse a la hora de definir qué información incluir y con qué frecuencia en las copias de seguridad.

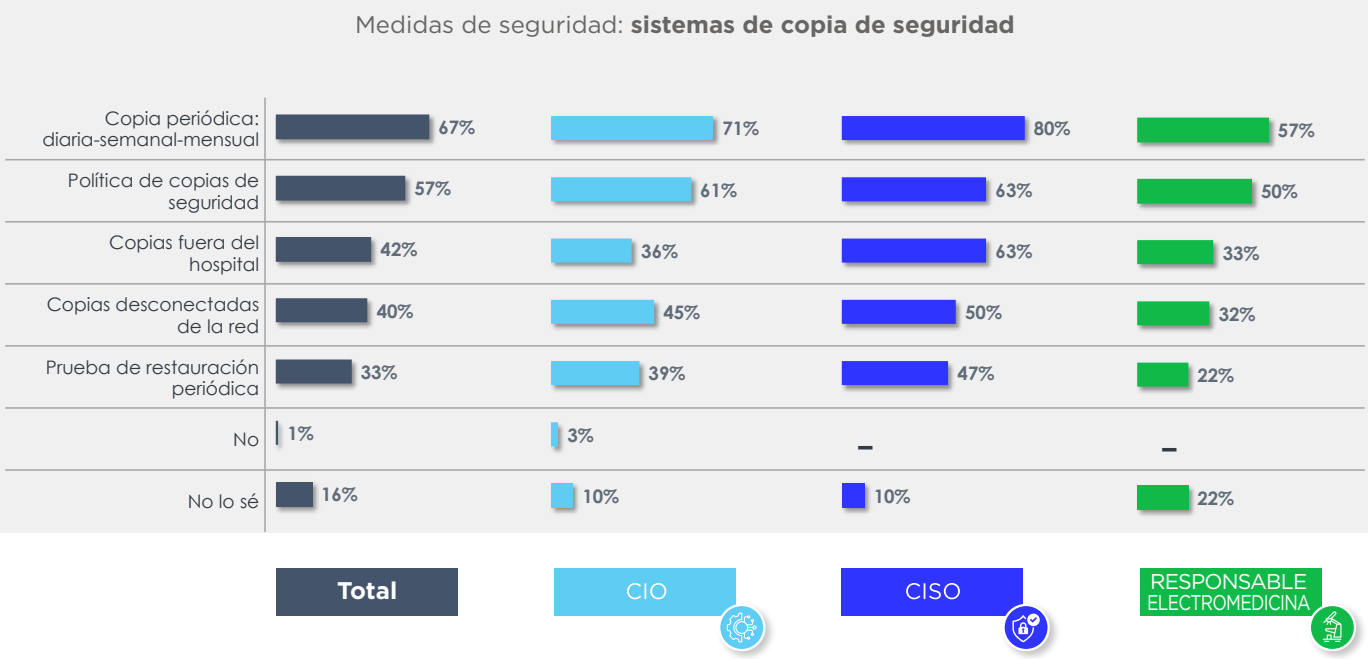


Ilustración 60. Medidas de seguridad: Copias de seguridad. Responsables

Gestión de incidentes

La gestión de incidentes es clave a la hora de recuperar los sistemas una vez que se ha producido el fallo de los sistemas o el ciber ataque. Es necesario tener sistemas definidos para detectar cuanto antes el incidente y evitar que el incidente se propague por la red y después, contar con los medios necesarios para intervenir y detener el incidente y recuperar el servicio del centro.

Esto normalmente se define con dos equipos técnicos que pueden (o no) integrarse en un mismo servicio: el equipo de monitorización de la red (SOC) y el equipo de respuesta a incidentes (CSIRT).

De las respuestas recogidas en la encuesta, vemos como un tercio de los participantes en España declaran contar con ambos servicios. Sin embargo, este porcentaje posiblemente sea mayor, ya que hay un 43% que no sabe si existen o no estos servicios. Puesto que estos servicios son gestionados o contratados por los responsables de las áreas técnicas de red, esta respuesta corresponde a los responsables de equipos médicos, más desligados de estas tareas.

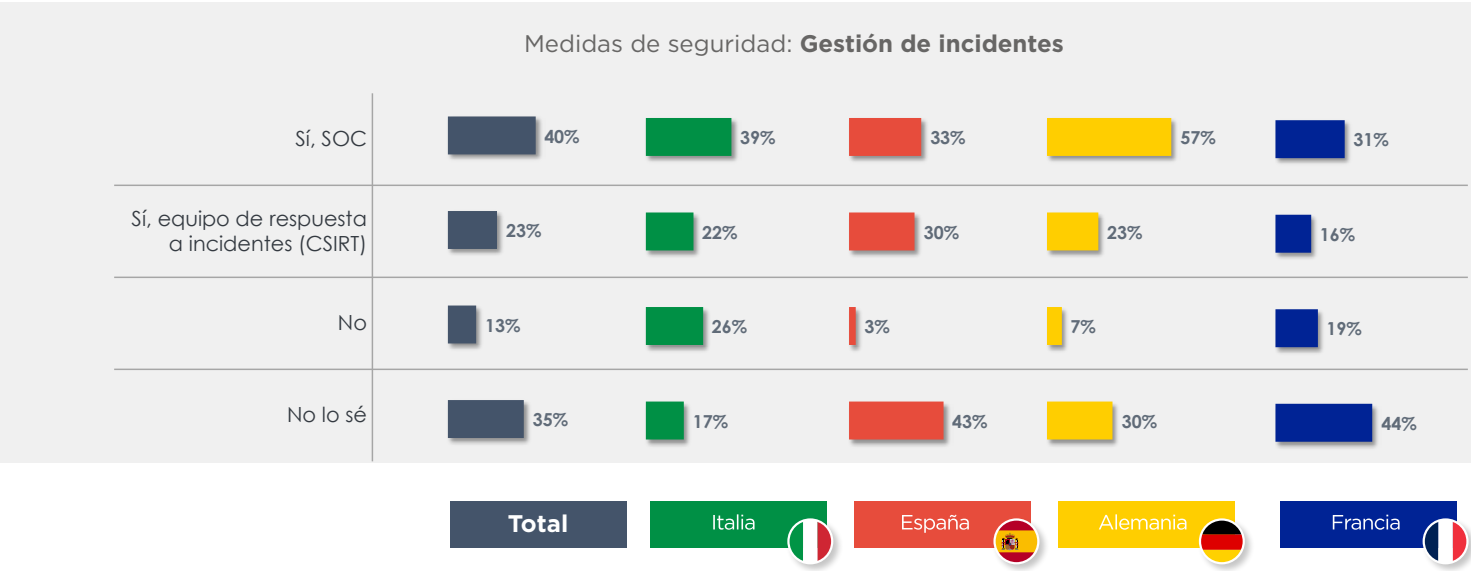


Ilustración 61. Medidas de seguridad: Gestión de incidentes. Países

Si analizamos los servicios de SOC, vemos que **en pocos centros existe un equipo interno**. Vemos que **la presencia de proveedores especializados es clave en estos servicios**. Esto se explica por la necesidad de incorporar expertos en diferentes tecnologías y una alta disponibilidad, condiciones difíciles de cumplir internamente en un centro sanitario. Como se refleja en la gráfica, la opción preferida es un equipo mixto, un servicio propio del centro colaborando con un equipo externo. En segundo lugar vemos los equipos totalmente externalizados.

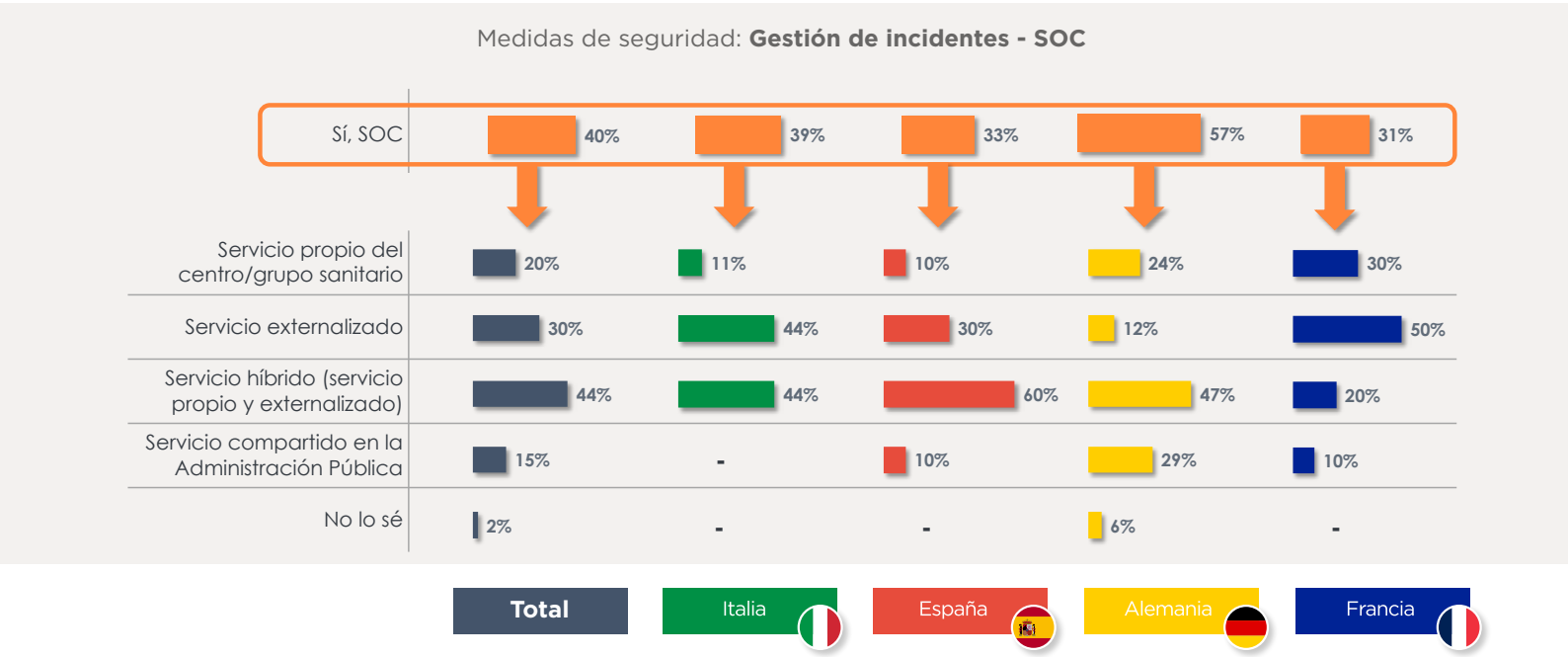


Ilustración 62. Medidas de seguridad: Tipo de SOC. Países

Respecto a los equipos de respuesta al incidente, vemos que varía algo la solución establecida. **En España sigue prevaleciendo la solución mixta (equipo interno junto con un proveedor externo)**. Sin embargo, la segunda opción es un equipo propio del centro por delante de una externalización completa. Cabe destacar también **un 22% de los centros encuestados que declaran un servicio compartido con la AAPP**. En este punto, vemos como **Francia**, con la agencia específica para ciberseguridad en el sector sanitario, es el país con un mayor porcentaje de equipos de la Administración Pública (40%).

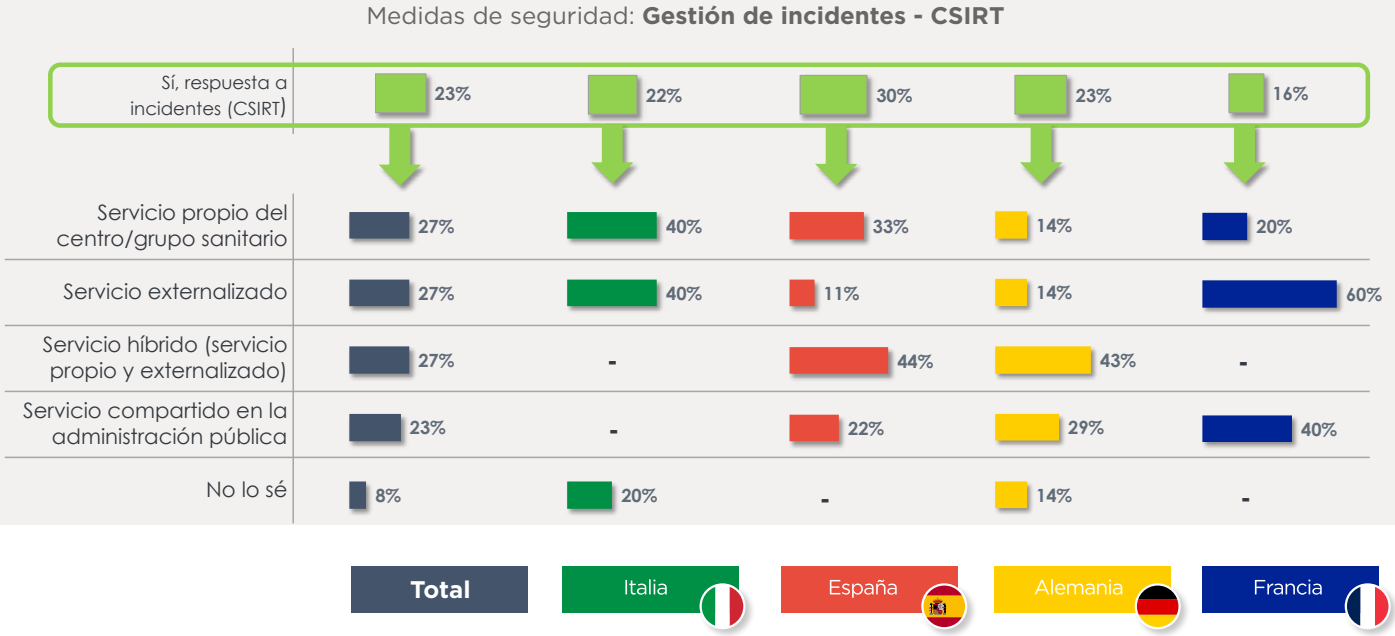


Ilustración 63. Medidas de seguridad: Tipos de CSIRT. Países

Planes de continuidad

Los planes de continuidad son aquellos que se diseñan para garantizar que el servicio médico no se vea interrumpido, concretamente en este caso ante incidentes relacionados con los sistemas de información. Estos planes se deben coordinar con la gestión de incidentes anterior, pero tiene otras actividades importantes como la coordinación de equipos del centro sanitario, la determinación de tiempos de parada y restauración, las pruebas y evaluación de los planes, etc. Es una tarea compleja donde es necesario el apoyo de la dirección y la coordinación entre los diferentes equipos.

En la siguiente gráfica vemos como el **57% de los participantes en España declaran contar con planes de continuidad**. Sin embargo, tan solo un 17% declara haber probado regularmente dichos planes (en respuesta a un procedimiento). **Este bajo porcentaje de procesos procedimentados y probados refleja una falta de madurez de este control.**

Vemos en ambas gráficas que un 33% de participantes declara no conocer si existen o no dichos planes, correspondiendo a los Responsables de Electromedicina. Esto nos muestra una baja involucración de estos equipos en los planes de continuidad, liderados por CIO y CISO. Sin embargo, debido al efecto de los incidentes de los equipos médicos en el servicio sanitario, es **fundamental integrar a estos responsables en la definición, desarrollo y pruebas de los planes de continuidad.**

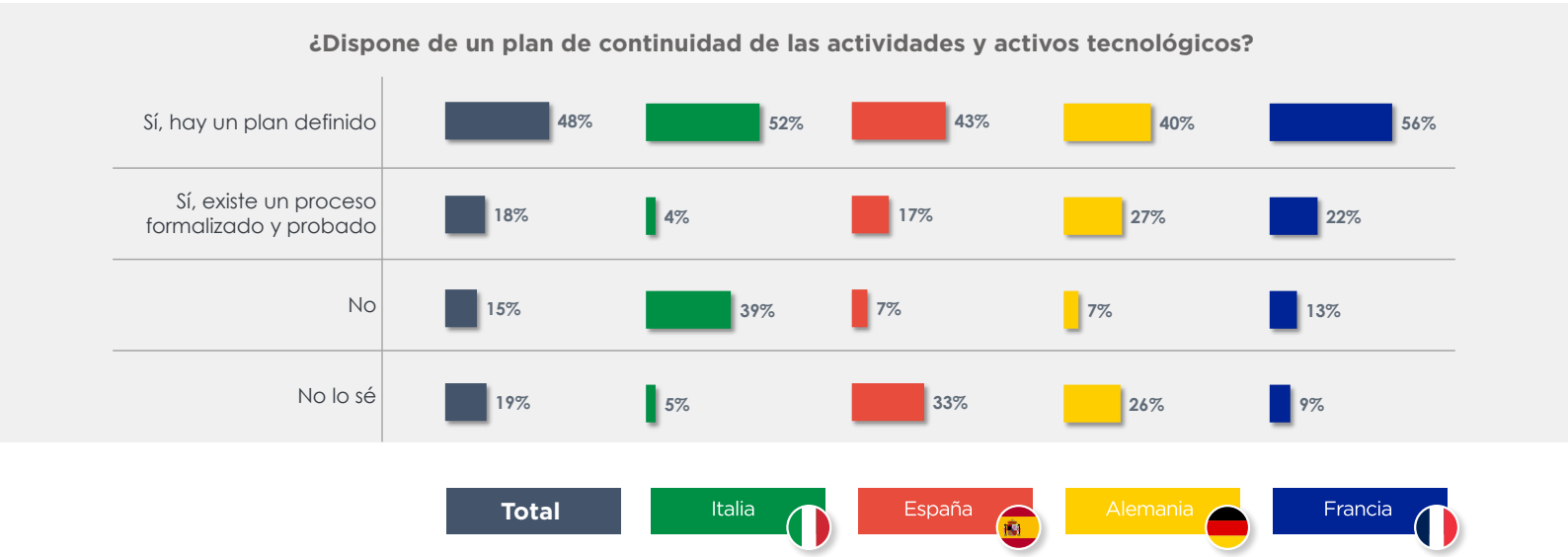


Ilustración 64. Medidas de seguridad: Planes de continuidad. Países

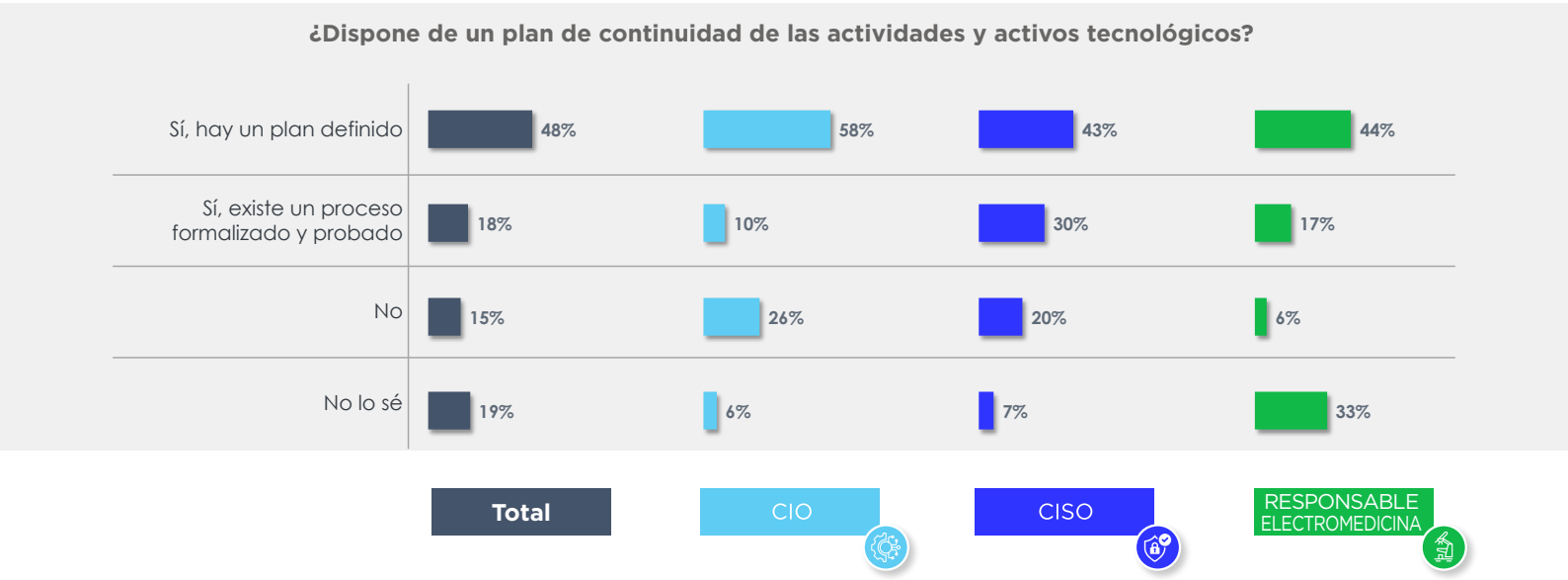


Ilustración 65. Medidas de seguridad: Planes de continuidad. Responsables

Contratación de ciber pólizas

Las pólizas de ciberseguros se consideran una medida de seguridad que ayuda a compensar los efectos de un ciber incidente de forma que el servicio del centro sanitario se vea protegido. Los ciberseguros compensan pérdidas del hospital por la interrupción del servicio, por responsabilidad civil, por gastos de intervención técnica, etc., pero también proporcionan servicios de gestión del incidente y equipos de respuesta para apoyar a los centros sanitarios a recuperar el servicio lo antes posible.

Estos seguros, debido al aumento de incidentes, su impacto y la dificultad en la valoración del riesgo, han tenido una oferta restringida y una baja penetración en el mercado como podemos observar. **En nuestro país no llega al 20% el número de los participantes que cuentan con un seguro o lo están valorando.**

Al mismo tiempo, vemos como la mitad de los participantes no conocen la situación de las pólizas ciber en su organización. Si observamos la gráfica por perfiles, vemos que la respuesta es bastante homogénea entre los distintos perfiles, lo que refuerza la idea de que es una medida con baja penetración todavía en el mercado.

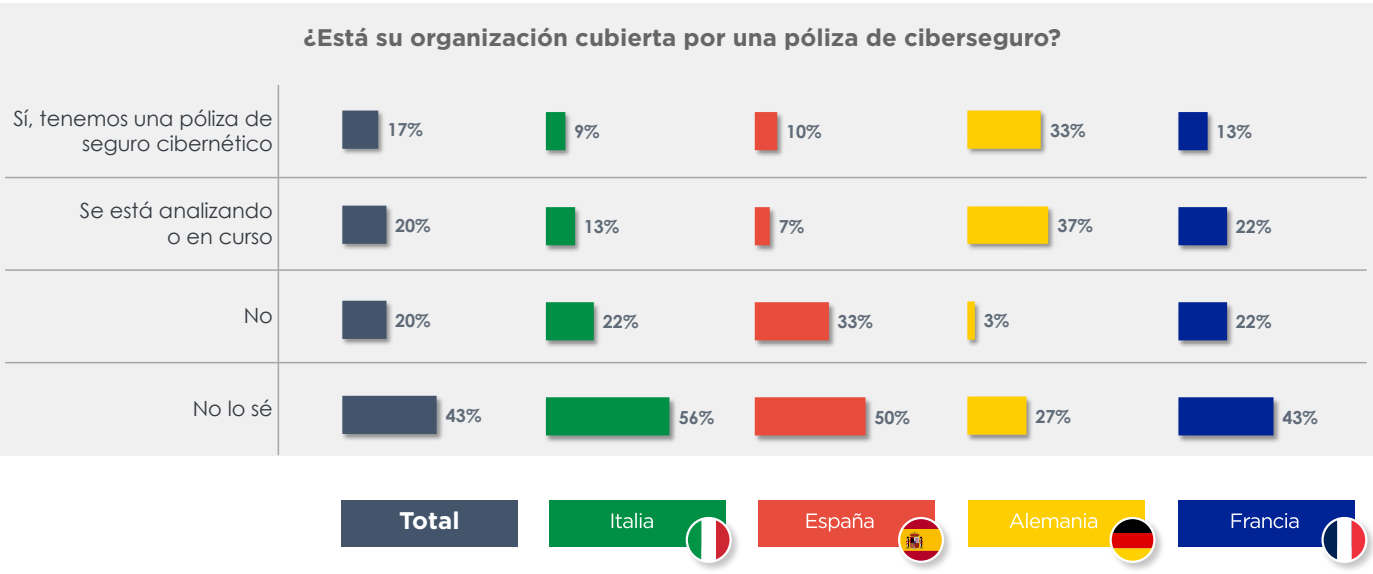


Ilustración 66. Medidas de seguridad: Póliza de ciberseguridad. Países

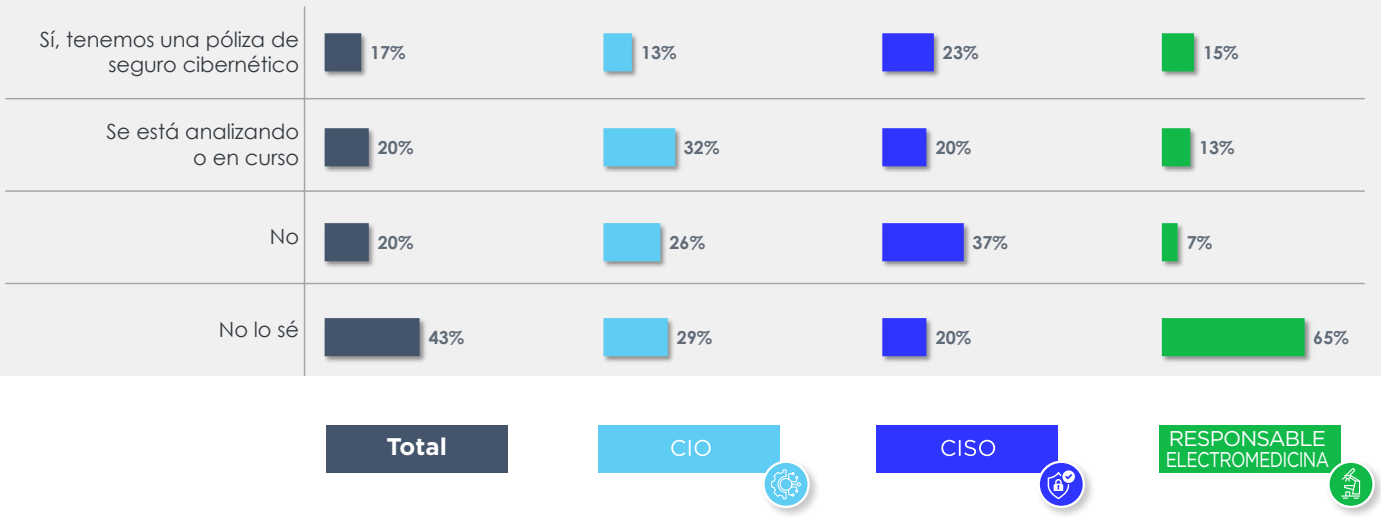


Ilustración 67. Medidas de seguridad: Póliza de ciberseguridad. Responsables

Valoración de las medidas de seguridad

Una vez hemos visto la implantación de las medidas de seguridad en los centros sanitarios, analicemos la valoración que hacen los centros y profesionales de la relevancia de estas medidas en sus sistemas.

En general, vemos que la **mayoría de las medidas son consideradas de alta prioridad**, con muy bajo peso de las medidas consideradas poco relevantes. Respecto a las respuestas en España, podemos ver cómo destaca la priorización de medidas como las aplicadas para la gestión de los equipos IoMT o la relevancia de las inversiones públicas sobre la media de los países analizados.

¿Qué importancia tiene para su organización cada uno de los siguientes aspectos relacionados con la ciberseguridad?

Ilustración 68. Valoración medidas de seguridad por los centros sanitarios. Países

Si revisamos la priorización por responsables, vemos que los CISO priorizan medidas como la seguridad de la infraestructura de red, principalmente, mientras el Responsable de Electromedicina destaca las medidas sobre los equipos IoMT, la seguridad en la nube y la telemedicina.

¿Qué importancia tiene para su organización cada uno de los siguientes aspectos relacionados con la ciberseguridad?

Ilustración 69. Valoración medidas de seguridad por los centros sanitarios. Responsables

EN CIFRAS

06

relyens
GRUPO MUTUALISTA EUROPEO
SEGUROS Y GESTIÓN DE RIESGOS

CIBERSANIDAD: UN ANÁLISIS EUROPEO DE LA CIBERSEGURIDAD SANITARIA

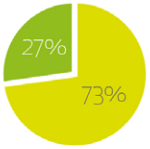
Estudio elaborado por Relyens en colaboración con SEIS y SEEIC para comprender el valor de la ciberseguridad del sector sanitario, evaluar la coordinación entre los diferentes responsables en la gestión del riesgo ciber, analizar la madurez de la gestión del riesgo cibernético hospitalario y recoger las principales preocupaciones y expectativas de futuro de los profesionales del sector respecto a la ciberseguridad.

MUESTRA DEL ESTUDIO

Perfiles de participantes

- Directores Generales
- CIOs (Responsables de TI)
- CISOs (Respons. de Ciberseguridad)
- Responsables de Electromedicina

Distribución



Sector público
Sector privado

Países participantes

- *España*
- *Italia*
- *Francia*
- *Alemania*

El 50% de los hospitales españoles participantes ha sufrido un ciberataque en los últimos 3 años

RESULTADOS

Los riesgos percibidos por los entrevistados se agrupan en 4 áreas:

- Seguridad del paciente
- Violación de la privacidad
- Impacto financiero
- Impacto reputacional

Principales preocupaciones actuales ante un ciberincidente

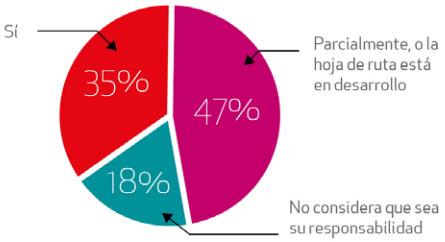
- 97% Seguridad del paciente
- 90% Compromiso con los datos clínicos
- 90% Continuidad de los servicios

¿Cuáles son sus principales preocupaciones en materia de ciberseguridad para los próximos años?

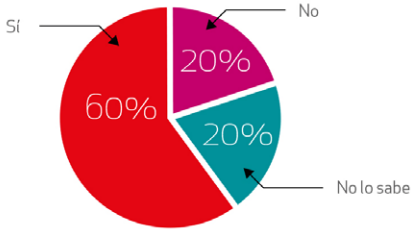
- 87% Filtraciones de datos
- 70% Seguridad en telemedicina
- 67% Ransomware

relyens
GRUPO MUTUALISTA EUROPEO
SEGUROS Y GESTIÓN DE RIESGOS

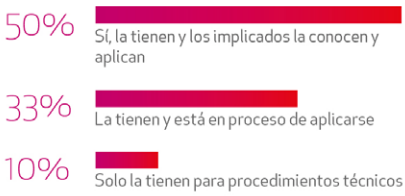
¿Está la ciberseguridad vinculada a los objetivos de su empresa o departamento?



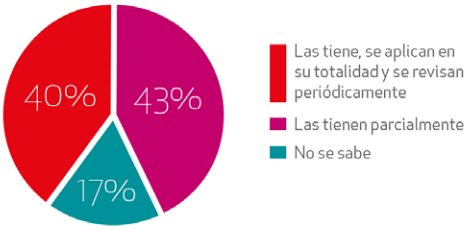
¿Existe un presupuesto dedicado a ciberseguridad?



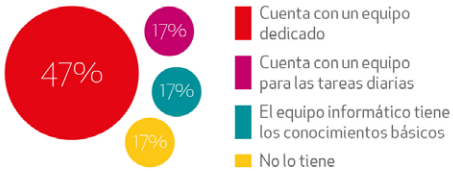
¿Existe una política de ciberseguridad/seguridad de la información en su organización?



¿Existen campañas de formación y concienciación sobre ciberseguridad en su empresa?



¿Cree que cuenta con expertos en ciberseguridad capaces de gestionar los ciberriesgos?



Las instituciones en España cuentan con las siguientes medidas de seguridad:

Solo el **10%** **cuenta con una póliza de ciberseguro**

** Datos obtenidos entre 2022 y 2023.*
*** Esta infografía muestra los resultados de España. Consultar el estudio completo para más información en www.relyens.eu/es/newsroom/mediateca/cibersanidad*

Anticipar hoy
para proteger mañana.

relyens
GRUPO MUTUALISTA EUROPEO SEGUROS Y GESTIÓN DE RIESGOS

relyens.eu

GRUPO MUTUALISTA EUROPEO
SEGUROS Y GESTIÓN DE RIESGOS