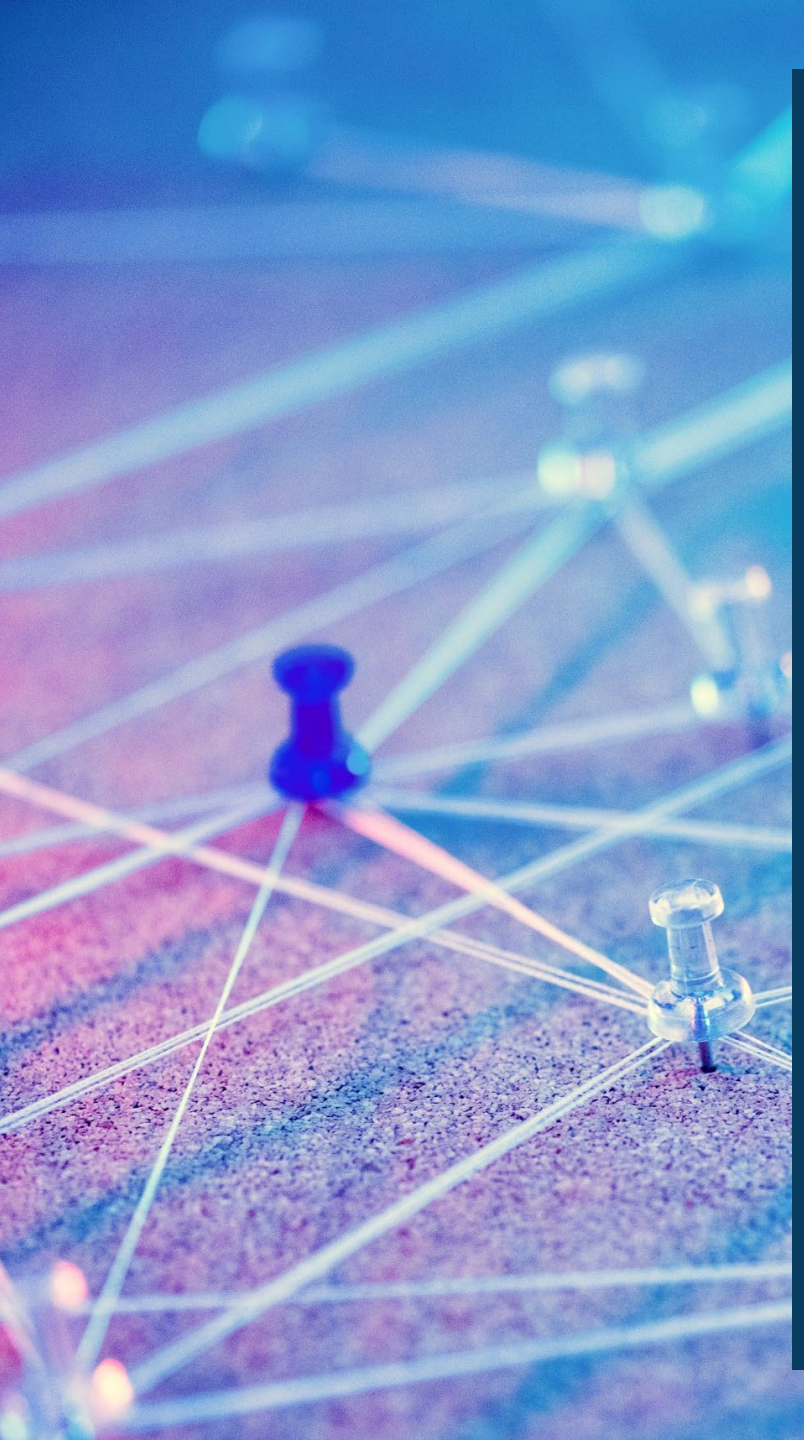
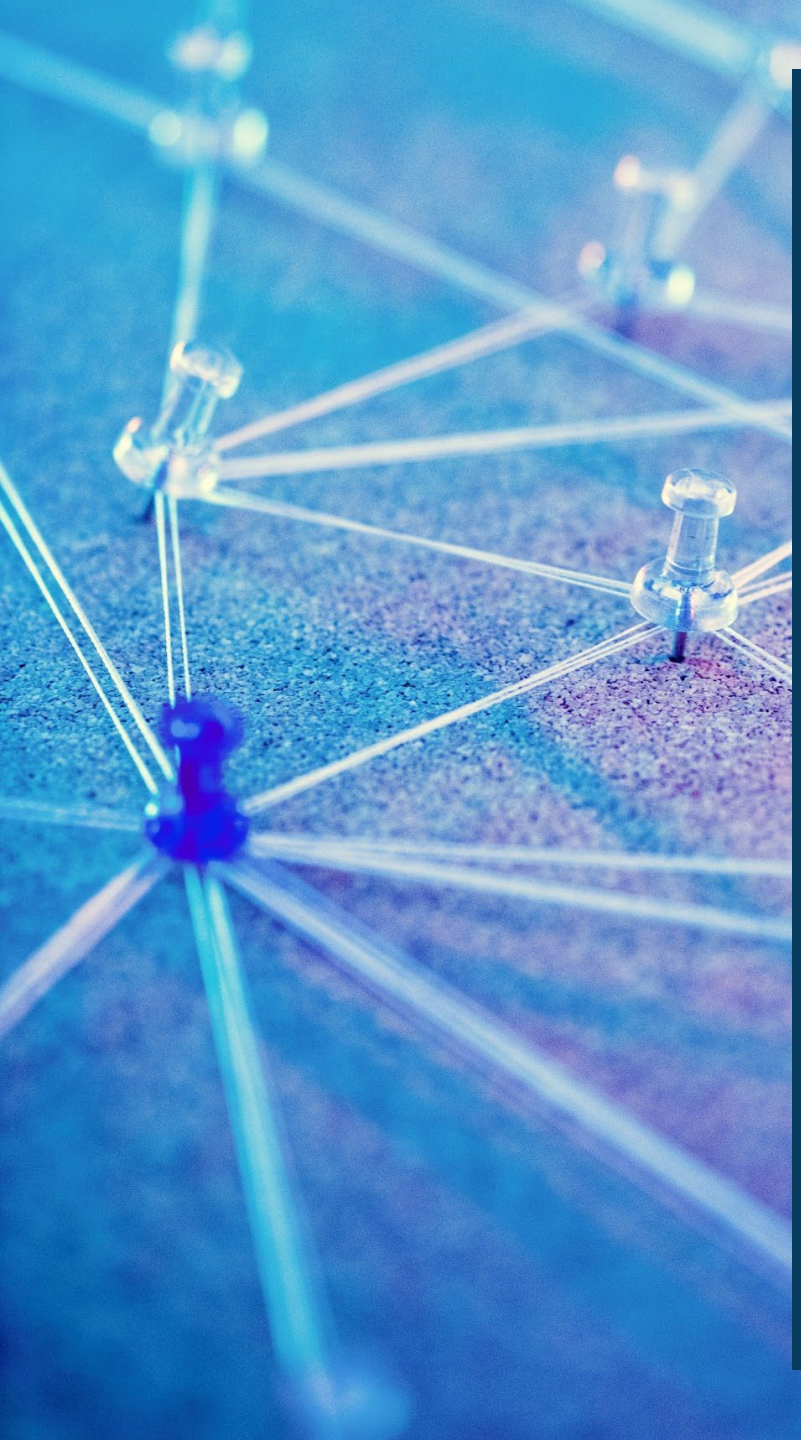
Informe anual sobre ciberseguridad de los sistemas de control de (CS)²AI-KPMG

2024



Índice

Mensaje del Presidente	04
Prólogo del Patrocinador Principal del Informe anual	05
Resumen ejecutivo	06
Programas $(CS)^2$	08
Madurez del programa $(CS)^2$ - Estudio longitudinal	09
Cliente $(CS)^2$ Madurez del programa - Regiones	10
Indicadores clave de rendimiento (KPI) de $(CS)^2$- Nivel alto de madurez frente a Nivel bajo de madurez	11
Marcos de seguridad en uso - Usuarios finales frente a proveedores	12
Planes de organización - Usuarios finales	13
Servicios de $(CS)^2$ - Usuarios finales	14
Tecnologías de $(CS)^2$ - Usuarios finales	15
Obstáculos para reducir la superficie de ataque $(CS)^2$	16
Obstáculos de $(CS)^2$- M alta vs. M baja	17
Obstáculos de $(CS)^2$ - Nivel organizativo	18
Obstáculos de $(CS)^2$ - Usuarios finales y proveedores	19
Obstáculos de $(CS)^2$ - Análisis regional	20
Gastos y presupuestos de $(CS)^2$	21
Áreas de mayor retorno de la inversión de $(CS)^2$ - Nivel organizativo	22
Áreas de mayor retorno de la inversión de $(CS)^2$ - M alta vs. M baja	23
Prioridades de gasto– Nivel organizativo	24
Lineamientos de los proveedores a los clientes en términos de presupuesto	25
Gastos de $(CS)^2$ - M alta vs. M baja vs. Todos	26
Principales gastos de $(CS)^2$ - Usuarios finales	27
Cambio presupuestario de $(CS)^2$- Estudio longitudinal	28
Inversiones previstas de $(CS)^2$- M alta vs. M baja	29
Inversiones previstas de $(CS)^2$ - Regiones	30
Presupuestos de $(CS)^2$ - M alta vs. M baja	31
Evaluaciones de $(CS)^2$	32
Frecuencia de las evaluaciones de $(CS)^2$ por parte de las organizaciones (M alta vs. M baja)	33
Frecuencia de las evaluaciones de $(CS)^2$ - Usuarios finales y proveedores	34
Componentes sujetos a evaluación de $(CS)^2$ - M alta vs. M baja	35
Componentes sujetos a evaluación de $(CS)^2$ - Usuarios finales y proveedores	36
Respuestas de la evaluación de $(CS)^2$ - M alta vs. M baja	37
Evaluaciones de Riesgo $(CS)^2$ previas a la adquisición - Madurez alta frente a madurez baja	38
Capacitación en seguridad	39
Integración de la capacitación de concientización $(CS)^2$ - Usuarios finales	40
$(CS)^2$ Integración de la formación de Concientización- Madurez alta frente a madurez baja	41
$(CS)^2$ Componentes de la Capacitación - Nivel alto de madurez frente a Nivel bajo de madurez	42
$(CS)^2$ Redes	43
Accesibilidad de los componentes del sistema de control	44
$(CS)^2$ Servicios gestionados - Nivel alto de madurez frente a Nivel bajo de madurez	47



Índice

Utilización de los servicios de (CS)² administrados - Estudio longitudinal	48
Servicios de (CS)² administrados actualmente – M alta frente a M baja	49
Tecnologías de (CS)² actuales – M alta frente a M baja	50
Monitoreo de redes de (CS)² – Estudio longitudinal	51
Incidentes de (CS)²	52
Respuestas de (CS)² al ataque - Usuarios finales	53
Incidentes de (CS)² recientes – Estudio Longitudinal	54
Vectores de Ataque por Incidente de (CS)² a clientes – Regiones	55
Impactos de incidentes de (CS)² – Estudio longitudinal	56
Vectores de ataque recientes de (CS)² – Estudio longitudinal	57
Actores de amenazas de (CS)2 – Estudio longitudinal	58
Lineamientos de proveedores	59
Principales lineamientos sobre los KPI de Clientes - Proveedores	60
Anexo A: Aspectos demográficos	61
Cargos de los encuestados - Usuarios finales y proveedores	62
Participación por región	63
Edad de los encuestados	64
Edad de los encuestados por categoría dentro de la organización	65
Nivel educativo de los encuestados	66
Categoría del encuestado dentro de la organización	66
Participación por industria (solo usuarios finales)	67
Tamaño de las organizaciones de los encuestados	68
Roles de decisión de los encuestados	68
Roles de decisión de los encuestados - Solo usuarios finales	68
Cargo y representación del encuestado dentro de la organización	69
Anexo B: Comité Directivo y Colaboradores del Informe Anual	71
Anexo C: Acerca de (CS)²AI	73
Anexo D: Patrocinadores del Informe	74

Mensaje del Presidente

Estimados colegas del sector:

Al comenzar un nuevo año, es esencial reflexionar sobre los avances que hemos logrado en el campo de la seguridad de los sistemas de control, así como sobre los desafíos que seguimos enfrentando. Aunque en el fondo soy optimista, de los cientos de contactos personales que he mantenido en el último año se desprende la sensación de que se está logrando un avance real en un largo camino. Lo que no ha cambiado es la cantidad de trabajo que nos queda por delante para garantizar sistemas seguros que posibiliten nuestro actual estilo de vida.

Me enorgullece anunciar esta tercera edición del Informe Anual sobre Ciberseguridad de los Sistemas de Control llevado a cabo por (CS)²AI-KPMG, producto no solo de nuestros propios analistas e investigadores, sino también del creciente grupo de colaboradores del Comité Directivo del Informe.

El informe de este año se basa en los resultados de una encuesta realizada a más de 630 miembros de la industria en general y a una muestra representativa de los miembros de (CS)²AI de todo el mundo (cerca de 34.000 miembros de la comunidad en la actualidad), con preguntas relativas a sus experiencias en relación con eventos de seguridad en los sistemas de control, patrones de ataque y sus respuestas, y dónde, las organizaciones, están concentrando sus sus recursos para proteger los sistemas y activos críticos.

El informe de 2024 arroja luz sobre varias tendencias y desafíos críticos en la industria de la seguridad de los sistemas de control. Aunque el aumento de los ciberataques es preocupante, las organizaciones se han vuelto más proactivas en sus presupuestos de ciberseguridad, se centran en la prevención y reconocen la amenaza de los ataques a la cadena de abastecimiento. Una de las cuestiones importantes destacadas en el informe es la escasez de profesionales capacitados en el ámbito de la ciberseguridad. Con el aumento de las ciberamenazas, la demanda
de profesionales especializados en ciberseguridad nunca ha sido tan alta.

Los encuestados informan de una mayor dificultad para contratar personal capacitado, y el informe destaca la necesidad de que las organizaciones inviertan en el desarrollo de las competencias y la formación en ciberseguridad de sus empleados actuales.

Esta publicación anual es fruto de un grupo cada vez mayor de colaboradores vitales. Nuestro mayor agradecimiento debe dirigirse a KPMG International, patrocinador principal del informe, por permitirnos lanzar este proyecto hace años y por su continuo apoyo y colaboración en la elaboración del informe. Waterfall Security Solutions y Fortinet también nos han acompañado con recursos y experiencia desde nuestra primera edición. Asimismo, queremos agradecerles a todos los demás socios cuyo respaldo y orientación han contribuido a hacer de esta una valiosa herramienta de apoyo para la toma de decisiones cada año (ver Apéndice D). Por supuesto, no sería justo dejar de nombrar a todos aquellos que se ofrecieron y se convirtieron en miembros de nuestro Comité Directivo del Informe Anual (ver Apéndice B).

Nuestro objetivo colectivo es que este informe aporte una valiosa visión de las experiencias de los colegas sobre este campo y sirva de herramienta de apoyo a las numerosas y difíciles decisiones que se toman todos los días. Es importante utilizar las conclusiones de este informe para tomar decisiones bien fundadas y priorizar las áreas que proporcionan el mejor retorno de la inversión en seguridad de los sistemas de control. Renovamos nuestro compromiso de apoyar a nuestra comunidad en sus esfuerzos por garantizar sistemas seguros que nos permitan vivir conforme a nuestra contemporaneidad.

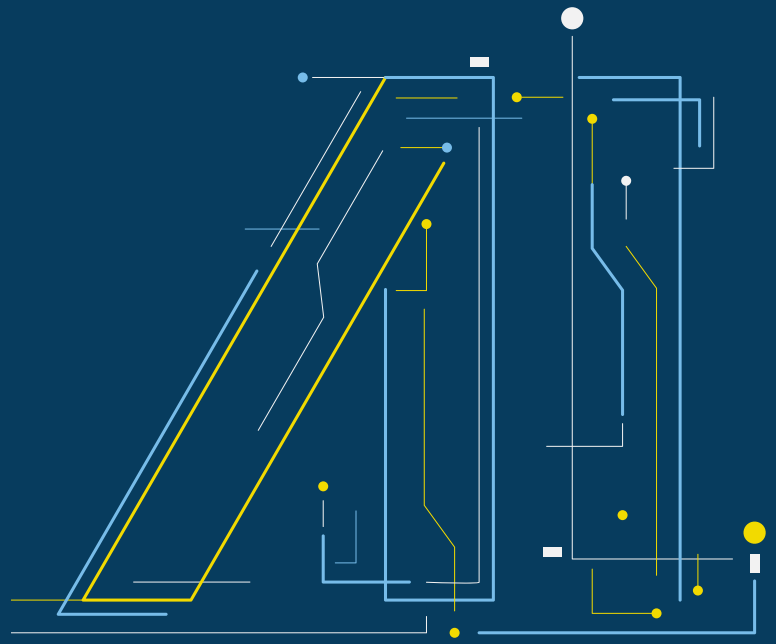
Cordialmente.

Derek R. Harp

Derek Harp

Fundador y Presidente de (CS)²AI

Prólogo del Patrocinador Principal del Informe anual



Walter Risi

Líder Global de Ciberseguridad OT
KPMG International y
Socio y Director de Consultoría
KPMG Argentina

Pablo Almada

Sub-Líder Global de Ciberseguridad OT
KPMG International y
Socio y Director de Ciberseguridad OT
KPMG Argentina

Aunque la ciberseguridad de la tecnología operativa (OT) se ha asegurado un lugar en las agendas de la mayoría de los directores industriales de seguridad de la información (CISO), sigue siendo, en muchos casos, una preocupación aislada dentro del panorama más amplio de la ciberseguridad. A pesar de los importantes avances realizados por numerosas empresas en los últimos años, existe un camino en proceso hacia una mayor madurez e integración en este ámbito. Los resultados de la colaboración de este año entre $(CS)^2AI$ y KPMG International arrojan luz tanto sobre los avances logrados como sobre los desafíos continuos a los que nos enfrentamos.

En cuanto al nivel de madurez, casi la mitad (49%) de las organizaciones encuestadas siguen operando en los niveles de madurez 1 y 2, que van desde apagar el incendio hasta la gestión básica, respectivamente. Aunque la necesidad de establecer un programa de ciberseguridad OT ya no es un concepto novedoso, y a pesar de la disponibilidad de soluciones tecnológicas maduras, no ha habido un salto sustancial en los niveles de madurez observable en los resultados de la encuesta. La escasez de personal capacitado, un problema bien conocido y con el que el sector lleva años luchando, es uno de los factores que más dificultan el progreso.

A pesar de estos desafíos y del ritmo relativamente gradual de desarrollo, nuestras conversaciones con ejecutivos del sector revelan una mayor concienciación sobre los riesgos asociados a la ciberseguridad OT. Mientras que en el pasado, podría haber sido difícil de vender, las conversaciones sobre ciberseguridad con ejecutivos de alto nivel giran cada vez más en torno a la ciberseguridad OT como punto central. Esto significa un mayor nivel de comprensión y reconocimiento de la importancia crítica del tema. No es sorprendente descubrir que los ejecutivos también están más dispuestos a participar en simulacros de crisis y ejercicios teóricos centrados en la ciberseguridad OT.

Creemos que la colaboración anual entre KPMG International y $(CS)^2AI$ desempeña un papel fundamental en la sensibilización de la dirección. Al basarse en las opiniones reales de profesionales y líderes de todo el mundo, nuestra encuesta ofrece una perspectiva imparcial de la evolución mundial de este campo. Ayuda a tomar decisiones de inversión con conocimiento de causa y destaca el creciente interés en este ámbito. Creemos que nuestro informe conjunto constituye un valioso recurso tanto para los profesionales y líderes de la ciberseguridad OT como para la comunidad ejecutiva en general. En esta tercera edición, reafirmamos nuestro compromiso de ofrecer una perspectiva imparcial sobre los principales desafíos que rodean a la ciberseguridad de las tecnologías operativas, tal y como la perciben los líderes mundiales en este campo.

Invitamos a nuestros lectores a profundizar en las ideas del informe de este año, con la esperanza de que nuestro esfuerzo anual les permita, tanto en sus roles de líderes como de ejecutivos o profesionales, tomar decisiones más fundadas e invertir en este ámbito. Consideramos la ciberseguridad OT como un viaje continuo sin final. Esta encuesta, al igual que la propia ciberseguridad, es parte integrante de este viaje continuo, dedicado a ofrecer mejores perspectivas en este campo crítico año tras año.

Resumen ejecutivo

PRINCIPALES HALLAZGOS

- Casi la mitad de las organizaciones que respondieron (49%) siguen sin contar con programas de ciberseguridad ICS/OT o solo con uno básico, al carecer de planes, procedimientos o procesos de mejora de la función.
- Los encuestados de distintos niveles organizativos revelaron prioridades muy diferentes en la asignación de fondos discrecionales adicionales, lo que plantea la cuestión de si sus incentivos están alineados y por qué sus objetivos son diferentes.
- La supervisión completa de la actividad de la red de sistemas de control va en aumento, con un incremento del 80% en el último año.
- Evaluamos la accesibilidad a muchos componentes de sistemas de control (PLC, IED, RTU, HMI, Servidores, Estaciones de Trabajo e Históricos) desde redes empresariales, internet, la nube, y por integradores/proveedores. A menudo hay poca diferencia entre las organizaciones con programas de nivel alto de madurez y las de nivel bajo de madurez en este ámbito. De hecho, los componentes de las organizaciones de nivel alto de madurez suelen ser más accesibles que los de nivel bajo de madurez.
- Consulte en la página 8 las definiciones de nivel alto de madurez y nivel bajo de madurez.

Este informe es el más reciente de una serie de publicaciones anuales elaboradas a partir de las investigaciones de Control System Cybersecurity Association International (también conocida como (CS)^{2}AI), su comunidad de casi 34.000 miembros y decenas de Socios de Alianzas Estratégicas (SAP). Sobre la base de décadas de desarrollo, investigación y análisis de encuestas sobre ciberseguridad dirigidas por el fundador y presidente de (CS)^{2}AI, Derek Harp, y el cofundador y presidente, Bengt Gregory-Brown, el equipo de (CS)^{2}AI invitó a nuestros miembros de todo el mundo y a miles de personas de nuestra amplia comunidad a participar. Las preguntas clave giran en torno a sus experiencias en las primeras líneas de operatividad, protección y defensa de los sistemas y activos de tecnología operativa (OT) que cuestan entre millones y miles de millones en desembolsos de capital, impactan tanto o más en los ingresos en curso, y afectan a la vida cotidiana de las personas y las operaciones comerciales de las empresas en todo el mundo. Más de 630 de los encuestados respondieron a nuestra encuesta principal y muchos más participaron de otras actividades de recopilación de datos que llevamos a cabo a través de nuestros programas educativos (CS)^2 en curso.

Este conjunto de datos, presentados de forma anónima para garantizar la exclusión de consideraciones que de otro modo podrían influir en las respuestas de los participantes, ofrece una visión de las experiencias del mundo real de las personas y organizaciones responsables de las operaciones y de los activos de los sistemas de control que va más allá de lo que podría incluirse en este informe. Esperamos que los detalles que hemos incluido proporcionen la herramienta de apoyo para la toma de decisiones que nuestros lectores necesitan.

Objetivo y metodología de la encuesta

El presente informe utiliza el término general «Sistemas de control» (CS) y «Tecnología operativa» (OT) para referirse a todos los sistemas que administran, supervisan o controlan los dispositivos físicos y los procesos. Por consiguiente, debe entenderse que CS, (CS) y OT incluyen los Sistemas de Control Industrial (ICS), el Control de Supervisión y Adquisición de Datos (SCADA), los Sistemas de Control de Procesos (PCS), los Dominios de Control de Procesos (PCD), Sistemas de Control, Automatización y Gestión de Inmuebles/Instalaciones (BACS / BAMS / FRCS...), los dispositivos médicos conectados a la red, etc.

Del mismo modo, el término «(CS)²» se refiere al campo, la profesión, los programas y el personal relacionados con la Ciberseguridad de los Sistemas de Control.

La edición del Informe anual sobre ciberseguridad de los sistemas de control 2024 de (CS)2AI-KPMG se lanzó en 2019 para producir contenidos que ayudaran a la toma de decisiones por parte de todos aquellos que se ocupan de asegurar los activos y las operaciones de los sistemas de control, ya sean usuarios finales o proveedores, ejecutivos, gerentes o recursos operativos, en cualquier parte del mundo.

Este informe es fruto de la colaboración de estas entidades:

- (CS)²AI: Como creador del proyecto, (CS)²AI desempeñó el papel principal respecto de la planificacion, dirección y ejecución del proyecto, y fue responsable de la recopilación y análisis de datos y la autoría de este informe.
- KPMG International: En su calidad de patrocinador principal del informe, KPMG proporcionó financiación primaria y apoyo a los recursos organizativos para aumentar las capacidades propias de (CS)²AI.
- Patrocinadores secundarios adicionales: Fortinet, Waterfall Security Solutions y Opscura aportaron financiación adicional y otros recursos. (Ver Apéndice D: Informe de patrocinadores)

De acuerdo con los objetivos antes mencionados, (CS)²AI y nuestros patrocinadores distribuyeron encuestas en línea a los miembros de la comunidad de ciberseguridad CS/OT que se desempeñan en este campo, recopilan datos clave en torno a eventos, actividades y tecnologías relacionados con los controles de seguridad, y la información sobre cómo están respondiendo las organizaciones al contexto de amenazas[1] en constante cambio.

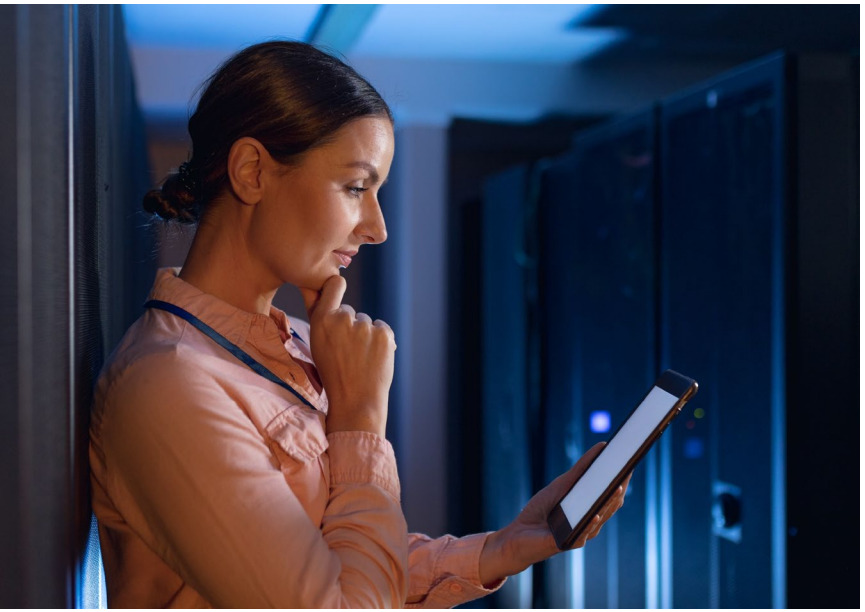
(CS)²AI invitó a participar a sus miembros asociados, reconocidos defensores e investigadores de la seguridad de la tecnología operativa. Distribuyó la encuesta a través de invitaciones directas y diversos canales de difusión en los medios de comunicación, y la promocionó en sitios que prestan servicio al personal de ciberseguridad de sistemas de control, con la intención de recuperar una muestra lo más amplia posible. Los encuestados se autoseleccionaron al afirmar su implicación actual o reciente en el campo (CS)² . Entre ellos se encuentran profesionales de todos los niveles organizativos: especialistas en ciberseguridad y expertos en temas específicos (PYME), así como aquellos cuyo trabajo incluye, aunque no consiste necesariamente y únicamente, en garantizar y proteger los sistemas de control.

La capacidad de separar a nuestros participantes en diferentes grupos y comparar sus aportes a la luz de estas agrupaciones es clave para el análisis de los conocimientos derivados de este proyecto de investigación anual. Si bien consideramos que el nivel de madurez del programa (CS)²AI de los participantes de la encuesta es la dimensión más importante, también se consideran sus niveles organizativos, sus regiones y su relación con los activos (CS)² (proveedores, usuarios, propietarios u operadores). Por supuesto, también realizamos estudios longitudinales y, en los casos en que detectamos tendencias interesantes, también las compartimos.

[1] Contexto de amenaza: la suma de todas las posibles amenazas a las operaciones y activos de SC/TO. El contexto de amenazas es

Programas (CS)²

Medir el nivel de madurez del programa (CS)² de las organizaciones encuestadas es clave para gran parte de nuestro análisis anual, ya que proporciona una métrica para evaluar muchos de los demás datos que proporcionan. ¿Qué es lo que hacen de diferente o qué otras cosas hacen con más frecuencia las organizaciones que mantienen programas[2] con un nivel de madurez mayor? En los casos en que encontramos diferencias significativas entre las respuestas de estos grupos, se lo indicamos al lector. Pedimos a cada participante que eligiera cuál de los siguientes descriptores se ajustaba mejor a la situación de su organización.



Niveles de madurez del programa de ciberseguridad del sistema de control

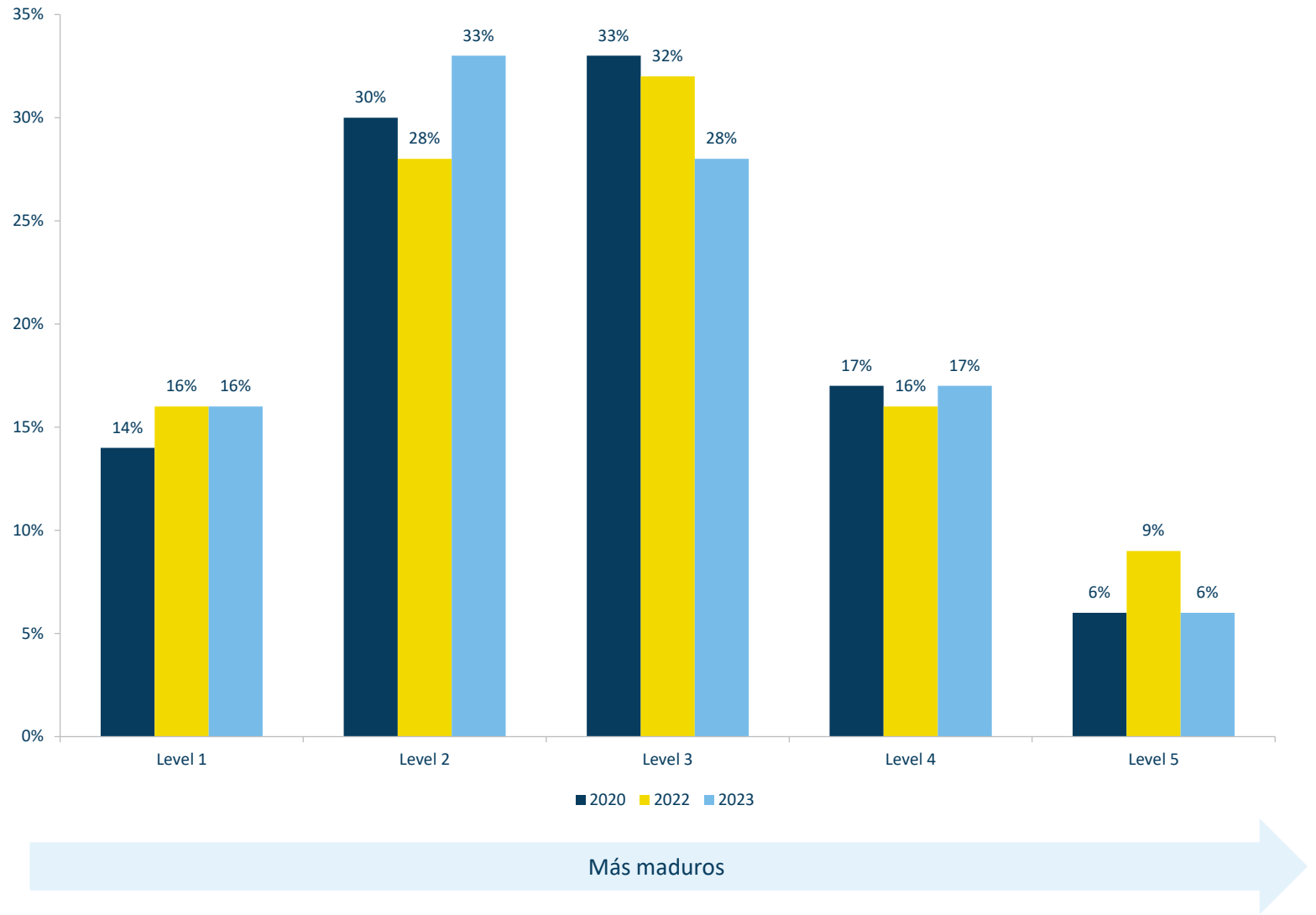
Nivel 5	Nivel 4	Nivel 3	Nivel 2	Nivel 1
Los procesos de ciberseguridad se mejoran continuamente a través de la retroalimentación de los procesos existentes y se adaptan para responder mejor a las necesidades de la organización. El personal que lleva a cabo los procesos tiene las competencias y los conocimientos adecuados. Optimización, automatización, integración y previsibilidad. Defensa activa, inteligencia de amenazas, administración de incidentes.	Nivel 4 —El programa de Ciberseguridad utiliza la recopilación y el análisis de datos para mejorar sus resultados. Las actividades se rigen por directivas organizacionales documentadas, las políticas incluyen requisitos de cumplimiento de normas y / o lineamientos específicos. El personal responsable de las tareas de seguridad del sistema de control está capacitado y tiene experiencia. El programa se gestiona, es proactivo, realiza un seguimiento de las métricas, tiene cierta automatización. Defensa activa, sistema SIEM, detección de anomalías y violaciones.	La ciberseguridad funciona sobre la base de procesos y procedimientos documentados. Las partes interesadas clave están identificadas e involucradas. Se proporcionan los recursos adecuados para dar soporte al proceso (personas, financiación y herramientas). Se han identificado normas y/o lineamientos para guiar las implementaciones. Defensa pasiva	En las implementaciones de ciberseguridad se siguen prácticas básicas de gestión de proyectos; el éxito sigue requiriendo personas clave, pero se está desarrollando un corpus de conocimiento. Se llevan a cabo prácticas recomendadas, aunque para situaciones puntuales. Defensa pasiva	Apagar incendios. Los procesos de ciberseguridad no están organizados ni documentados, ni organizados en un "programa". El éxito depende de los esfuerzos individuales; no es repetible ni escalable porque los procesos no están suficientemente definidos y documentados. Defensa pasiva

[2]El grupo de nivel alto de madurez incluye todos los encuestados autocalificados en los niveles 4 o 5; el grupo de nivel bajo de madurez incluye los que identifican como niveles 1 o 2.

Madurez del programa (CS)² - Estudio longitudinal

El número de participantes en cada clasificación ha variado (se observa un aumento de las respuestas de nivel 2 este año), sin embargo, hemos observado pocos cambios en los tamaños de los grupos de nivel alto de madurez /nivel bajo de madurez totalizados a lo largo de los años. Los participantes siguen calificando sus propios programas (CS)² de forma coherente. Nuestro equipo considera que esto respalda la validez de esta autoevaluación. Lo utilizamos ampliamente en nuestros análisis de contrastes y similitudes entre los grupos de Alta Madurez (Niveles 4 y 5) y Baja Madurez (Niveles 1 y 2) en los que basamos las recomendaciones.

En su opinión, ¿cuál de estas situaciones describe mejor su programa de ciberseguridad del sistema de control?



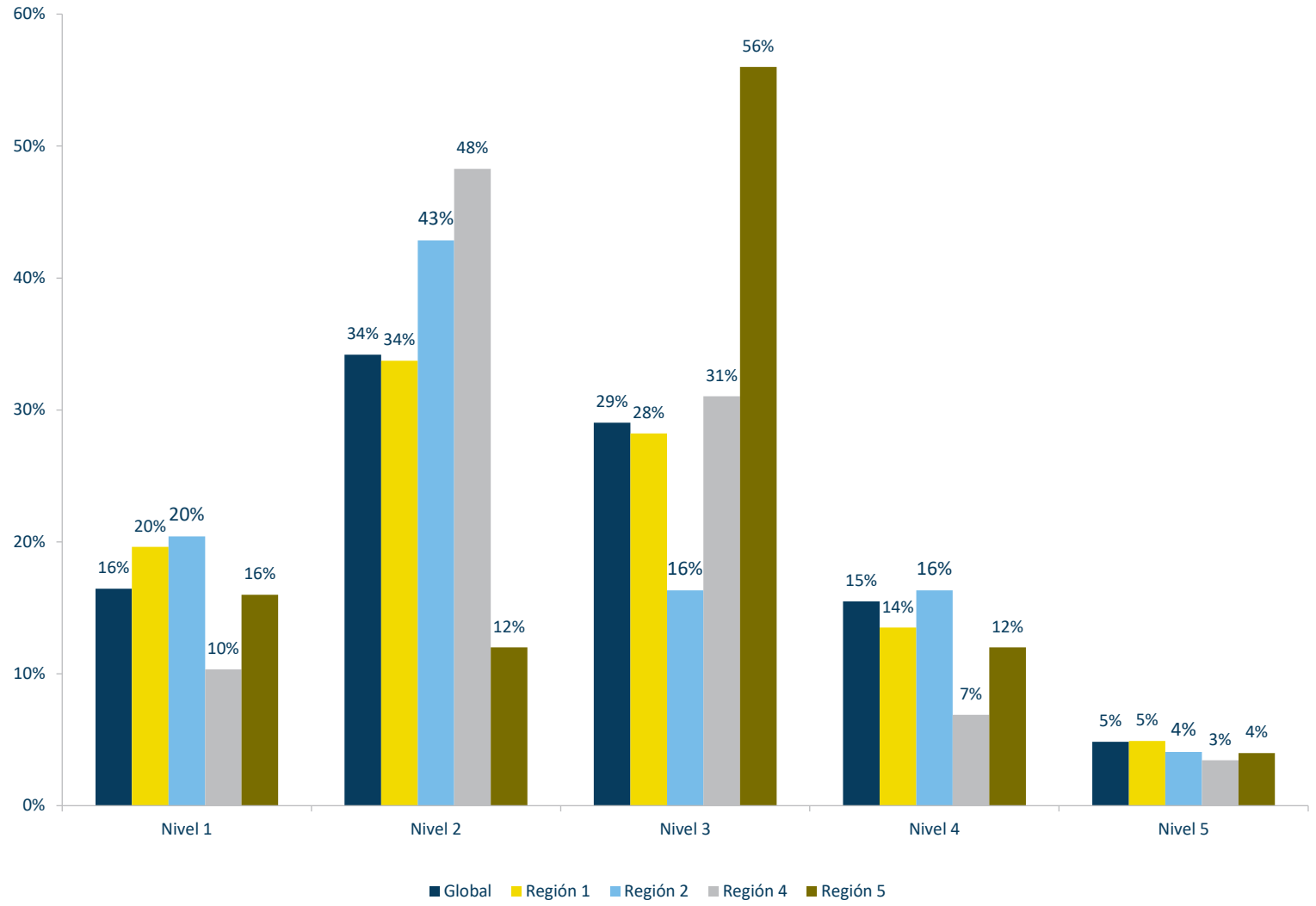
Cliente (CS)² Madurez del programa - Regiones³

Los consultores (proveedores de equipo, proveedores de servicios, integradores) de todo el mundo no comparten la misma opinión acerca de la madurez de los programas (CS)² de sus clientes. Las diferentes regiones tienen distintas opiniones con respecto a la madurez. La Región 2 obtiene autocalificaciones más bajas, con un 63% en los niveles 1 y 2, la Región 4 se centra en torno al nivel 2 (48%) y la Región 5 en torno al nivel 3 (56%). Las Regiones 3, 6 y 7 carecían de participación suficiente para incluirlas en este análisis (ver la nota a pie de página³).

³(CS)²AI está organizada en siete Regiones.

1) América del Norte;
2) Europa (Central, Occidental, Septentrional y Meridional);
3) Eurasia;
4) Indo-Pacífico;
5) Oriente Medio y Norte de África;
6) África Meridional;
7) América Latina y el Caribe

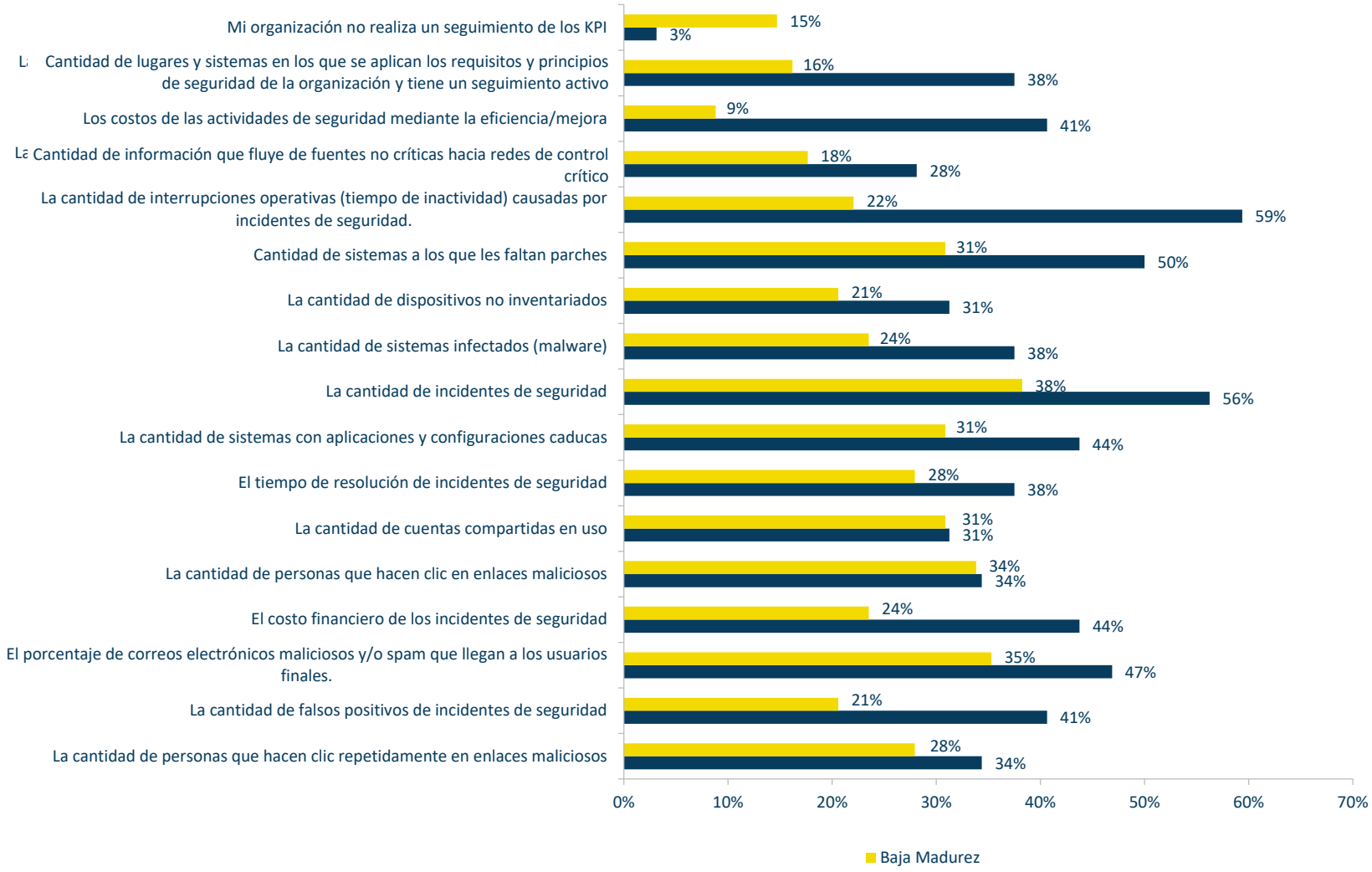
En su opinión, ¿cuál de estas situaciones describe mejor el programa de ciberseguridad del sistema de control de sus clientes?



Indicadores clave de rendimiento (KPI) de (CS)²- Nivel alto de madurez frente a Nivel bajo de madurez

Aunque el mayor seguimiento de algunos Indicadores Clave de Rendimiento (KPI) por parte de los programas más maduros no sorprende (por ejemplo, se estima el aumento de casi cinco veces en los *Costos de la Actividad de Seguridad a través de Eficiencias/Mejoras* en un 8% respecto del Nivel bajo de madurez frente a un 40% del Nivel alto de madurez, ya que se trata de una actividad básica utilizada para mejorar cualquier programa a lo largo del tiempo), consideramos preocupante que tantos programas realicen tan poco seguimiento. Este año hemos tenido aproximadamente el doble de encuestados de nivel bajo de madurez que de nivel alto de madurez, y aunque un alentador 85,3% de ellos realiza el seguimiento de algunos KPI, la mayoría solo realiza el seguimiento de unos pocos. Recomendamos encarecidamente a estas organizaciones que amplíen sus métricas para obtener una mayor visibilidad de la eficacia de los esfuerzos de sus programas de seguridad.

KPI típicos de (CS)² supervisados por las organizaciones

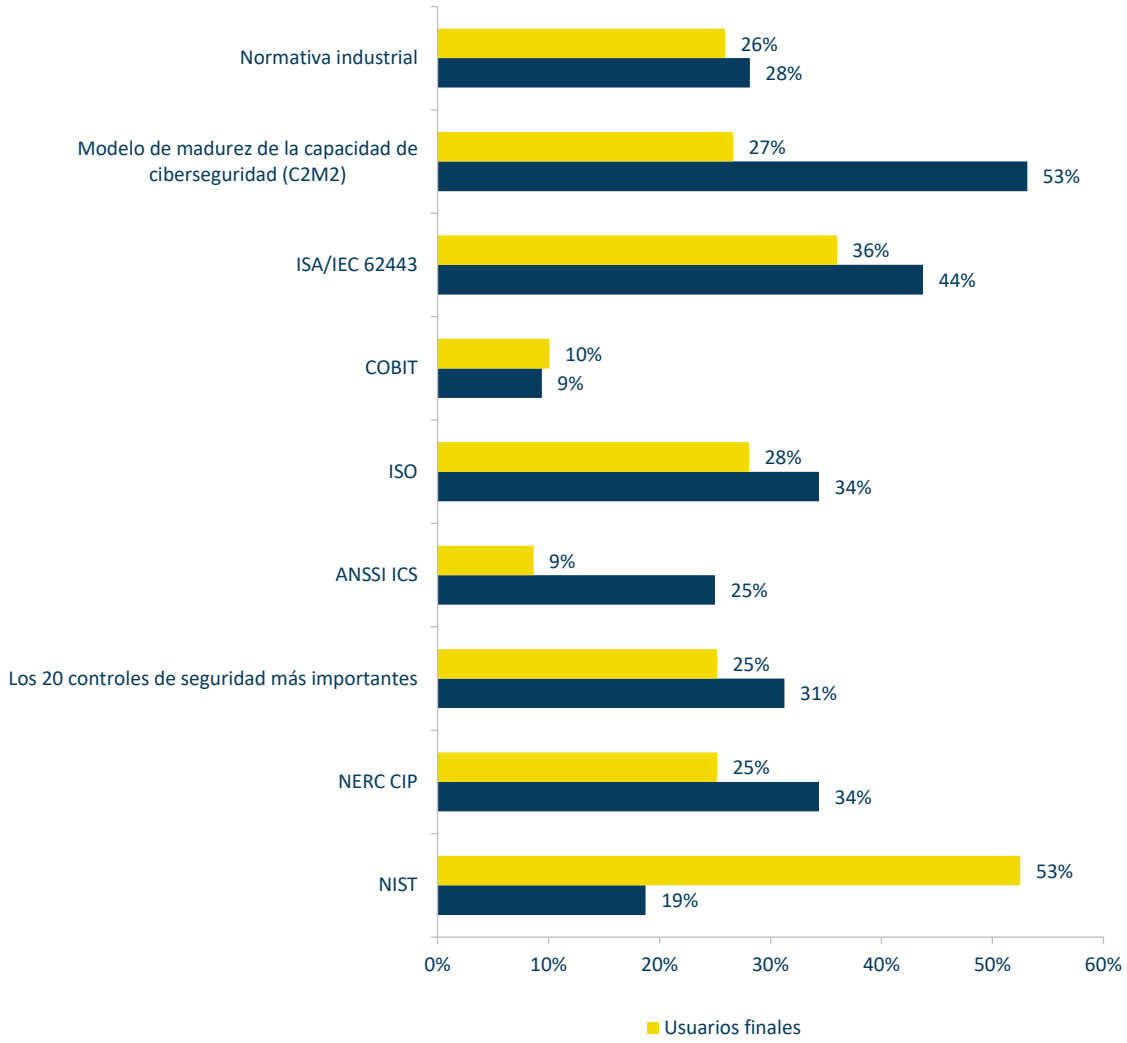


Marcos de seguridad en uso - Usuarios finales frente a proveedores

Comparar los puntos de vista de grupos dispares tiene sus detractores, pero consideramos que ver las perspectivas de estos participantes lado a lado es útil, ya que ambos tienen la responsabilidad de la seguridad de los sistemas de control, y vemos aquí que mientras los destacados son el *C2M2* y el *NIST*, el primero lo es para los Proveedores y el segundo para los Usuarios Finales. El uso del *C2M2* informado por los usuarios finales coincide efectivamente con los datos globales del año pasado (2022-*C2M2* 26,3%), pero ese informe no diferenciaba entre usuarios finales y proveedores.

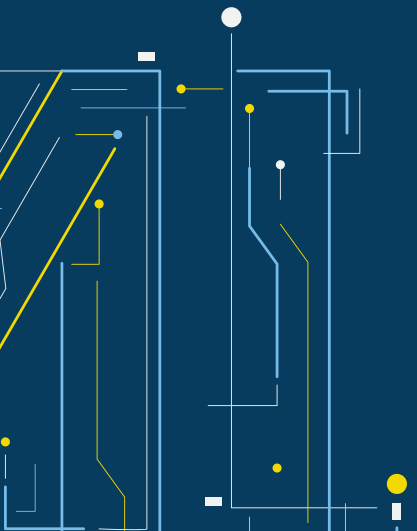
En la última edición de nuestra encuesta, los proveedores respondieron por separado e informaron que utilizaban el *C2M2* con una frecuencia de casi el doble (Usuarios finales *C2M2:* 26,6% vs proveedores *C2M2*: 53,1%). El uso del *NIST* no parece haber cambiado tanto, ya que la respuesta de todos los participantes el año pasado fue del 45,7% (2022), y la media de los dos grupos se sitúa en esa franja.

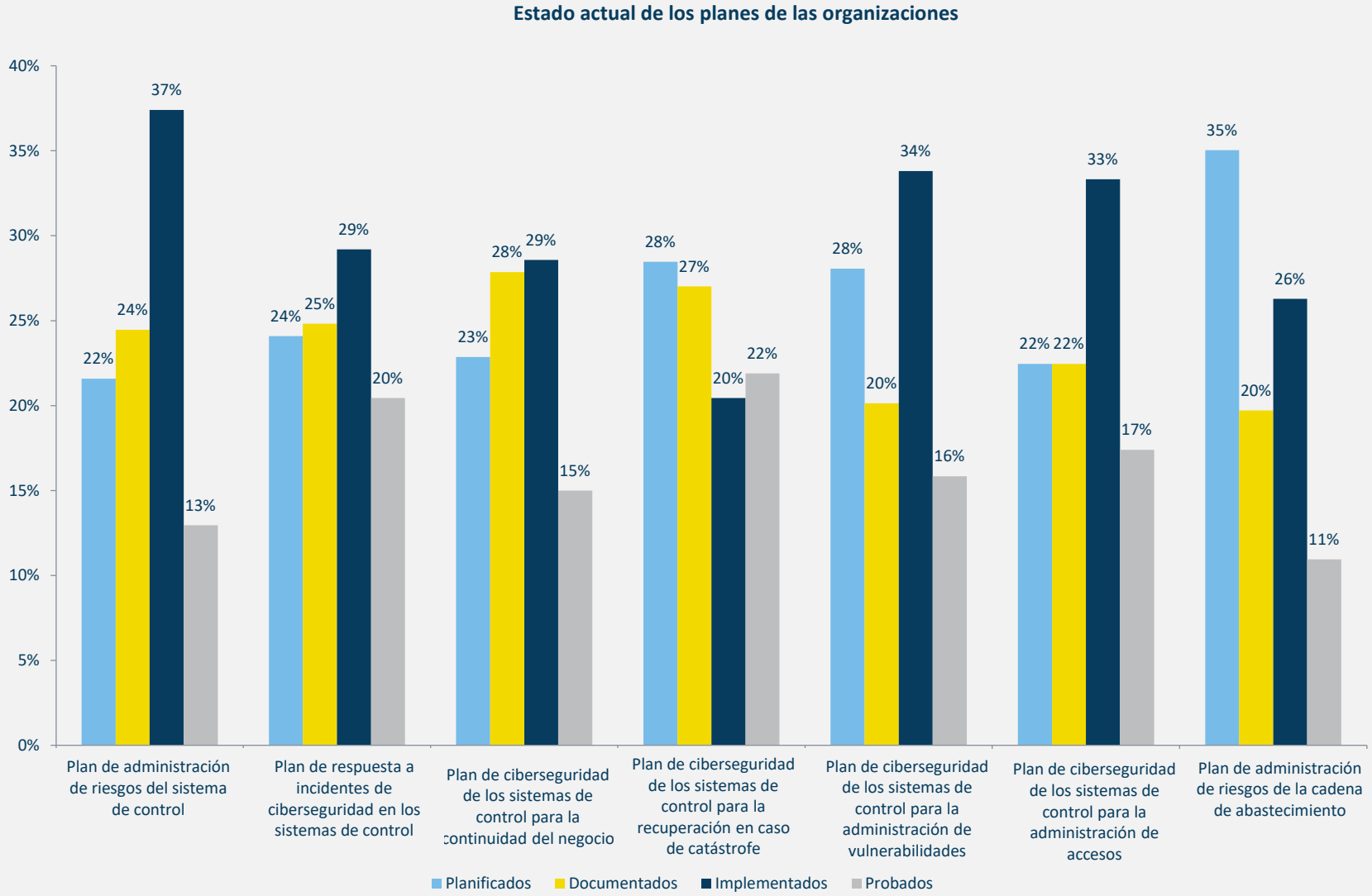
Marcos utilizados por los equipos de seguridad de los sistemas de control



Planes de la organización - Usuarios finales

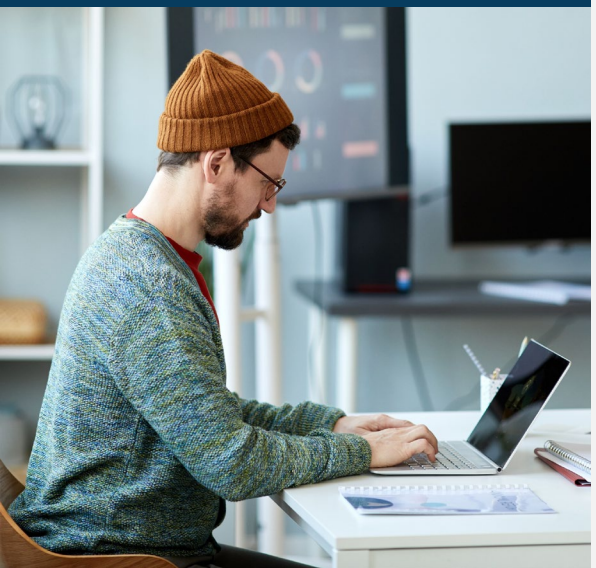
En opinión de nuestro equipo, toda organización con responsabilidades en materia de (CS)² debe administrar sus riesgos de forma exhaustiva, con planes y procedimientos documentados, aplicados y probados para reducir los incidentes y minimizar el impacto en la empresa, en los empleados y en los clientes. Dado que los planes totalmente *implementados* y *probados* son la regla de oro, la gran cantidad de empresas encuestadas con planes en su mayoría solo *documentados* o *planificados* es preocupante, ya que no están preparadas desde el punto de vista de los procedimientos para administrar y responder a los tipos de eventos para los que dichos planes están pensados.





Servicios de (CS)² – Usuarios finales

¿Adónde recurren las organizaciones para encontrar la ayuda que necesitan con el fin de proteger sus activos (CS)² , su personal y sus operaciones? Según los encuestados, en donde puedan. La respuesta destacada de *Recursos internos de seguridad de IT* (56,2%) sugiere que la ciberseguridad de OT está siendo impulsada por los grupos de IT en la mayoría de las organizaciones, con la probabilidad concomitante de que se estén aplicando métodos y tecnologías de seguridad de IT en estos entornos.



Muchos CISO se sienten intimidados por los proyectos de seguridad OT, ya que la cura de la ciberseguridad en las plantas industriales es peor que la enfermedad. Fui CISO, así que lo entiendo. La OT exige priorizar el proceso, mientras que IT prioriza la seguridad durante el tiempo de paradas de la planta.

Estamos perdiendo la guerra contra los "malos", en gran medida debido a la inacción. Proteger la OT con las herramientas informáticas tradicionales es costoso, no solo por la consultoría, la planificación y el equipamiento, sino también por la cantidad de tiempo de inactividad.

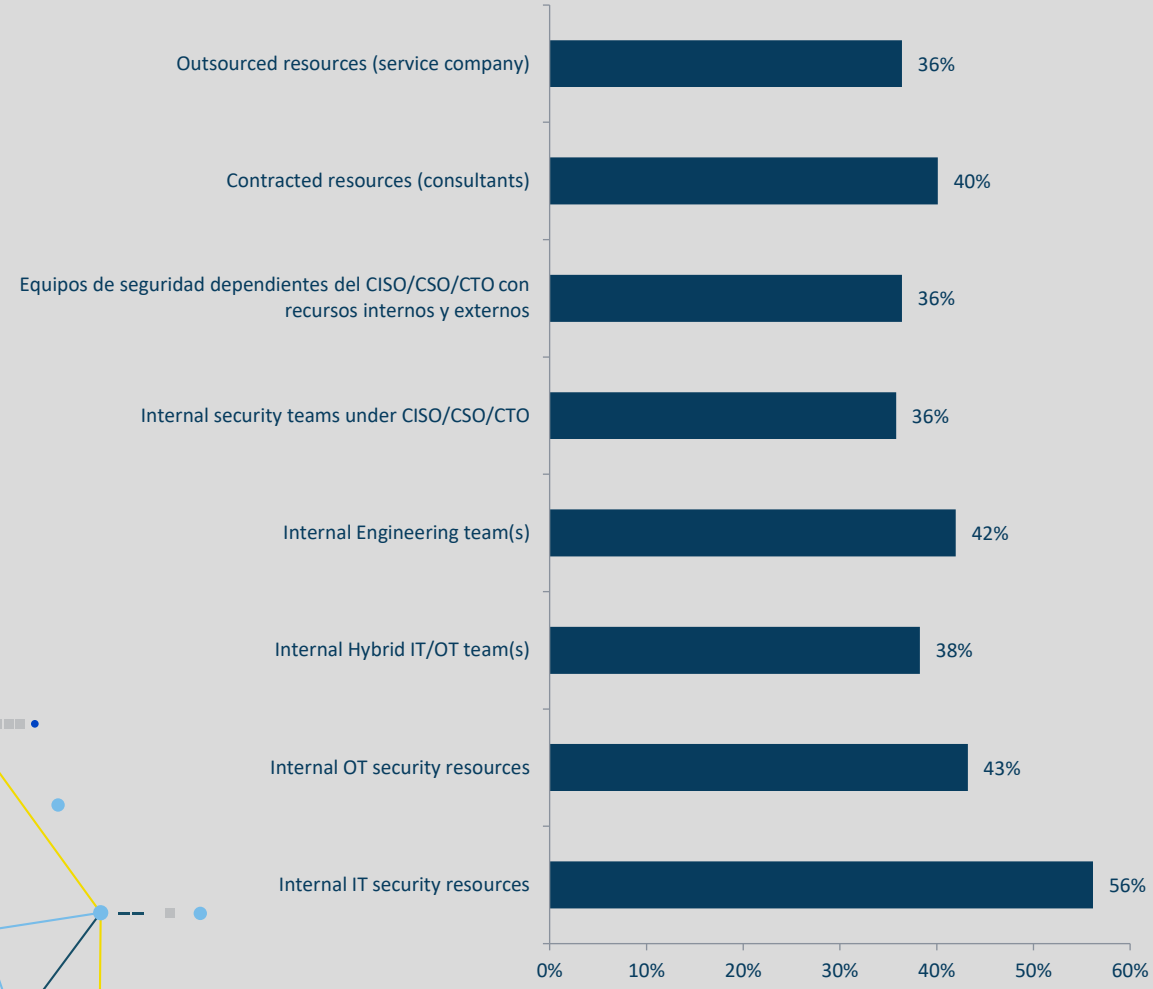
Los operadores tienen que tomar decisiones difíciles para reconfigurar sus redes, sustituir activos que funcionan (pero que han llegado al final de su vida útil) y desplegar equipos de seguridad. Todo ello con la planta parada durante días, si no semanas. Les estamos obligando a tomar la difícil decisión de NO avanzar en la ciberseguridad de sus líneas operativas e instalaciones. En muchos casos, el tiempo de parada de la planta es más caro que el propio proyecto de seguridad.

Asociémonos para que la seguridad y el mantenimiento de nuestras plantas y fábricas sean menos costoso en términos de tiempos, más razonable en términos económicos y, lo que es más importante, con mucho menos tiempo (si no cero) de inactividad.

Juntos podemos eliminar las barreras informáticas tradicionales y unirnos para proteger las infraestructuras de nuestro mundo.

Brian Brammeier,
Director General de Opscura

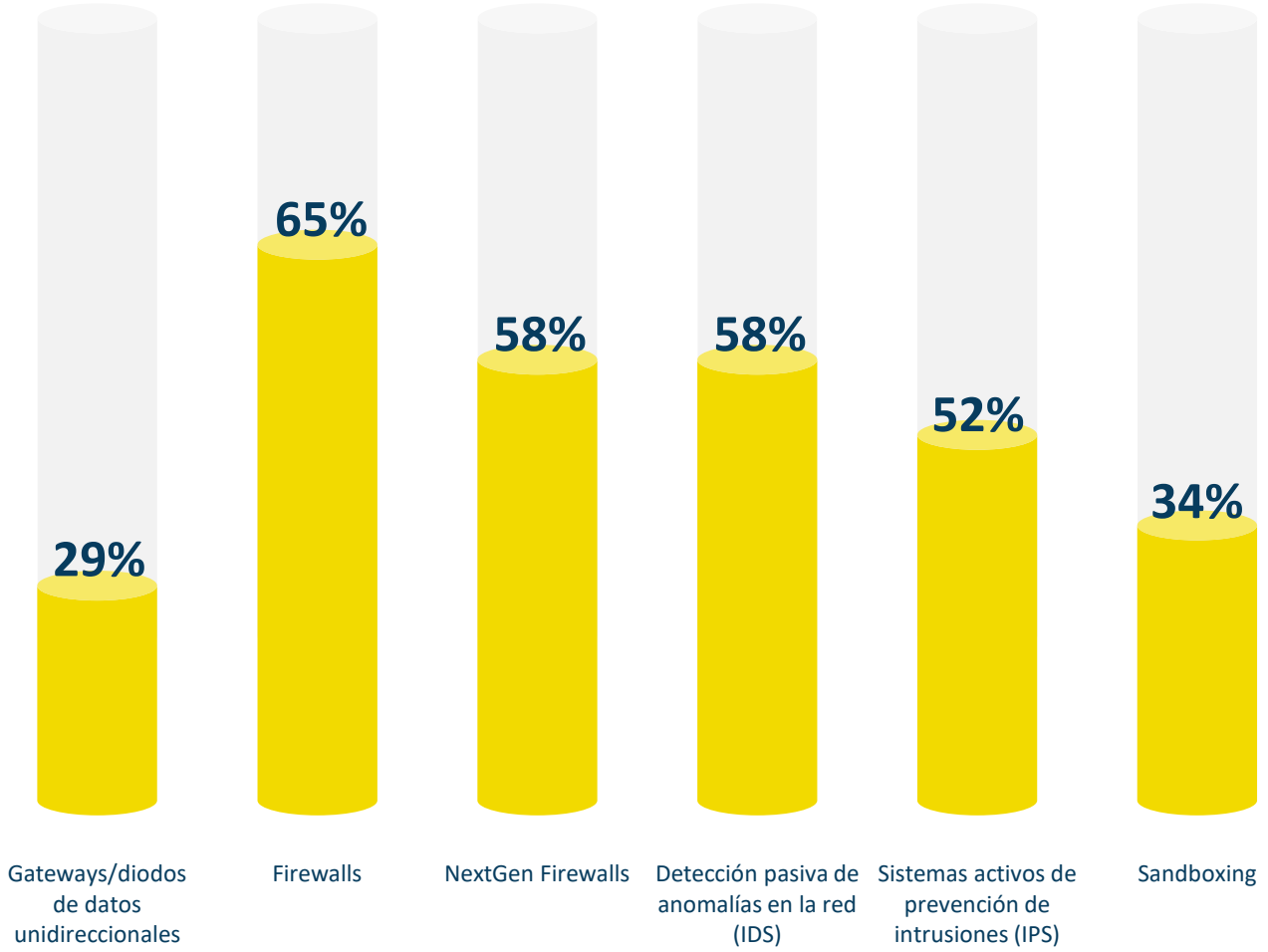
Fuentes de los servicios de seguridad de los sistemas de control utilizados por las organizaciones



Tecnologías de (CS)2 - Usuarios finales

No todas las tecnologías se adaptan a las necesidades y requisitos de todos los entornos. Dicho esto, consideramos probable que las organizaciones propietarias u operadoras de activos ICS/OT que indicaron que disponen de *detección pasiva de anomalías en la red* (58% IDS) se beneficiarían con la implementación de *sistemas activos de prevención de intrusiones (IPS)* . Los Firewalls de NextGen tienen una utilidad igualmente amplia y deberían proteger más entornos de ICS de las amenazas originadas en su empresa o en otras redes externas. *Los gateways/diodos de datos unidireccionales* se han considerado complejos y costosos debido a que se usan principalmente en los entornos de seguridad más altos (por ejemplo, las centrales nucleares), pero recientemente hemos visto que ambos factores están disminuyendo y se espera un mayor despliegue en el futuro.

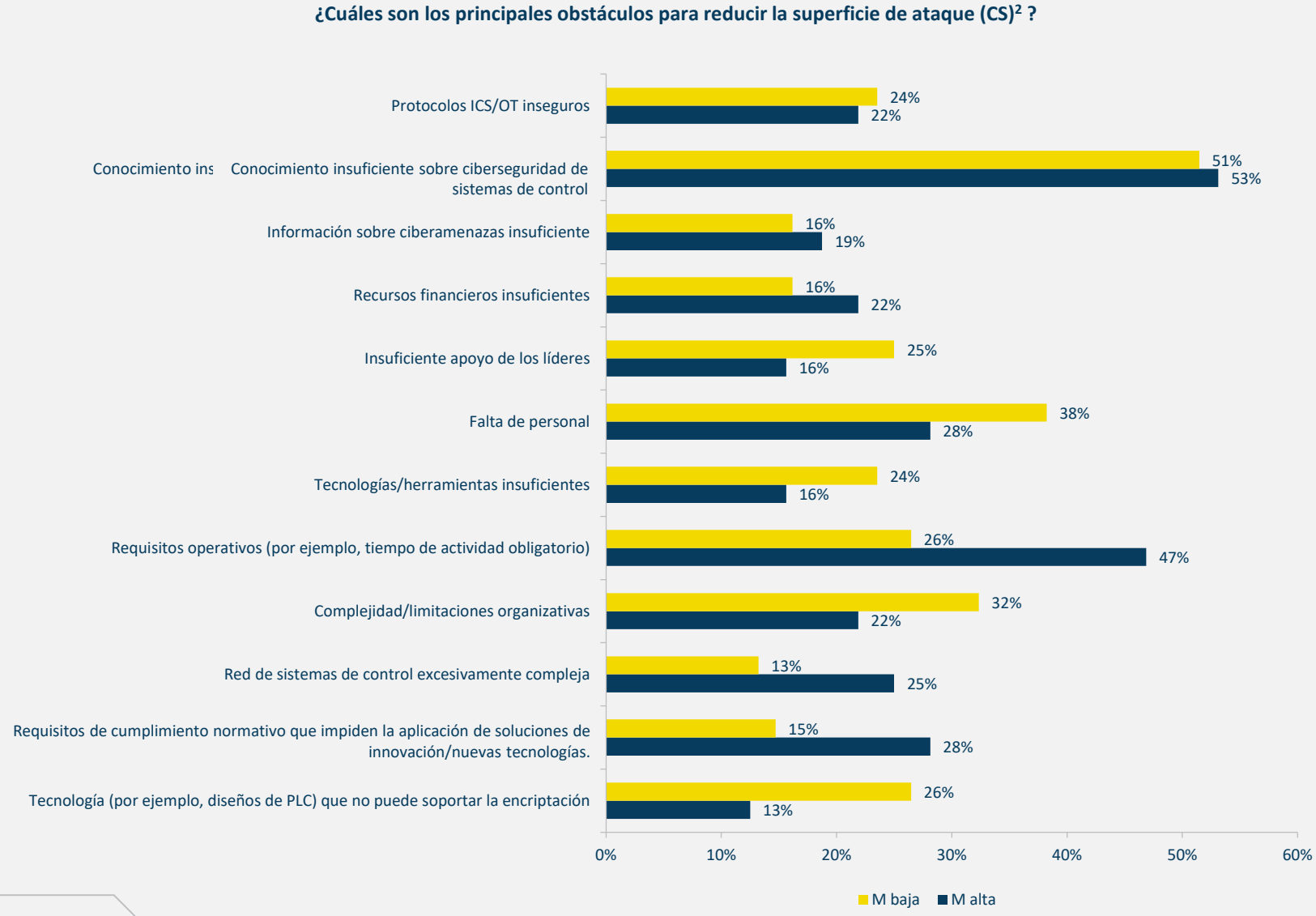
Tecnologías de seguridad utilizadas por las organizaciones para proteger los activos de los sistemas de control frente a las ciberamenazas



Obstáculos para reducir la superficie de ataque $(CS)^2$

Obstáculos de (CS)²- Nivel alto de madurez frente a Nivel bajo de madurez

Cada año comparamos las condiciones y perspectivas entre distintos grupos; aquí consideramos aquello que se entiende como los mayores obstáculos a través de la lente de la madurez relativa de los programas de ciberseguridad de los sistemas de control de las organizaciones encuestadas (M alta frente a M baja) para identificar lo que funciona, lo que no, y cómo cambian las cosas a medida que las organizaciones avanzan en su viaje para mejorar su seguridad. En la tabla anterior vemos que algunos obstáculos están ampliamente consensuados, como la *Insuficiente experiencia en ciberseguridad de los sistemas de control* (M baja 51,5%, M alta 53,1%) y los *Protocolos ICS/OT inseguros* (M baja 23,5% frente a M alta 21,9%), mientras que otros difieren ampliamente, como la *Tecnología que no admite el cifrado* (M baja 26,5% frente a M alta 12,5%) y el *Insuficiente apoyo del liderazgo* (M baja 25,0% frente a M alta 15,6%). Esto sugiere que los programas más maduros han superado algunos de los obstáculos con los que se siguen enfrentando los programas menos maduros.



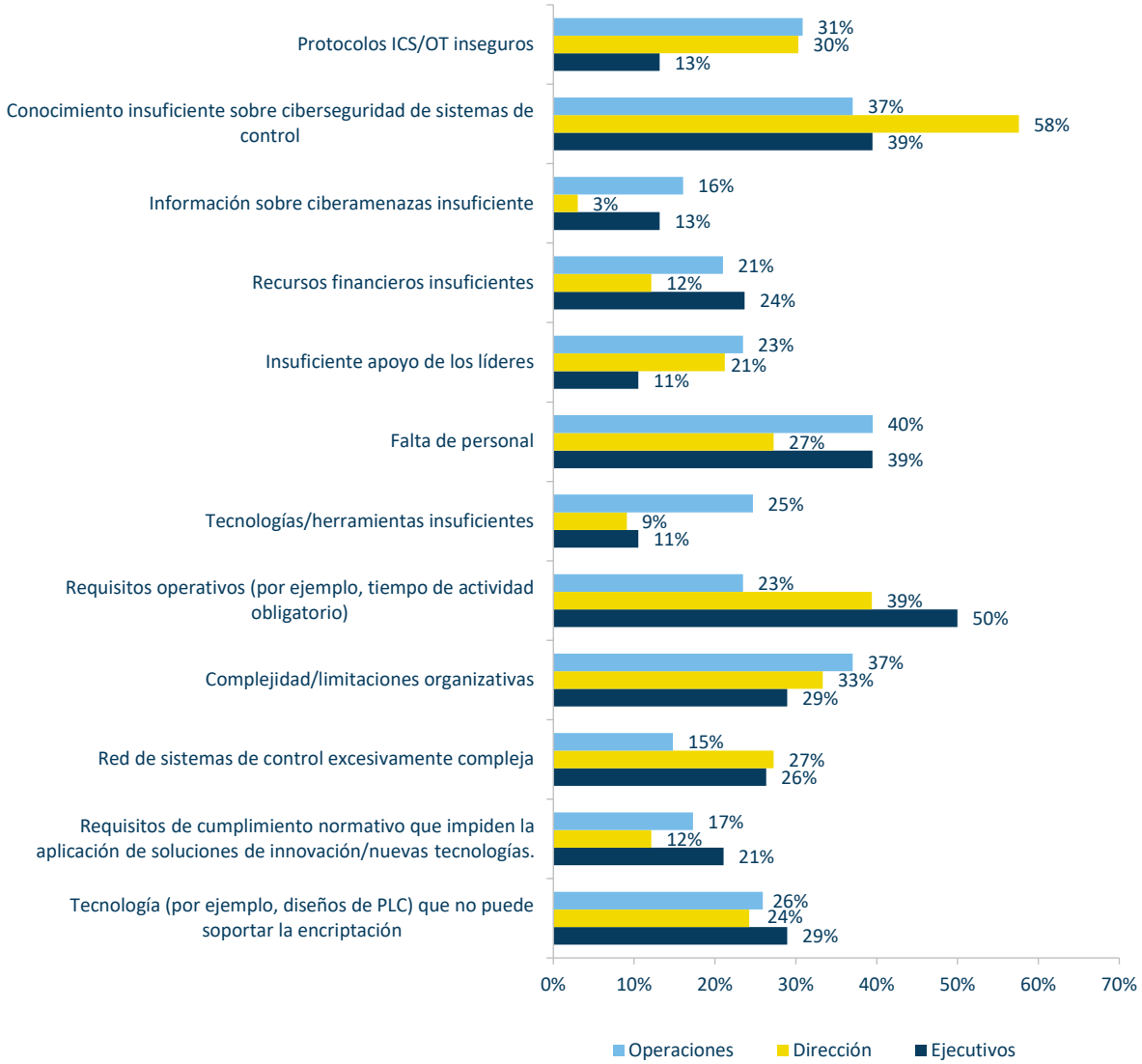
Obstáculos de (CS)² - Nivel organizativo[4]

Es muy improbable que una sola persona pueda tener tanto una visión completa como todos los detalles del entorno de un sistema de control moderno, y las diferencias en los puntos de vista de las personas conducen inevitablemente a diferencias en sus percepciones de lo que hay que hacer. Aquí vemos que el consenso de los ejecutivos de que los *requisitos operativos* (50,0%), *la falta de personal* (39,5%) y los *conocimientos técnicos insuficientes sobre (CS)²* (39,5%) son los mayores obstáculos coincide en parte con el personal de operaciones (los más altos de este grupo son la falta de personal (39,5%) y los conocimientos técnicos insuficientes sobre (CS)² (37,0%), pero los de operaciones creen que los requisitos operativos son un obstáculo mucho menor (sexto en la lista de operaciones con un 23,5%).

La dirección discrepa con frecuencia de una o ambas partes, lo que pone de relieve la importancia de conocer el rol de los usuarios finales dentro de su organización cuando les ayudamos a resolver sus problemas.

[4]El número de participantes que responden a cada pregunta de nuestras encuestas varía. A veces, esto se traduce en una representación insuficiente de un subconjunto concreto de participantes para un análisis estadístico válido. En el caso de desglosar nuestros datos por participación de los distintos niveles de sus organizaciones, recibimos muy pocos encuestados del nivel de Liderazgo como para incluirlos en algunos gráficos.

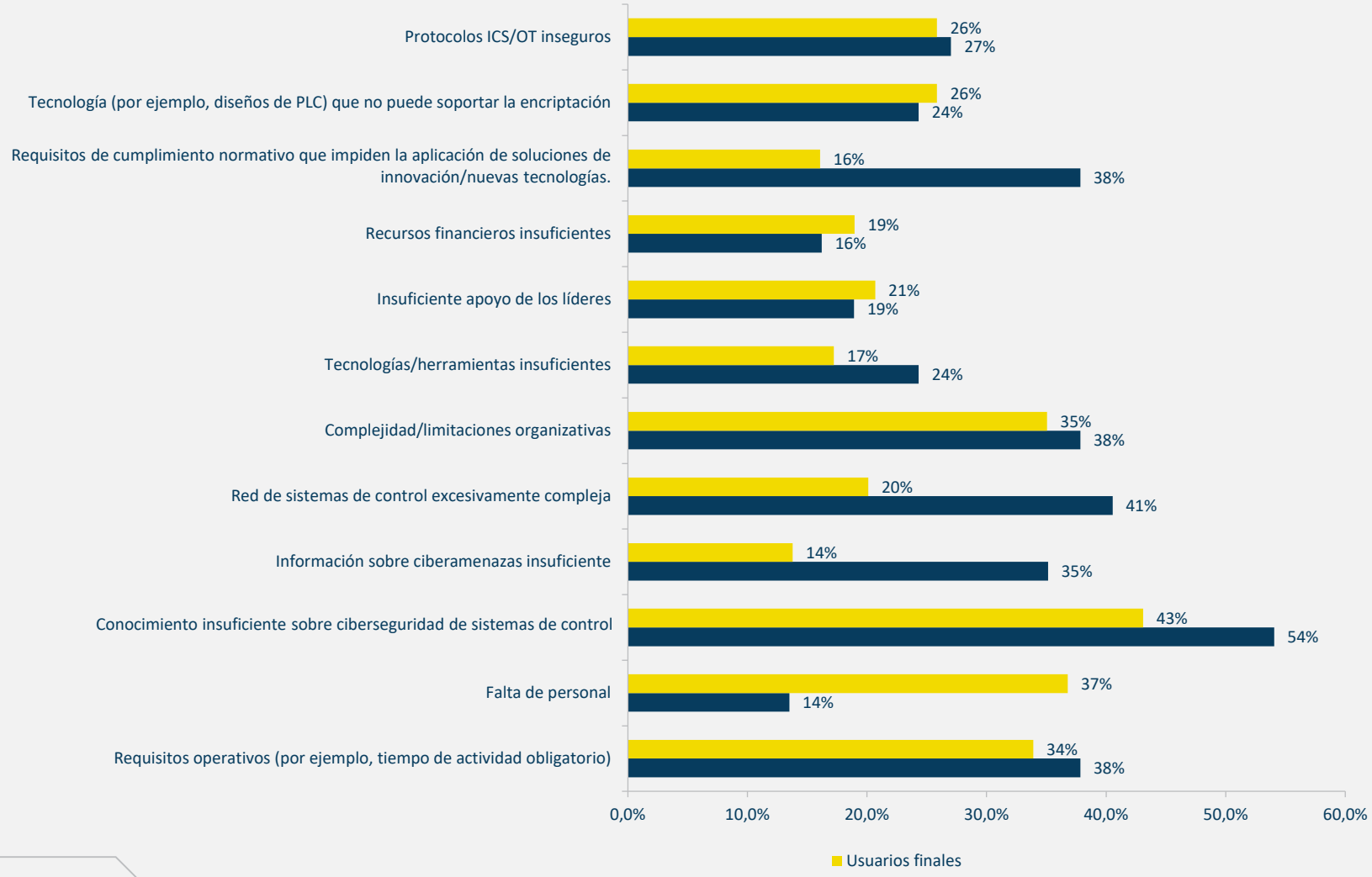
¿Cuáles son los principales obstáculos para reducir la superficie de ataque (CS)² ?



Obstáculos de (CS)² - Usuarios finales & proveedores

Nuestro equipo consideró que muchas de las diferencias en las perspectivas de los encuestados usuarios finales y proveedores son interesantes. ¿Se deriva esto de la diferencia entre la función de ser propietarios/operadores de los sistemas de control y la función de producción o supervisión de los activos del OT, de la existencia de diferentes recursos, de la variedad de responsabilidades fiscales o de una combinación de factores? Cabe destacar que los proveedores identificaron los *requisitos de cumplimiento normativo, las redes de sistemas de control excesivamente complejas* y la *insuficiente información sobre ciberamenazas* como los principales obstáculos de dos o tres veces mayor importancia que los usuarios finales. La única proporción similar de los usuarios finales es su opinión sobre la *falta de personal* (usuarios finales 36,8% frente a proveedores 13,5%). Aconsejamos a los proveedores que consideren lo que sus clientes usuarios finales identifican como los mayores obstáculos para poder ayudarlos mejor a superar esas barreras.

¿Cuáles son los principales obstáculos para reducir la superficie de ataque (CS)² ?



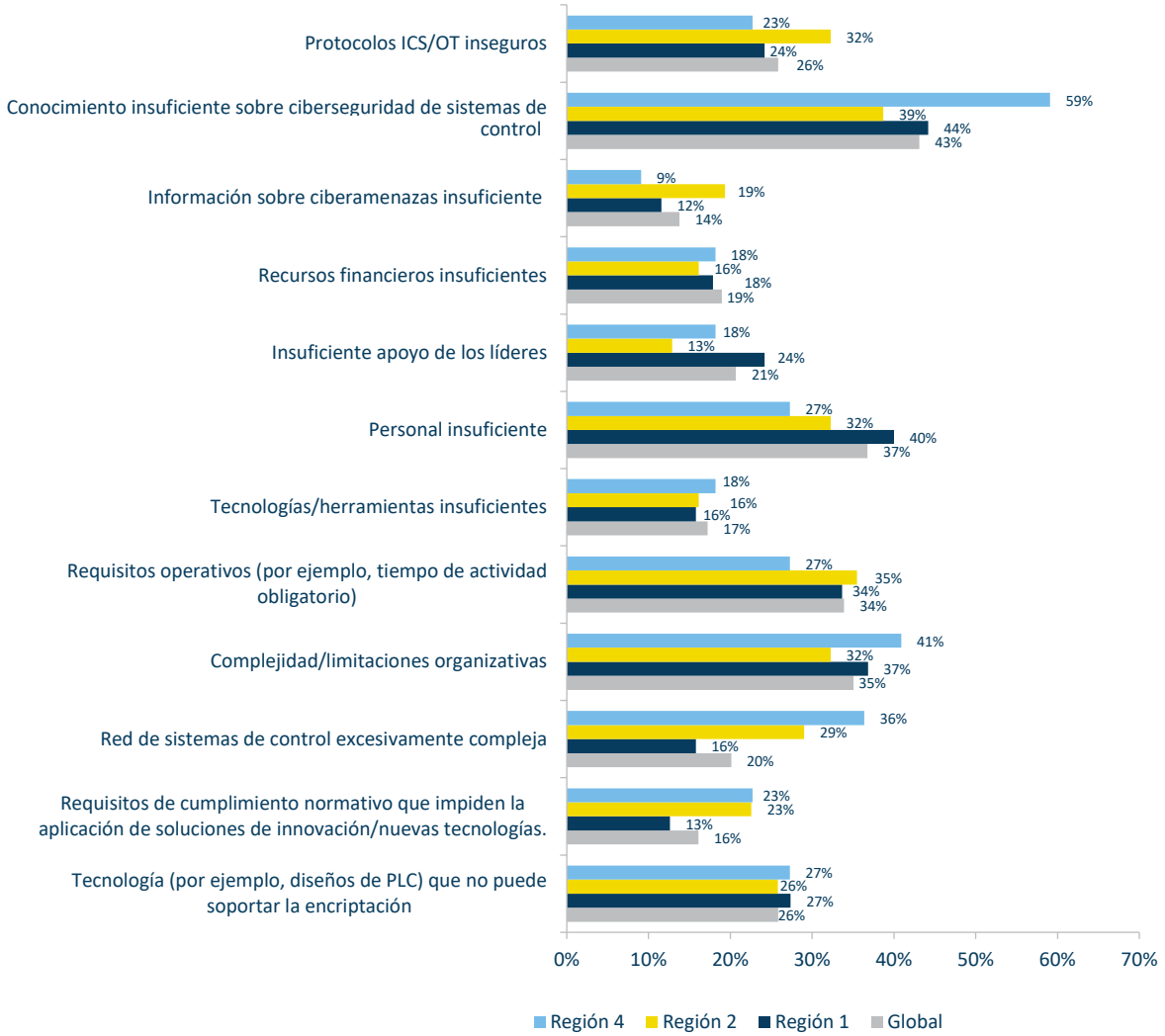
Obstáculos de (CS)² - Análisis regional [5] [6]

Para un análisis final de los obstáculos de seguridad, buscamos diferencias entre las respuestas de los encuestados de distintas regiones del mundo. Los sistemas de control en todo el mundo se basan en gran medida en tecnologías comunes, por lo que esperábamos un cierto grado de uniformidad en las respuestas, independientemente de la ubicación geográfica y, de hecho, este gráfico muestra una diferencia menor que la registrada en otros puntos del informe. Una distinción significativa es la identificación de la región 4 (APAC) de "Conocimiento insuficiente sobre ciberseguridad de sistemas de control" (59,1%), 15 puntos superior a la región 2, 1 o Global. Los encuestados de las Regiones 2 (Europa, Central, Occidental y Norte) y 4 (APAC) también están más preocupados por las *Redes de sistemas de control excesivamente complejas* que el resto del mundo (R2 29,0%, R4 36.4%, vs. Global 20.1%).

[5] Al igual que en nuestro análisis de las respuestas por nivel organizativo de los participantes, algunas regiones carecían de representación suficiente para realizar un análisis válido. Las tablas siguientes muestran únicamente las regiones con participación suficiente para incluirlas, así como la Global (todos los encuestados) a efectos comparativos.

[6] (CS)²AI se organiza en 7 regiones. 1) América del Norte; 2) Europa (Central, Occidental, del Norte y del Sur); 3) Eurasia; 4) Indo-Pacífico; 5) Oriente Medio-África del Norte; 6) África Austral; 7) América Latina-Caribe.

¿Cuáles son los principales obstáculos para reducir la superficie de ataque de (CS)² ?



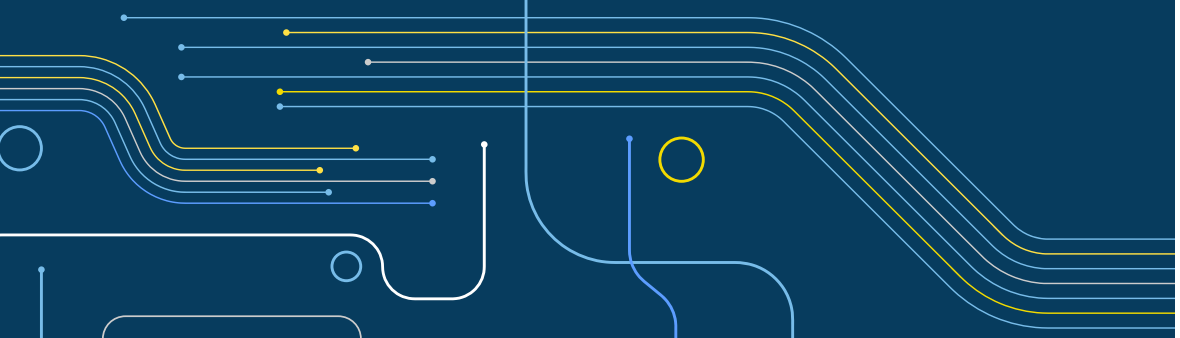
Gastos y presupuestos de $(CS)^2$

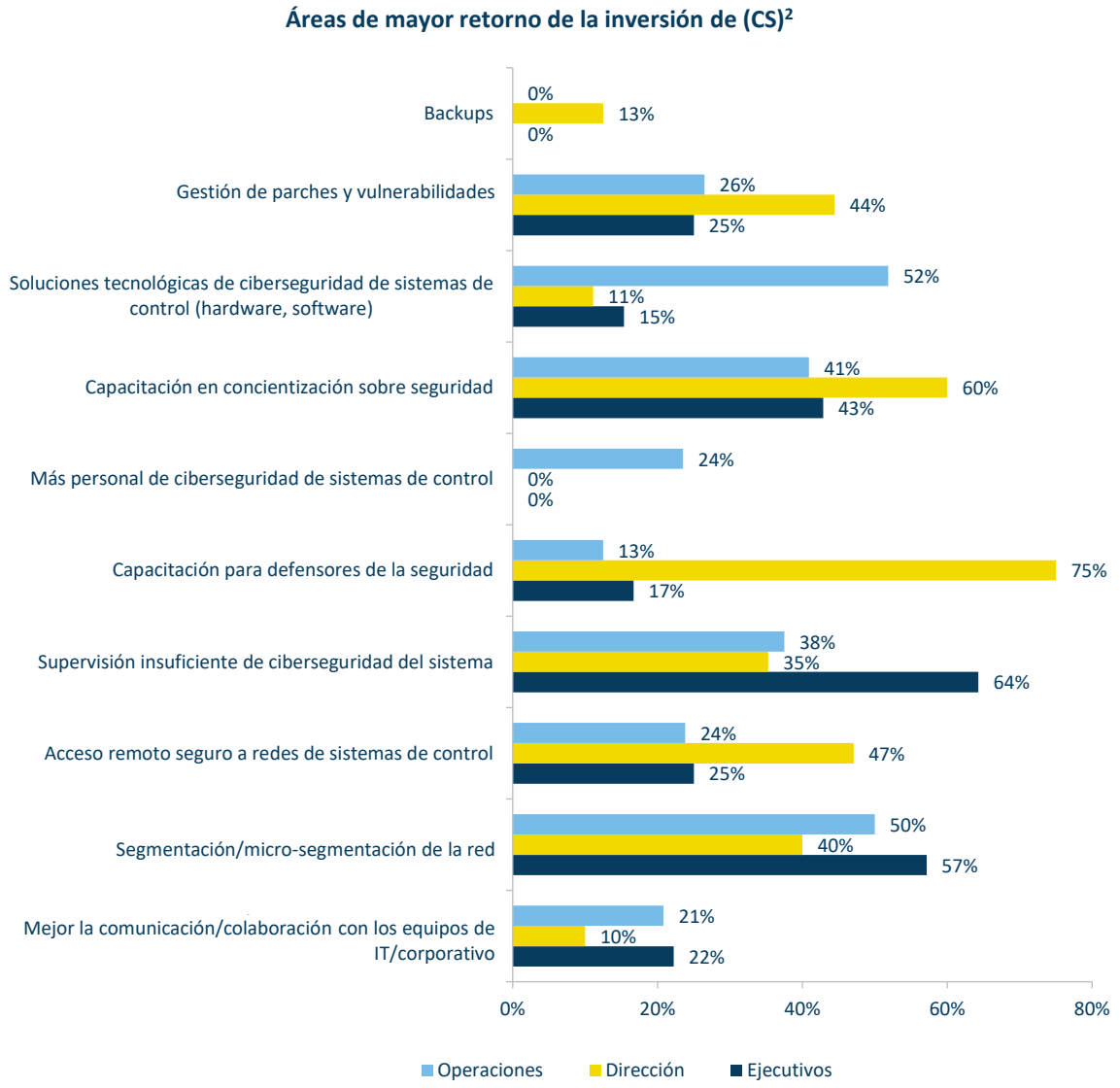
Áreas de mayor retorno de la inversión de (CS)² - Nivel organizativo[7]

El equipo de (CS)²AI y nuestros numerosos disertantes están familiarizados con las cuestiones de cómo obtener el respaldo ejecutivo para las necesidades de seguridad, en particular los proyectos de segmentación, que requieren un análisis de impacto y, en algunos casos, un importante trabajo de reestructuración de la red, por lo que puede observarse que la mayoría de los Ejecutivos participantes reconocen el ROI de esta implementación en sus organizaciones (57,1%), fundamental tanto para la seguridad como para la resiliencia. Es aún más positivo su apoyo a la supervisión de (CS)² (64,3%) luego de que las PYME sostuvieran durante años que la visibilidad es el paso 1 en cualquier programa de mejora de la seguridad. Por su parte, los encuestados del área de Dirección consideran que su mejor ROI está en la Capacitación, ya sea para la *Concientización sobre Seguridad* (60,0%) o para los *Defensores de la Seguridad* (75%).

Nuestro equipo considera importante destacar el hecho de que ninguno de los Ejecutivos o Directivos participantes considera que el *Aumento del Personal de Ciberseguridad de Sistemas de Control* sea un área de mayor retorno de la inversión (0% para ambos grupos) a pesar de que el 27-39% de ellos identifican el área *Personal insuficiente* (Ver Gráfico Obstáculos de (CS)² - Nivel Organizativo) entre sus mayores obstáculos para mejorar sus situaciones (CS)2.

[7]Se recibieron pocas respuestas de encuestados del nivel de Liderazgo como para incluirlos en este análisis.





Áreas de mayor retorno de la inversión de (CS)² - M alta vs. M baja

En comparación con sus perspectivas sobre los obstáculos de seguridad a superar, los programas de seguridad coinciden más en dónde encuentran el mayor retorno de la inversión (ROI) en sus gastos de (CS)² . Hay algunos valores atípicos, en particular el énfasis en *la Mejora de la comunicación/colaboración con los equipos de IT/corporativos* (M baja 16,7%, M alta 0%) y *Backups*[8] (M baja 0%, M alta 50%).

Una posibilidad es que los programas más maduros ya hayan integrado equipos e implementado sistemas y procedimientos sólidos de backup, por supuesto. La coincidencia de todos los grupos en que su área de mayor retorno de la inversión es la segmentación y microsegmentación de la red concuerda con los años de investigación y las recomendaciones de aplicarlo tanto para mejorar la seguridad general como para reducir el impacto de los incidentes cibernéticos.

[8]Un posible indicio de las experiencias del programa más maduras durante el reciente aumento de los ataques de ransomware.

El 50% de los encuestados cree que la segmentación de la red es el área más importante para el retorno de la inversión en programas de ciberseguridad. El pensamiento más reciente en ingeniería de redes es que lo más beneficioso en términos de límites de impacto es implementar cualquiera de los diversos enfoques de ***segmentación de la red de grado de ingeniería*** *. Los límites de impacto incluyen la interfaz IT/OT, cualquier interfaz OT/Internet y cualquier otra conexión entre redes donde el peor escenario difiere considerablemente. Los resultados de los análisis de ataques muestran que la segmentación de grado de ingeniería en dichos límites reduce la superficie de ataque de una red crítica hasta en 3 órdenes de magnitud.*

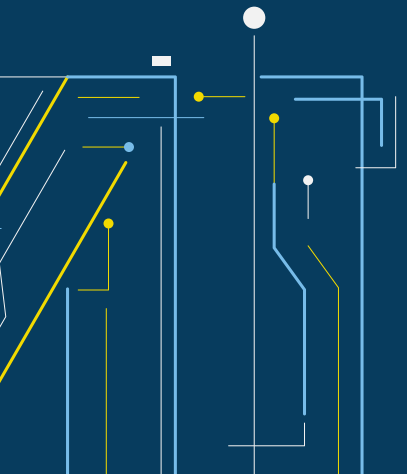
Andrew Ginter

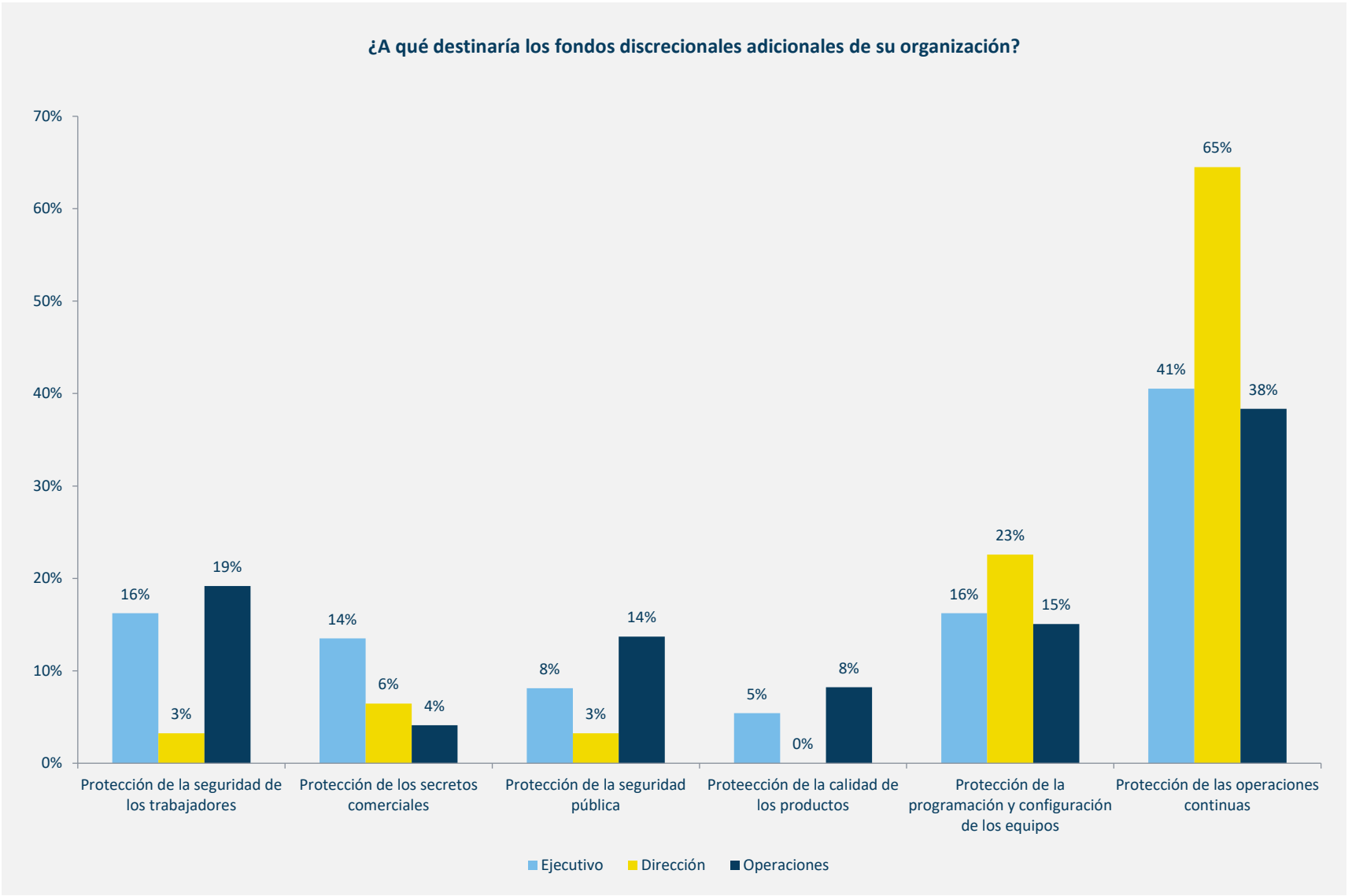
Vice Presidente de Seguridad Industrial, Waterfall Security Solutions

Áreas de mayor retorno de la inversión de (CS)2 (M alta VS M baja)

Prioridades de gasto – Nivel organizativo

Una pregunta nueva de este año; a nuestro equipo le resultaron interesantes las respuestas de los participantes. Dejando a un lado algunas coincidencias generales (como que todos los niveles identifican *la Protección de las operaciones continuas* como su principal objetivo para gastar fondos adicionales), las diferencias son notorias. Es de destacar la escasa importancia que los participantes del área de Dirección conceden a la *Protección de la Seguridad Pública* y a la *Protección de la Seguridad de los Trabajadores* (3,2% en ambas); sin que les den ninguna importancia a la *Protección de la Calidad de los Productos*. Dadas estas diferencias, se alienta a las organizaciones a promover debates sobre la alineación de las prioridades de negocios.

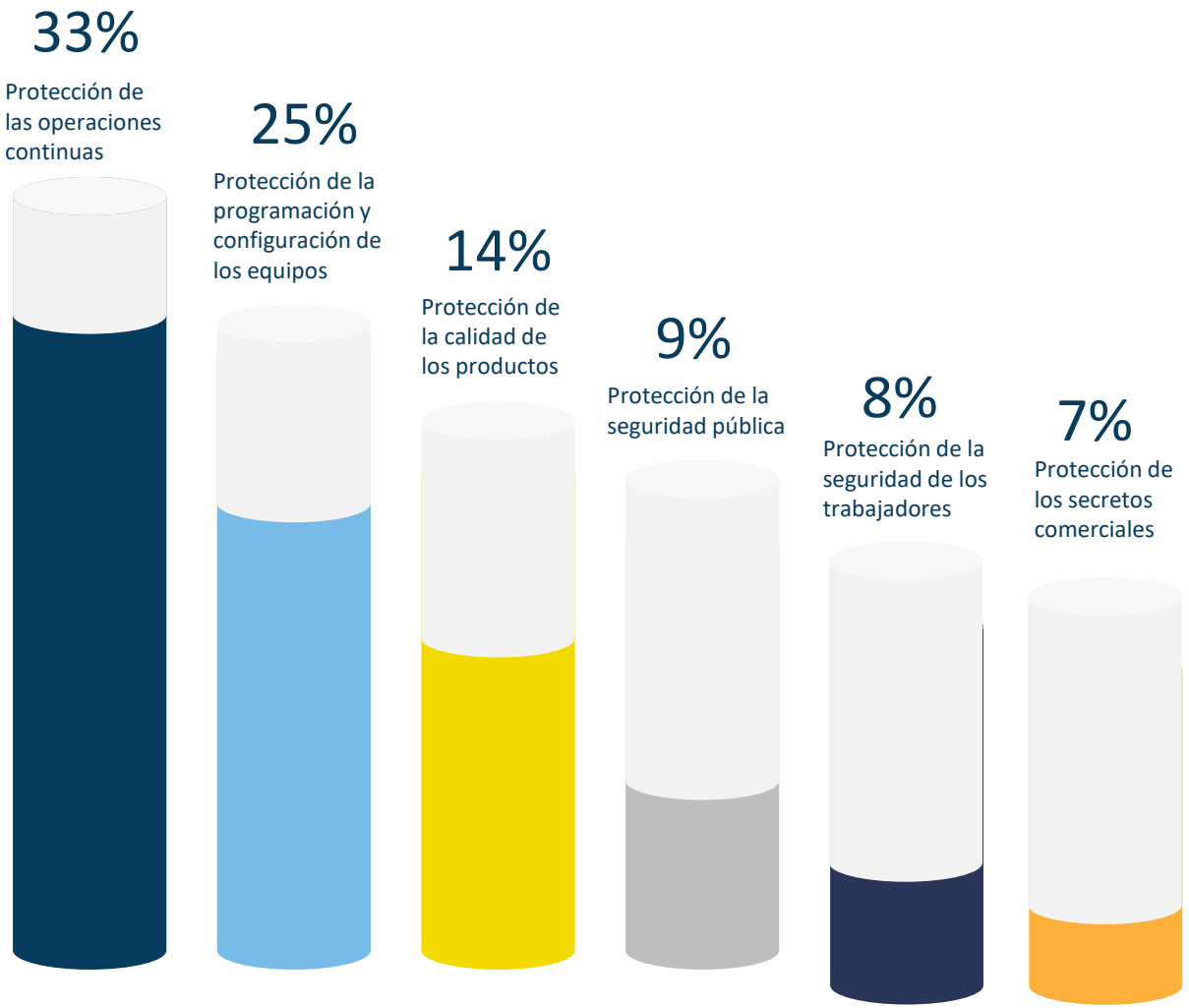




Lineamientos de los proveedores a los clientes en términos de presupuesto

Muchos propietarios/operadores de activos dependen del asesoramiento de sus proveedores confiables en materia de PYME, por lo que este año analizamos el asesoramiento de los proveedores en relación con la asignación de recursos. Comparando este gráfico con el anterior, vemos que el mayor énfasis sigue estando en la *Protección de las Operaciones Continuas*.

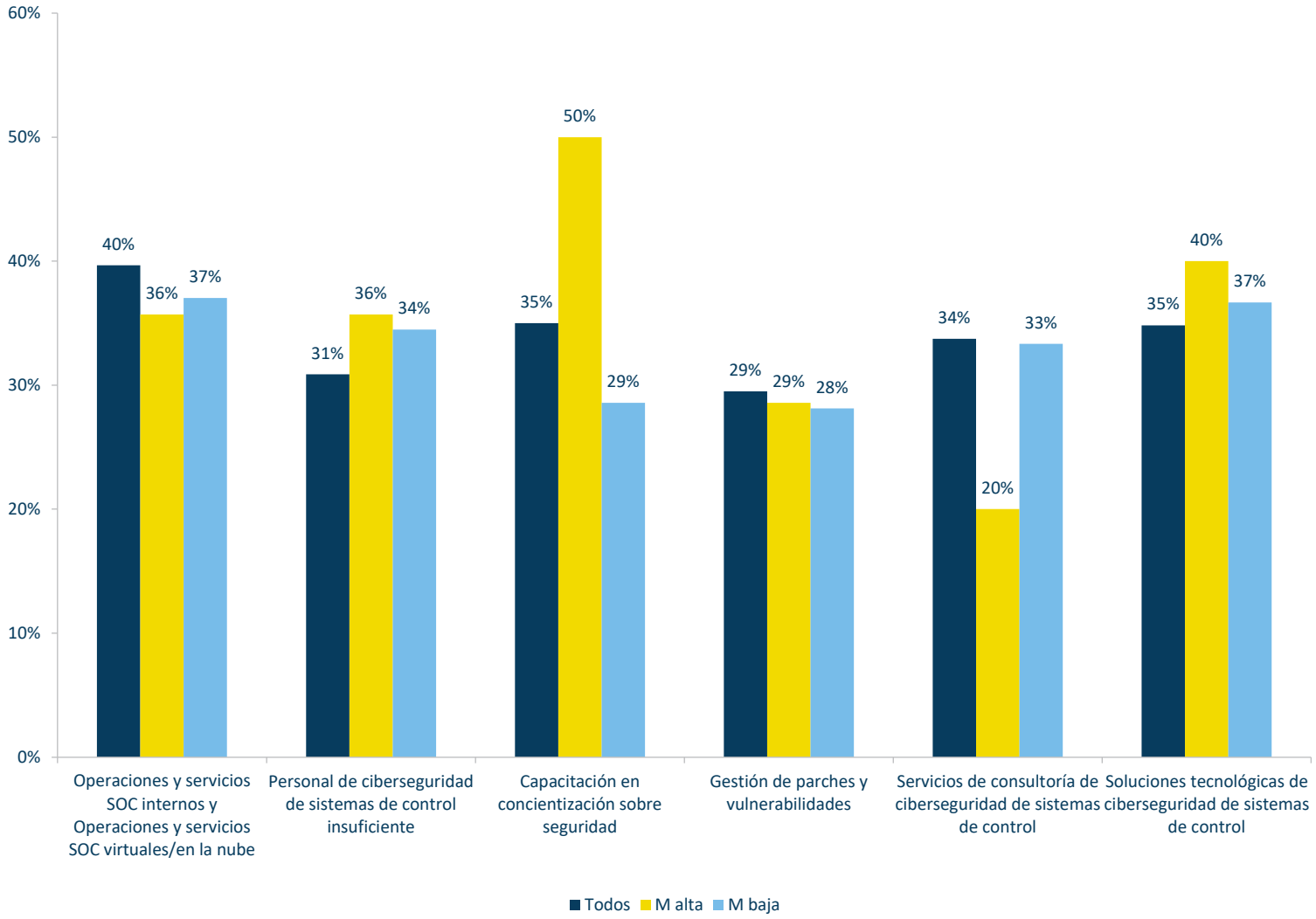
¿Adónde aconsejaría a la mayoría de sus clientes que destinaran más recursos el año próximo?



Gastos de (CS)² - M alta vs. M baja vs. Todos

Para facilitar la comparación, incluimos respuestas de todos los participantes en estos cuadros. Esto nos permite demostrar que el grupo de M alta M gasta significativamente más en *Capacitación en concienciación sobre seguridad* (50,0% M alta vs 28,6% M baja y 35,0% Todos) y cómo relativamente pocos de ellos se concentran en *Servicios de consultoría de ciberseguridad de sistemas de control* (20,0% M alta vs 33,3% M baja y 33,8% Todos).

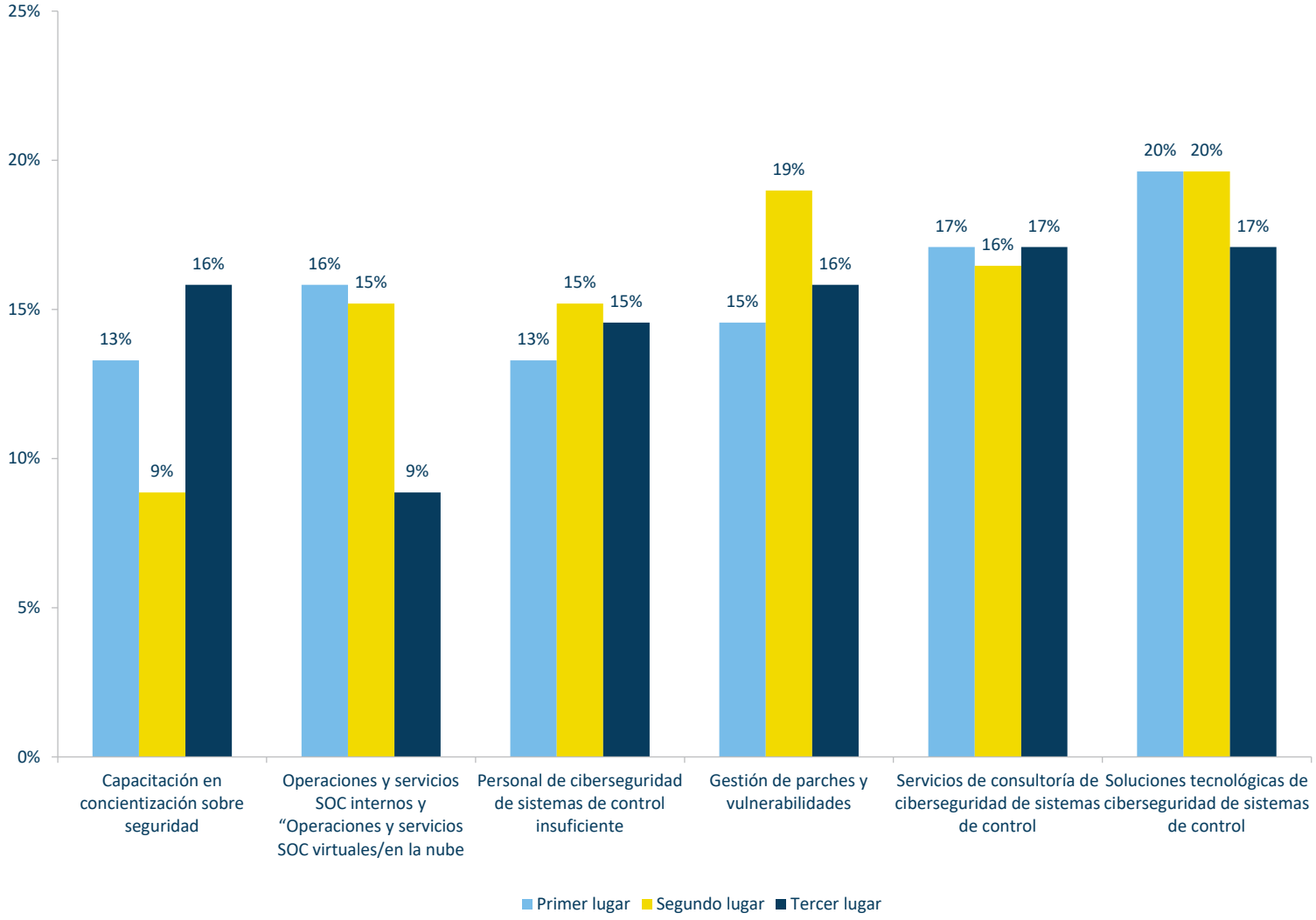
Áreas de mayor retorno de la inversión de (CS)² - M alta vs. M baja y Todos



Principales gastos de (CS)² - Usuarios finales

Para obtener otra visión sobre las prioridades presupuestarias de (CS)² más allá de los principales gastos de los grupos de M alta y M baja, también pedimos a nuestros usuarios finales que identificaran las tres áreas a las que sus organizaciones destinan sus recursos. Los *Servicios de consultoría en tecnología y seguridad* se llevan la mayor parte del presupuesto (con un total del 56,3% y el 50,6%, respectivamente). Nuestro equipo considera que es necesario investigar si la inversión relativamente baja en *Personal de Ciberseguridad de Sistemas de Control* es un factor que contribuye a que la demanda continua de trabajadores en este campo supere a la oferta.

Las tres áreas en las que las organizaciones invierten más recursos para la ciberseguridad de los sistemas de control



Cambio presupuestario de (CS)2- Estudio longitudinal

Una ligera mayoría de organizaciones sigue aumentando sus presupuestos de (CS)^2 (53%), siendo este el índice de respuesta promedio durante varios años (47% 2022, 52% 2020). Se observa un aumento constante en el grupo de crecimiento lento, aquellos con incrementos presupuestarios de (CS)^2 inferiores al 30%, con un incremento de 20% de los encuestados en 2020 a 34% de este año. El grupo de mayor crecimiento, aquellos con incrementos superiores al 30%, se redujo del 31% de los encuestados en 2020 al 19% actual. Los miembros de nuestro equipo de estudio señalaron ciertas ralentizaciones en el sector de los vendedores/proveedores de soluciones de (CS)^2 , posiblemente en respuesta al aumento de la competencia, o a la superación del apetito de mercado.

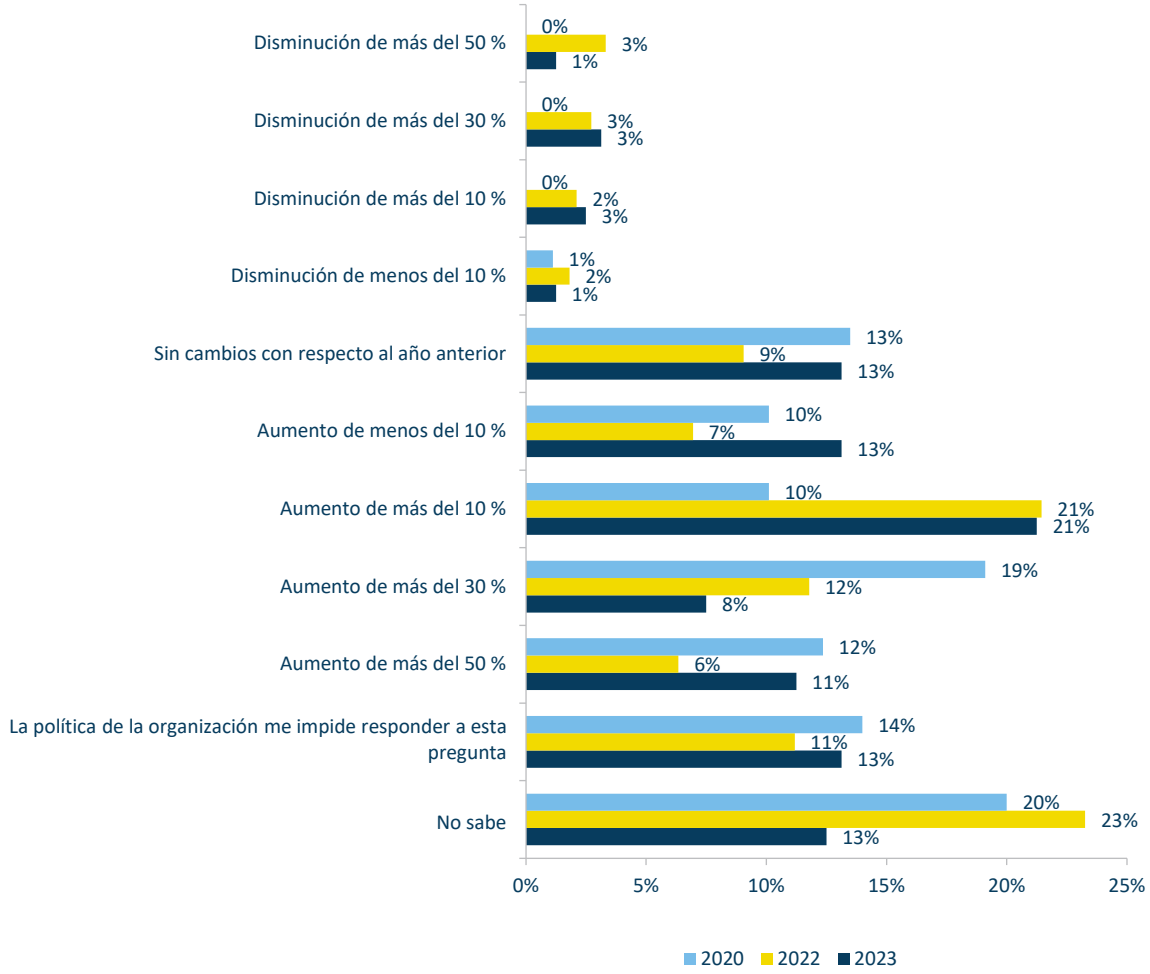
El compromiso continuado de aumentar el gasto interanual muestra que las organizaciones están comprendiendo mejor el panorama de amenazas en el que operan y cierto grado de exposición al que se enfrentan. Las noticias acerca de los recientes incidentes cibernéticos de (CS) aumentaron la concienciación sobre los riesgos cibernéticos actuales y las medidas necesarias para evitar que se produzca un acontecimiento similar.

Brad Raiford

Director, Servicios cibernéticos nacionales de IoT y OT

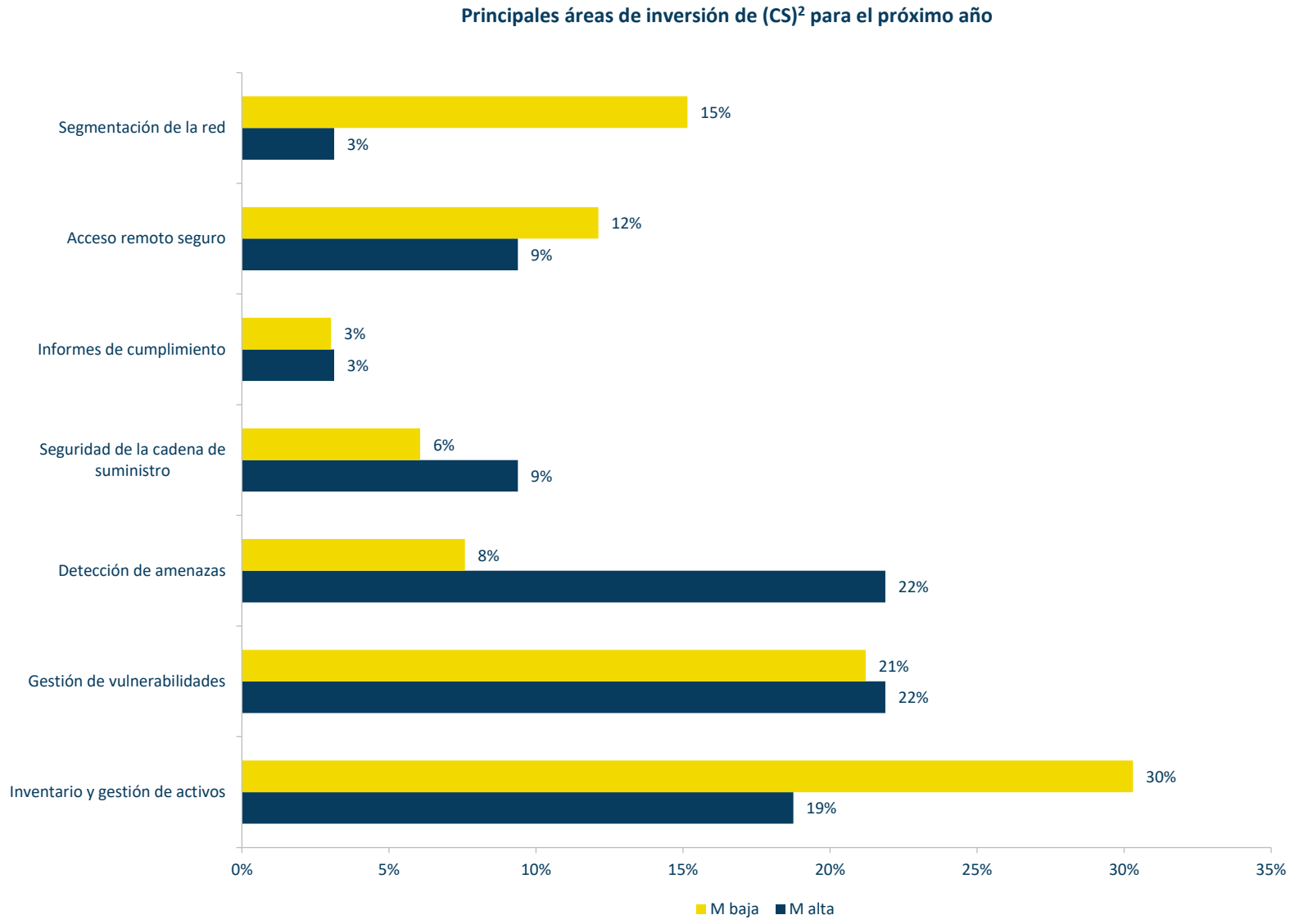
KPMG en los Estados Unidos

Estimaciones de cómo se compara el presupuesto de seguridad de sistemas de controles organizativos de este año con el del año anterior.



Inversiones previstas de (CS)² - M alta vs. M baja

Con el fuerte apoyo al valor de la *segmentación de la red* (ver los gráficos sobre área de mayor retorno de la inversión) consideramos notable que pocas organizaciones planeen centrar su próximo gasto en seguridad en esa área. La explicación puede ser que las organizaciones de M alta ya hayan segmentado significativamente su red, por lo que ahora gastan mucho menos (3%) que las de M baja (15%). Un factor similar puede estar detrás de la diferencia en sus gastos previstos en *Inventario y Gestión de Activos* y *Detección de Amenazas.*

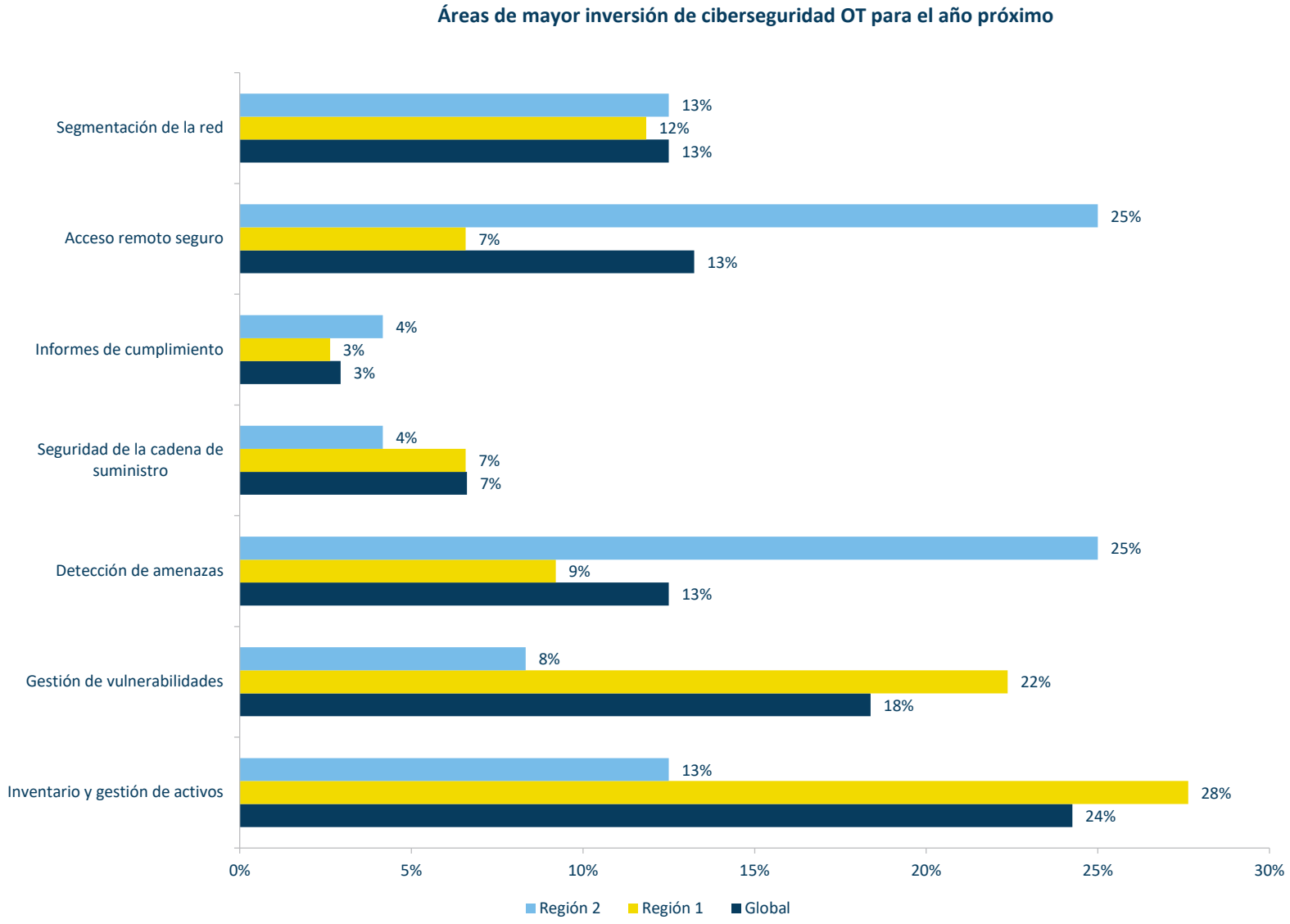


Inversiones previstas de (CS)² - Regiones

Las respuestas a esta pregunta fueron insuficientes en las Regiones 3-7[9] para ser incluidas, pero los planes son muy diferentes entre los encuestados de las Regiones 1 y 2. Los participantes de la Región 2 se concentran actualmente en el *Acceso Remoto Seguro* y la *Detección de amenazas*[10] (25% en ambos), mientras que sus colegas norteamericanos parecen considerar más urgentes la *Gestión de Vulnerabilidades* y el *Inventario y Gestión de Activos* (18,4% y 24,3%, respectivamente). Una posibilidad planteada en nuestra revisión es que las organizaciones de la Región 2 hayan resuelto estos problemas de *gestión* en cierta medida no lograda en la Región 1.

(CS)²AI se organiza en 7 regiones. 1) América del Norte; 2) Europa (Central, Occidental, del Norte y del Sur); 3) Eurasia; 4) Indo-Pacífico; 5) Oriente Medio-África del Norte; 6) África Austral; 7) América Latina-Caribe.

[10]Un posible factor es que los organismos reguladores de Europa (tanto nacionales como internacionales) hayan avanzado/sancionado leyes que exige la detección de amenazas en múltiples industrias y sectores de infraestructura.



Presupuestos de (CS)² - M alta vs. M baja

Hemos visto que las organizaciones de M alta tienden a mostrar presupuestos más altos en Ciberseguridad de sistemas de control. Una teoría es que las organizaciones más grandes (es decir, las que cuentan con más recursos) suelen estar más avanzadas en su camino hacia la seguridad que las más pequeñas. Si bien reconocemos que los desafíos financieros a los que se enfrentan las empresas más pequeñas que asignan recursos suficientes para mejorar su seguridad son a menudo mayores, también queremos señalar que esas mismas limitaciones fiscales pueden significar que tengan menos capacidad para hacer frente y recuperarse de los efectos de los ciberincidentes perjudiciales. La amenaza de un ciberataque que paralice sus operaciones durante un periodo prolongado puede ser más perjudicial para ellos, y sus procesos de gestión de riesgos deben tenerlo en cuenta.

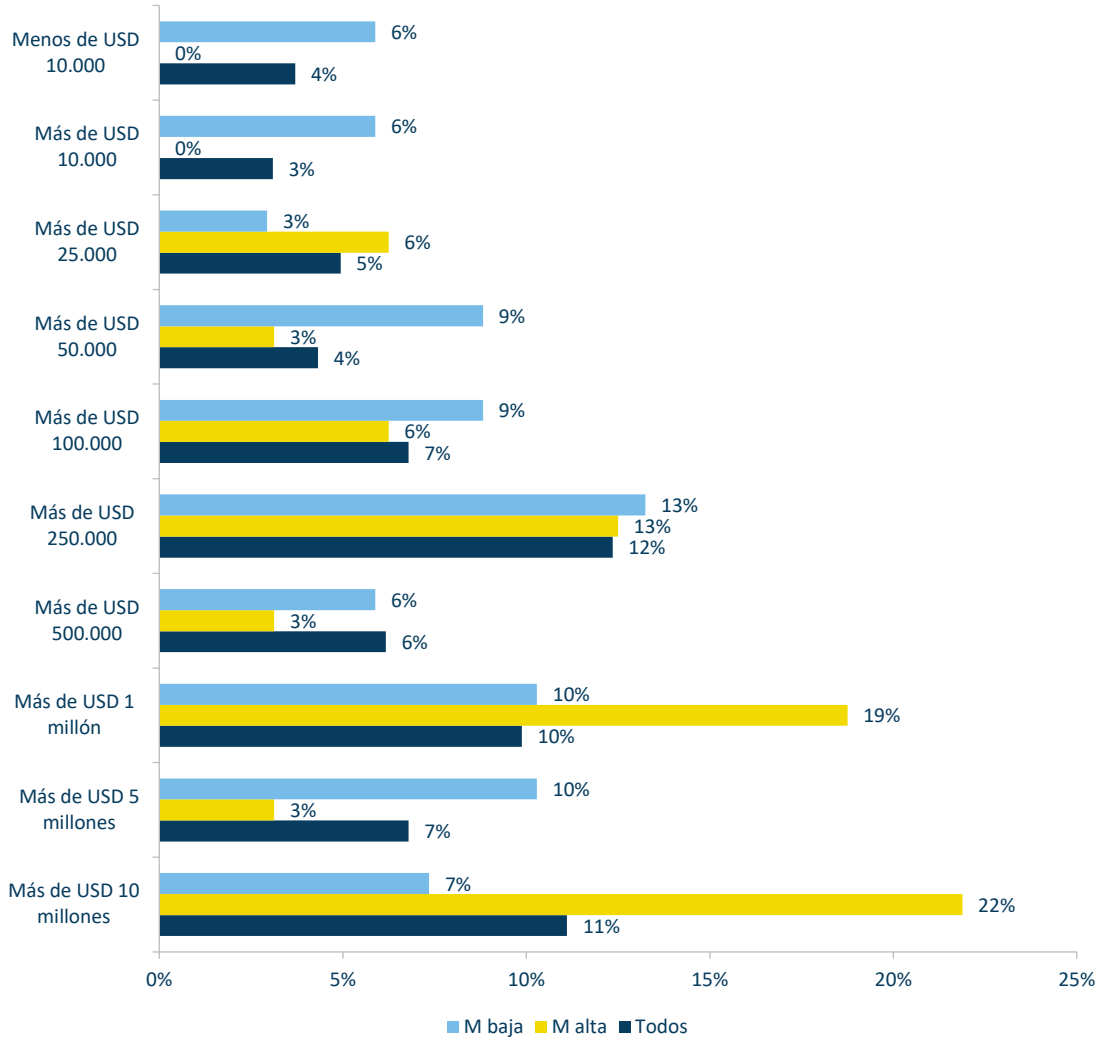
Esta correlación también pone de manifiesto la necesidad de que el área de (CS)² preste mejores servicios a los clientes más pequeños con soluciones y servicios que se ajusten a sus presupuestos.

Rod Locke

Director de Gestión de Productos

Fortinet

Total de estimaciones presupuestarias de (CS)² por organizaciones para el ejercicio anterior

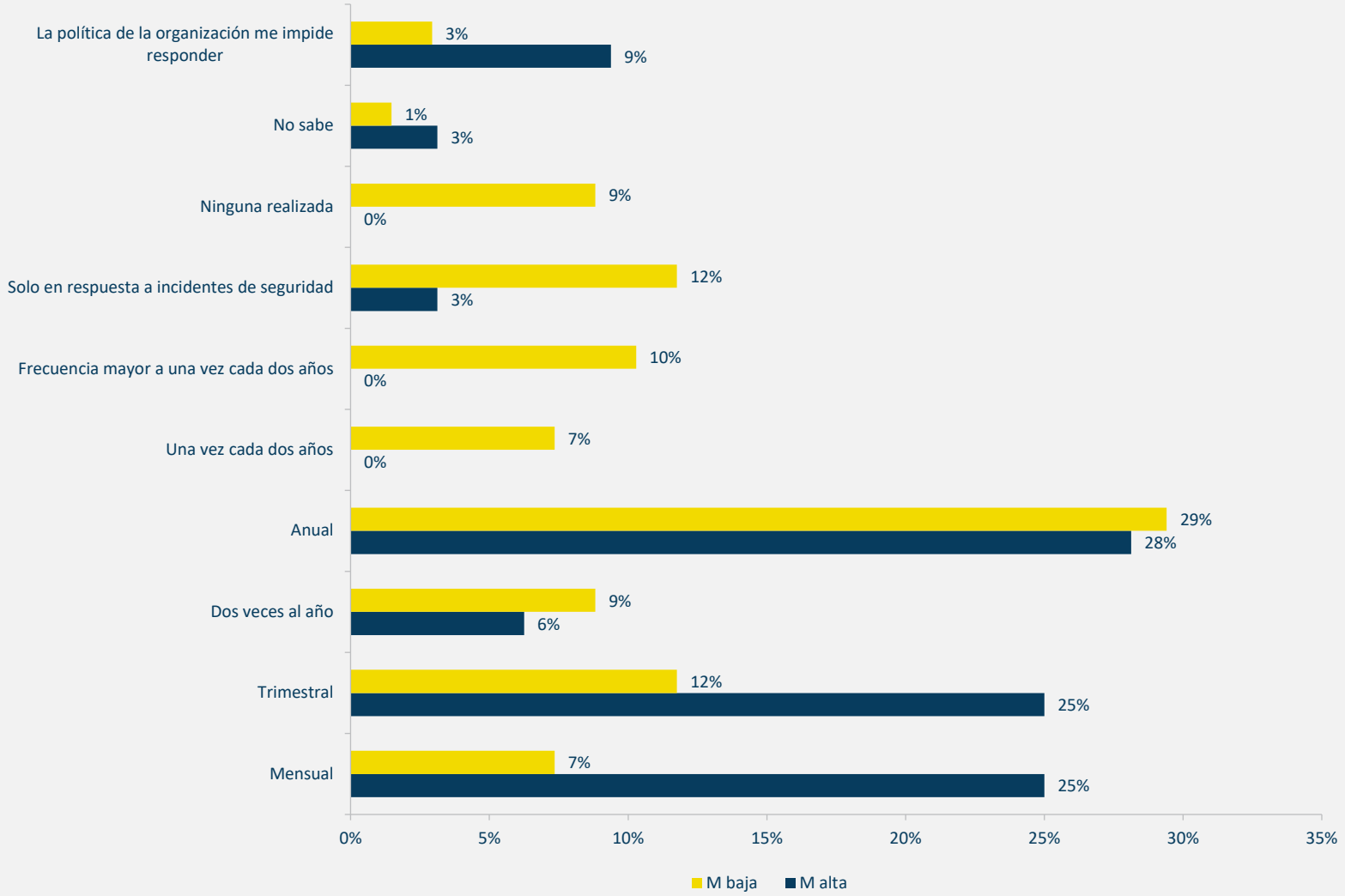


Evaluaciones de $(CS)^2$

Frecuencia de las evaluaciones de (CS)² - M alta vs. M baja

Una de las diferencias más claras entre los programas de distintos niveles de madurez es la frecuencia de las evaluaciones de ciberseguridad de sus sistemas de control. La mitad de los programas de M alta las realizan al menos trimestralmente, mientras que más de la mitad de los programas de M baja solo las realizan anualmente o con una frecuencia mayor. El hecho de que el 9% de los programas de M baja no realicen o no hayan realizado evaluaciones de seguridad habla por sí mismo.

Frecuencia de las evaluaciones de (CS)² por parte de las organizaciones (M baja vs. M alta)



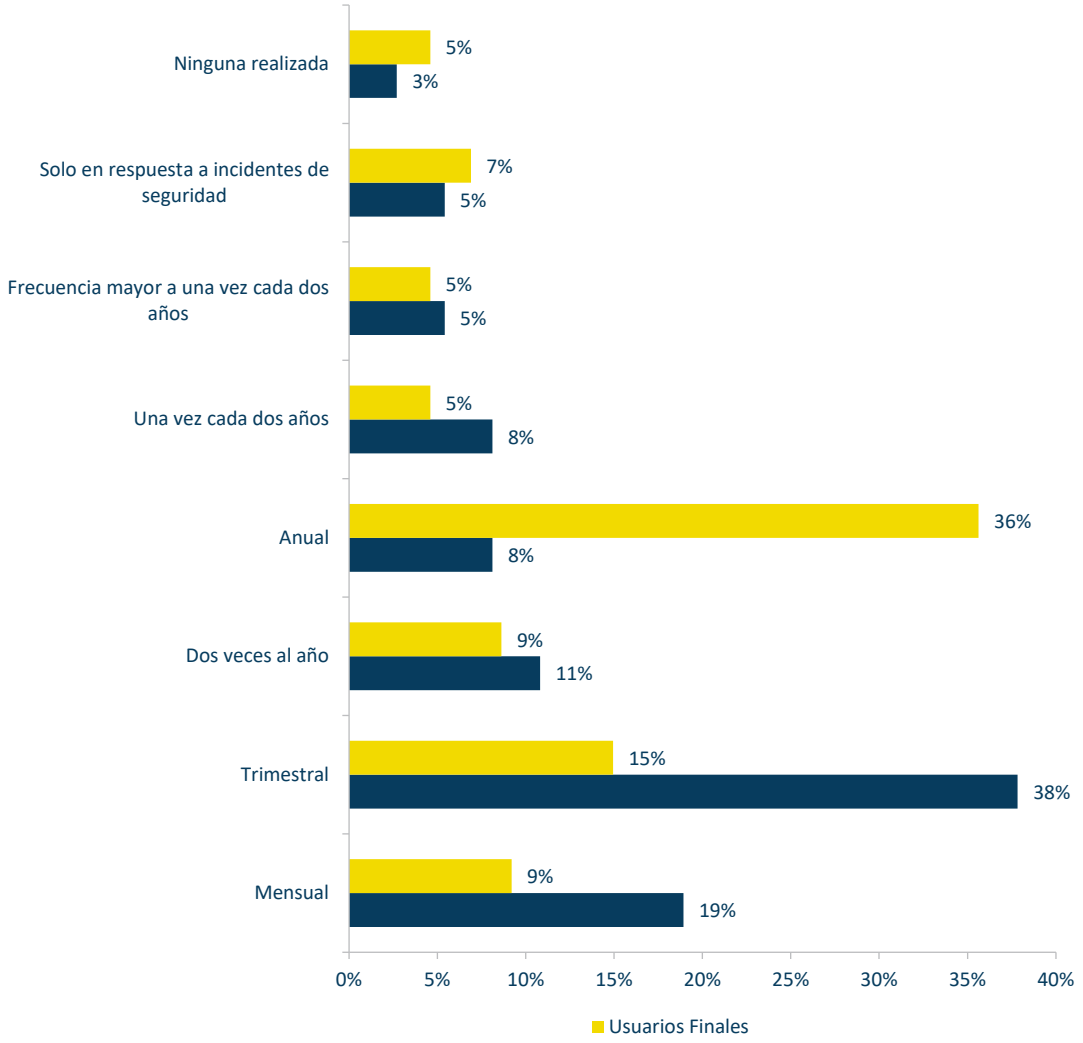
Frecuencia de las evaluaciones de (CS)² - Usuarios finales y proveedores

La responsabilidad de los proveedores en materia de seguridad es distinta de la de los usuarios finales, ya que no solo deben protegerse a sí mismos, sino también a sus clientes, que a menudo dan acceso privilegiado para la supervisión, el mantenimiento y las actualizaciones en curso. A nuestro equipo le alegró ver que los proveedores realizan evaluaciones de (CS)² con frecuencia, ya que más de dos tercios (67,6%) las realizan al menos *dos* veces al año. Su posición en las cadenas de suministro de los usuarios finales los convierte en un objetivo muy valioso para los atacantes[11]. El hecho de que las organizaciones de usuarios finales lo hagan con menos frecuencia, ya que el grupo más numeroso sólo *realiza una evaluación anual* (35,6%), es menos alentador.

Tecnología, personal privilegiado, métodos y capacidades de ataque. Los cambios se producen en todas estas áreas continuamente e, incluso con IPS/IDS (Intrusion Prevention/Detection Systems) algunas víctimas sólo descubren que los atacantes han accedido a sus redes durante la actividad de evaluación. Las evaluaciones más frecuentes pueden reducir en gran medida estos tiempos y, por los tanto, los posibles daños de todo tipo. Recomendamos a todas las organizaciones, tanto a los usuarios finales como a los proveedores, que evalúen sus redes y activos de (CS)² al menos trimestralmente.

[11]Ver cualquiera de los diversos artículos que informan sobre los ataques a la cadena de suministro de Solar Winds en 2021.

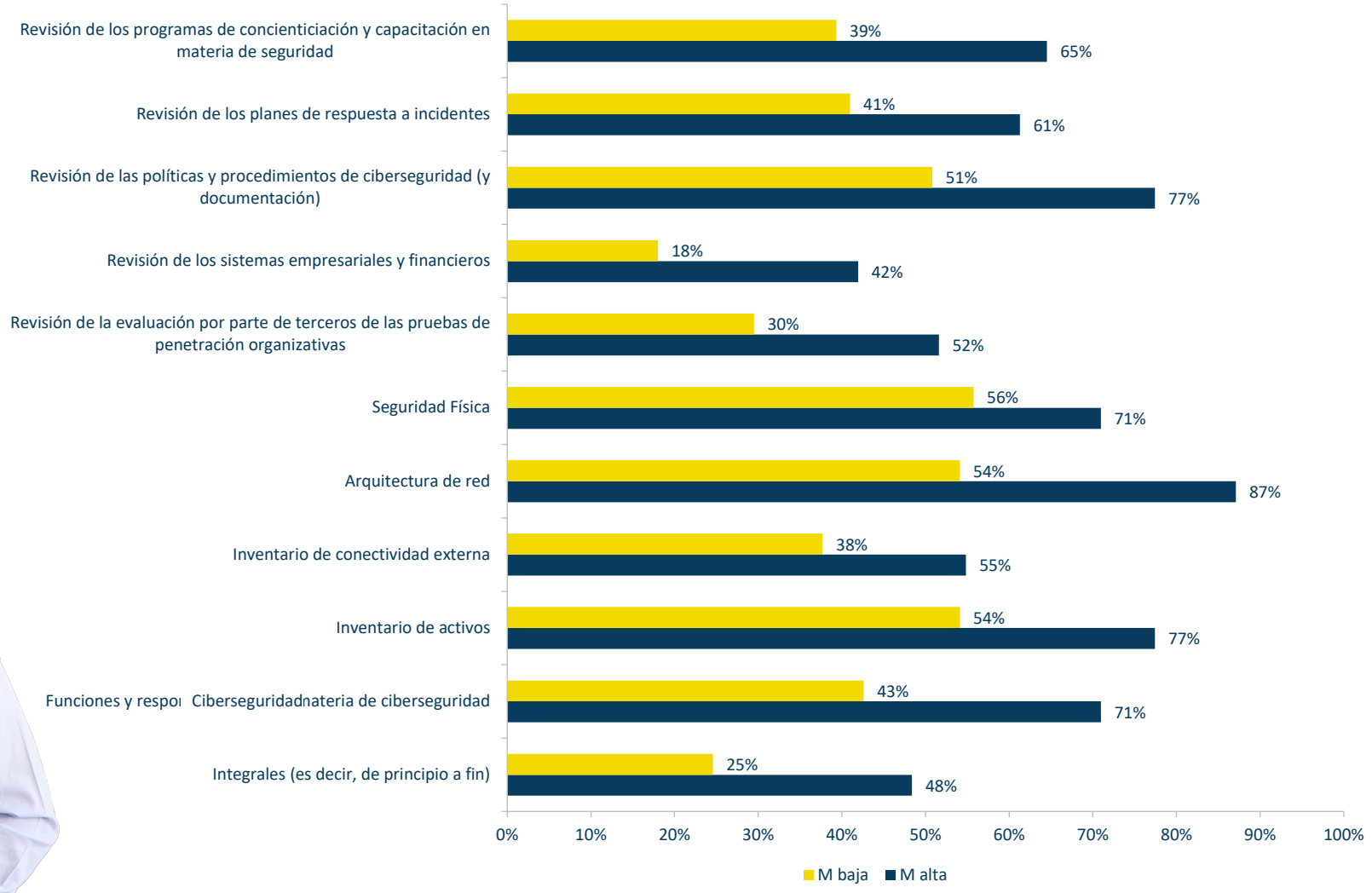
Frecuencia de las evaluaciones de (CS)² por parte de las organizaciones



Componentes sujetos a evaluación de (CS)² M alta vs. M baja

No menos importante que la frecuencia de las evaluaciones de seguridad es su nivel de detalle y, como indica esta tabla, los programas de M alta realizan evaluaciones más completas que los de M baja en todas las métricas que utilizamos, al menos en un 50% de casi todas las categorías.

Componentes sujetos a evaluación de (CS)² por parte de las organizaciones

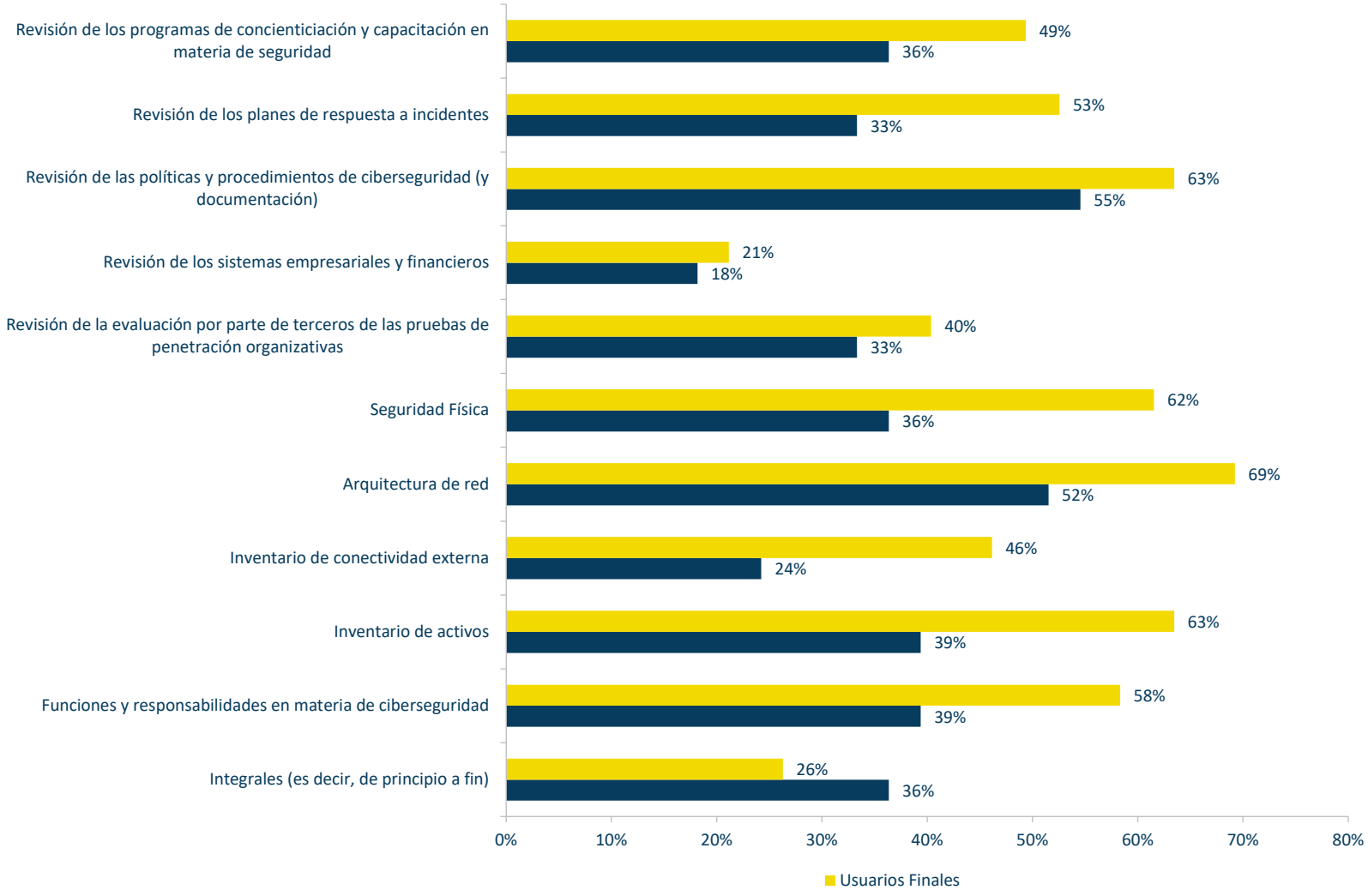


Componentes sujetos a evaluación de (CS)² - Usuarios finales y proveedores

Una observación interesante es que los usuarios finales parecen llevar a cabo todas estas verificaciones de seguridad más que los proveedores, excepto las *evaluaciones* integrales (usuarios finales 26% vs. proveedores 36%). Esto sugiere que las evaluaciones de los usuarios finales, aunque incluyen múltiples actividades importantes (Usuarios finales: *Seguridad física* 62%, *Arquitectura de red* 69%, *Inventario de activos* 63%, etc.) suelen ser menos completas que las de los proveedores o clientes de los proveedores. Es posible que los usuarios finales carezcan de la visibilidad de extremo a extremo necesaria en este caso. También es importante tener en cuenta que los proveedores suelen estar en el medio del proceso y deben considerar la seguridad de su propia cadena de suministro y la seguridad de las aplicaciones, así como lo que proporcionan a sus clientes.

Cada uno de los componentes enumerados en este cuadro aborda puntos críticos para impedir que los atacantes avancen en su cadena de delito (o para detectarlos cuando actúen). Recomendamos desarrollar planes que incluyan todos estos componentes, cada uno con ciclos definidos de evaluación y remediación.

Componentes sujetos a evaluación de (CS)² por parte de las organizaciones



Respuestas de la evaluación de $(CS)^2$ - M alta vs. M baja

Para completar los factores de evaluación de la organización $(CS)^2$ investigamos qué hacen después de sus análisis. Una vez más, vemos que los programas de M alta siguen las conclusiones de la evaluación con más frecuencia que los programas de M baja en cada métrica. Se destacan especialmente sus acciones para *Desarrollar e implementar*.

Los *Planes de remediación* (41,0% M baja vs. 67,7% M alta) y *Reemplazo de hardware, software, dispositivos, etc. de sistemas de control vulnerables*. (29,5% vs. 61,3%).

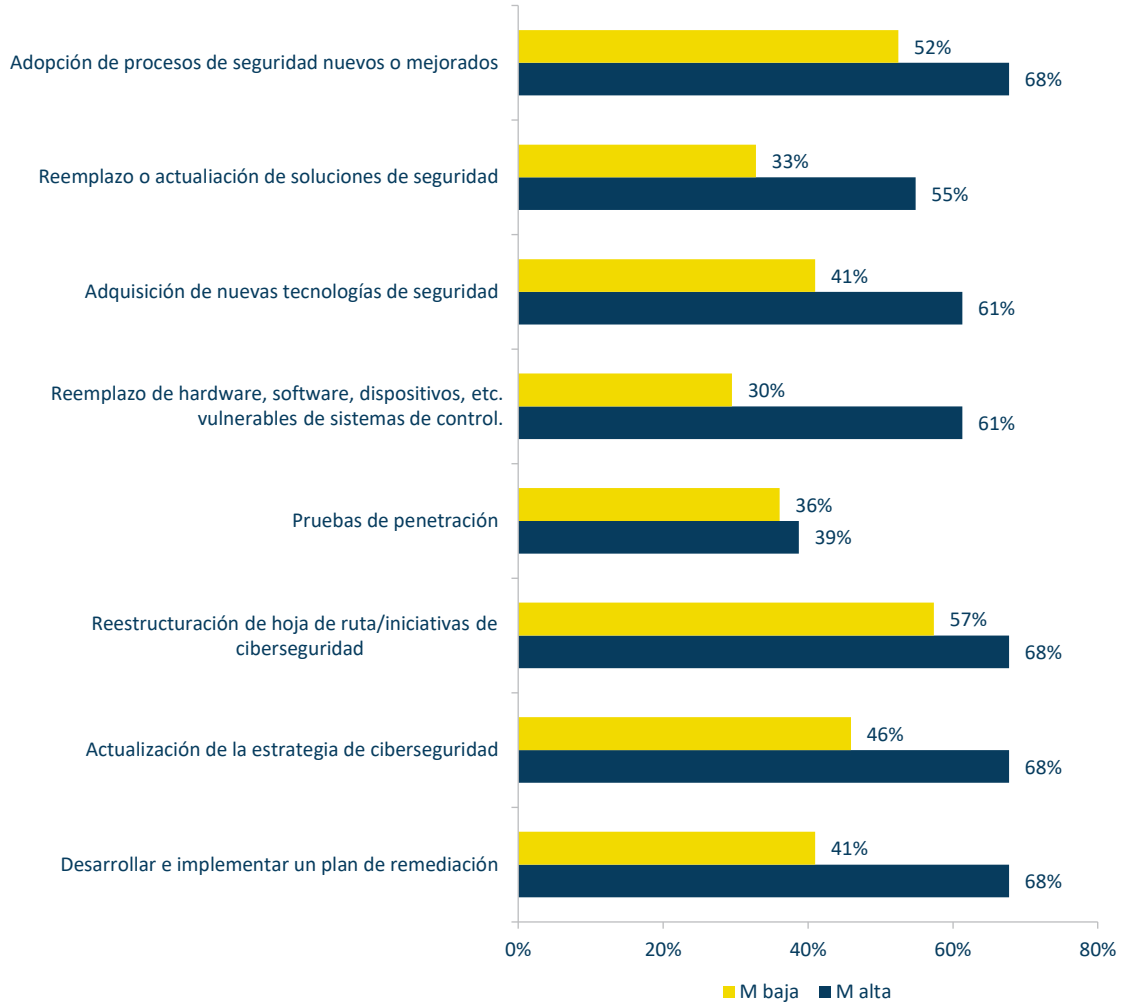
Si bien las inversiones en actividades de higiene cibernética (por ejemplo, segmentación de redes, capacitación y parches para vulnerabilidades) son clave para evitar una posible amenaza a una red industrial, será difícil evitar que un atacante muy motivado y técnicamente sofisticado acceda a la red. La capacidad de recuperarse rápidamente de un incidente cibernético será fundamental para minimizar la interrupción del funcionamiento o del suministro de productos esenciales como electricidad o agua a los consumidores.

Deben revisarse las evaluaciones de backup y recuperación para mejorar la ciberresiliencia de los sistemas críticos o industriales.

Eddie Toh

Socio de KPMG en Singapur y Director de Forensic Technology, KPMG en Asia-Pacífico

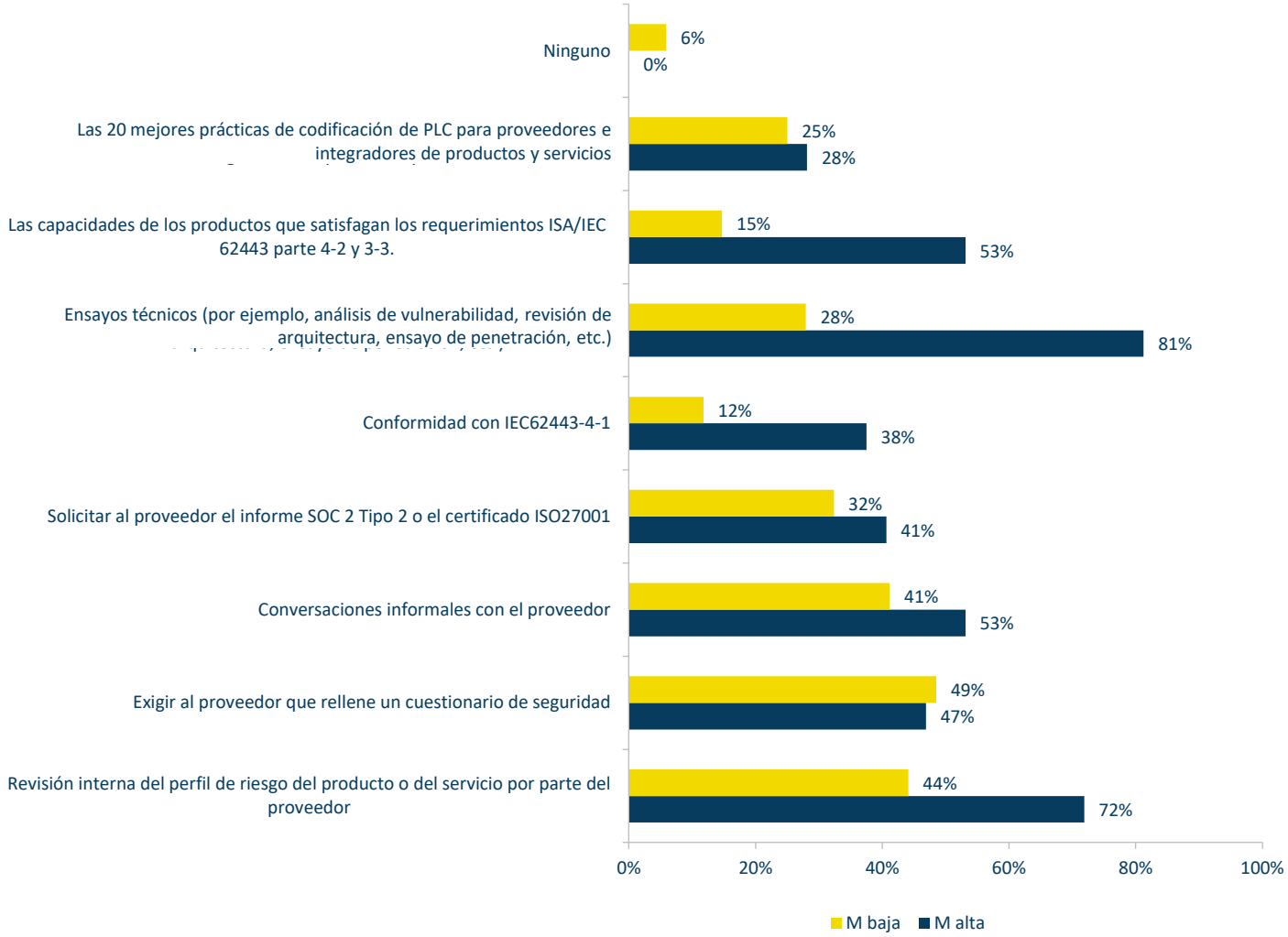
Actividades realizadas/planificadas en respuesta a las conclusiones de las evaluaciones de $(CS)^2$ realizadas por las organizaciones en los últimos 12 meses.



Evaluaciones de Riesgo de (CS)² previas a la adquisición - M alta frente a M baja

La evaluación del riesgo de los nuevos dispositivos y/o software no es la misma que las evaluaciones cíclicas de seguridad y debe considerarse por separado. Al igual que vimos que las organizaciones con programas de M alta (CS)² llevan a cabo evaluaciones generales de seguridad con mayor frecuencia, observamos que es más probable que realicen casi todos los tipos de evaluación de riesgos previa a la adquisición (el *Cuestionario de Seguridad* es la excepción). El aumento de la actividad reguladora en EE.UU. es probablemente un factor en los deltas que afectan al cumplimiento para muchos de nuestros encuestados, pero nos parece que es positiva la alta tasa de *Pruebas Técnicas* entre los de M alta (27,9% M baja vs 81,3% M alta) y pese a que sólo proporciona datos del tipo "fotografia instantánea" es complementaria de las evaluaciones periódicas de seguridad.

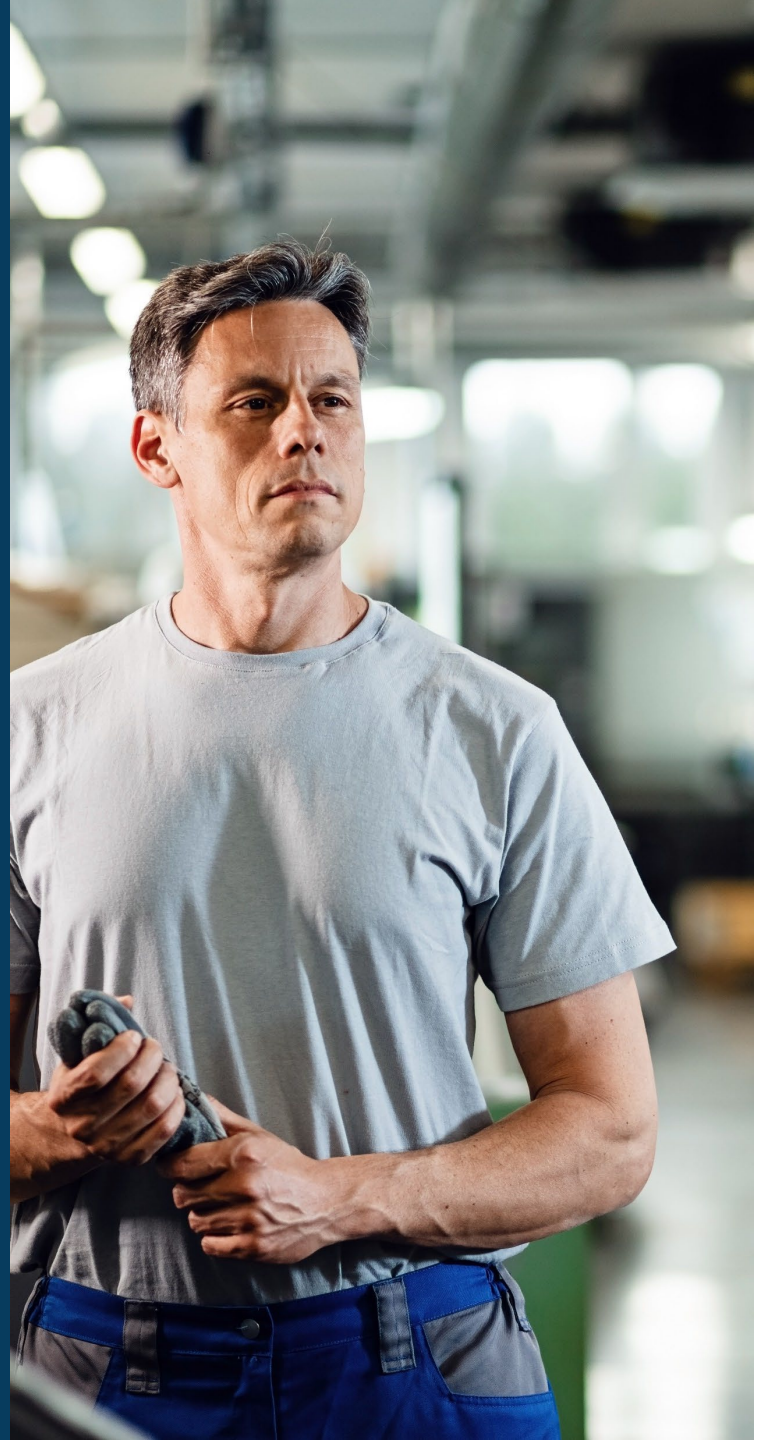
Evaluaciones de riesgos realizadas por las organizaciones antes de adquirir productos o servicios del sistema de control (M alta frente a M baja)



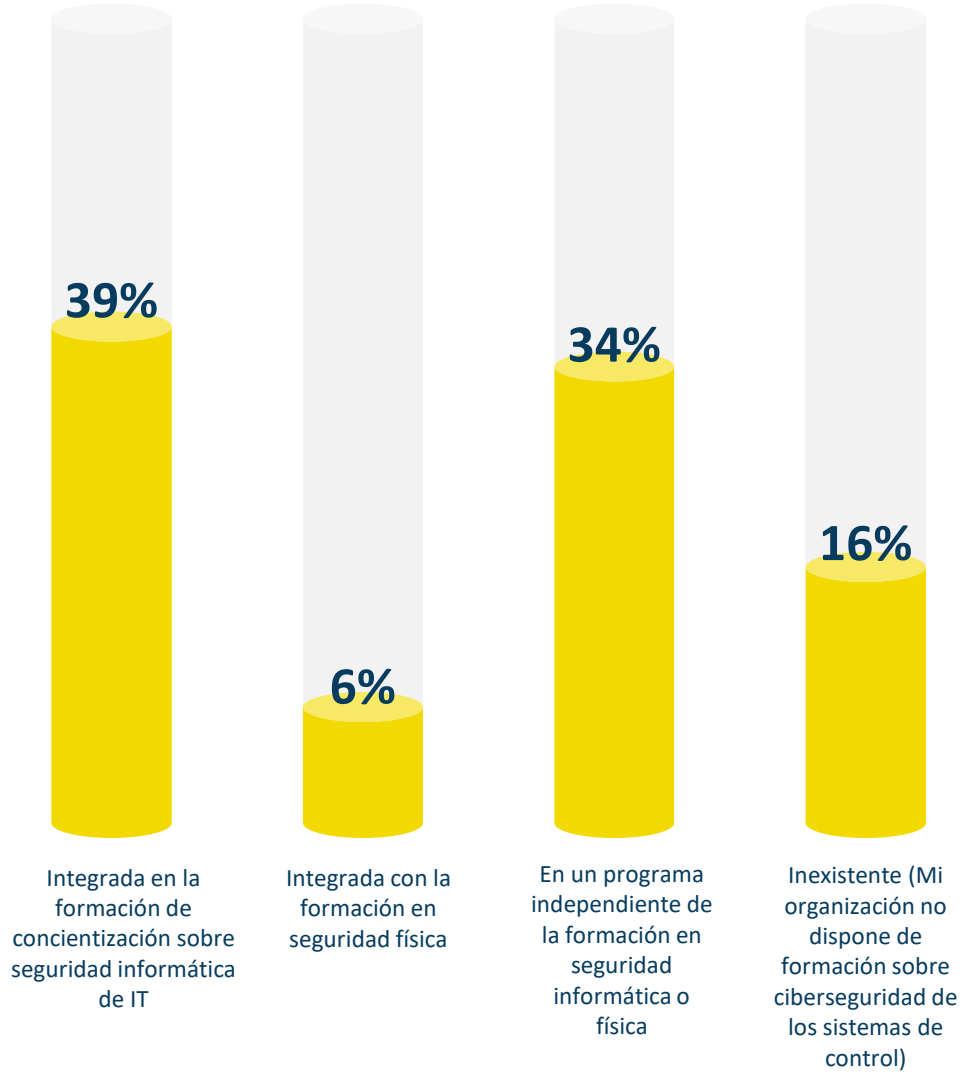
Formación en seguridad

Integración de la formación de concientización de (CS)² - Usuarios finales

En este caso, la preocupación obvia es que existan tantas organizaciones de usuarios finales que carecen de formación para la concientización de (CS)² (16,1% *inexistente*). Ya sea impulsado por los departamentos de IT, los programas de Administración de Riesgos, totalmente dentro de Operaciones o algún otro diseño, lograr y mantener un alto nivel de concientización sobre las amenazas de (CS)² , métodos de ataque, vulnerabilidades y procedimientos es esencial para administrar los riesgos inherentes a cualquier entorno operativo ICS/OT. Es vital que todas las organizaciones con responsabilidades sobre activos/ operaciones implementen este tipo de programas.



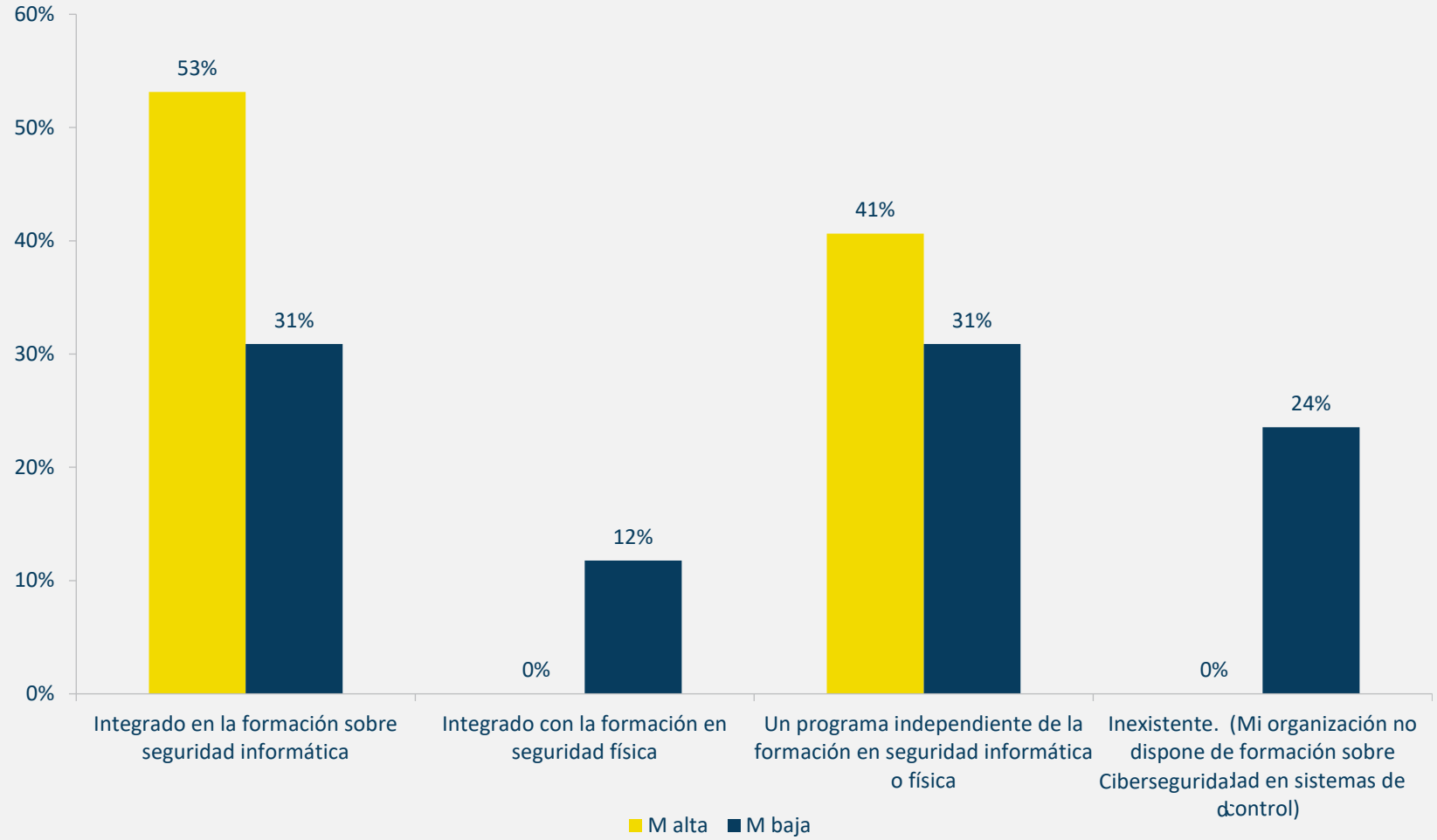
La formación para la concientización sobre la seguridad de los sistemas de control de mi organización está...



Integración de la formación de Concientización de (CS)² - M alta frente a M baja

El desglose de nuestros datos por grupos de nivel de madurez revela que son exclusivamente las organizaciones con programas de seguridad de (CS)² con M baja las que carecen de la *formación para la concientización* pertinente (24% *Inexistente* frente a 0% M alta), mientras que la mayoría de sus colegas del grupo de M alta cuentan con formaciones para la concientización en Ciberseguridad *Integrada* de Seguridad de TI y *Sistemas de Control* .

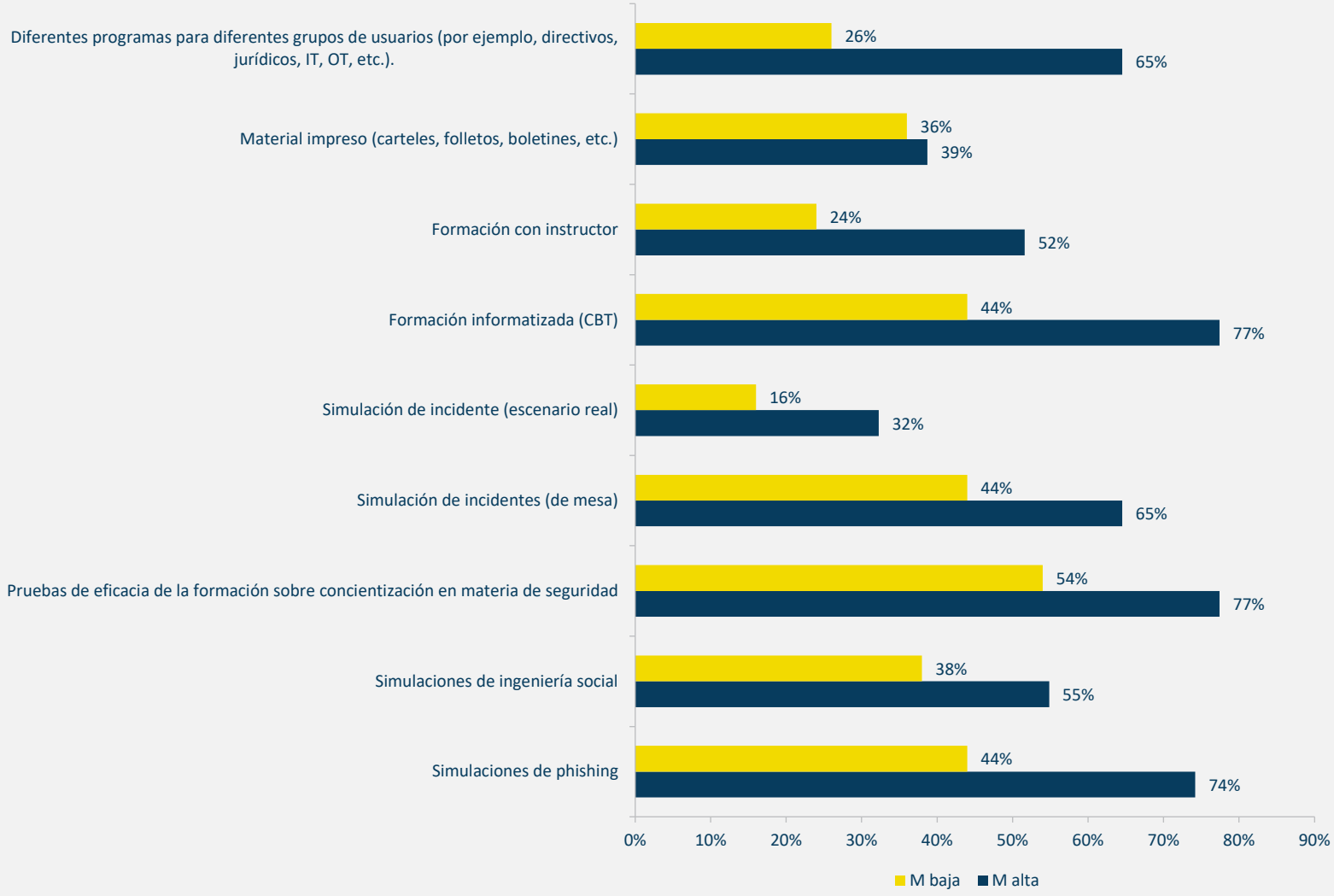
El tema de la formación para la concientización sobre la seguridad de los sistemas de control de mi organización está....



Componentes de la formación en (CS)² - M alta frente a M baja

Aunque no incluimos la formación en seguridad en nuestras descripciones de los distintos niveles de madurez de los programas de seguridad, de este gráfico se desprende claramente que las organizaciones con M alta invierten más en garantizar que su personal esté capacitado. El único componente en el que los dos grupos están siquiera cerca el uno del otro es en el uso de material impreso, que a menudo se considera menos eficaz que cualquiera de los otros. De hecho, es en las áreas más eficaces, como las *simulaciones* (cualquiera) y la *formación dirigida por un instructor* , donde se observan algunos de los mayores deltas. El mayor uso de las *Pruebas de Eficacia de la Formación en Concientización sobre Seguridad* (M alta 77% frente a M baja del 54%) debería permitir a estas empresas centrarse en lo que funciona mejor y mejorar continuamente sus programas de formación.

Componentes incluidos en la formación relacionada con la seguridad de los sistemas de control de la organización




SERVER ROOM ASSISTANT
12-8976-3457-567
1 ACCESS CATEGORY
FG12558BKLSPPP166161

$(CS)^2$ en Redes

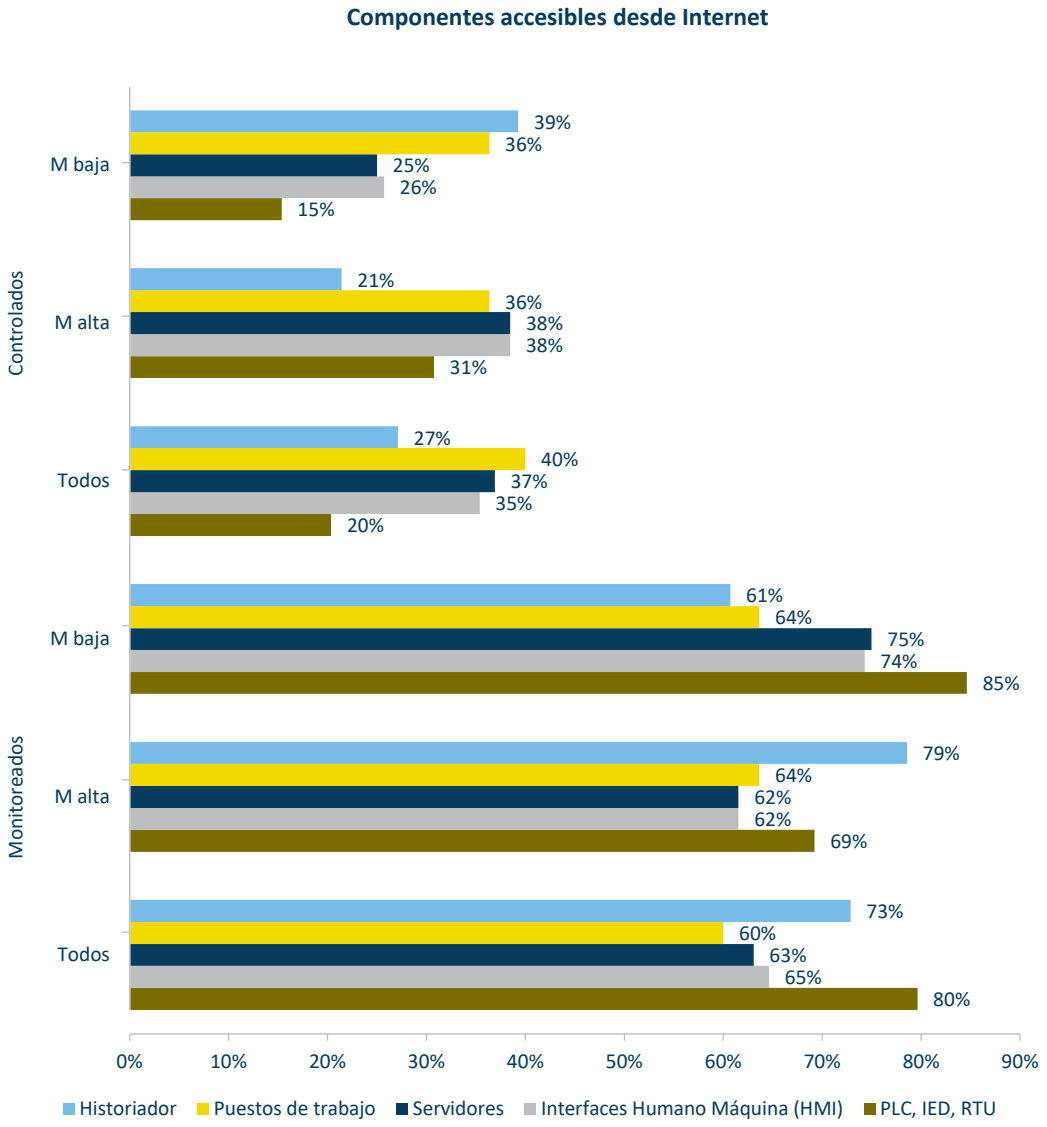
Accesibilidad de los componentes del sistema de control

En general, este gráfico y los siguientes son bastante preocupantes. Tener tantos elementos de sistemas de control accesibles, incluso controlables, desde Internet (desde el 15% de los PLC de M baja hasta el 39% de los historiadores de M baja) indica que los atacantes tienen una superficie de ataque muy grande y el potencial de grandes impactos en estas empresas.

Algunos de nuestros contribuyentes PYME han señalado la importancia de tener en cuenta que «accesible» revela los *controles* o el *método de* dicha accesibilidad. Podría tratarse de sistemas con puertos abiertos a Internet (por ejemplo, ¿pantalla de inicio de sesión de una HMI?), con acceso remoto permitido desde Internet (por ejemplo, VPN / RDP), o alcanzable a partir de otra máquina expuesta a Internet (por ejemplo, un host intermediario), o en una red accesible a un host intermediario. Las características específicas de su accesibilidad y los controles de protección de dicha accesibilidad son factores esenciales para evaluar sus niveles de riesgo.

Nos parece curioso que tantos componentes sean tan frecuentemente controlables a través de Internet en las organizaciones de M alta como en las de M baja. De hecho, los servidores, los HMI y los PLC/IED/RTU suelen ser más accesibles de este modo en los primeroos[12]. Este patrón continúa en los siguientes gráficos que muestran la accesibilidad a los componentes desde las redes empresariales, los proveedores/integradores y la nube.

[12]Aquí puede influir la elevada rentabilidad de la segmentación de la red para el grupo más maduro (75%, véase el gráfico de Top ROI - M alta frente a M baja).



Accesibilidad de los componentes del sistema de control (cont.)

Estas respuestas indican que el acceso externo a los sistemas de control es frecuente hoy en día, incluso desde redes empresariales, proveedores y la nube. Debido a esta creciente convergencia IT/OT, es imperativo que las organizaciones consideren la seguridad de los sistemas de control como parte de su programa general de seguridad, en lugar de como un ámbito separado. Esto se aplica tanto a los programas de gestión de la seguridad (según normas como IEC 62443 e ISO 27001) como a los controles utilizados para asegurar y supervisar estos sistemas.

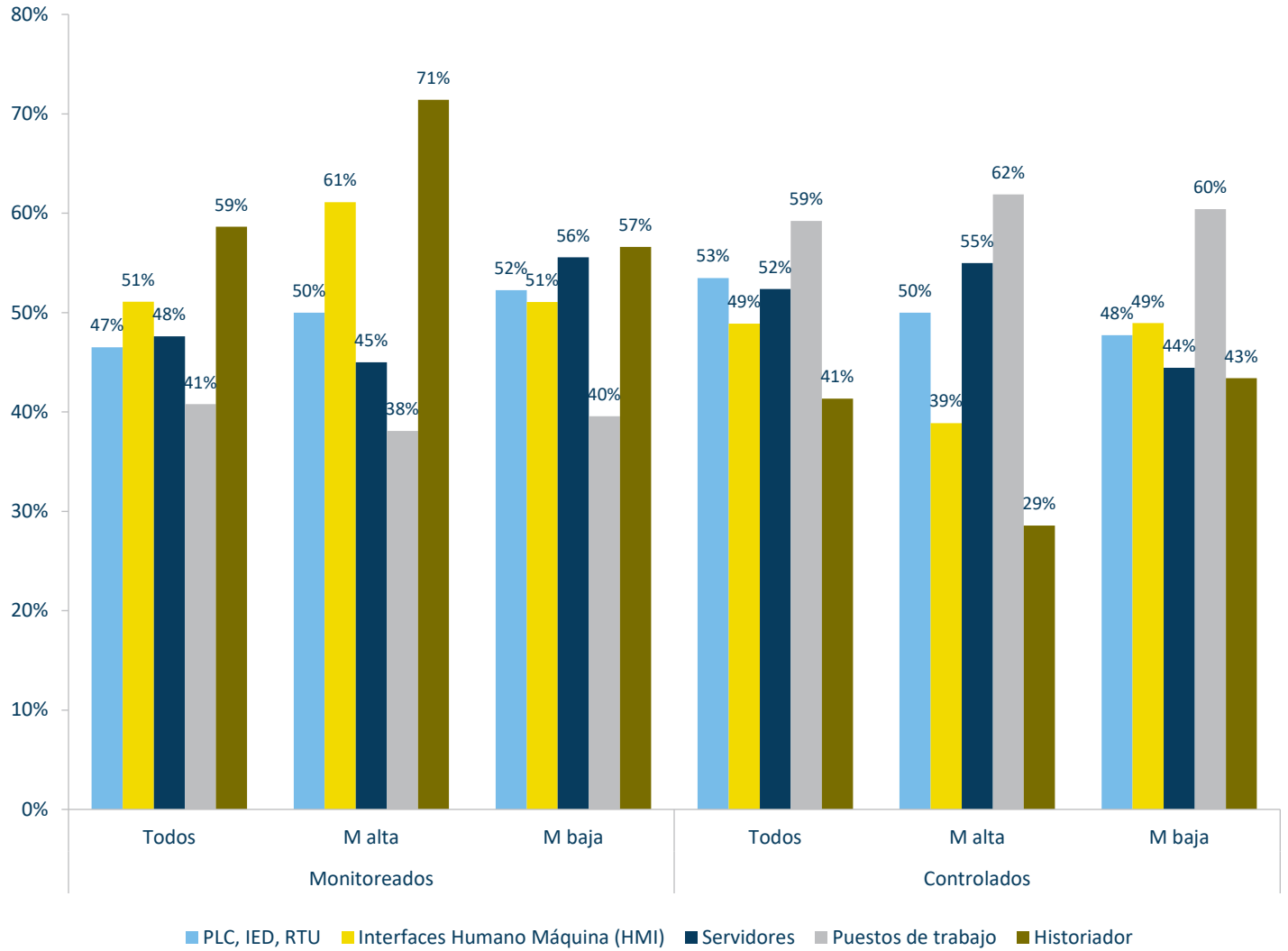
En el Informe sobre el Estado de la Tecnología Operativa y la Ciberseguridad 2023 de Fortinet, los encuestados indicaron que la seguridad de la tecnología operativa forma parte de las responsabilidades del CISO en casi todas las organizaciones (95%). La realidad de la convergencia IT/OT también se reflejó en la visión de las organizaciones sobre el panorama de las amenazas, donde una gran mayoría de organizaciones (77%) consideró que el ransomware fue una preocupación mayor que otras amenazas para el entorno OT.

Rod Locke

Director de Gestión de Productos

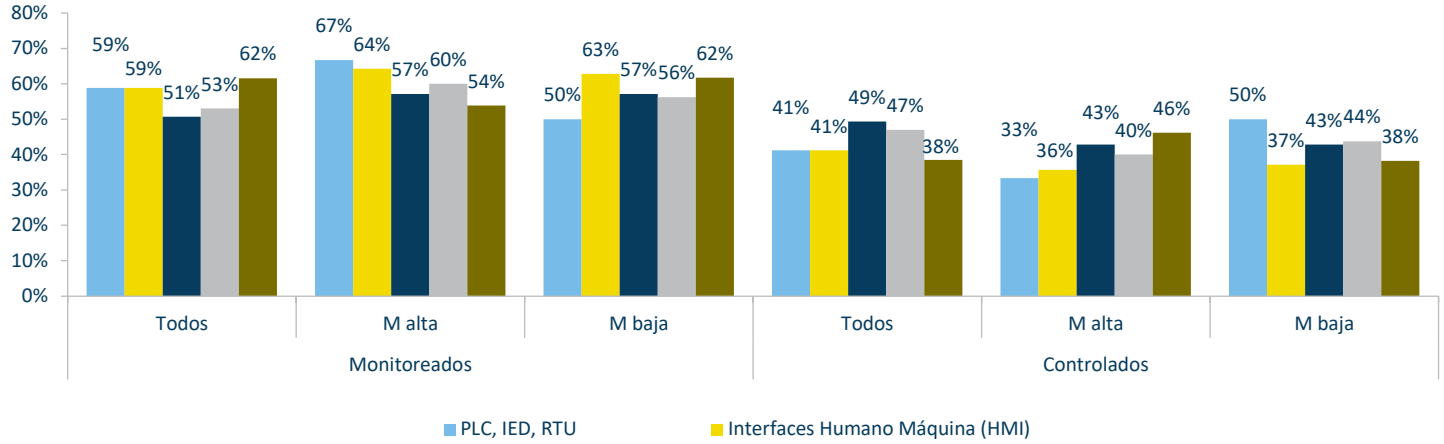
Fortinet

Componentes accesibles desde la red empresarial

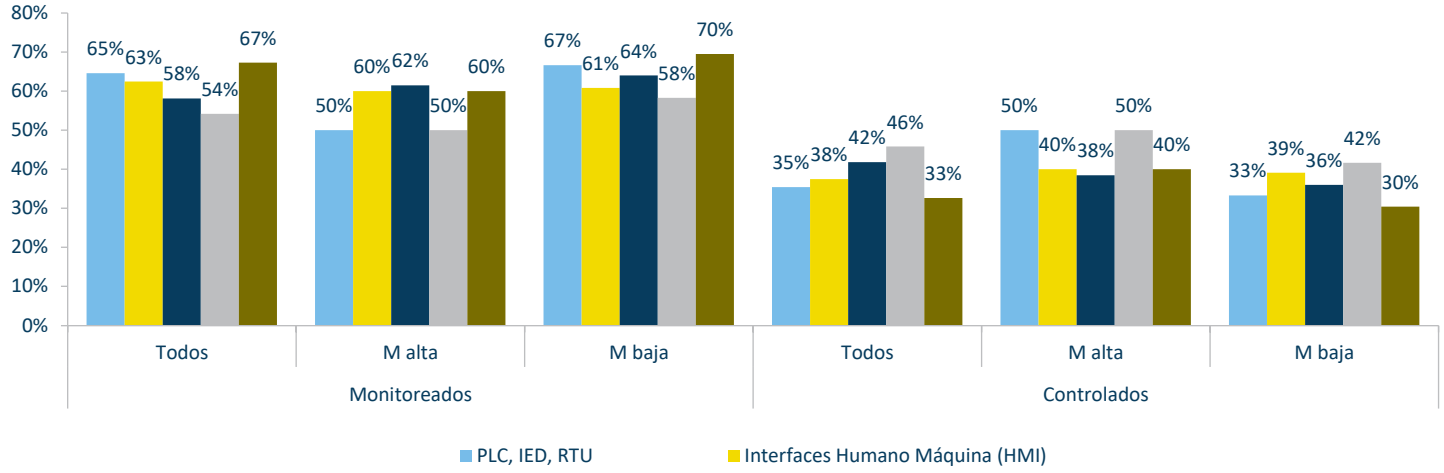


Accesibilidad de los componentes del sistema de control (cont.)

Componentes accesibles a distancia por el proveedor/integrador



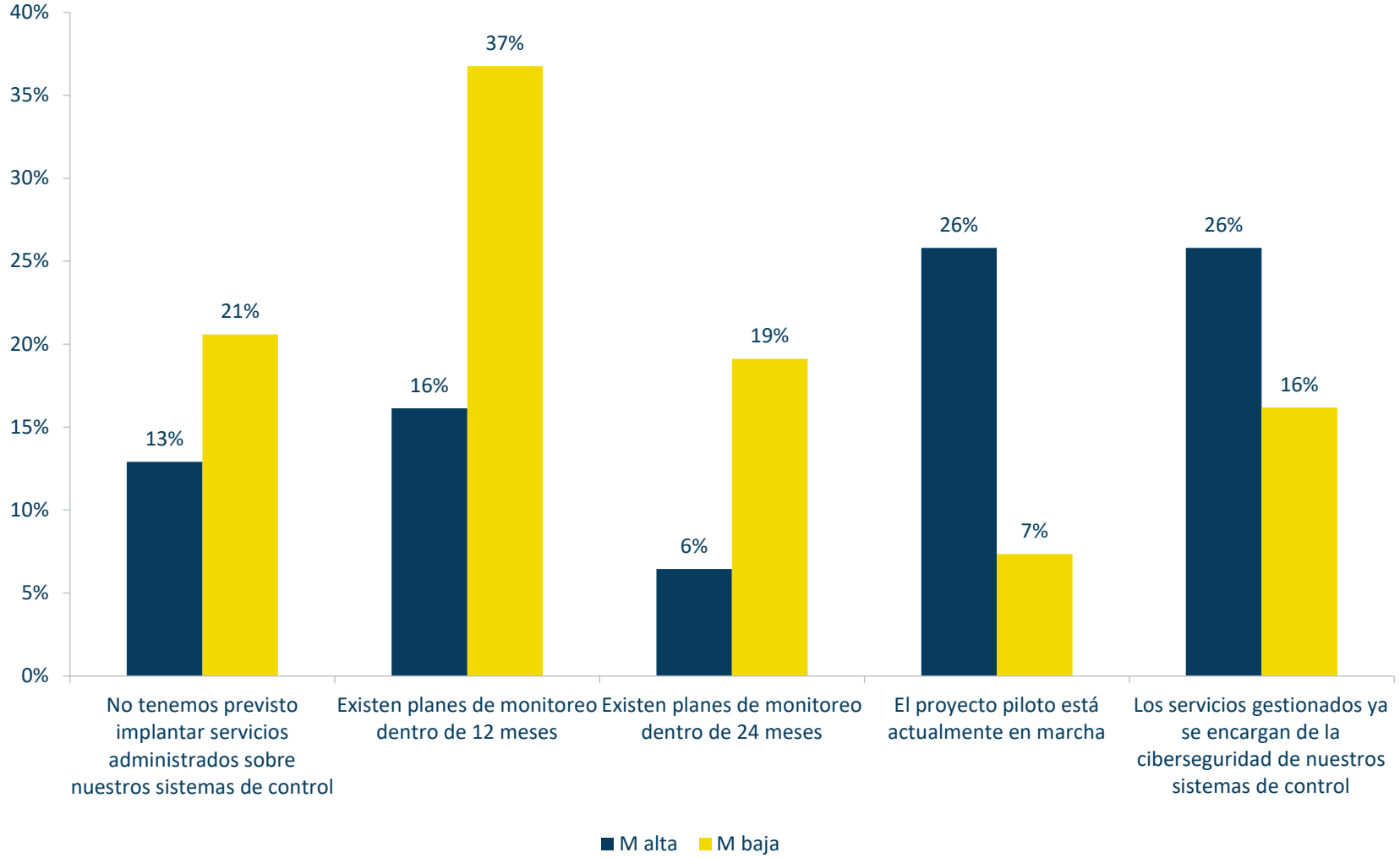
Componentes accesibles desde la nube



Servicios de (CS)² administrados actualmente - M alta frente a M baja

Los participantes de este año han vuelto a indicar que es más probable que las organizaciones con M alta cuenten ya con servicios gestionados que se ocupan de su ciberseguridad (25,8% M alta frente a 16% M baja) o estén en proceso de hacerlo con *Proyectos Piloto* (25,8% M alta frente a 7% M baja).

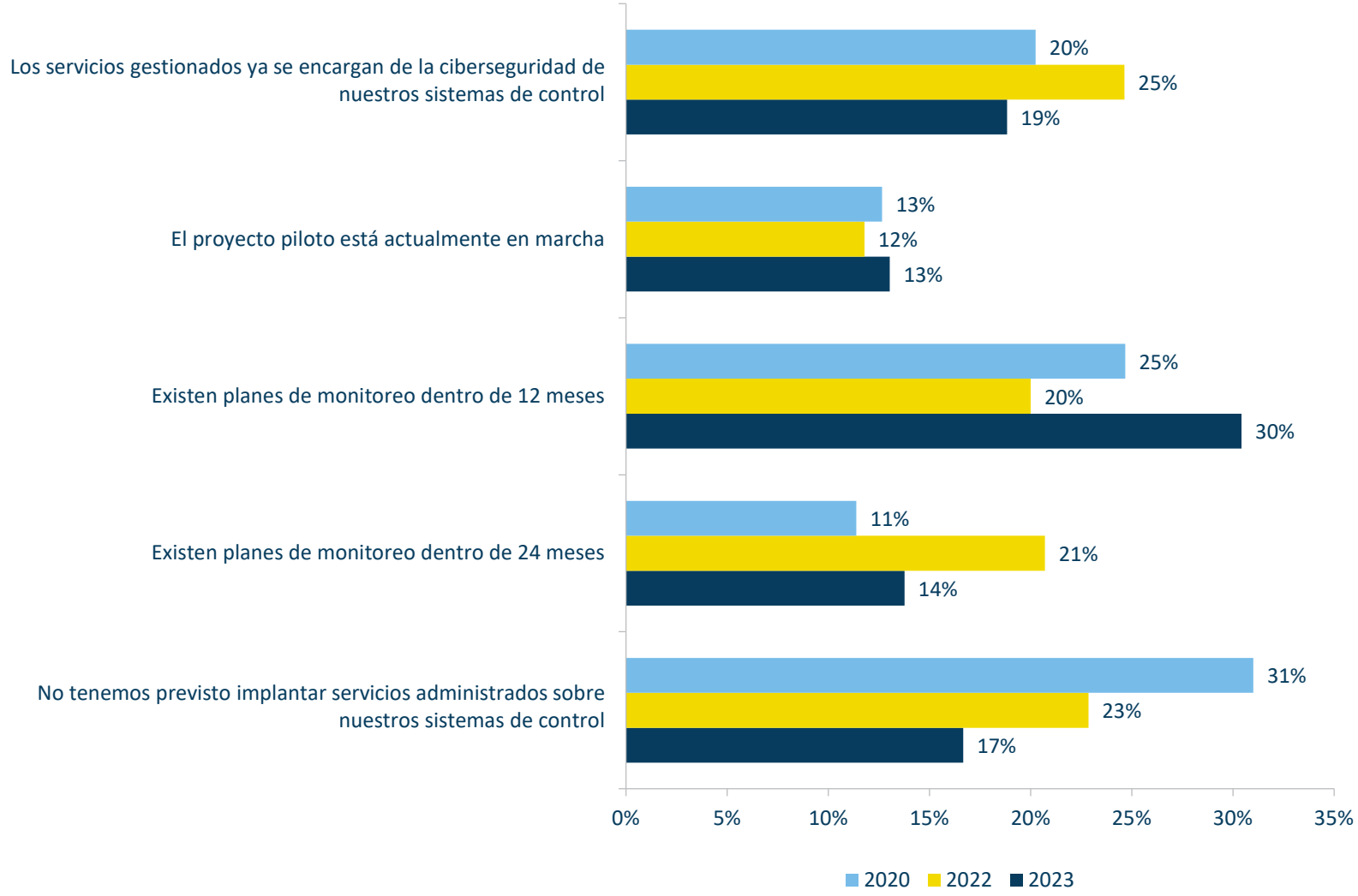
Estado actual de los servicios de seguridad del sistema de control gestionado de la organización (M alta VS M baja)



Utilización de los servicios de (CS)² administrados - Estudio longitudinal

El cambio hacia el uso de servicios de (CS)² administrados está en consonancia con muchos años de nuestros consejos a los lectores. La formación y la educación de los recursos internos tienen puntos indiscutibles, pero se trata de inversiones más largas (y posiblemente menos seguras a corto plazo). La oferta de (CS)² de profesionales con conocimientos y experiencia ha sido insuficiente durante mucho tiempo para satisfacer las demandas de la tecnología y las prácticas que cambia a alta velocidad, y la creciente hiperconectividad de los dispositivos de los sistemas de control. Es inevitable que esto alimente un mercado de servicios de (CS)² en expansión . Nuestra recomendación para las empresas con recursos suficientes es que pongan en marcha programas de desarrollo de recursos internos y recurran a expertos externos para hacer frente a las necesidades inmediatas de protección de sus activos y operaciones. Creemos que este es el mejor enfoque para mejorar las perspectivas a largo plazo de sus organizaciones.

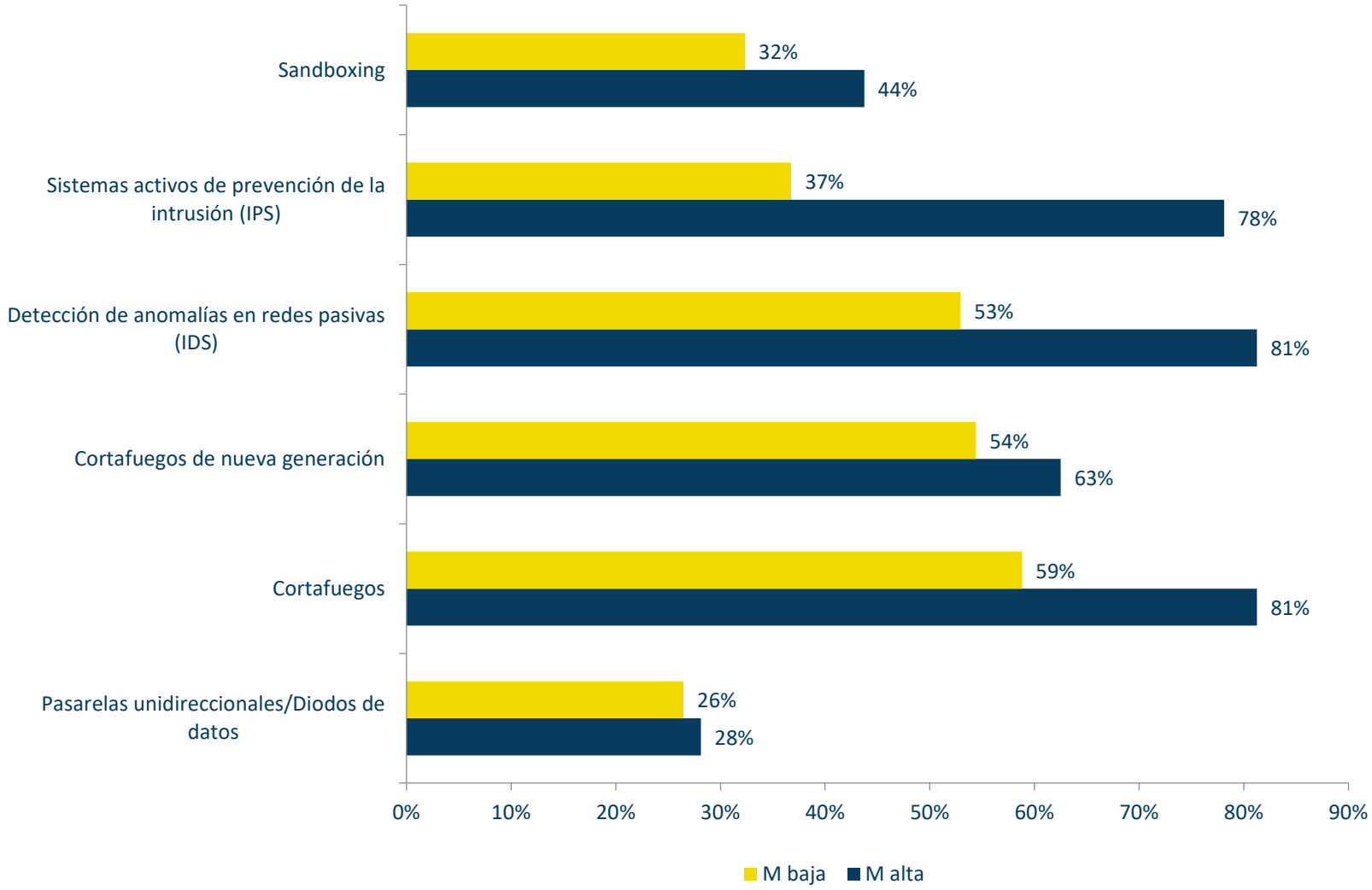
Estado actual de los servicios de seguridad del sistema de control de la organización (longitudinal)



Tecnologías de (CS)² actuales- M alta frente a M baja

Aparte de la tendencia general de que las organizaciones con un M alta utilizan todas las tecnologías de seguridad con más frecuencia que el grupo con una M baja, los grandes deltas entre el uso de *sistemas activos de prevención de intrusiones* (M alta, 78,1% frente a M baja, 36,8%) y la *detección pasiva de anomalías en la red* (M alta, 81,3% frente a M baja, 36,8%) indican una probabilidad mucho mayor de que estas empresas identifiquen y bloqueen intentos de incursión en plazos más cortos, reduciendo así el impacto potencial en sus sistemas.

Tecnologías de seguridad utilizadas para proteger los activos de los sistemas de control de la organización frente a las ciberamenazas



Monitoreo de redes de (CS)² - Estudio longitudinal

La visibilidad en nuestras redes de sistemas de control es crucial para proteger esas redes y los activos conectados. Mientras que la cultura de la OT era históricamente resistente a la introducción de tecnologías de monitoreo de la red (comprensiblemente, debido a algunos casos de perturbaciones operativas que se produjeron al hacerlo) en sus entornos, las herramientas y técnicas que proporcionan esta información han seguido madurando y mejorando, con un aumento de la aceptación de su relación riesgo / beneficio. Resulta alentador observar el crecimiento interanual de las organizaciones que han implantado el monitoreo de redes de (CS)² y tienen previsto reforzarlo, que ha pasado de ninguna hace unos años al 17,9% actual. Las organizaciones que no tienen previsto implantar ningún tipo de monitoreo de la actividad de la red han bajado a un porcentaje de un solo dígito (9%) por primera vez. Los resultados muestran que las organizaciones seguirán implantando y reforzando la supervisión de la actividad de la red en el futuro. En un principio se pensó que el aumento del número de organizaciones que no tenían previsto implantar la supervisión en 2022 (19%) era un indicio de que muchas estaban pasando al estado "Todo está monitoreado", pero los resultados de este año lo ponen en duda. Seguiremos armando este rompecabezas.

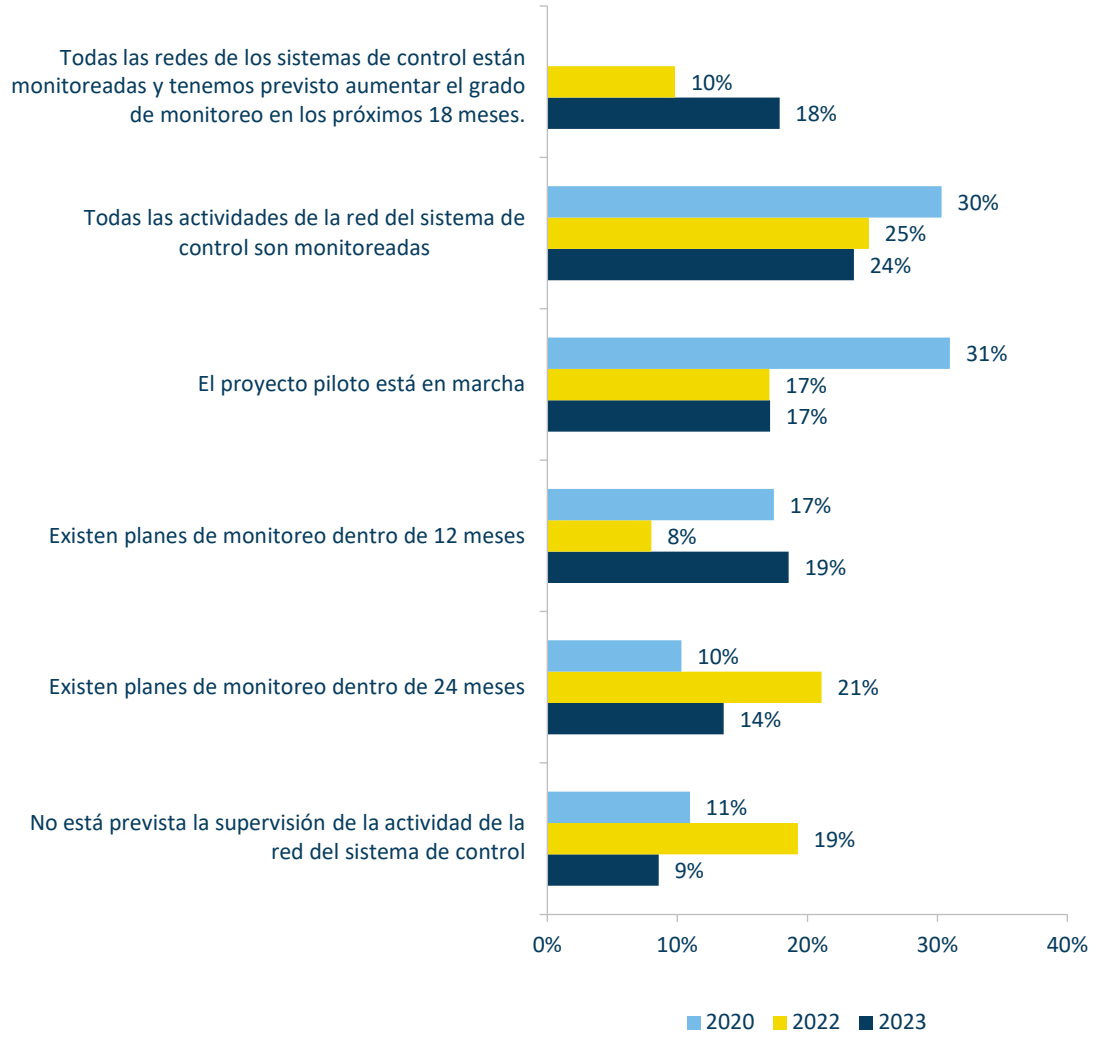
A medida que la tecnología operativa se moderniza, la superficie de ataque sigue ampliándose cuando los sistemas OT se conectan cada vez más a los sistemas IT. Los actores de las amenazas seguirán empleando sofisticadas "Tácticas, Técnicas y Procedimientos" y explotándolas contra cualquier eslabón débil para perturbar dichos sistemas. Por ejemplo, dado el aliento de su funcionalidad, Pipedream es un ejemplo de la creciente sofisticación y capacidad de los actores de amenazas para perturbar los sistemas industriales.

Para detectar actividades maliciosas y responder a tiempo a tales eventos, será imperativo tener visibilidad y monitoreo continuo en la red OT/IT/IIOT.

Eddie Toh

Socio de KPMG en Singapur y Director de Tecnología Forense KPMG en Asia-Pacífico

Estado actual del Monitoreo del Sistema de Control de la Actividad de Redes de la organización



(CS)² Visibilidad - Usuarios finales

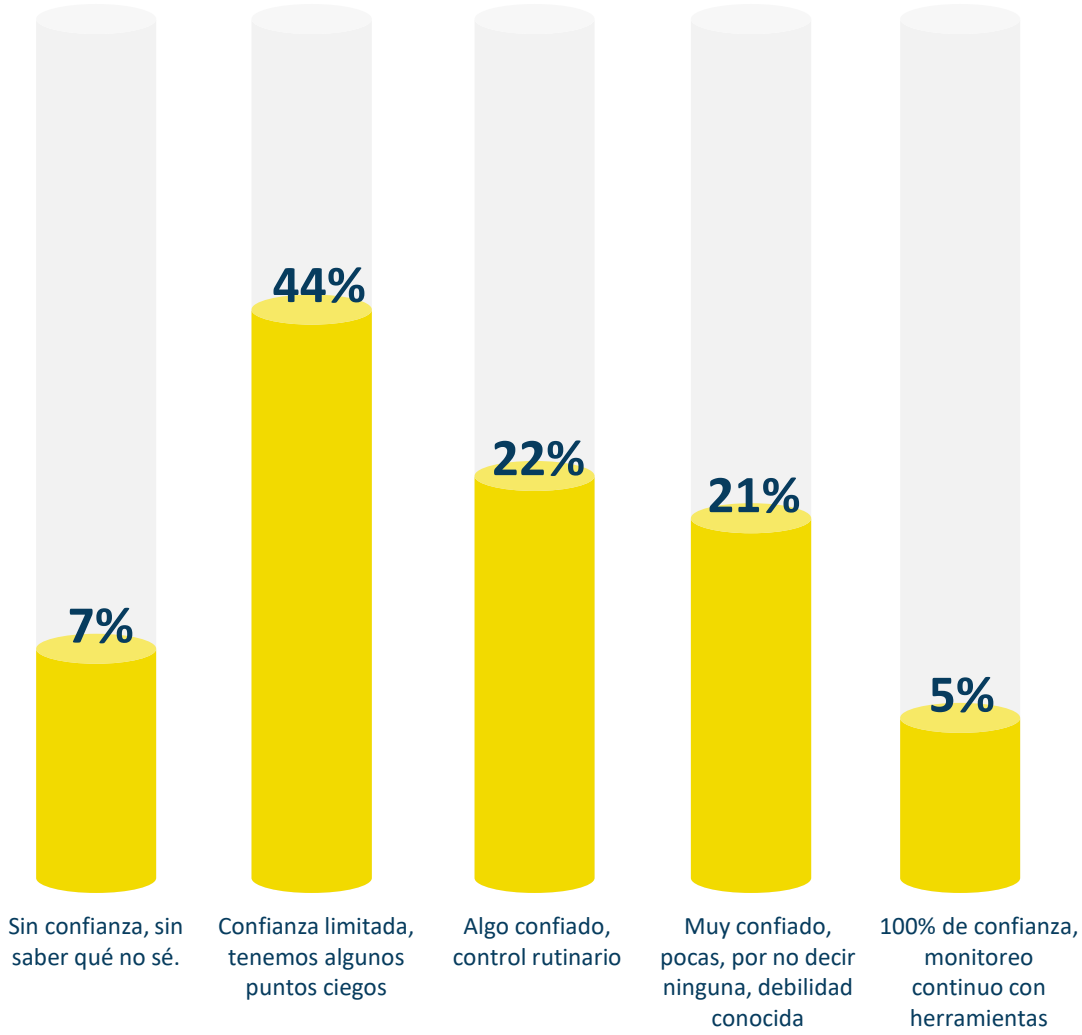
Nuestro equipo considera que el nivel de confianza de nuestro mayor grupo de usuarios finales encuestados (*Confianza limitada, tenemos algunos puntos ciegos* 43,7%) es bastante realista. La visibilidad en las redes de sistemas de control siempre ha sido un problema, y solo en los últimos años se han extendido las herramientas para adquirir esta importante capacidad. Recomendamos a nuestro lector que, si aún no lo ha hecho, utilice estas herramientas para superar los puntos ciegos y proporcionar[2] los conocimientos esenciales que necesitan para desempeñar sus funciones a sus defensores de (CS)[2].

El modelado de redes fuera de línea es el método más rápido y eficaz de proporcionar una visibilidad completa de la red de forma no intrusiva. Ayuda a construir una comprensión precisa de los entornos de red que nos comprometemos a proteger sin interrumpir las operaciones. Al analizar las configuraciones de red, las topologías y las políticas de seguridad en un entorno fuera de línea, obtenemos información detallada sobre las rutas de comunicación críticas y las lagunas de cobertura que, de otro modo, permanecerían ocultas durante una sesión de análisis de red en directo. Este método preserva la integridad y el rendimiento de la red al tiempo que identifica y aborda rápidamente las áreas que carecen de visibilidad, reforzando así la defensa de la red frente a posibles ciberamenazas.

Robin Berthier

CEO y cofundador, Network Perception

Confianza en la visibilidad de los dispositivos, usuarios y aplicaciones en las redes de la organización

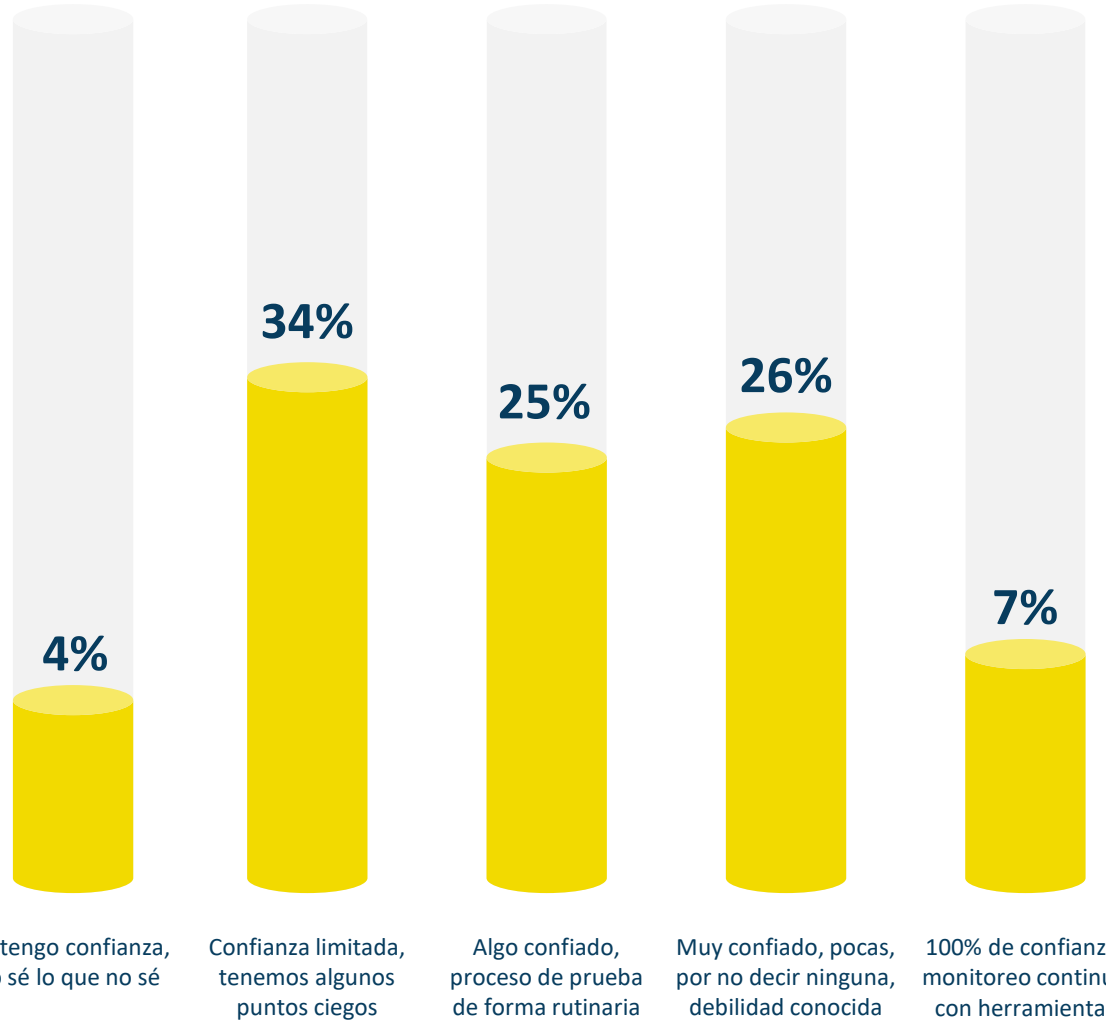


Incidentes de (CS)²

Respuestas de (CS)² al ataque - Usuarios finales

Nuestro equipo se alegró de ver el nivel de confianza en los procesos de respuesta a incidentes de ciberataques entre los propietarios/operadores de activos (usuarios finales), ya que, el 58%, como mínimo, está *Algo confiado* y la mayoría de ellos *Muy confiado o 100% confiado*. Se trata de una confianza mayor que la que este grupo tenía en la visibilidad de sus propias redes (véase el cuadro anterior sobre Visibilidad).

Confianza en los procesos de respuesta de la organización en caso de ciberataque



Incidentes de (CS)² recientes - Longitudinal

Aunque se ha producido un ligero aumento de los encuestados implicados en más *de 50* incidentes de (CS)² en el último año (del 5,2% del último informe al 5,8% actual), los resultados más destacados son el gran aumento de las respuestas de *Ninguno* (2022: 14,8% frente a 2023: 25,4%) y el descenso de 26-50 (2022: 19,4% frente a 2023: 10,1%). Se espera que esto muestre los resultados de los esfuerzos de protección y resiliencia en curso en lugar de ignorancia o error.

Se prevé que los ciberataques no hagan más que aumentar: es el lado negativo de la digitalización de la producción industrial. Cada vez hay más interfaces dentro de una organización, pero también con socios externos, lo que desgraciadamente aumenta los vectores de ataque.

Por lo tanto, es importante adoptar un enfoque prioritario y centrado para proteger los sistemas y procesos de producción. Un enfoque de seguridad adecuado en el marco de la OT no solo abarca los aspectos técnicos, sino también los procesos de seguridad, la gobernanza y el factor humano.

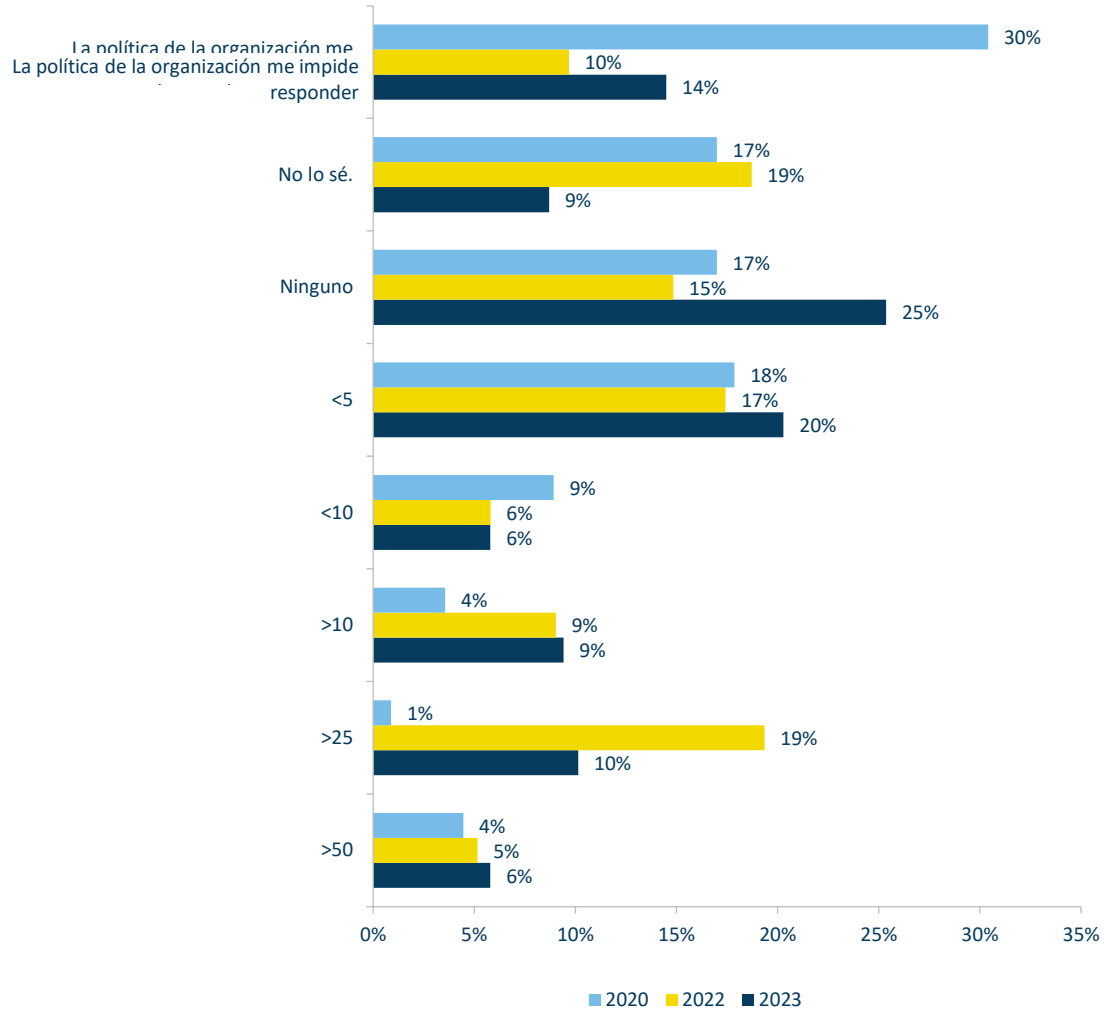
La clave para la prevención, detección y defensa es mantenerse al día. Porque la ciberseguridad de la OT se caracteriza por dos rasgos cruciales: Cambio y velocidad.

Marko Vogel

Socio y Director de Ciberseguridad de OT

KPMG Alemania

Estimaciones de cuántos incidentes de ciberseguridad de sistemas de control se han producido en su organización en los últimos 12 meses.



Vectores de Ataque por Incidente de (CS)² a clientes - Regiones[13]

El *correo* electrónico (35% a nivel mundial) y las *cuentas de usuario comprometidas* (31% a nivel mundial), preocupaciones potencialmente superpuestas, son los dos principales vectores de ataque este año, apenas desplazando a los *medios extraíbles infectados* del segundo lugar, a pesar de que también se encontraron con más frecuencia (24% el año pasado, 26% este año). En la región 5 (Oriente Medio y Norte de África) se produjeron más incidentes de *actualizaciones comprometidas de proveedores* (36%) que en ninguna otra, con más del 70%, mientras que se experimentó casi el mismo nivel de actividad de sitios *web organizativos comprometidos* que en la región 4 (APAC) (28% y 31% respectivamente). La región 4 destaca por la frecuencia del *compromiso de Wi-Fi* (24%) y de *dispositivos móviles o teléfonos infectados o comprometidos* (28%), ambas cifras muy por encima de las demás.

La[13](CS)²AI está organizada en siete Regiones. 1) América del Norte; 2) Europa (Central, Occidental, del Norte y del Sur); 3) Eurasia; 4) Indo-Pacífico; 5) Oriente Medio-África del Norte; 6) África Subsahariana; 7) América Latina-Caribe.

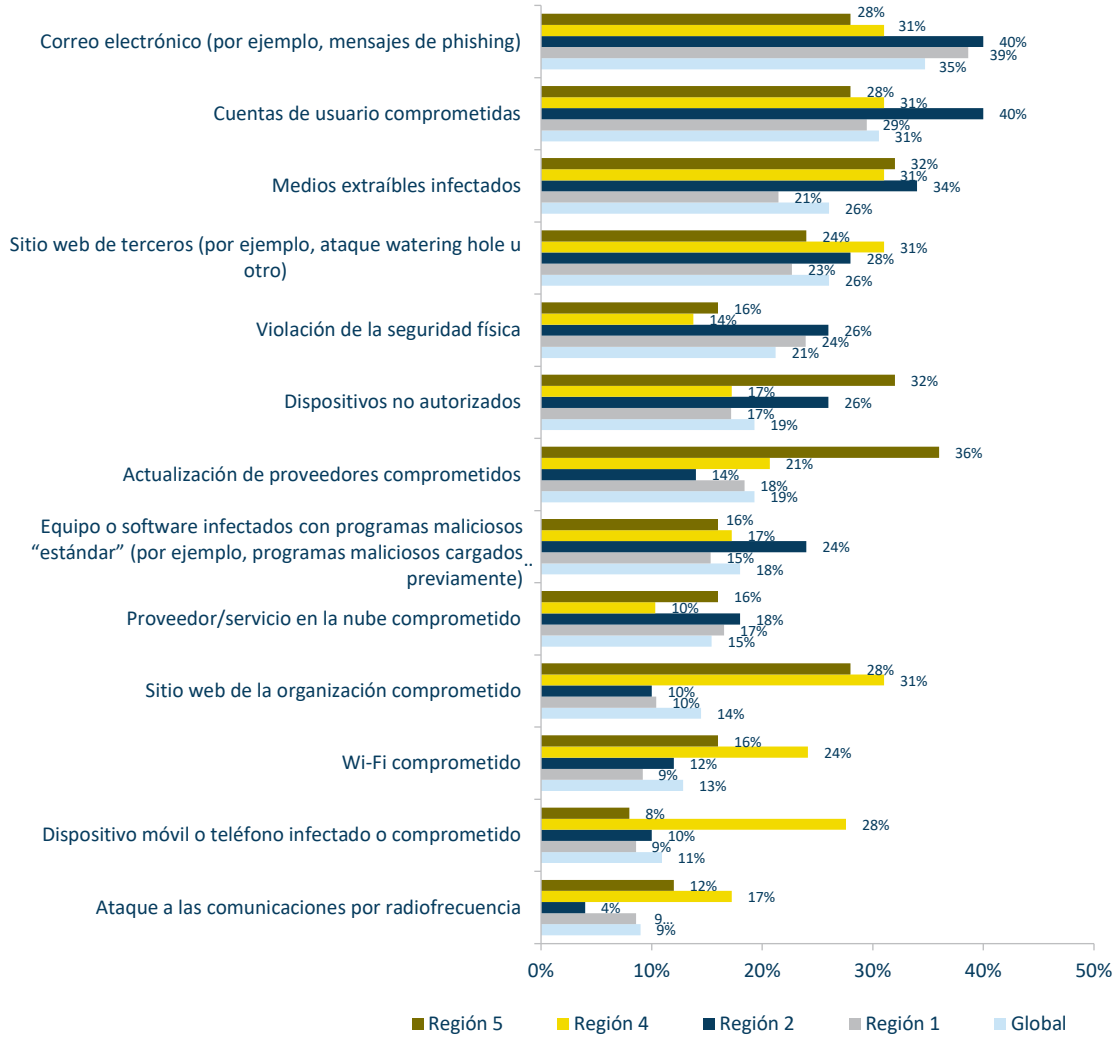
En muchas organizaciones, la postura de madurez de seguridad de IT es mayor que la postura de seguridad de OT por varias razones de peso, sin embargo, hay una gran oportunidad para que las organizaciones eleven la postura de seguridad de OT, mejoren la eficiencia operativa de seguridad y eleven las innovaciones empresariales mediante la aplicación de la convergencia cibernética de IT/OT que ayudará a las organizaciones a tener una postura de seguridad unificada, reducir la superficie de ataque, permitir que IIoT facilite la transformación digital y apoye las tecnologías avanzadas para mejorar la toma de decisiones para muchas empresas.

Hossain Alshedoki

Líder de Ciberseguridad y privacidad Dirección de Energía y Recursos Naturales

KPMG en Arabia Saudita

Vectores de ataque en incidentes de (CS)2 de clientes a los que se ha dado respuesta en los últimos 12 meses



Impactos de incidentes de (CS)² – Estudio longitudinal

Esta pregunta ha variado en los años que llevamos preparando estos informes, mientras que las opciones de respuesta aumentaron para mejorar el valor de la información (y los hallazgos), por lo tanto, existen diversas opciones para las que ninguna respuesta de 2020 fue posible.

Los aumentos interanuales llamativos en *Pérdida financiera por disrupción de operaciones, daño, pérdida de productos* son aspectos clave de esta información. Recuerde el énfasis en la continuidad de las operaciones revelado anteriormente (ver cuadros sobre prioridades de asignación de fondos discrecionales (página 24), lineamientos del proveedor a los clientes (página 25)).

Las respuestas sobre *Pérdida de vidas* han sido un interrogante constante en los últimos años. Podría esperarse que un ciberataque malintencionado que causara muertes humanas fuera noticia de primera plana. Incluso si el acontecimiento se produce en un lugar donde las empresas o los gobiernos suprimen este tipo de informes, es difícil ver cómo en las dos últimas encuestas, entre el 5 y el 6% de los encuestados informaron *Pérdida de vidas* debida a "incidentes cibernéticos" sin que la prensa se haya hecho eco de un solo incidente de este tipo. Entre nuestros participantes hay personas que protegen hospitales, centros de salud, etc., donde la interrupción de los sistemas puede provocar directa o indirectamente muertes, pero no tantos encuestados como para explicar este resultado. ¿Son estos "incidentes" en realidad errores y omisiones informáticos que se confunden con ataques deliberados?

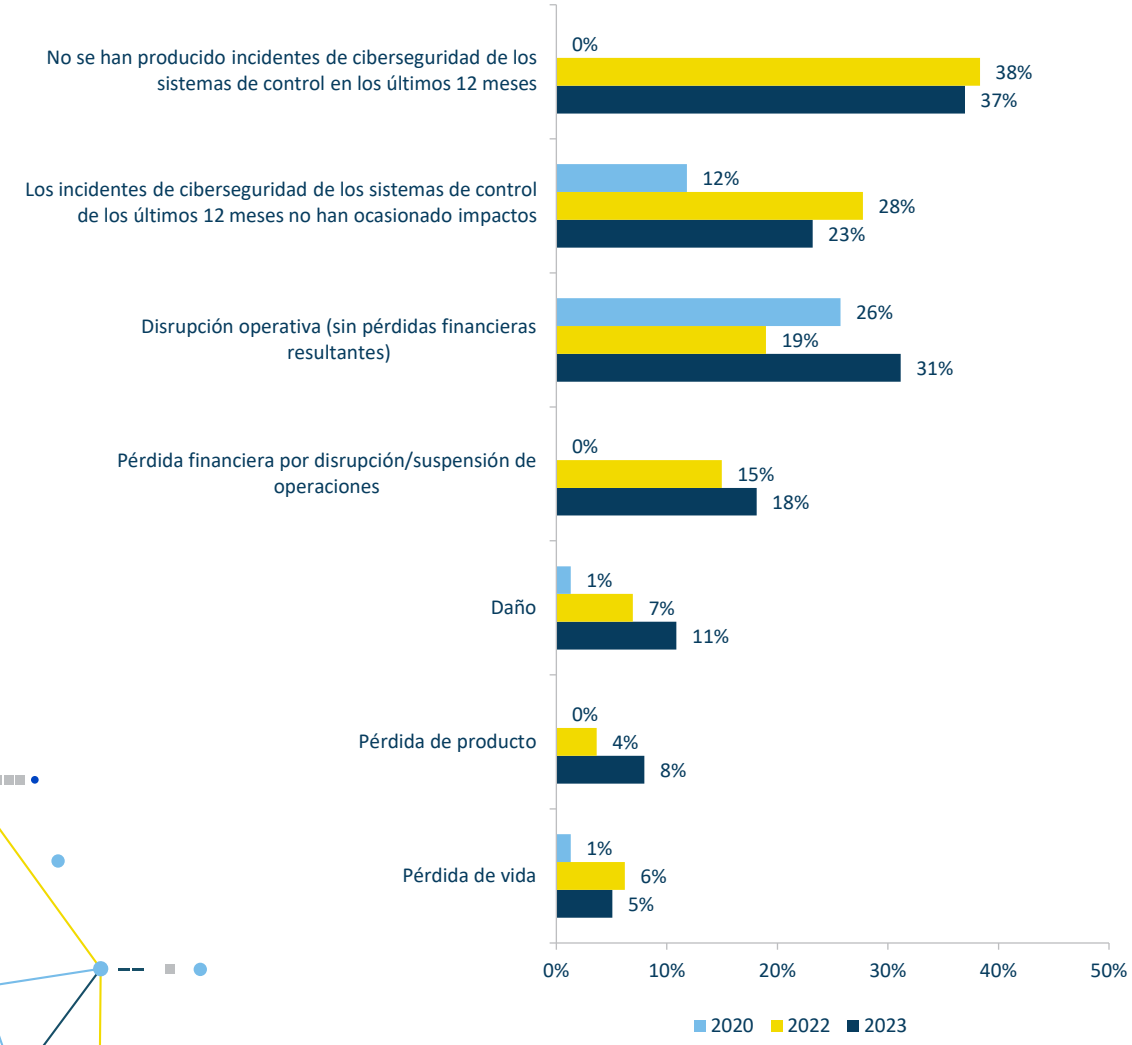
La información sobre intrusiones de la encuesta (CS)² muestra que los incidentes de seguridad están provocando un aumento en la disrupción de las operaciones, y que estas disrupciones están provocando resultados más graves. El Informe sobre el estado de la tecnología operativa y la ciberseguridad 2023 de Fortinet reveló índices similares, donde 49% de las organizaciones experimentan algún impacto en los entornos operativos. El informe también reveló que las organizaciones que informan madurez más alta experimentaron intrusiones de red más bajas y menores impactos en las operaciones. Estas organizaciones también eran más propensas a incluir la postura de ciberseguridad OT como un factor significativo en los informes de riesgo compartidos con los líderes ejecutivos y los directorios.

Rod Locke

Director, Gestión de Productos

Fortinet

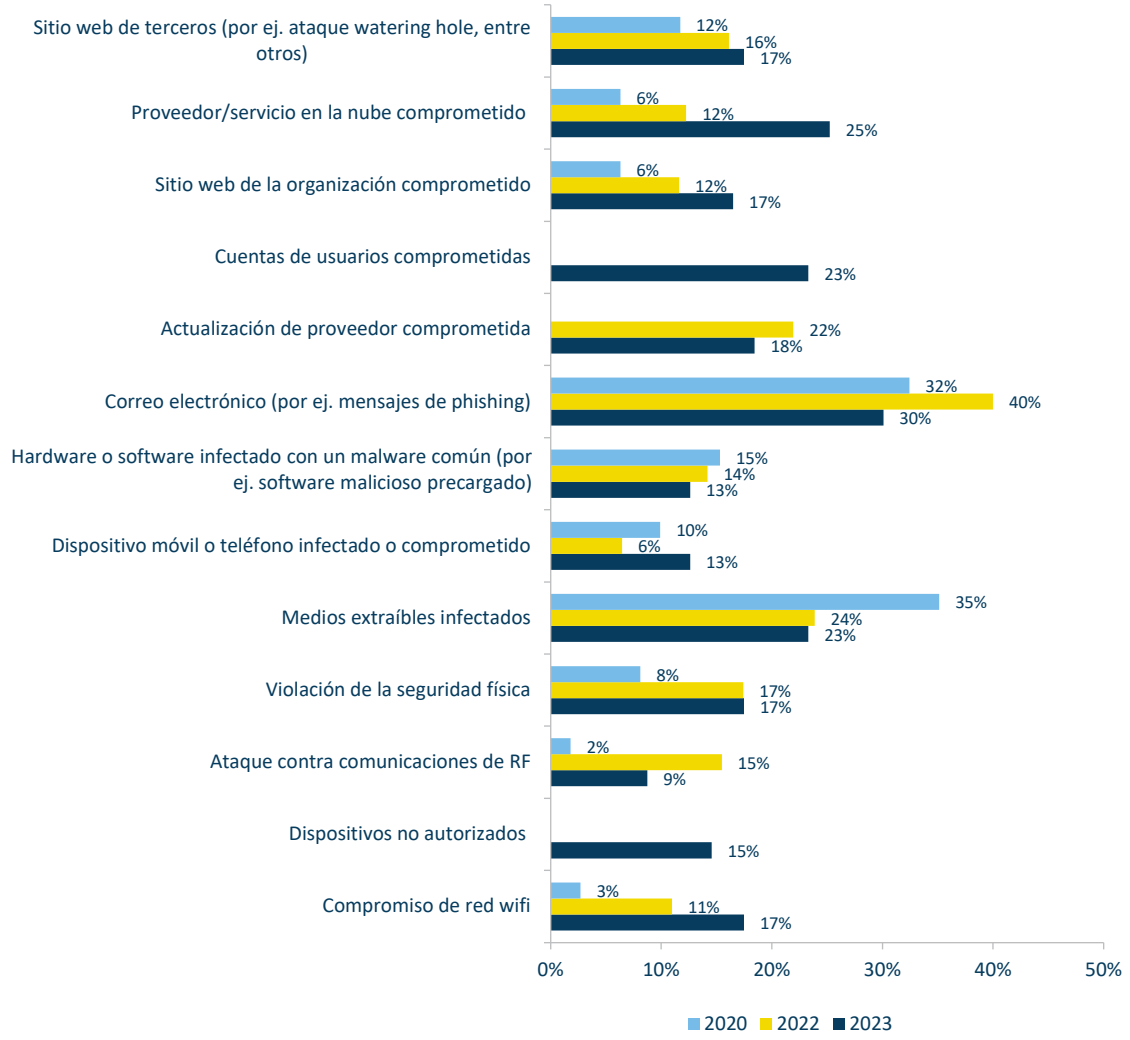
Impactos de los incidentes de seguridad de los sistemas de control en su organización en los últimos 12 meses



Vectores de ataque recientes de (CS)² – Estudio longitudinal

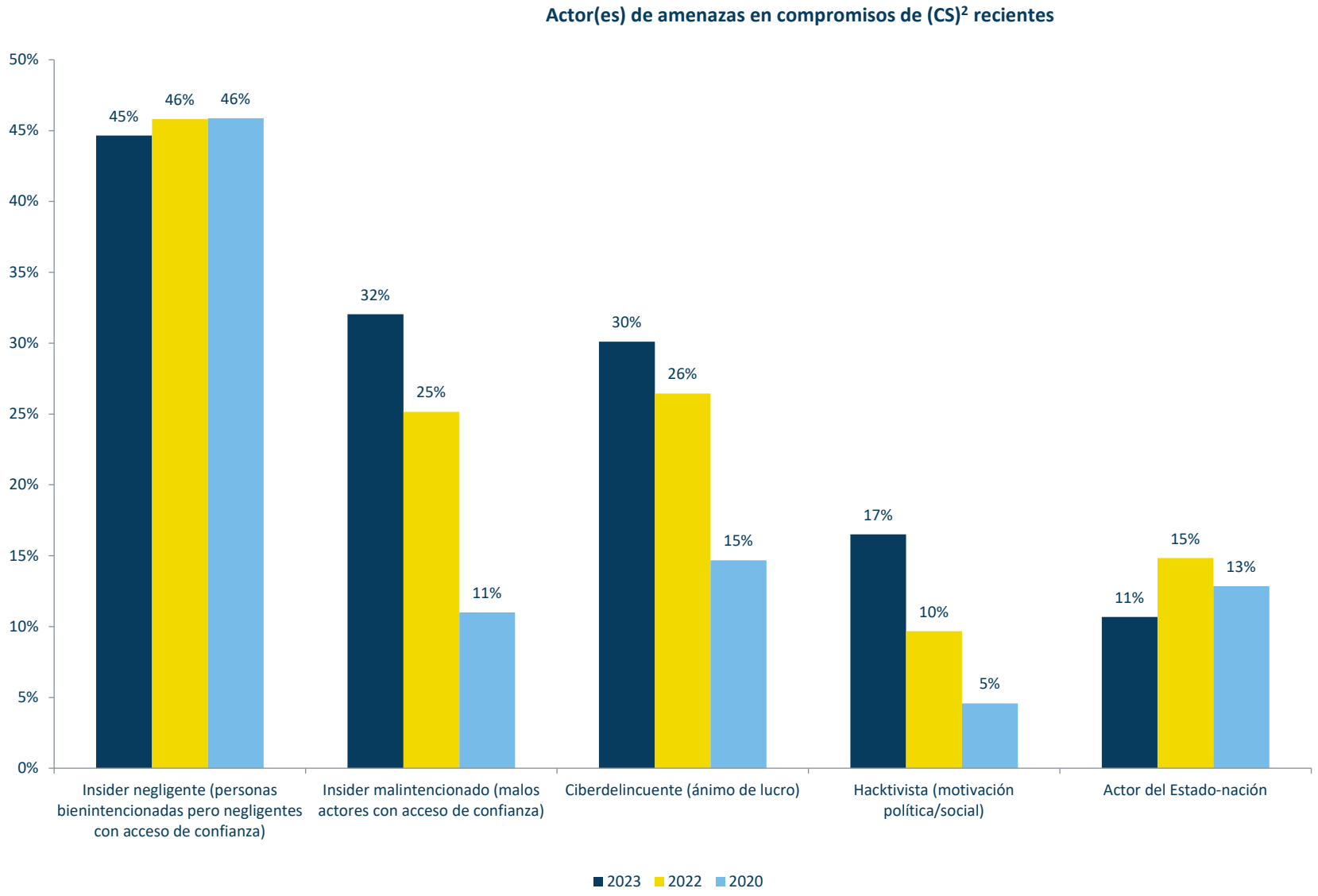
En otras ocasiones hemos examinado la frecuencia de vectores de ataque específicos en función de las diferencias regionales. Aquí buscamos tendencias interanuales y encontramos varios patrones de crecimiento claros. Es notable el aumento continuo de respuestas sobre *Proveedor/servicio en la nube comprometido* (2020 6% vs. 2023 25%), *Compromiso de red wifi* (2020 3% vs. 2023 18%) y *Sitio web de la organización comprometido* (2020 6% vs. 2023 17%) y respalda las investigaciones sobre amenazas que indican que los atacantes están ampliando su campo de acción más allá del phishing a otras partes de la superficie de ataque de sus objetivos. La Nube y la red wifi pueden atribuirse, al menos en parte, al aumento del uso de estas soluciones dentro de los entornos (CS)² en los últimos años. Observe que *Cuentas de usuarios comprometidas y Dispositivos no autorizados* son elecciones nuevas de este año, por lo que no aparecen en la información de 2020-2022. *Actualización de proveedor comprometida se agregó en 2022.*

Vectores de ataque usados en alguno de los incidentes de (CS)² en las organizaciones en los últimos 12 meses



Actores de amenazas de (CS)2 – Estudio longitudinal

Mientras que los casos de los Actores del estado-nación y del Insider negligente se mantienen relativamente estables (este último sigue siendo el más citado), cabe destacar el aumento anual de las denuncias de actividades de Hacktivistas, Ciberdelincuentes e Insider malintencionado. No encontramos diferencias regionales significativas. Los informes de los medios de comunicación y las agencias de inteligencia nacionales apoyan la creencia de que la actividad de los ciberdelincuentes con ánimo de lucro ha aumentado considerablemente en los últimos años, y nuestros resultados coinciden. Por otra parte, el aumento de los compromisos de $(CS)^2$ por parte de Insiders malintencionados no ha estado en la mira de la opinión pública. Puede ser un subproducto del aumento de las divisiones y tensiones sociales.



Lineamientos de proveedores

Principales lineamientos sobre los KPI de Clientes - Proveedores

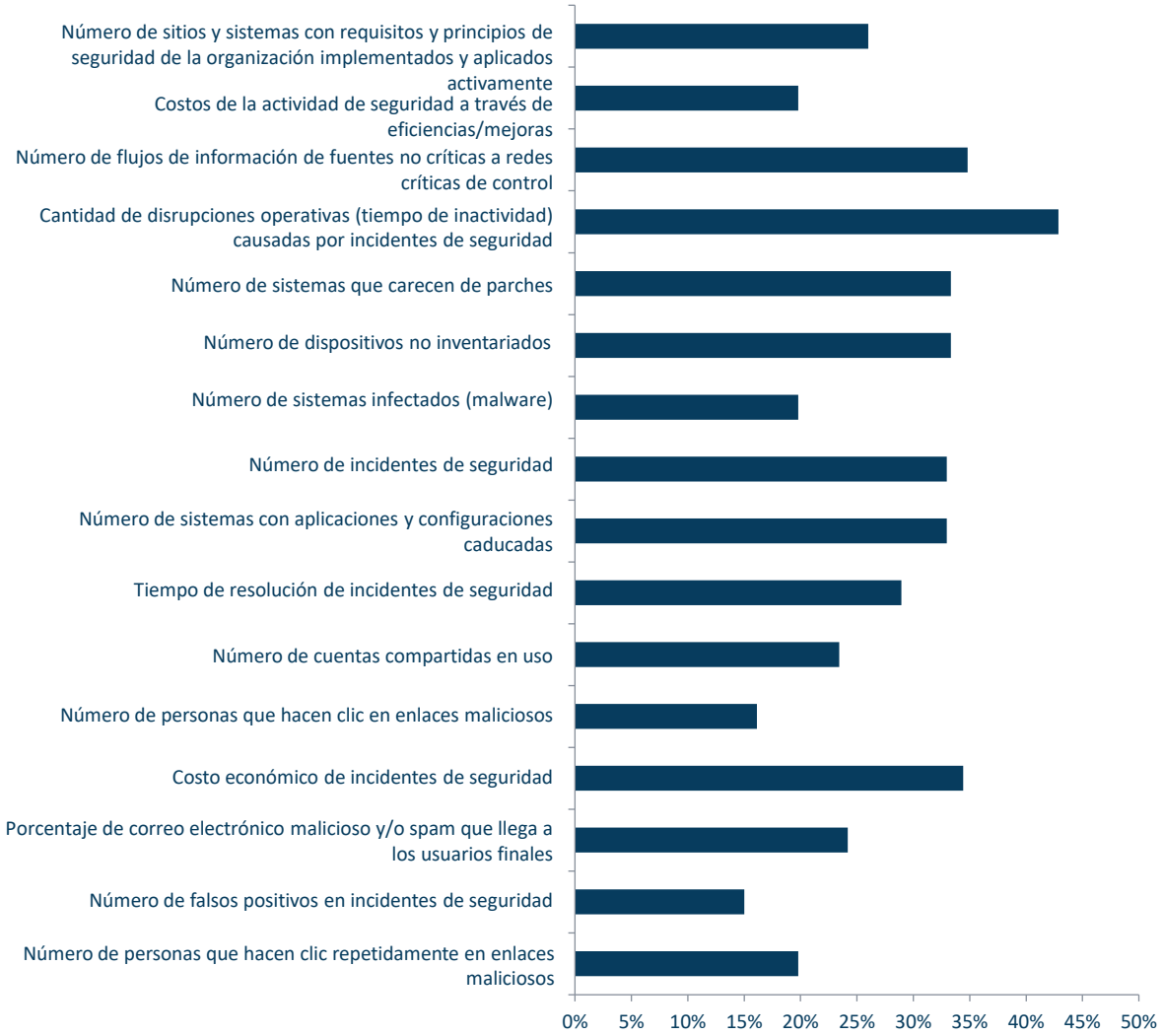
El Informe sobre amenazas de Waterfall Security and ICSStrive 2023 muestra que los ataques con consecuencias de OT aumentaron exponencialmente en los últimos 4 años.
Aquí vemos que los tres principales KPI son la disrupción operativa (tiempo de inactividad), el número de flujos de información que entran en redes críticas y los costos financieros de dichos incidentes.

Estos indicadores muestran un fuerte deseo tanto de mitigar las consecuencias como de desplegar soluciones sólidas. Estas ambiciones se ven respaldadas por potentes soluciones de ingeniería que reducen las consecuencias físicas y controlan los flujos de información, soluciones que son parte de la nueva Estrategia de ingeniería cibernética liderada por Idaho National Laboratories.

Andrew Ginter

Vice Presidente de

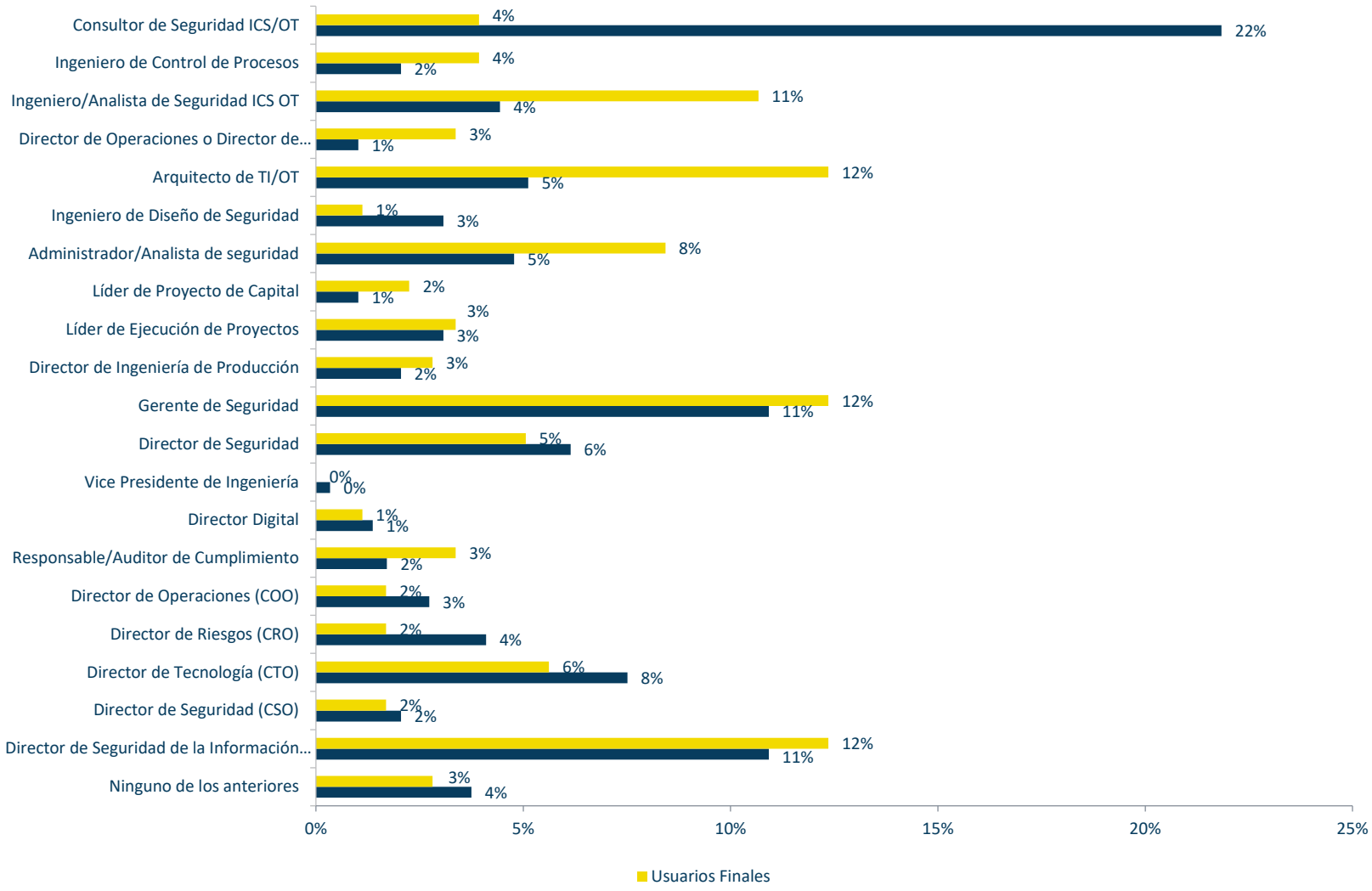
Seguridad Industrial,
Waterfall Security Solutions



Anexo A: Aspectos demográficos

Cargos de los encuestados - Usuarios finales y proveedores

Cargos de los encuestados con respecto al trabajo relacionado con la seguridad de los sistemas de control

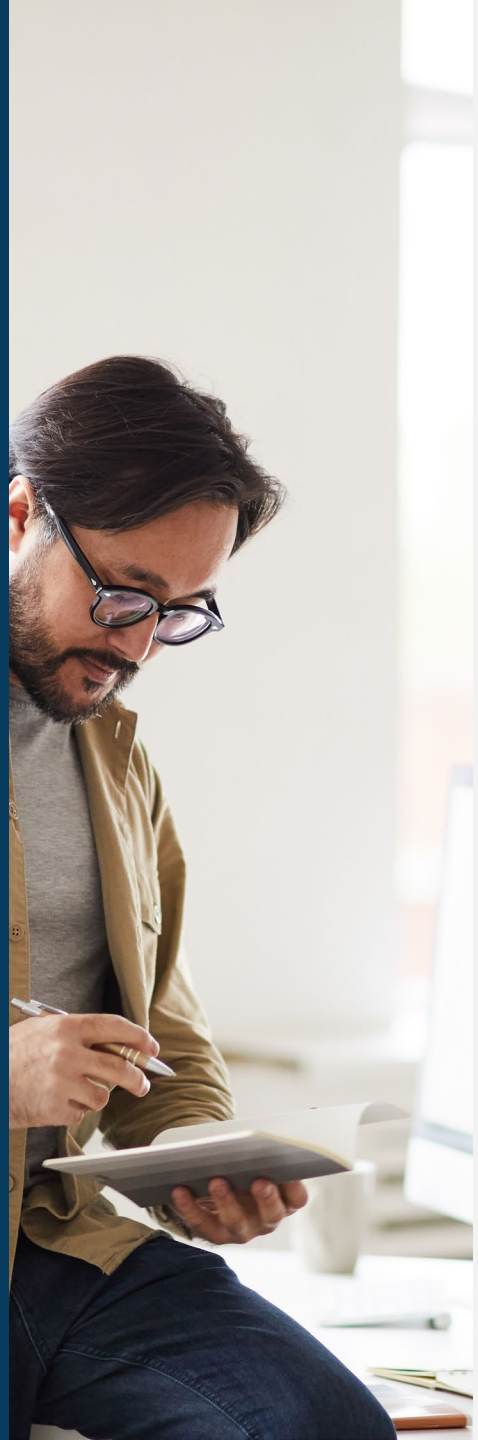


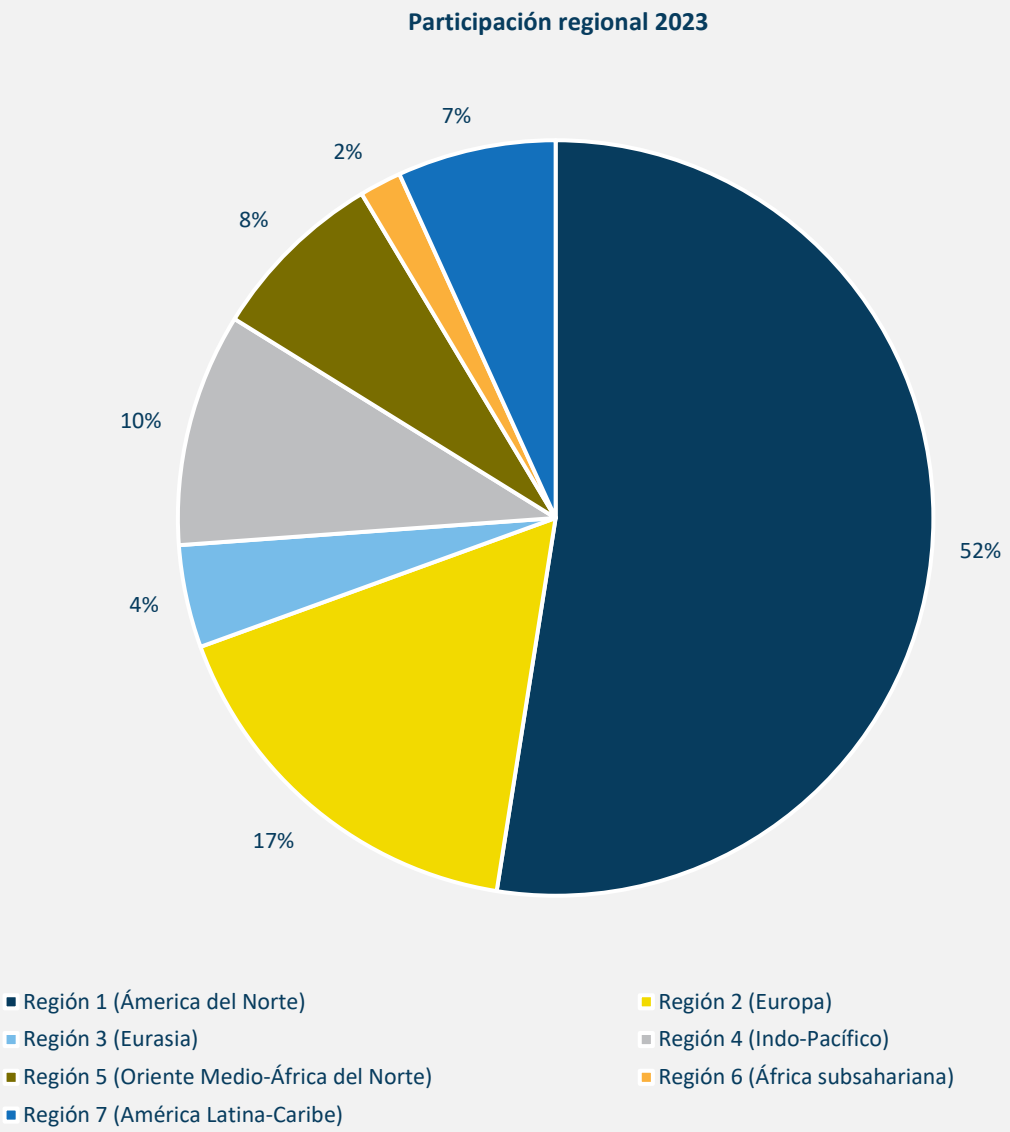
Participación por región

Control System Cybersecurity Association International abarca siete regiones:

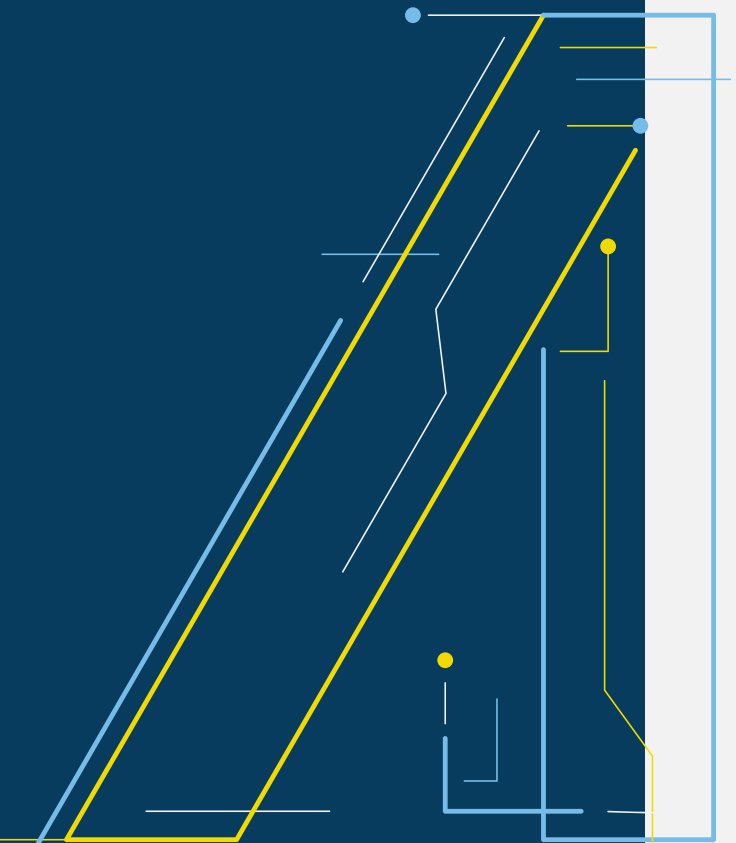
1. América del Norte
2. Europa (Central, Occidental, del Norte y del Sur)
3. Eurasia
4. Indo-Pacífico
5. Oriente Medio-África del Norte
6. África subsahariana
7. América Latina-Caribe

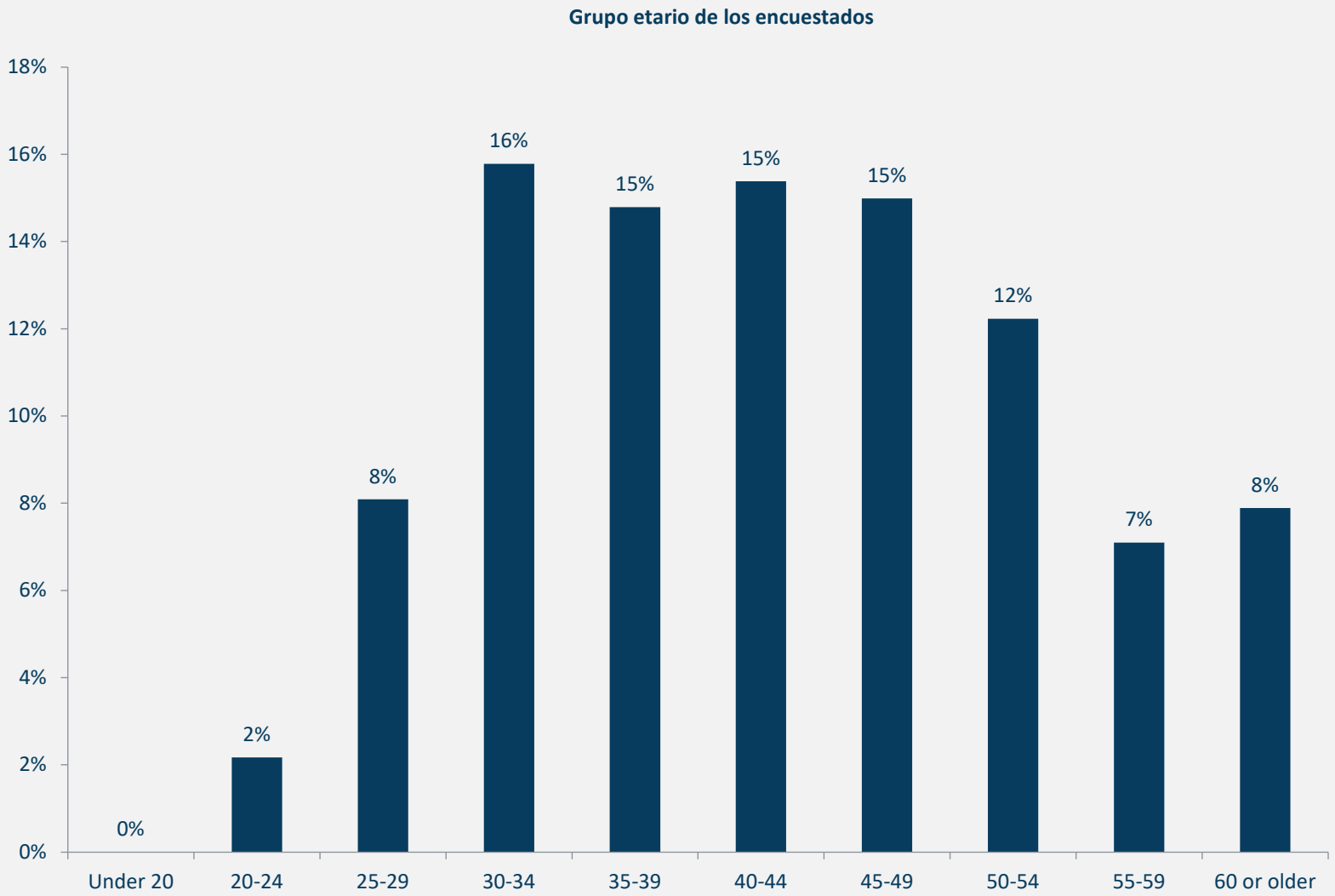
Este año la representación creció en las regiones 2, 5 y 7. Nuestro objetivo actual es aumentar la participación en todas las regiones, tanto para obtener suficientes respuestas a todas las preguntas para el análisis estadístico como para llegar a más consumidores de información sobre (CS)², ya sean profesionales, gerentes, ejecutivos o estudiantes.





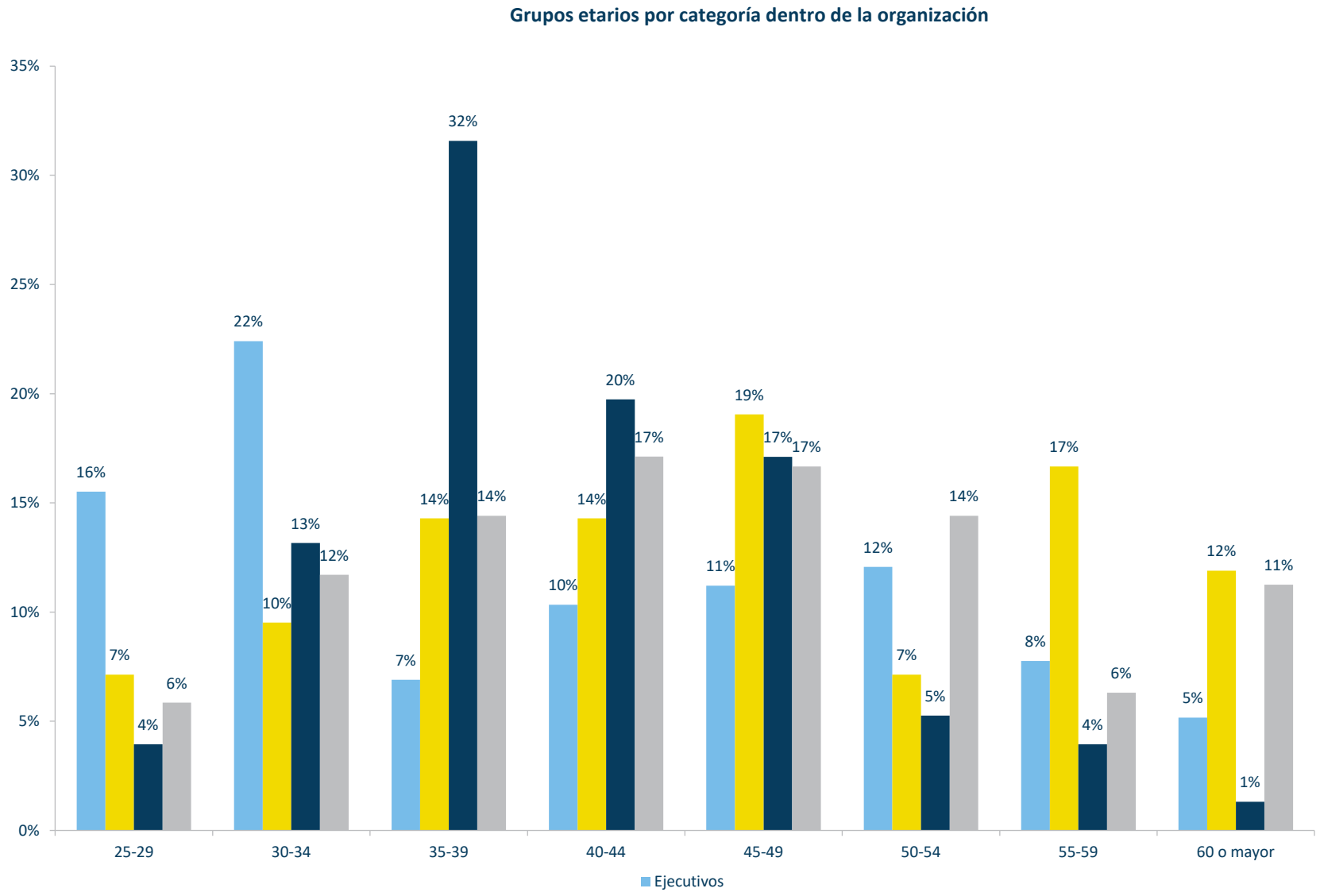
Edad de los encuestados





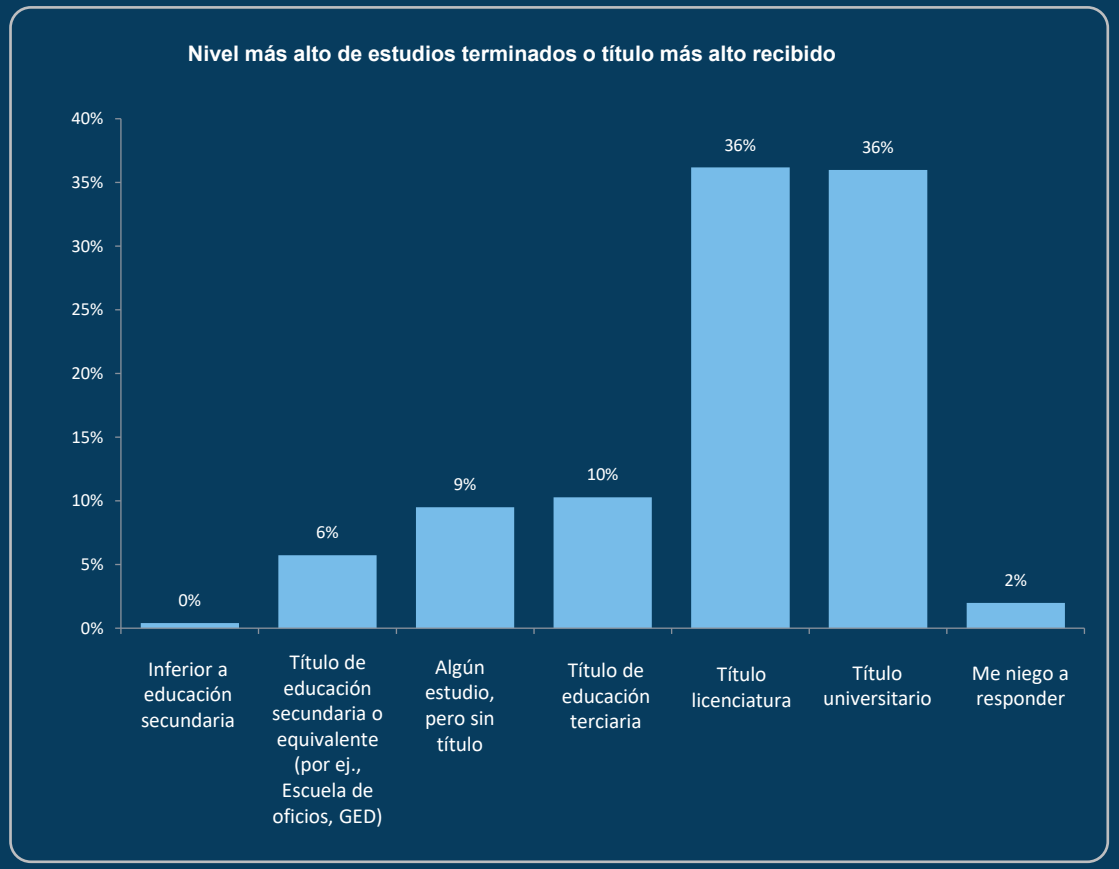
Edad de los encuestados por categoría dentro de la organización

Gran mayoría (N>60%) de los encuestados en el grupo etario de 30-50 años. Tendemos a centrarnos en gran medida en el equipo de Operaciones, ya que es el que trabaja más directamente con los activos/sistemas y constituye un banco crítico de conocimientos técnicos y experiencia que se va con ellos cuando se jubilan. Para mantener y mejorar la protección de nuestros sistemas de control es fundamental conservar ese acervo generacional y, al mismo tiempo, mantenerse al día con los avances, por lo que es positivo que los grupos que se encuentran en la mitad y el principio de sus carreras, los que aprenden de los recursos sénior, estén representadas por un número tan elevado.



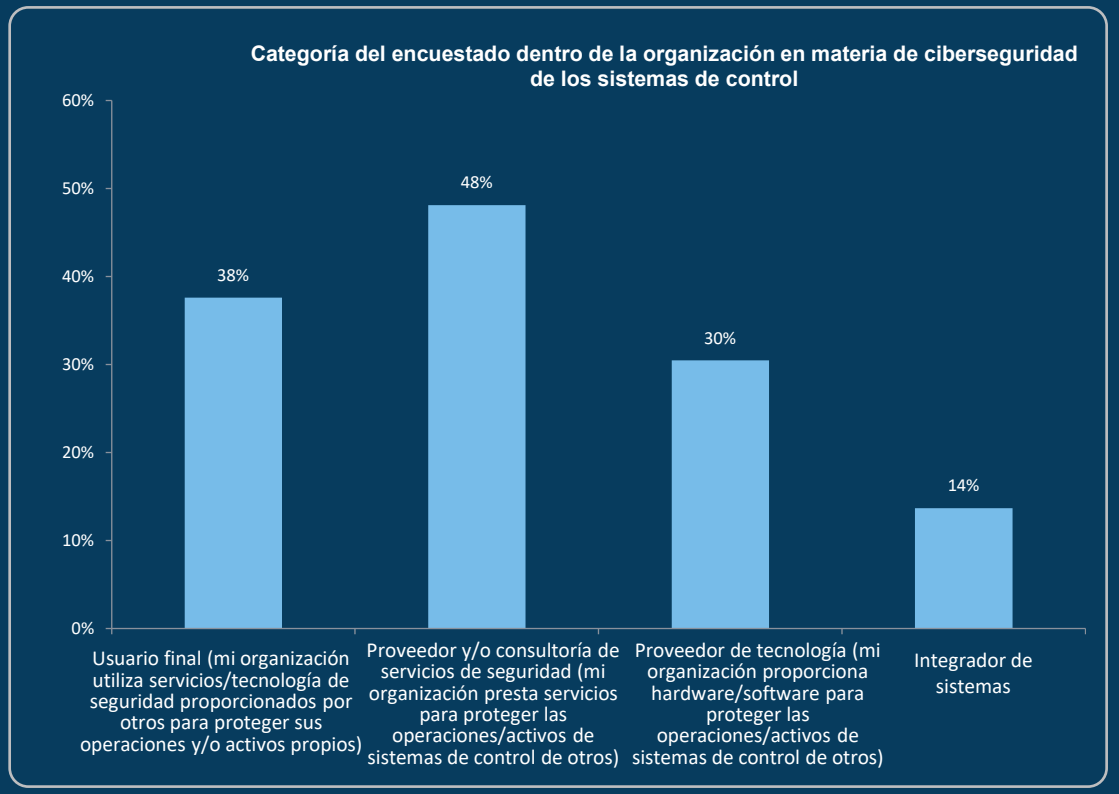
Nivel educativo de los encuestados

El perfil educativo de los participantes es muy similar al de años anteriores.



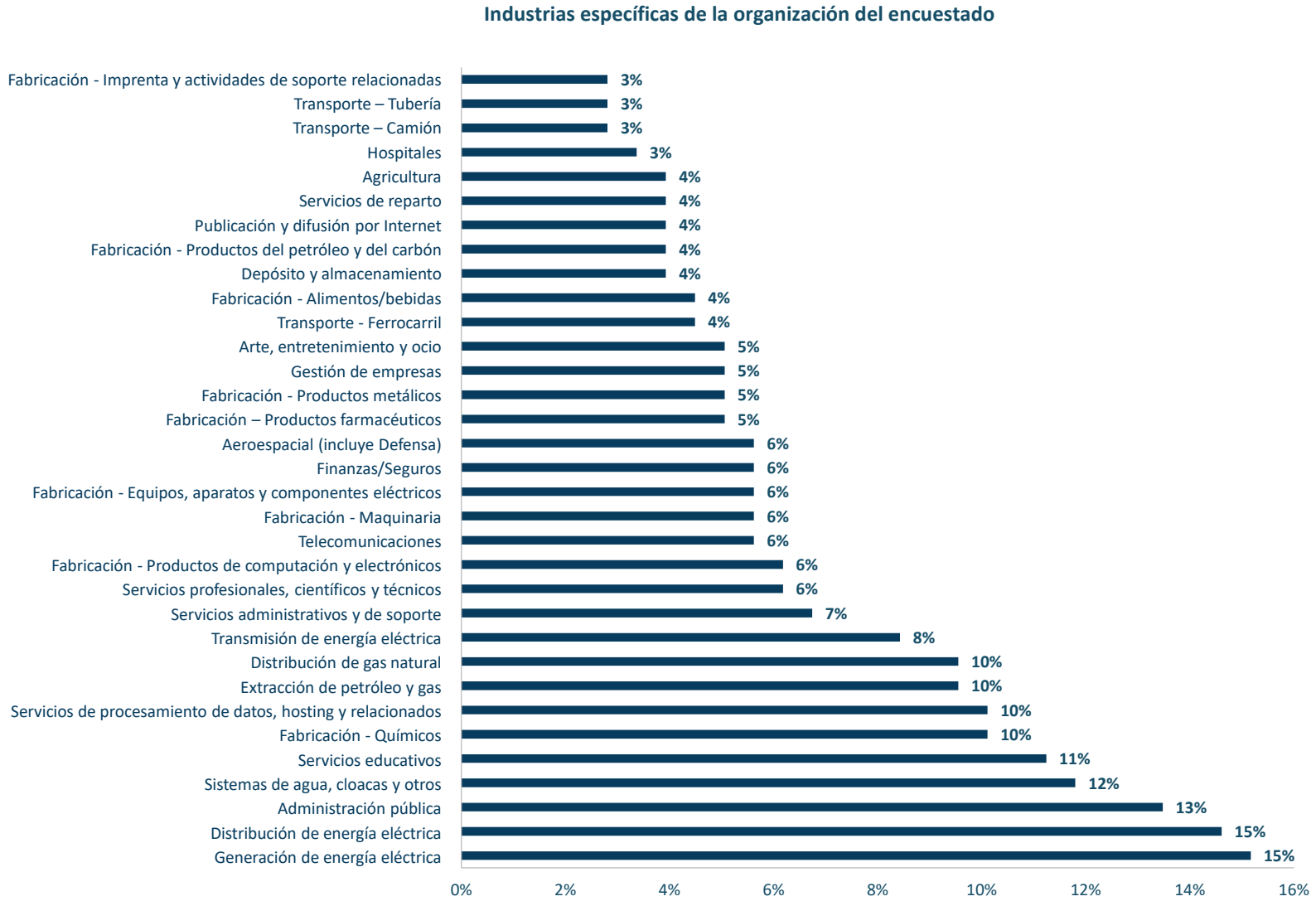
Categoría del encuestado dentro de la organización

Intercambio porcentual casi equitativo entre el Usuario Final (UF) y el Proveedor de Tecnología (TPT) (el UF baja 10 puntos, el PT sube 7). Este año se incorpora la categoría nueva de Integrador de Sistemas. Esta era una pregunta “Selecciona todas las respuestas que correspondan”, por lo que el total supera ampliamente el 100%. Este año también se incorporó la categoría “Otro”, la cual obtuvo 5% de las respuestas.



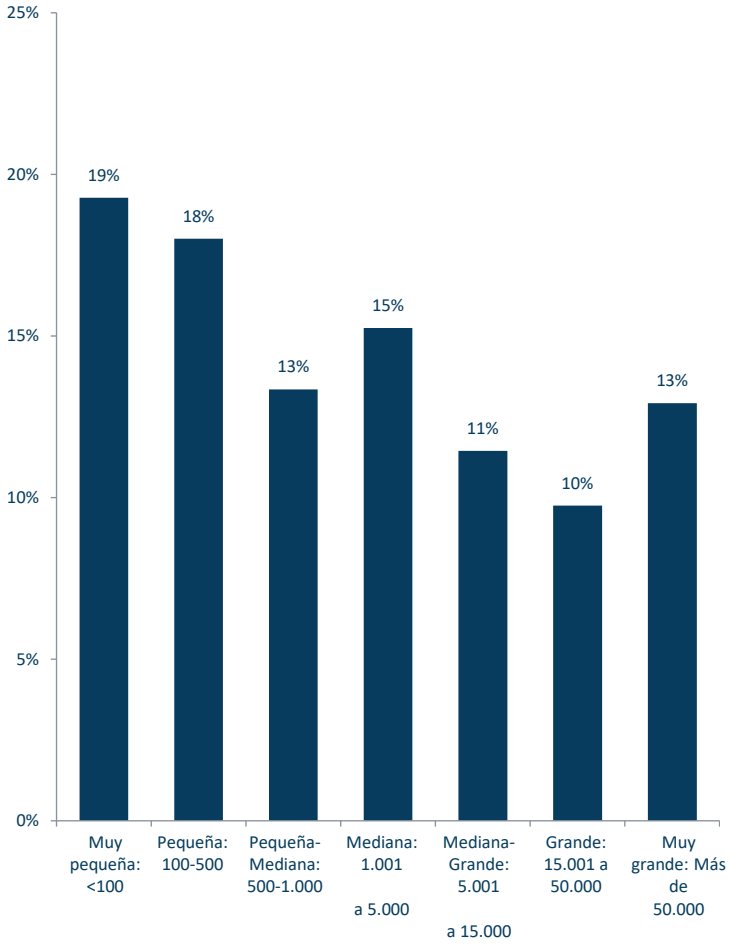
Participación por industria (solo usuarios finales)

¿A dónde acuden las organizaciones para encontrar la ayuda que necesitan para proteger sus activos, personas y operaciones de $(CS)^2$? A todos los sitios posibles, según nuestros encuestados. La respuesta destacada de Recursos internos de seguridad de IT (56,2%) sugiere que la ciberseguridad OT está siendo impulsada por los equipos de IT en la mayoría de las organizaciones, con la probabilidad concomitante de que se estén aplicando métodos y tecnologías de seguridad de IT en estos entornos.



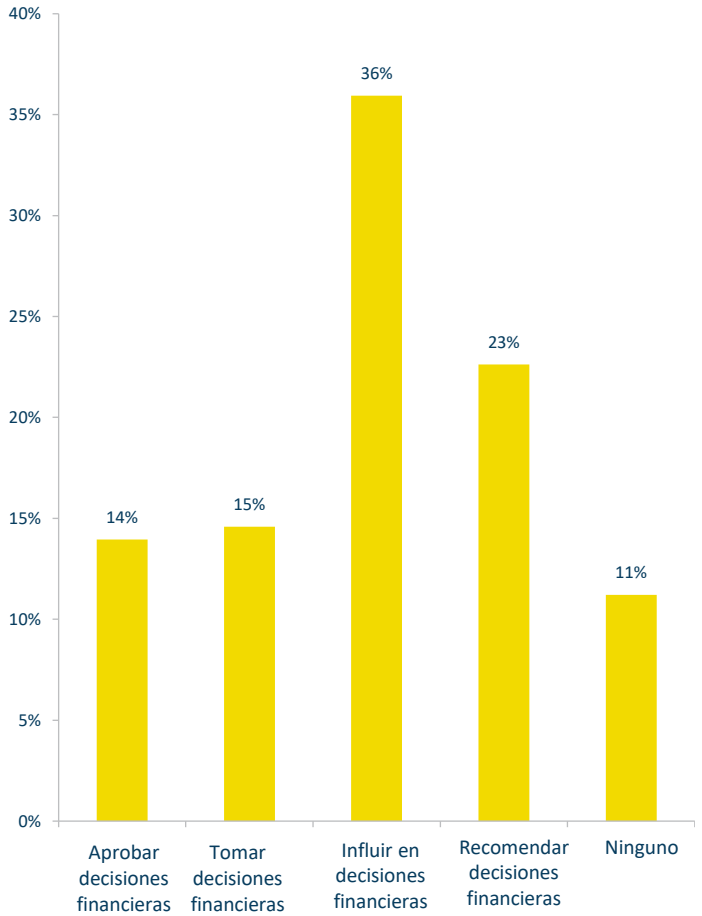
Tamaño de las organizaciones de los encuestados

Mejor estimación en cuanto al número de empleados de la organización



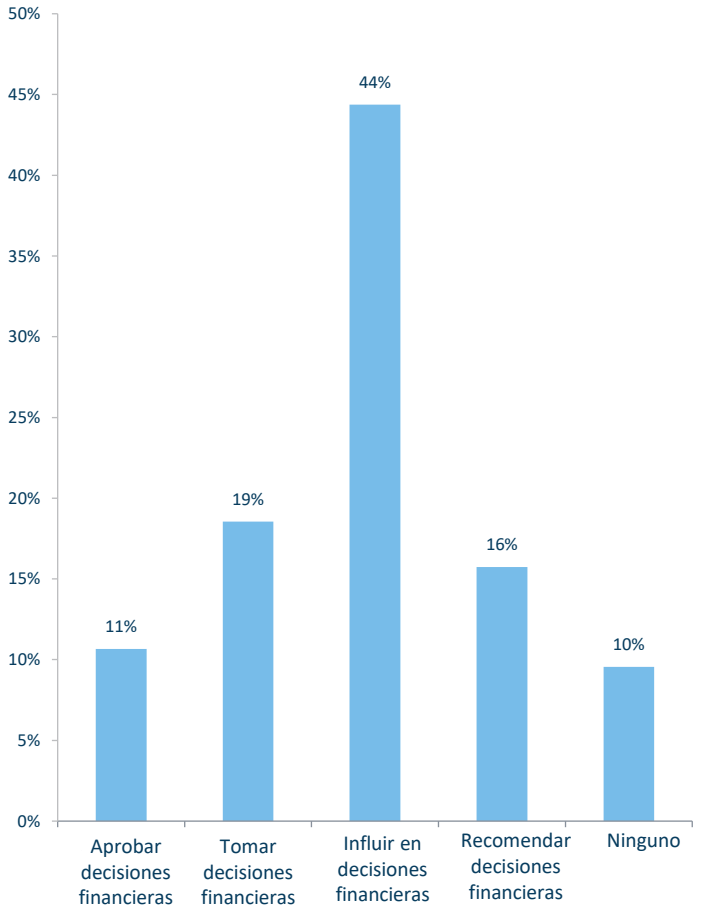
Roles de decisión de los encuestados

Rol en la toma de decisiones sobre gastos relacionados con la seguridad de los sistemas de control

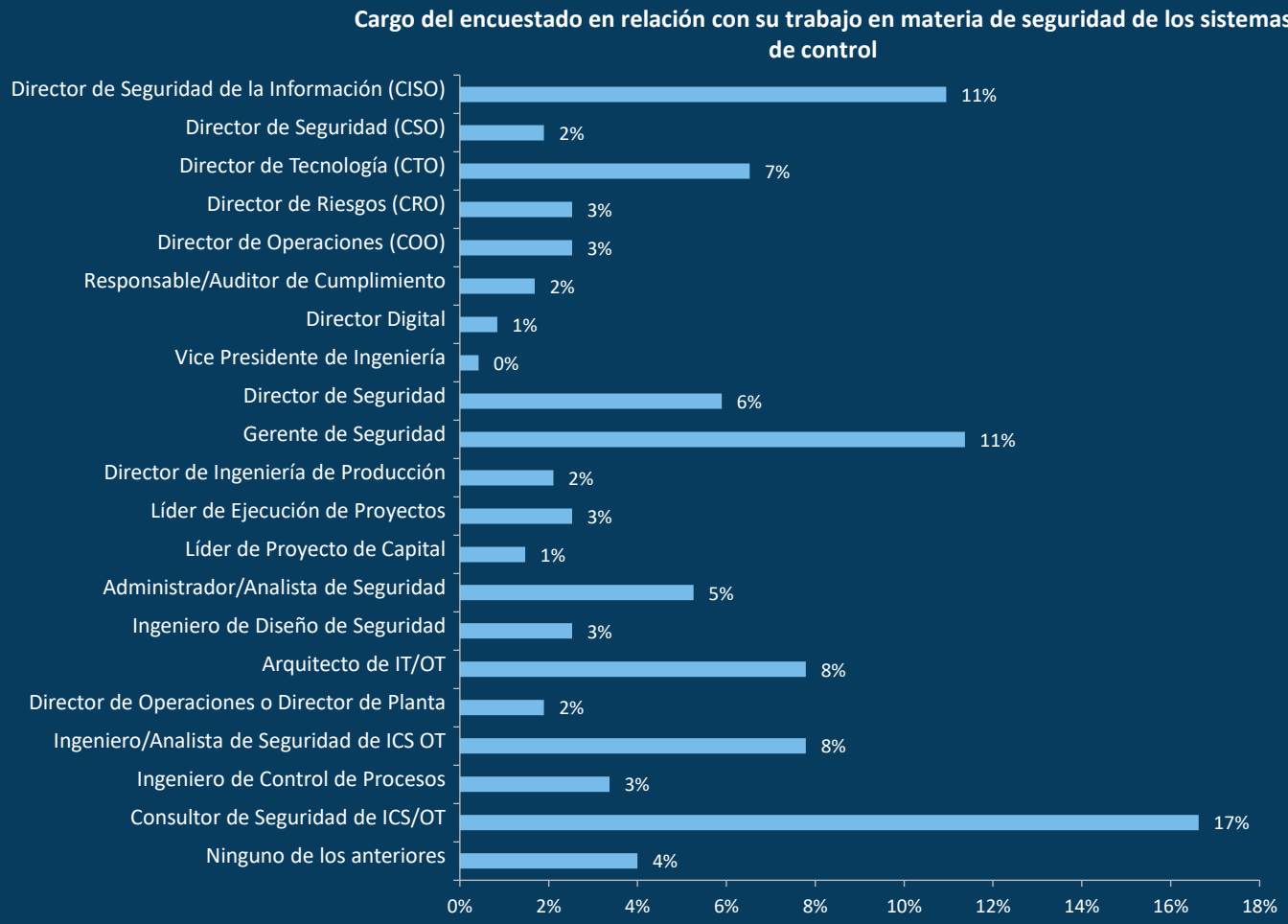


Roles de decisión de los encuestados – Solo usuarios finales

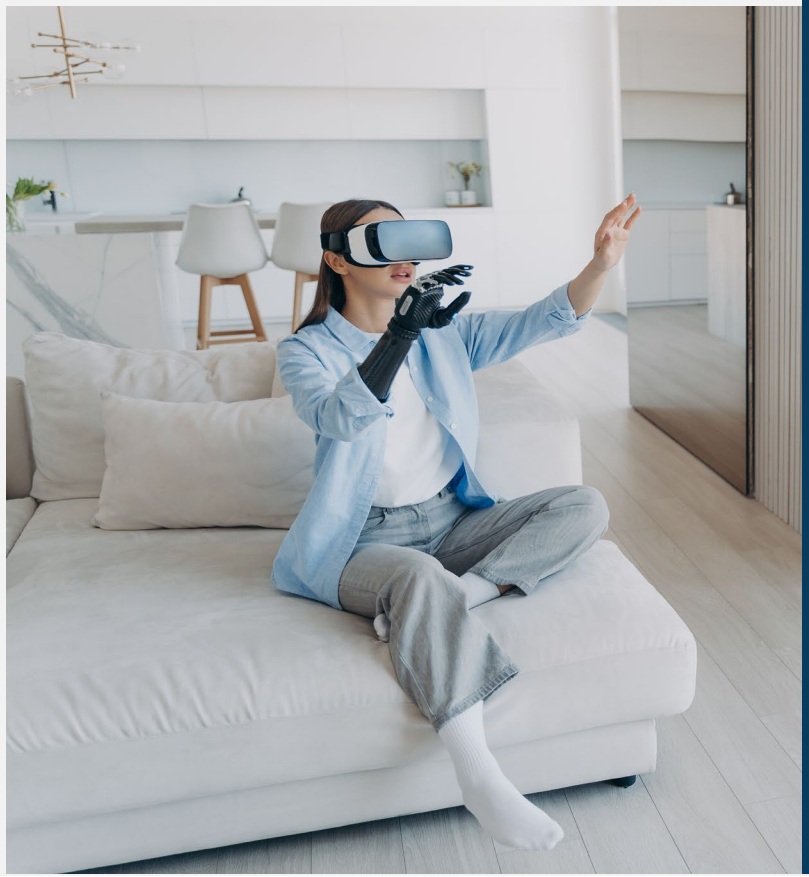
Rol de los participantes en la toma de decisiones sobre gastos relacionados con la seguridad de los sistemas de control (solo usuarios finales)

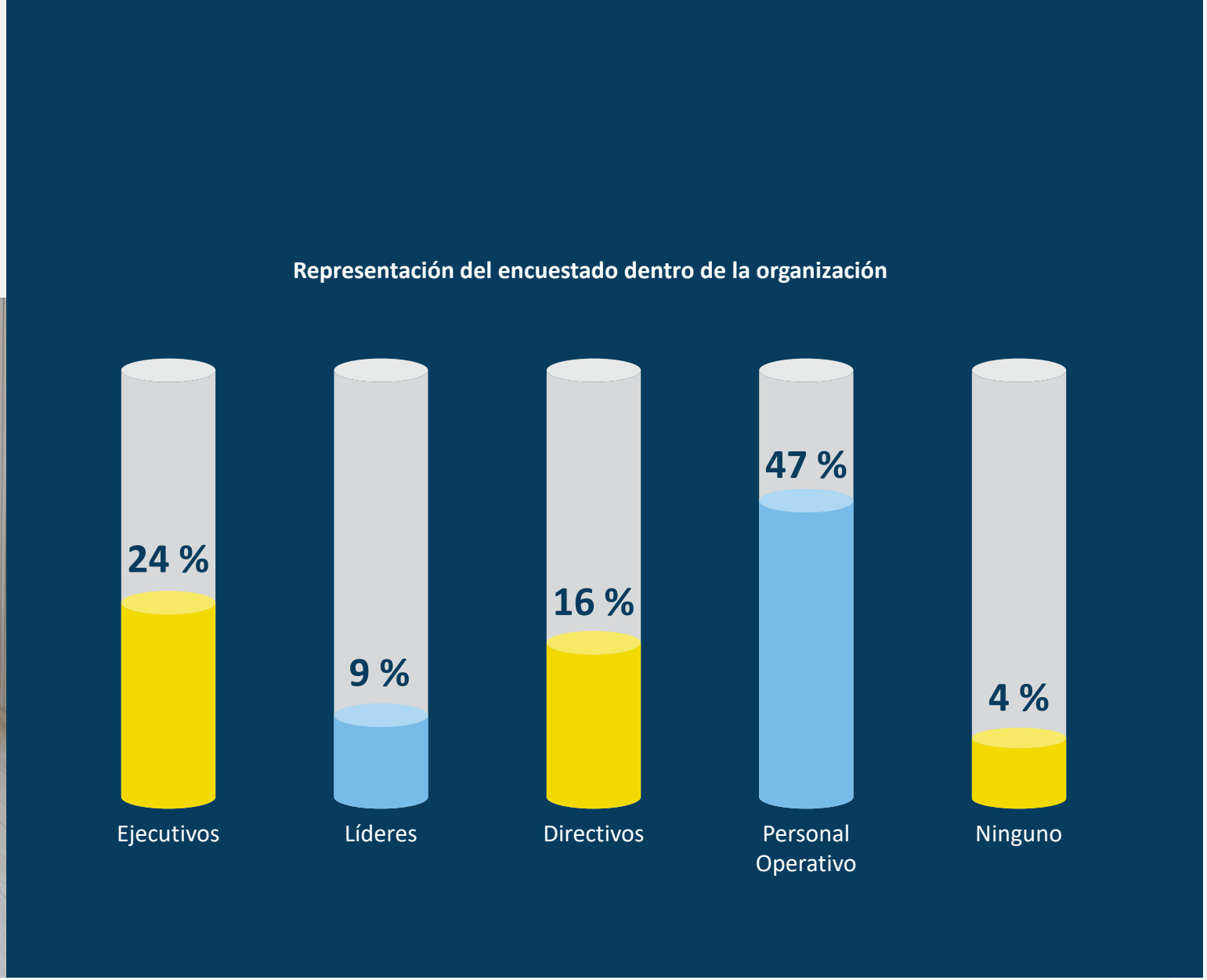


Cargo y representación del encuestado dentro de la organización



Cargo y representación del encuestado dentro de la organización (cont.)





Anexo B: Comité Directivo y Colaboradores del Informe Anual

Derek Harp

Fundador y Presidente del Comité Directivo,
Presidente de la Encuesta e Informe Anual,
Coautor de (CS)²AI

derek.harp@cs²ai.org

Bengt Gregory-Brown

Cofundador y Presidente,
Director de la Encuesta e Informe Anual,
Diseñador y Analista Líder, Coautor de (CS)²AI

bengt.gregory-brown@cs²ai

Walter Risi

Enlace Socios de Alianzas Estratégicas de (CS)²AI

Equipos de Diseño de Encuestas y Análisis de Informes

Líder Global de Ciberseguridad OT,
KPMG International y
Socio y Líder de Consulting,
KPMG en Argentina

wrisi@kpmg.com.ar

Andrew Ginter

Equipos de Diseño de Encuestas y Análisis de Informes
Miembro Fundador de (CS)²AI

Autor y Expositor
Vice Presidente de Seguridad Industrial
Waterfall Security Solutions

andrew.ginter@waterfall-security.com

Queremos agradecer a las siguientes personas su aporte al análisis, diseño y demás tareas de elaboración de este informe.

Ana Girdner, Vice Presidenta de Seguridad, Cognite

Brent Huston, CEO, MicroSolved

Daryl Haegley, Director Técnico, Ciberresiliencia de Sistemas de Control, Departamento de Defensa de los Estados Unidos

Mark Bristow, Director, CIPIC MITRE

Michael Chipley, Presidente, The PMC Group

Rees Machtemes, Director de Seguridad Industrial, Waterfall Security Solutions

Rod Locke, Director de Gestión de Productos, Fortinet

Steve Mustard, Presidente & CEO, National Automation

Vivek Ponnada, Director de Soluciones Tecnológicas, Nozomi Networks

Anish Mitra, Director, KPMG en India

Hossain Alshedoki, Director, KPMG en Arabia Saudita

Jayne Goble, Directora, KPMG en Reino Unido

Craig Morris, Director, KPMG en Australia

Joshua Turner, Consultor, KPMG en Japón

Brad Raiford, Director, KPMG en Estados Unidos

Pablo Almada, Socio, KPMG en Argentina

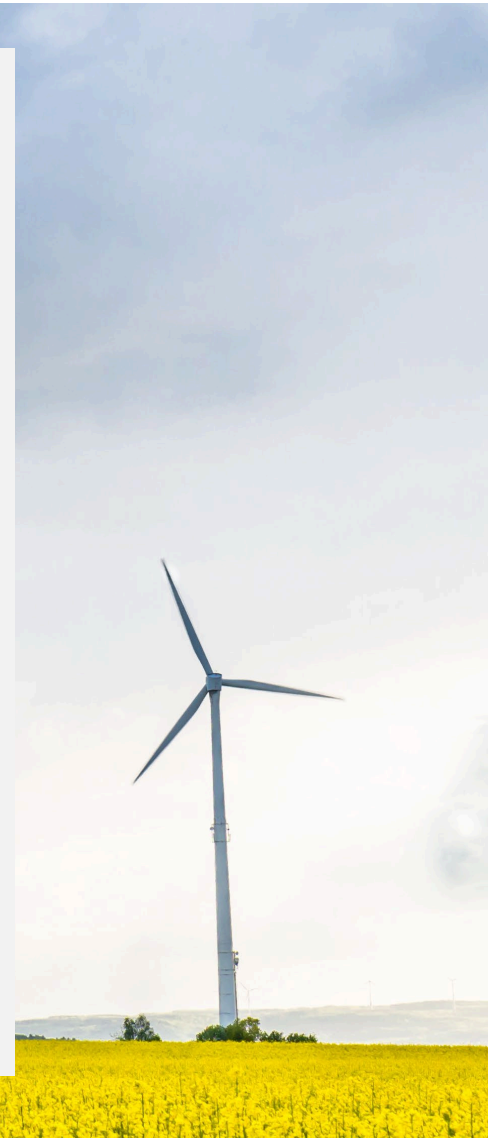
Thomas Gronenwald, Gerente Senior, KPMG en Alemania

Marko Vogel, Socio, KPMG en Alemania

Eddie Toh, Socio, KPMG en Singapur

Sarah Puziewicz, Senior, KPMG en Alemania

Valentin Steinforth, Consultor en Ciberseguridad, KPMG en Alemania



Anexo C: Acerca de (CS)²AI

Visión

Fortalecer las infraestructuras críticas globales fomentando el desarrollo y la generación de contactos entre pares en materia de ciberseguridad de sistemas de control.

Misión

Una organización internacional que posibilita la vinculación entre pares y brinda apoyo desde los primeros esfuerzos.

Objetivos

- Contactos profesionales
- Alianzas globales
- Desarrollo profesional
- Llegada a los miembros de la comunidad
- Oportunidades de liderazgo

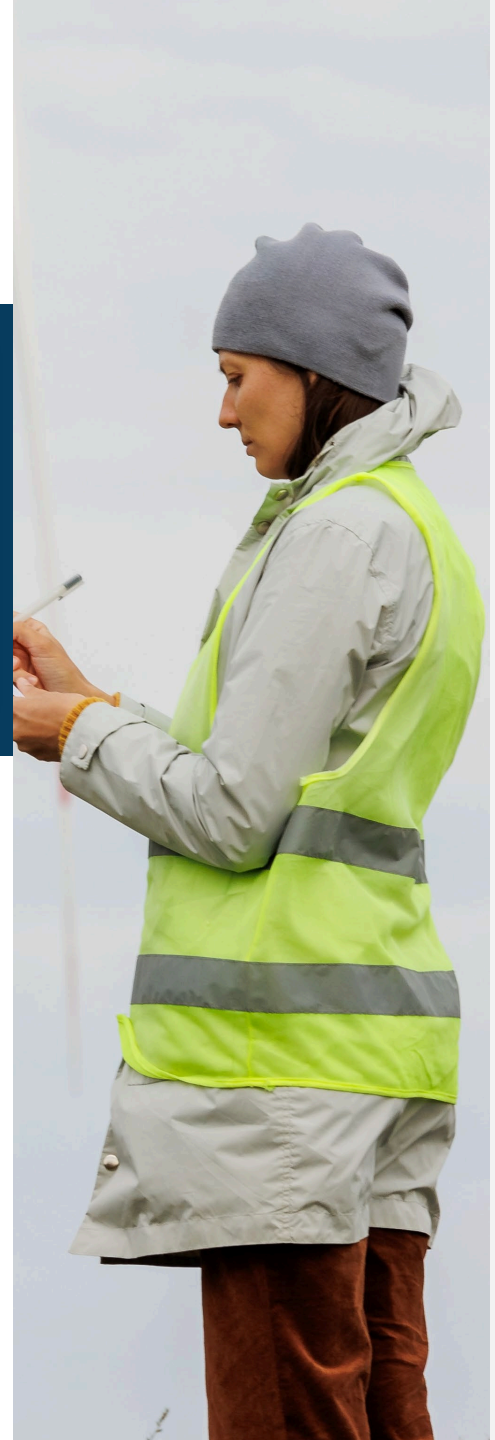
(CS)²AI ("See-Say" abreviado en inglés) es una entidad global sin fines de lucro en rápido crecimiento, que cuenta con 34.000 miembros en todo el mundo. La principal organización mundial sin fines de lucro de desarrollo de mano de obra, que brinda apoyo a los profesionales de todos los niveles encargados de garantizar la seguridad de los sistemas de control. Proporcionamos la plataforma para que los miembros se ayuden entre sí, fomentamos el intercambio significativo entre pares, continuamos la formación profesional y apoyamos directamente el desarrollo profesional de la ciberseguridad en todos los sentidos.

https://www.cs2ai.org

Contacto entre pares alrededor del mundo

Como miembro de (CS)²AI, accederá a una comunidad global de profesionales de ciberseguridad de sistemas de control motivados para mejorar y desarrollarse personal y profesionalmente en este campo tan crítico y relevante. (CS)²AI ofrece un lugar para conectarse entre pares, interactuar en grupos reducidos con los principales expertos del sector, intercambiar experiencias, desafíos y mejores prácticas, y los recursos necesarios para desarrollarse y crecer. Explore la creciente gama de oportunidades exclusivas para los miembros de (CS)²AI diseñadas para ayudar a alcanzar el siguiente nivel en su carrera profesional.

Si aún no es miembro activo de la Asociación Internacional de Ciberseguridad de Sistemas de Control, lo invitamos a sumarse a la iniciativa conjunta de ayuda entre los miembros de nuestra comunidad INVOLUCRÁNDOSE hoy mismo. Nuestra asociación cuenta con muchas formas de contribución, ya sea como miembro global, expositor, profesor, mentor, socio, colaborador, miembro del comité, miembro de (CS)²AI o participante de una investigación.



Anexo D: Patrocinadores del Informe

Patrocinador Nivel 1

KPMG

Patrocinador Nivel 3

Fortinet
Waterfall Security Solutions

Patrocinador Nivel 5

Opscura
Network Perception

Patrocinador Nivel 6

Bridewell

Walter Risi

Líder Global de Ciberseguridad OT
KPMG International y
Socio y Líder de Consultoría
KPMG en Argentina

Pablo Almada

Líder Global Adjunto de Ciberseguridad OT
KPMG International y
Socio y Líder de Ciberseguridad OT
KPMG en Argentina

http://www.cs2ai.org/

CREATE: CRT152075