Caracterización del uso y necesidades potenciales de *ciberseguridad*

en empresas costarricenses

Erick J. Apuy
Dirección de Inteligencia Comercial
Mayo 2022

El presente documento es de carácter público y gratuito y fue realizado por la Promotora del Comercio Exterior de Costa Rica con base en la información que ha sido recopilada de buena fe y proveniente de fuentes legítimas.

El objetivo de este estudio es brindar información de carácter general sobre el tema analizado, por lo que su contenido no está destinado a resolver problemas específicos o a brindar asesoría puntual para un determinado individuo o entidad pública o privada.

Por la misma naturaleza de esta publicación, PROCOMER no tendrá responsabilidad alguna sobre la utilización o interpretación que se le dé a este documento, ni responderá por ningún supuesto daño o perjuicio directo o indirecto derivado del contenido de este estudio.

Dirección de Inteligencia Comercial, PROCOMER

Resumen Ejecutivo

Con base en la muestra encuestada, se identifica que **siete de cada diez** empresas costarricenses (73%) ha invertido o invierte actualmente en ciberseguridad, mientras que las restantes no lo han hecho nunca. Del total, destaca una **población crítica** de empresas, el 8% de la muestra, que a pesar de que nunca han gastado en ciberseguridad tampoco contempla hacerlo en el corto plazo, es decir, **resultan los más vulnerables** y expuestos ante amenazas de seguridad.

Entre las empresas que invierten, la **protección** mediante la aplicación de controles para mitigar riesgos y proteger activos es su principal prioridad; seguido de otros intereses como la **detección** de amenazas (para el 85% de empresas); y la **identificación** de las probabilidades sobre riesgos (81%). Este perfil de prioridades refleja que el abordaje de ciberseguridad en las empresas es mayormente **preventivo**, pero con poco enfoque en acciones centradas en **respuesta** (38%) y **recuperación** ante ataques (66%). Por otra parte, si se considera que el **89% de encuestados se ha visto afectado por ciberdelincuencia**, es claro que la continuidad del negocio ante estos ataques resulta tan importante como las acciones preventivas.

Entre las soluciones más utilizadas están paquetes habituales e imprescindibles de seguridad cotidiana, como antivirus (91% de empresas), firewall (87%); antimalware (85%) y VPNs (81%). No obstante, se evidencia que otras **plataformas más exhaustivas y especializadas tienen poca participación**, por ejemplo, el XDR (23%), Zero Trust (17%) o SASE (15%); sistemas hacia los que las empresas deberían de orientarse cada vez más, así como también hacia la **gobernanza** de la ciberseguridad (40% únicamente).

En conjunto, las empresas analizadas indican un **presupuesto sumado de $15,1 millones de USD** y se evidencia que el gasto en ciberseguridad, como parte de la inversión total en tecnología, representa **una quinta parte del presupuesto**, que si bien puede parecer bajo, resulta congruente con la tasa promedio en el mundo (21% en 2021). No obstante, si se considera que en el último año el presupuesto global aumentó un 13% en promedio, es previsible que las empresas locales se vean también obligadas a **incrementarlo de forma sostenida**, lo cual de hecho es acorde con las **perspectivas de gasto** en el corto plazo entre la muestra, con un 72% de ella que considera necesita aumentar su presupuesto de ciberseguridad; mientras que tan solo el 2% lo reducirá.

Para Costa Rica, son los virus, phishing y malware las infecciones más comunes, atacando a cerca de 6 de cada 10 empresas. No obstante es el **Ransomware**, que ha afectado al 37% de empresas, el que señalan como su **mayor amenaza**; algo previsible al considerar que es uno de los ataques de mayor crecimiento en el mundo (+78% en 2021 vs año anterior). En general, es claro que **la ciberseguridad es una necesidad, prioridad y obligación país;** una que involucra de manera inescapable a todos los sectores del ecosistema, haciendo un llamado a la creación de sinergias e intercambio de experiencias para el fortalecimiento de capacidades.

Objetivo principal

Caracterizar la demanda potencial de servicios de ciberseguridad entre empresas costarricenses de los sectores varios, con énfasis en banca-finanzas, industria alimentaria y químico-farmacéutico; y su vinculación con la oferta local.

Objetivos específicos

1. Mostrar el desempeño general de Costa Rica en indicadores internacionales en materia de ciberseguridad.
2. Perfilar brevemente la oferta de servicios de ciberseguridad en Costa Rica.
3. Conocer el contexto actual sobre el ecosistema de ciberseguridad en el país.
4. Comprender las necesidades tecnológicas de servicios de ciberseguridad entre una muestra de empresas pertenecientes a los sectores definidos, cómo estas se satisfacen y su proceso de operativización en sus compras (niveles de seguridad actual vs necesidades).
5. Conocer las experiencias en que la oferta se vincula con sus clientes en ámbitos de ciberseguridad.

Contenido

a. **Breve contexto de la ciberseguridad en Costa Rica**

b. **Perfil de la muestra encuestada**

1. **Capítulo 1:** Caracterización del uso y necesidades potenciales de ciberseguridad entre empresas costarricenses

2. **Capítulo 2:** Necesidades potenciales y principales amenazas de ciberseguridad a las que se han expuesto las empresas

3. **Capítulo 3:** Características de la oferta costarricense de ciberseguridad

Metodología

El desarrollo de esta investigación se sustentó en la siguiente metodología:

a. **Reunión y entrevistas a actores del ecosistema local de ciberseguridad:**
   a. Empresas demandantes de ciberseguridad
   b. Desarrolladores de tecnología
   c. Cámaras y agrupaciones vinculadas

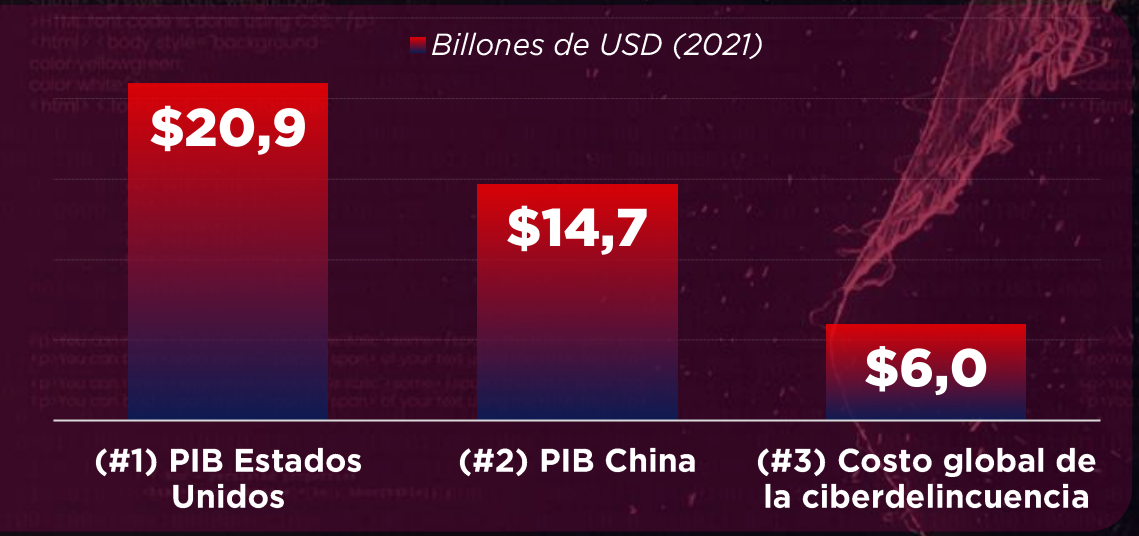
b. **Diseño y aplicación de encuesta: (entre el 09 de marzo y el 08 de abril, 2022)**
   - Encuesta #1: entre empresas usuarias de ciberseguridad, de naturaleza pública y privada.
   - Encuesta #2: entre empresas costarricenses oferentes de ciberseguridad.

c. **Análisis y procesamiento de datos.**

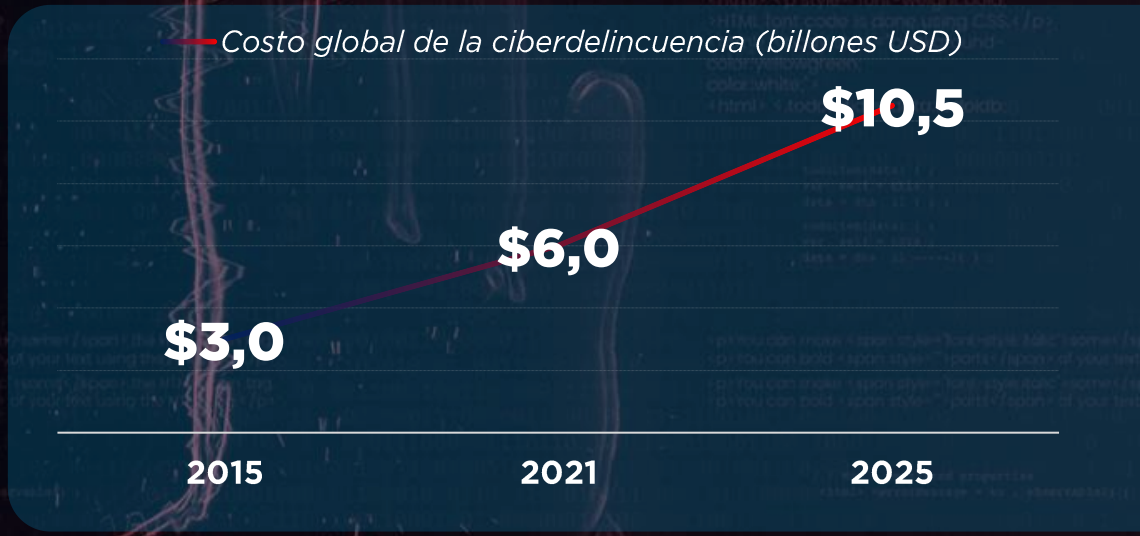
a. **Desarrollo del informe final y presentación pública al ecosistema.**

a. Breve contexto de la ciberseguridad en Costa Rica

El costo global de la ciberdelincuencia alcanzó **$6 billones de USD** en 2021. En perspectiva, equivaldría a la 3ra economía más grande en el mundo según PIB



A 2025 se proyecta que la ciberdelincuencia global supere los **$10,5 billones de USD**, un crecimiento anual promedio del **15%** entre 2021-25



COSTA RICA

En 2020 el país sufrió al menos **201 millones de ciberataques**, caracterizados por un alto grado de sofisticación y eficiencia; una alta incidencia de phishing con archivos maliciosos; malware basado en web y nuevas metodologías basadas en inteligencia artificial, además de botnets enfocados en dispositivos de IoT

Fuente: Cybersecurity Ventures / Fortinet

1” 2” 3” 4” 5” 6” 7” 8” 9” 10”

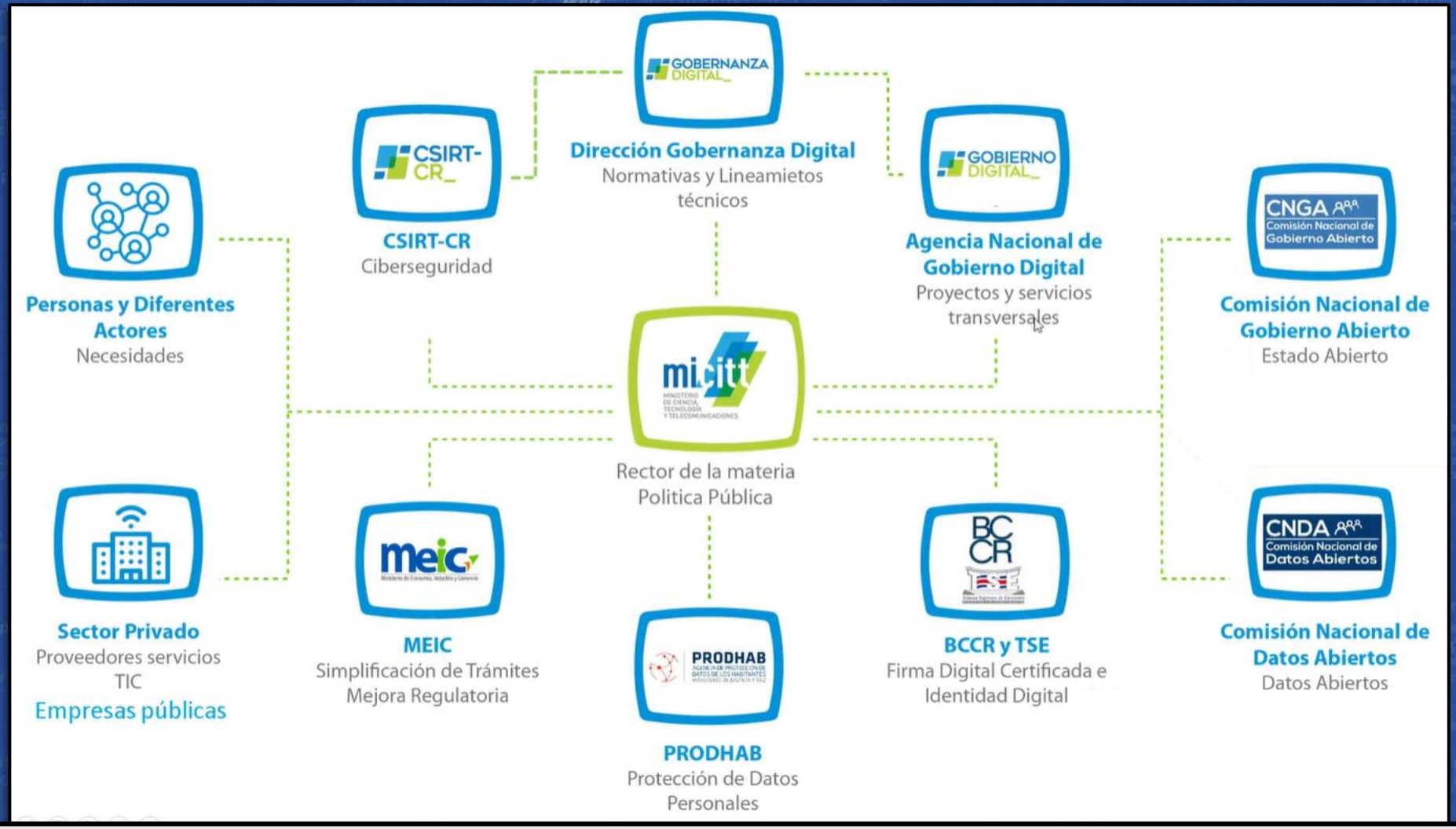
En los **10 segundos** que se tarda en leer esta información, se han registrado pérdidas en el mundo estimadas en **$1.900.000 USD** producto de la ciberdelincuencia

COSTA RICA

Si se tardase **1 hora** en abordar y detallar esta investigación, al finalizar, Costa Rica habría sido expuesto a cerca de **22.945 ataques cibernéticos** en promedio

Fuente: Cybersecurity Ventures / Fortinet

Ecosistema nacional de la ciberseguridad



El Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) es el rector Estatal en política pública sobre ciberseguridad, encargado de la estrategia país en este ámbito y el responsable de articular todas las acciones entre entidades públicas y privadas del ecosistema vinculado, así como de promover la participación de todas las partes interesadas, incluidos CSIRT-CR, PRODHAB, la Unidad de Delitos Informáticos del OIJ y otros actores relevantes como, la SUTEL, los proveedores de servicios de internet y administradores de infraestructura crítica

Fuente: MICITT

Costa Rica: desempeño en ciberseguridad

Diferentes indicadores globales miden el desempeño de Costa Rica en materia de ciberseguridad o desarrollo digital. En promedio, el país se ubica en la posición #61 en el mundo (de 139), aunque con una puntuación competitiva con respecto a los demás países de América, rondando en la posición #6, superado normalmente por Estados Unidos, Canadá, Chile, Uruguay o Paraguay.

De conformidad con el BID, Costa Rica muestra oportunidades de mejora en los siguientes indicadores: **i) protección de infraestructura crítica; ii) manejo de crisis; iii) defensa cibernética; iv) controles criptográficos; y v) cumplimiento de estándares**

Global Cybersecurity Index
ITU (2020; 182 países)
- #76 en el mundo
- #8 en América

National Cyber Security Index
(2020; 160 países)
- #59 en el mundo
- #6 en América

Network Readiness Index
(2021; 130 países)
- #56 en el mundo (ranking general)
  #81 en indicador ciberseguridad
- #5 en América

E-Government Development Index
ONU (2020; 193 países)
- #56 en el mundo
- #7 en América

Global Innovation Index
OMPI (2020; 132 países)
- #59 en el mundo
- #3 en América

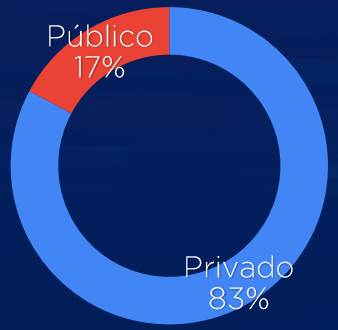
Fuente: ONU, OMPI, ITU, NCSI, BID

b. Perfil de la muestra encuestada

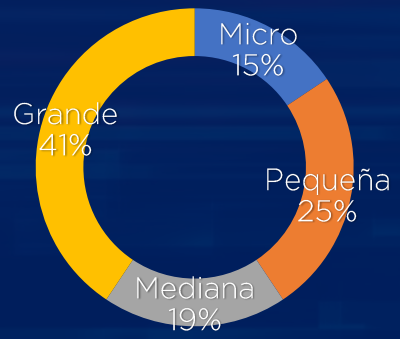
Perfil de participantes: se encuestó a un total de 64 empresas demandantes de diferentes sectores, de las cuales 73% de ellas invierten actualmente en ciberseguridad o lo ha hecho recientemente; mientras que el 27% restante nunca ha invertido. Para esta investigación, se ha dividido el análisis de ambas poblaciones en dos capítulos diferentes.

Cantidad total de encuestados:	64 empresas
Perfil de participantes:	• CTO/coordinador de informática – **40%** • CEO/gerencia general – **25%** • CISO – **11%** • Otros cargos de TI – **15%** • Los demás – **9%**

Según naturaleza:



Según tamaño:



Según ámbito productivo:

Sector	Part. (n=64)
TIC's	30%
Educación	11%
Industria alimentaria	11%
*Químico-farmacéutico	8%
Gobierno	8%
Servicios corporativos	6%
Finanzas y banca	5%
Agrícola	5%
Publicidad y mercadeo	5%
Ingeniería y arquitectura	5%
Logística y transporte	2%
Entretenimiento	2%
Plástico	2%
Dispositivos médicos	2%
Salud	2%
Total general	**100%**

Invierte actualmente en ciberseguridad o lo ha hecho en el pasado (n=48) — **73%**

Nunca ha invertido en ciberseguridad (n=17) — **27%**

Fuente: elaboración propia a partir de datos de encuesta / *Incluye además agroquímicos, cuidado personal y limpieza

CAPÍTULO 1

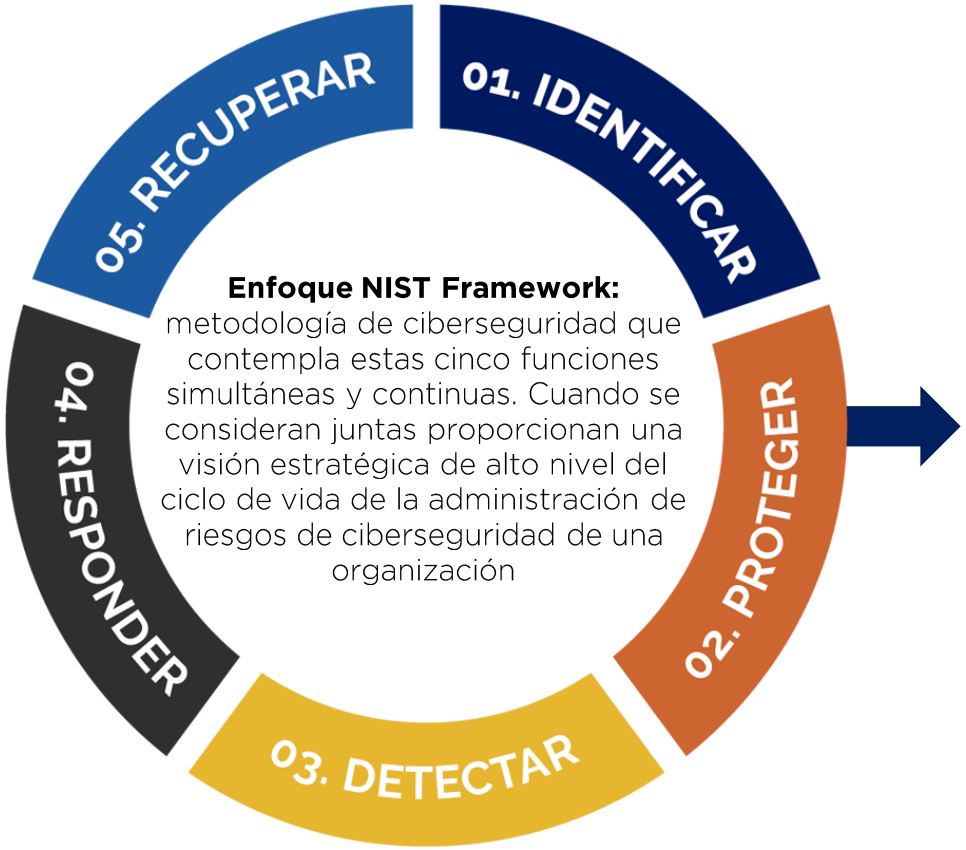
Caracterización del uso de ciberseguridad en empresas costarricenses

(n=48)

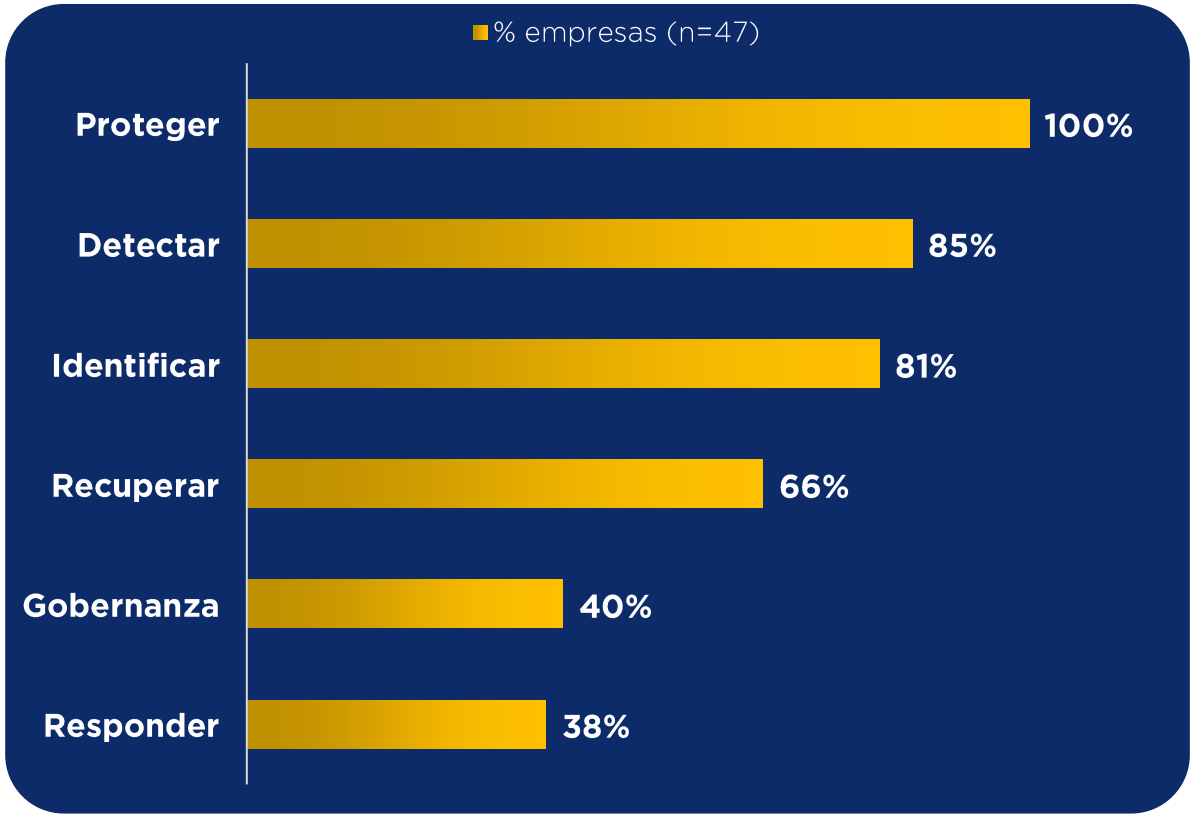
Este capítulo busca comprender el uso y características del consumo de ciberseguridad, aborda únicamente al grupo de empresas de la muestra que invierte actualmente o ha invertido recientemente en este ámbito (73% del total). Se excluyen a las empresas que nunca han invertido)

1. Soluciones de ciberseguridad implementadas, según función

El total de empresas que invierten en ciberseguridad tienen como principal prioridad la **protección** integral de sus operaciones; seguido de otras funciones clave, como la **detección** (85%) de programas maliciosos; la **identificación** de amenazas existentes o vulnerabilidades en sistemas (81%); la **recuperación** (66%) de datos, infraestructura y continuidad del negocio ante eventos; la **gobernanza** (40%) de la ciberseguridad como un marco que designe y administre responsables de la seguridad digital en la organización; y la **respuesta** (38%) ante ataques o incidentes de seguridad en tiempo real.



Soluciones implementadas según función principal::



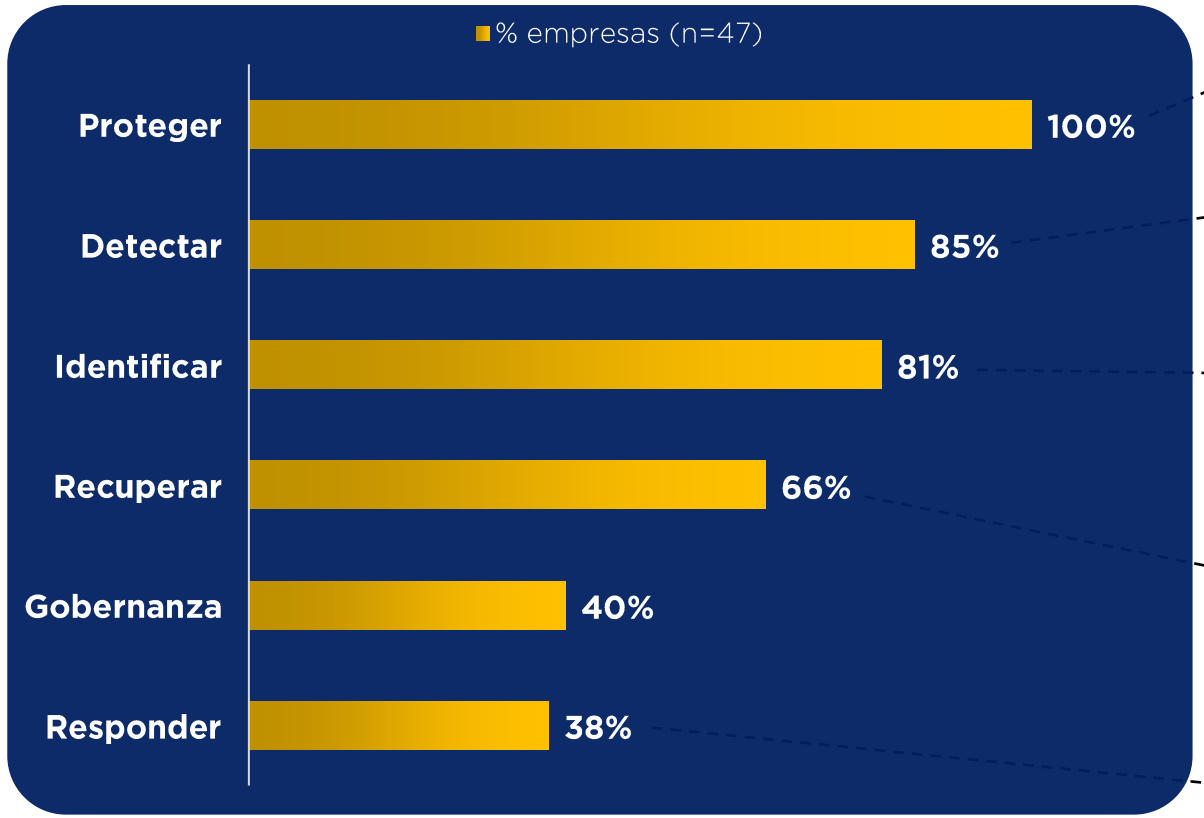
P/ ¿Cuáles tipos de soluciones de ciberseguridad ha implementado a la fecha? Según la función de seguridad que cumple la solución.

Fuente: elaboración propia a partir de datos de encuesta / La Gobernanza no forma parte del enfoque, pero se incluye por ser una actividad clave para la organización

1. Soluciones de ciberseguridad implementadas, según función

El total de empresas que invierten en ciberseguridad tienen como principal prioridad la **protección** integral de sus operaciones; seguido de otras funciones clave, como la **detección** (85%) de programas maliciosos; la **identificación** de amenazas existentes o vulnerabilidades en sistemas (81%); la **recuperación** (66%) de datos, infraestructura y continuidad del negocio ante eventos; la **gobernanza** (40%) de la ciberseguridad como un marco que designe y administre responsables de la seguridad digital en la organización; y la **respuesta** (38%) ante ataques o incidentes de seguridad en tiempo real.

Soluciones implementadas según función principal::



P/ ¿Cuáles tipos de soluciones de ciberseguridad ha implementado a la fecha? Según la función de seguridad que cumple la solución.

Protección: es la aplicación de controles (técnicos, políticas, procesos) para mitigar riesgos, contempla proteger los activos de la organización tomando como criterio la información obtenida durante la identificación de amenazas y riesgos

Detección: es el control y monitoreo, contempla actividades para identificar la ocurrencia oportuna de un evento de ciberseguridad

Identificar: busca comprender el contexto, conocer los activos e identificar las amenazas existentes y la probabilidad de que se materialicen. Desarrolla la comprensión organizacional para administrar el riesgo de ciberseguridad para sistemas, activos, datos y capacidades

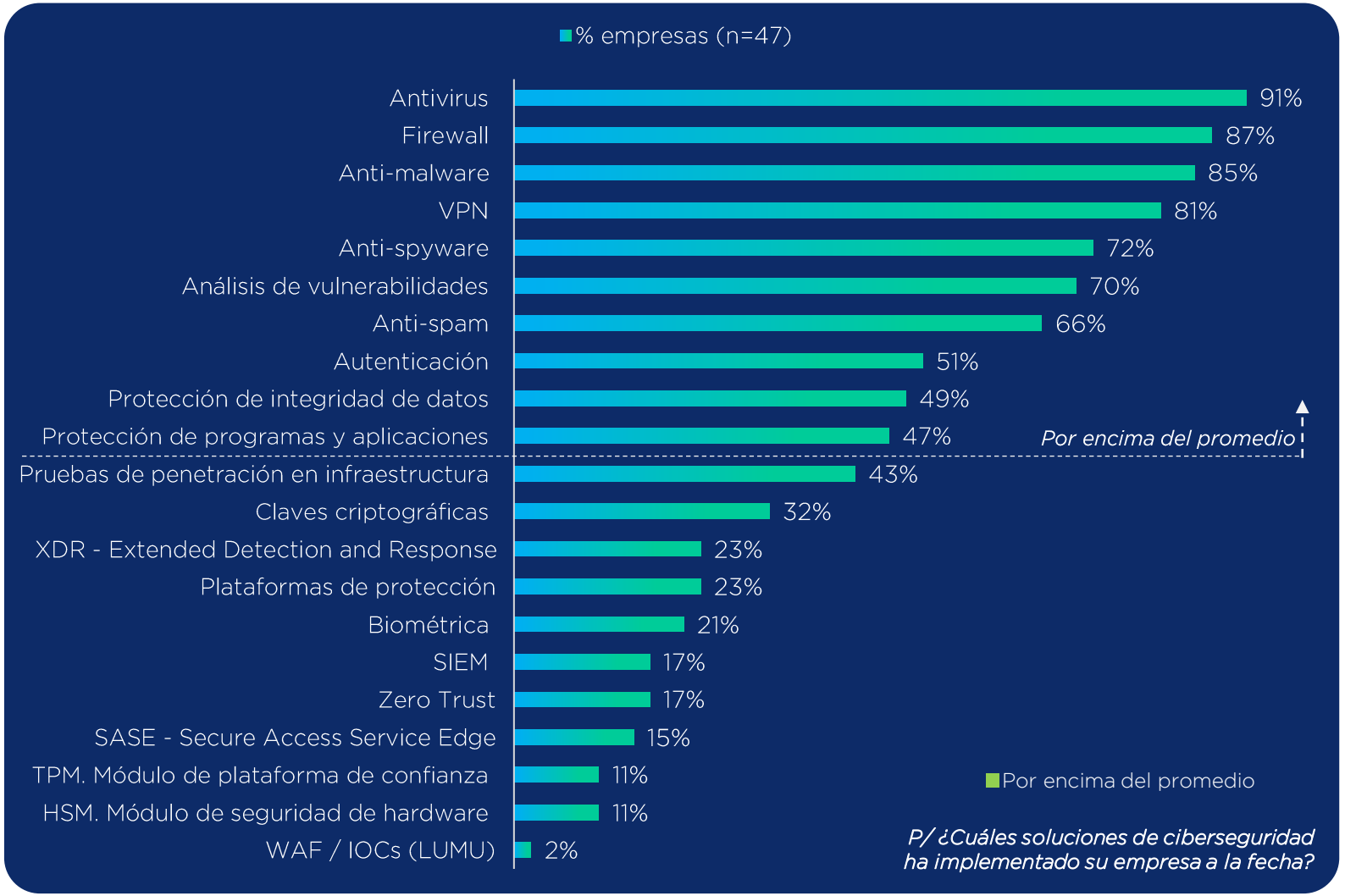
Recuperar: desarrolla e implementa actividades para mantener los planes de resiliencia y restaurar las capacidades/servicios afectados en un incidente. Una vez resuelta la crisis, se ejecutan tareas para recuperar el sistema afectado y devolverlo a su estado original

Responder: incluye actividades necesarias para tomar medidas con respecto a un incidente de ciberseguridad detectado, desarrollando la capacidad de contener el impacto de un potencial incidente

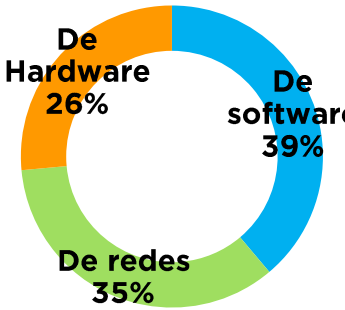
Fuente: elaboración propia a partir de datos de encuesta / NIST

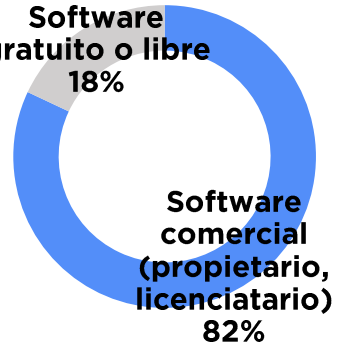
2. Soluciones de ciberseguridad utilizadas, según tipo y detalle

Según categoría, el 40% de las empresas implementa soluciones de **seguridad de software**, que se encarga de proteger las aplicaciones y programas de amenazas exteriores, por ejemplo, mediante antivirus, entre otros. En segundo lugar, el 35% utiliza **seguridad de red**, encargada de proteger toda la información accesible a través de internet y que podría ser utilizada de forma malintencionada, utiliza, por ejemplo, firewalls. Finalmente, el 26% **seguridad de hardware**, basada en la protección de dispositivos.



Naturaleza de las soluciones:
(n=47)





Cantidad de soluciones utilizadas por empresa	% empresas
2 a 5	23%
6 a 10	39%
11 a 15	32%
15 a 19	6%
Total general	**100%**

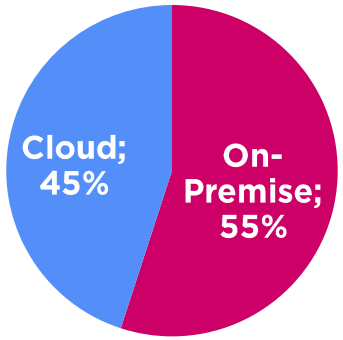
Fuente: elaboración propia a partir de datos de encuesta

3. Soluciones de ciberseguridad según modelo de implementación

Una mayoría de empresas (55%) emplea soluciones basadas On-Premise, un modelo habitual pero que puede ofrecer menor flexibilidad al depender de servidores físicos propios para los que, si hay que escalar el negocio, será necesaria la compra e implementación de nuevos servidores de mayor capacidad. Por el contrario, soluciones basadas en Cloud ofrecen opciones de escalabilidad flexibles, pudiendo ajustar los recursos requeridos, aunque con algunas preocupaciones entre usuarios sobre la seguridad de los datos en la nube.

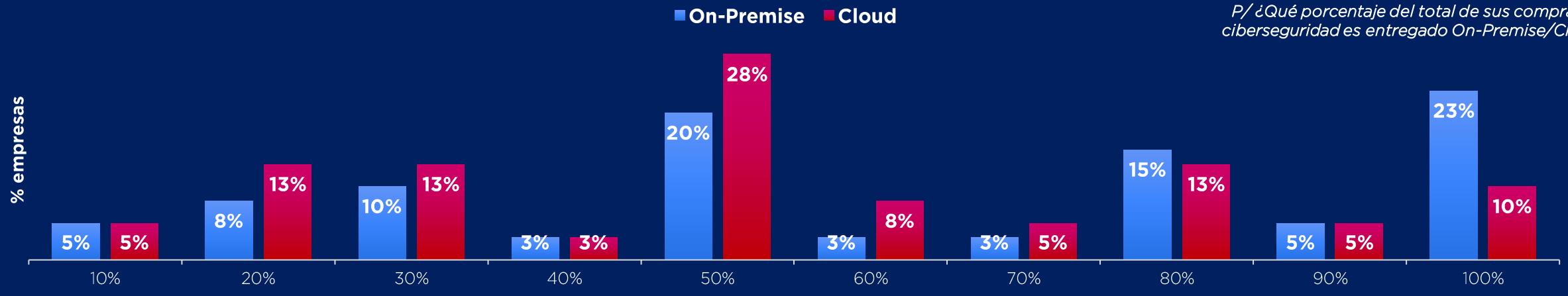
Mediante cloud: las empresas reciben los servicios de ciberseguridad mediante soluciones basadas en la nube, alojadas en servidores de terceros y que se acceden por web

% empresas (n=48)



On-Premise: las empresas reciben los servicios de ciberseguridad mediante soluciones que se instalan de manera local en equipos y servidores de la empresa

P/ ¿Qué porcentaje del total de sus compras de ciberseguridad es entregado On-Premise/Cloud?



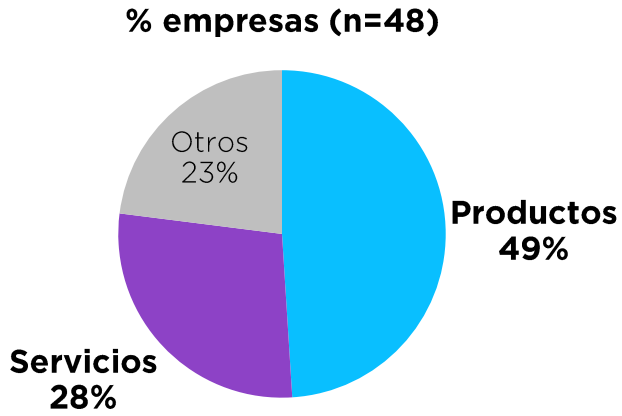
Participación del modelo (on-premise o cloud) en el gasto de ciberseguridad de la empresa

Fuente: elaboración propia a partir de datos de encuesta

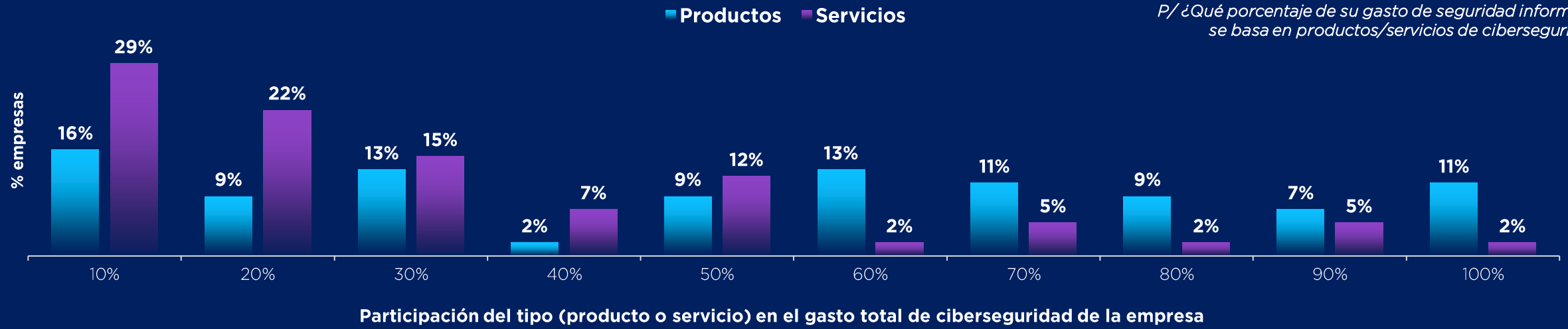
4. Soluciones de ciberseguridad según naturaleza de la solución

Cerca de la mitad de las empresas analizadas consumen **productos** de ciberseguridad, representando también cerca del 50% de su gasto en ciberseguridad vs servicios. Esto es comprensible dado que la seguridad se sustenta en soluciones que opera mayormente On-Premise de manera local (55% de empresas). Por otra parte, un 28% de los encuestados invierte en **servicios** de ciberseguridad, que pueden basarse, por ejemplo, en entrenamiento, soporte de sistemas, gobernanza de seguridad organizacional, gestión de crisis, otros.

Servicios de ciberseguridad: servicios operativos o de mantenimiento, por ejemplo, monitoreo en tiempo real, soporte, capacitación, asesoría, etc.



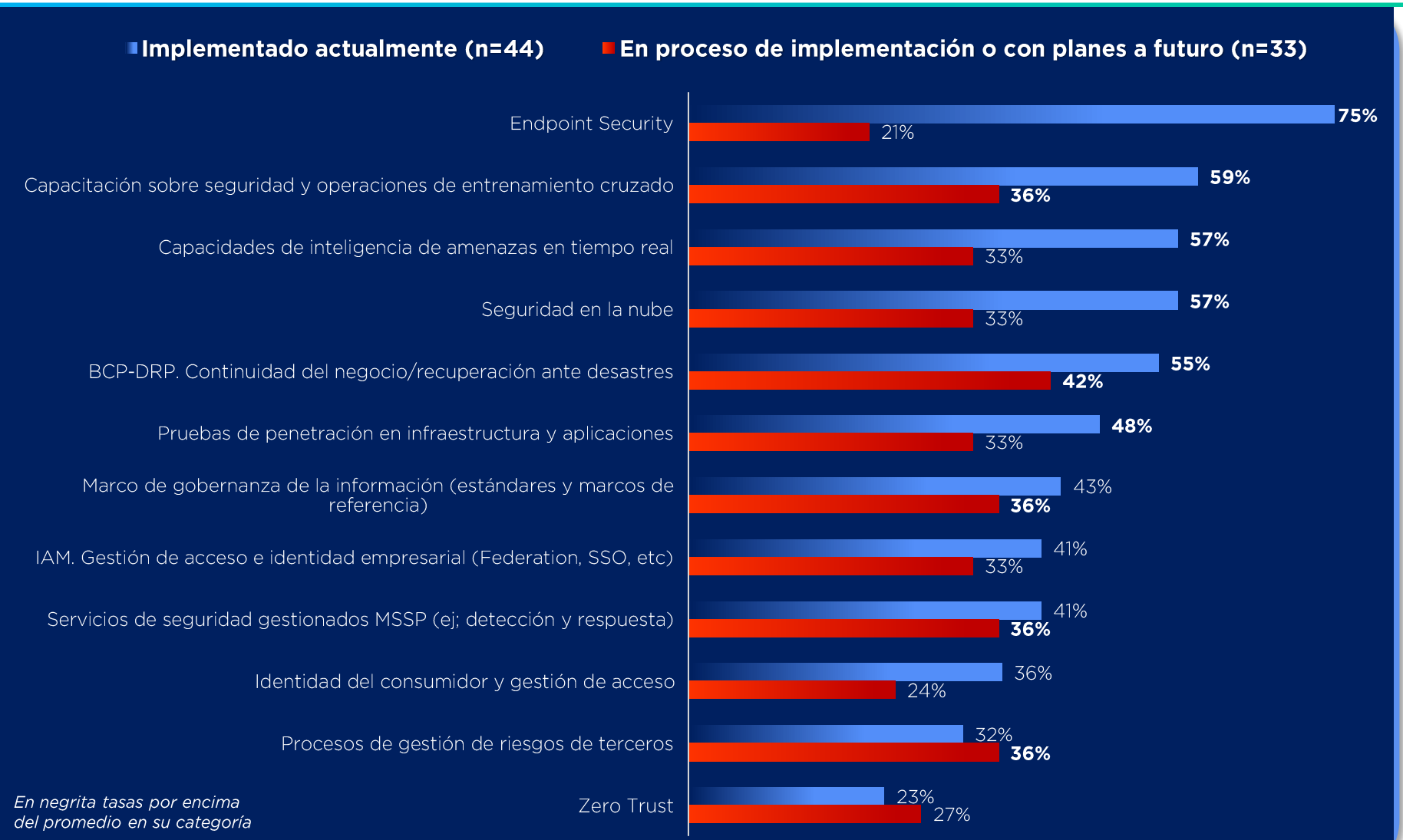
Productos de ciberseguridad: se trata de soluciones basadas en propiedad intelectual, normalmente software y plataformas especializadas



Fuente: elaboración propia a partir de datos de encuesta / En categoría "otros" se incluyen, por ejemplo, gastos en recurso humano, infraestructura, etc.

5. Status de implementación de soluciones, según categorías estratégicas

Endpoint Security destaca como la principal solución implementada actualmente entre las empresas (75% de ellas), un enfoque para defender los puntos finales (dispositivos) de la actividad maliciosa. Se utiliza para prevenir ataques de malware, detectar actividades maliciosas y proporcionar capacidades de investigación y remediación para responder a incidentes de seguridad. En paralelo, **BCP-DRP** son las soluciones que más empresas (42%) están en proceso de implementar o con planes de hacerlo a futuro.



En negrita tasas por encima del promedio en su categoría

Nivel de implementación	% empresas (n=44)
Alto nivel: 9 a 12 categorías *(Heavy Users)*	**27%**
Grande	20%
Pequeña	5%
Mediana	2%
Medio nivel: 5 a 8 categorías *(Light Users)*	**28%**
Grande	9%
Mediana	9%
Pequeña	5%
Micro	5%
Bajo nivel: 1 a 4 categorías *(New Users)*	**45%**
Grande	23%
Pequeña	14%
Mediana	7%
Micro	2%
Total general	**100%**

Fuente: elaboración propia a partir de datos de encuesta

6. Status de implementación de soluciones, según categorías estratégicas

Con respecto a la diapositiva anterior, Zero Trust y la gestión de riesgos de terceros son las únicas dos soluciones de ciberseguridad en donde la tasa de intención de implementarse a futuro es superior a la tasa de implementación actual. Para empresas oferentes de ciberseguridad, esto **podría significar una demanda dinámica** por estos servicios en el corto-mediano plazo vs otros en los que las empresas ya han finalizado por realizar sus adquisiciones e implementaciones a escala.

Soluciones de ciberseguridad	Implementado vs en proceso (diferencia en puntos porcentuales)
Zero Trust	**4%**
Procesos de gestión de riesgos de terceros	**4%**
Servicios de seguridad gestionados MSSP (ej; detección y respuesta)	-5%
Marco de gobernanza de la información (estándares y marcos de referencia)	-7%
IAM. Gestión de acceso e identidad empresarial (Federation, SSO, etc)	-8%
Identidad del consumidor y gestión de acceso	-12%
BCP-DRP. Continuidad del negocio/recuperación ante desastres	-13%
Pruebas de penetración en infraestructura y aplicaciones	-15%
Capacitación sobre seguridad y operaciones de entrenamiento cruzado	-23%
Capacidades de inteligencia de amenazas en tiempo real	-24%
Seguridad en la nube	-24%
Endpoint Security	-54%

La tasa de intención es superior a la tasa de implementación actual, lo cual podría sugerir que la demanda por estas soluciones tendrá en el corto o mediano plazo un dinamismo por encima de otras que ya están actualmente implementadas a escala

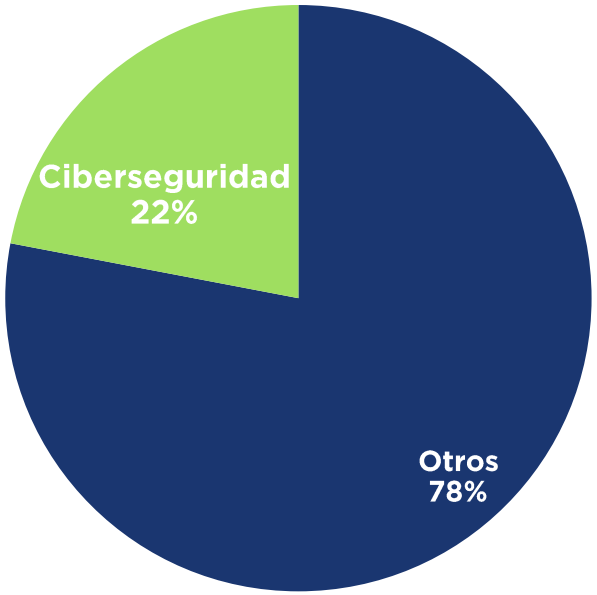
Categorías donde la diferencia entre la implementación y la intención de hacerlo a futuro es mayor. Esto podría significar que las empresas tienen mejor satisfechas sus necesidades en estos ámbitos y que planean poco implementar a cabalidad en el futuro

Fuente: elaboración propia a partir de datos de encuesta

7. Presupuesto destinado a ciberseguridad entre la muestra encuestada

El gasto en ciberseguridad, como parte de la inversión total en tecnología, representa una quinta parte del presupuesto total de las empresas. En el mundo, la tasa promedio fue de 21% en 2021, lo cual refleja que las empresas costarricenses se encuentran dentro de este parámetro. En 2021 y estimulado por la oleada de ataques cibernéticos durante la pandemia, esta tasa global se incrementó con respecto a 2020 (13%) y 2019 (10%). En total, las empresas analizadas indican un presupuesto colectivo de hasta $15,1 millones de USD.

Participación de la ciberseguridad en el presupuesto anual total de tecnología de las empresas
(n=43; promedio 2021)



P/ ¿Cuál es el porcentaje en inversión en seguridad respecto a su presupuesto general de tecnología?

$15.144.000 USD
es el **presupuesto total** de ciberseguridad entre la muestra encuestada (en 2021)

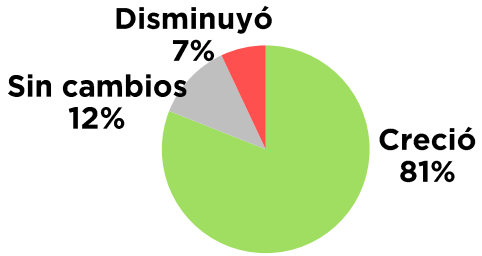
$49.860 USD
es el **presupuesto anual promedio** por empresa
(se excluye a tres empresas con un presupuesto desproporcionado con respecto a la muestra)

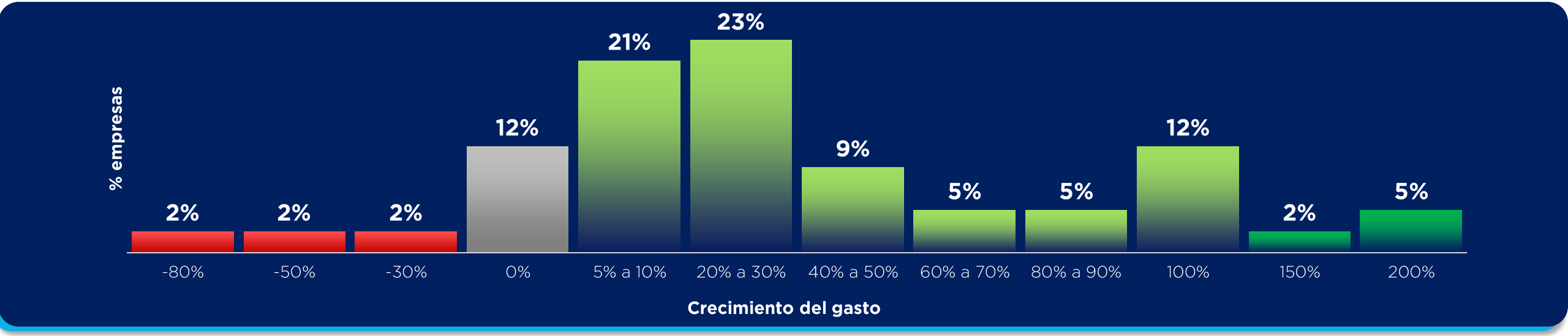
Fuente: elaboración propia a partir de datos de encuesta / Informe de Ciberpreparación de Hiscox 2021

8. Crecimiento del gasto en los últimos cinco años

Durante los últimos cinco años, entre 2017 y 2021, el 81% de las empresas incrementó su gasto en ciberseguridad; 12% de ellas presentó gastos estáticos sin cambios y un 7% lo disminuyó (lo cual puede considerarse destacable al considerar el contexto provocado por la pandemia en este período). En promedio, entre el grupo de empresas que incrementó su gasto, lo hizo a una tasa media de +53%.
En el mundo, por ejemplo, el 82% de las empresas incrementó su gasto en ciberseguridad en 2021 con respecto al año anterior.

Crecimiento del gasto en ciberseguridad en los últimos cinco años
2017-2021
(% empresas; n=43)





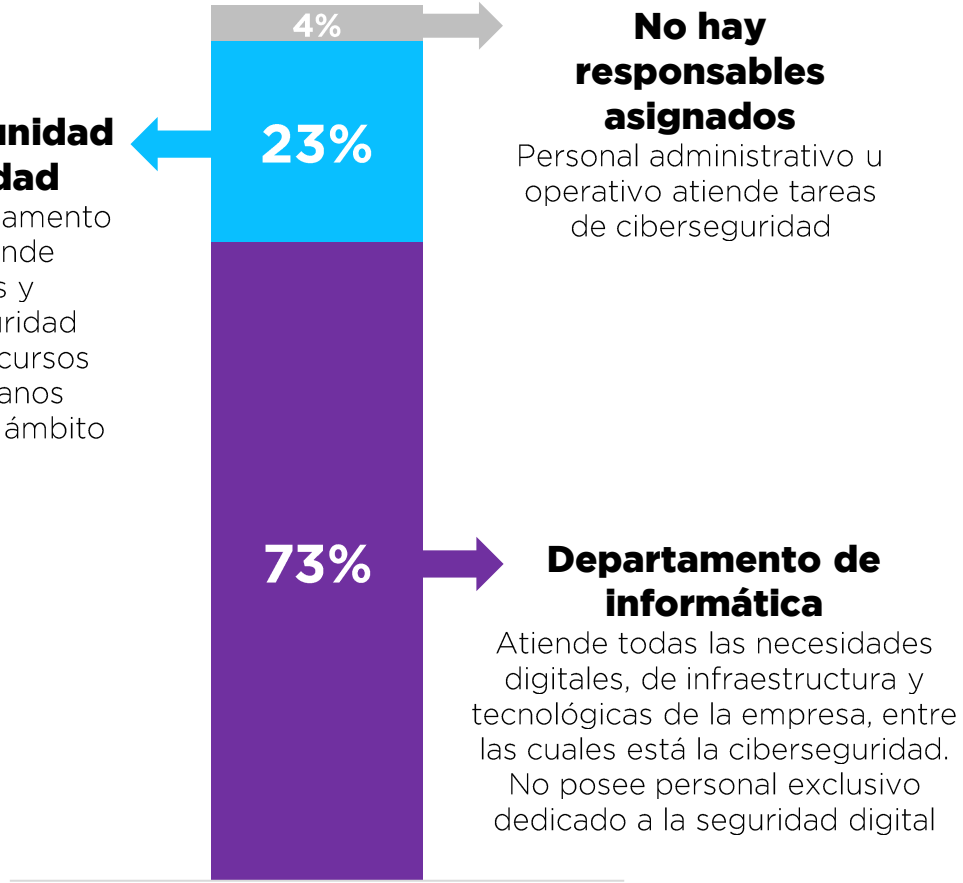
P/ Con respecto a hace cinco años (año 2017), ¿en qué porcentaje ha crecido su presupuesto/gasto de ciberseguridad comparado con el actual?

Fuente: elaboración propia a partir de datos de encuesta / Estado de la Ciberresiliencia 2021, Accenture

9. Proveedores de ciberseguridad a lo interno de la organización

El 73% de empresas atiende sus necesidades de seguridad digital mediante su departamento de informática, el cual tiene a su vez asignadas todas las responsabilidades generales de tecnología de la organización, lo cual puede restarle capacidades de atención y monitoreo. Por otra parte, el 23% de empresas sí cuenta con un departamento o unidad de ciberseguridad, lo cual es alentador, al tratarse de recurso humano especializado para la atención preventiva, activa y reactiva de la ciberseguridad.

A lo interno, ¿quién se encarga de la ciberseguridad de la empresa?
(% empresas; n=48)



No hay responsables asignados
Personal administrativo u operativo atiende tareas de ciberseguridad

Departamento o unidad de ciberseguridad
Equipo anexo al departamento de informática, atiende únicamente tareas y necesidades de seguridad digital. Cuenta con recursos tecnológicos y humanos especializados en este ámbito

Departamento de informática
Atiende todas las necesidades digitales, de infraestructura y tecnológicas de la empresa, entre las cuales está la ciberseguridad. No posee personal exclusivo dedicado a la seguridad digital

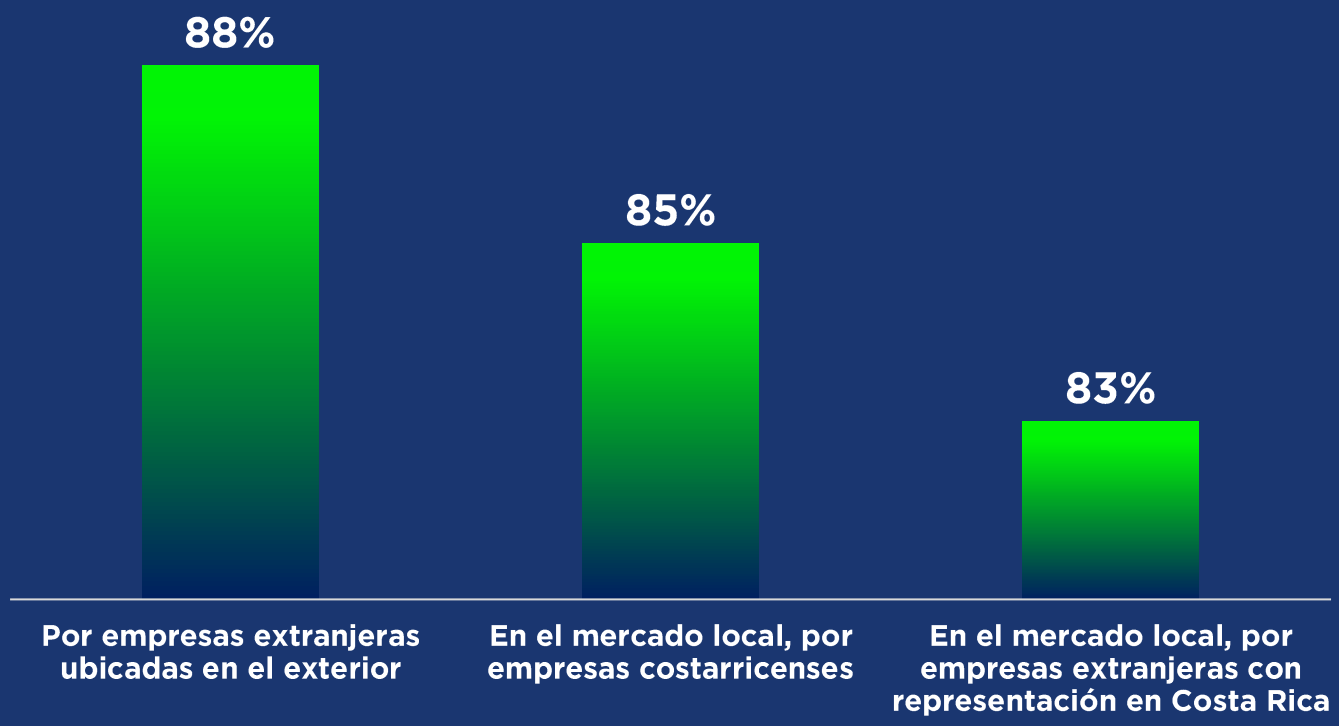
Origen de la ciberseguridad	% empresas
Departamento de informática	**73%**
Grande	40%
Pequeña	15%
Mediana	13%
Micro	6%
Departamento/unidad de ciberseguridad	**23%**
Grande	15%
Pequeña	6%
Mediana	2%
No hay responsables asignados	**4%**
Pequeña	2%
Mediana	2%
Total general	**100%**

Fuente: elaboración propia a partir de datos de encuesta

10. Proveedores de ciberseguridad a lo externo de la organización

El 73% de empresas atiende sus necesidades de seguridad digital mediante su departamento de informática, el cual tiene a su vez asignadas todas las responsabilidades generales de tecnología de la organización, lo cual puede restarle capacidades de atención y monitoreo. Por otra parte, el 23% de empresas sí cuenta con un departamento o unidad de ciberseguridad, lo cual es alentador, al tratarse de recurso humano especializado para la atención preventiva, activa y reactiva de la ciberseguridad.

A lo externo, ¿cuál es el origen de las soluciones o servicios de ciberseguridad de la empresa?
(% empresas; n=48)



Origen de la ciberseguridad	% empresas
Por empresas extranjeras ubicadas en el exterior	**88%**
Grande	44%
Pequeña	21%
Mediana	17%
Micro	6%
En el mercado local, por empresas costarricenses	**85%**
Grande	44%
Pequeña	21%
Mediana	15%
Micro	6%
En el mercado local, por empresas extranjeras con representación en Costa Rica	**83%**
Grande	46%
Pequeña	19%
Mediana	13%
Micro	6%

Datos clave:

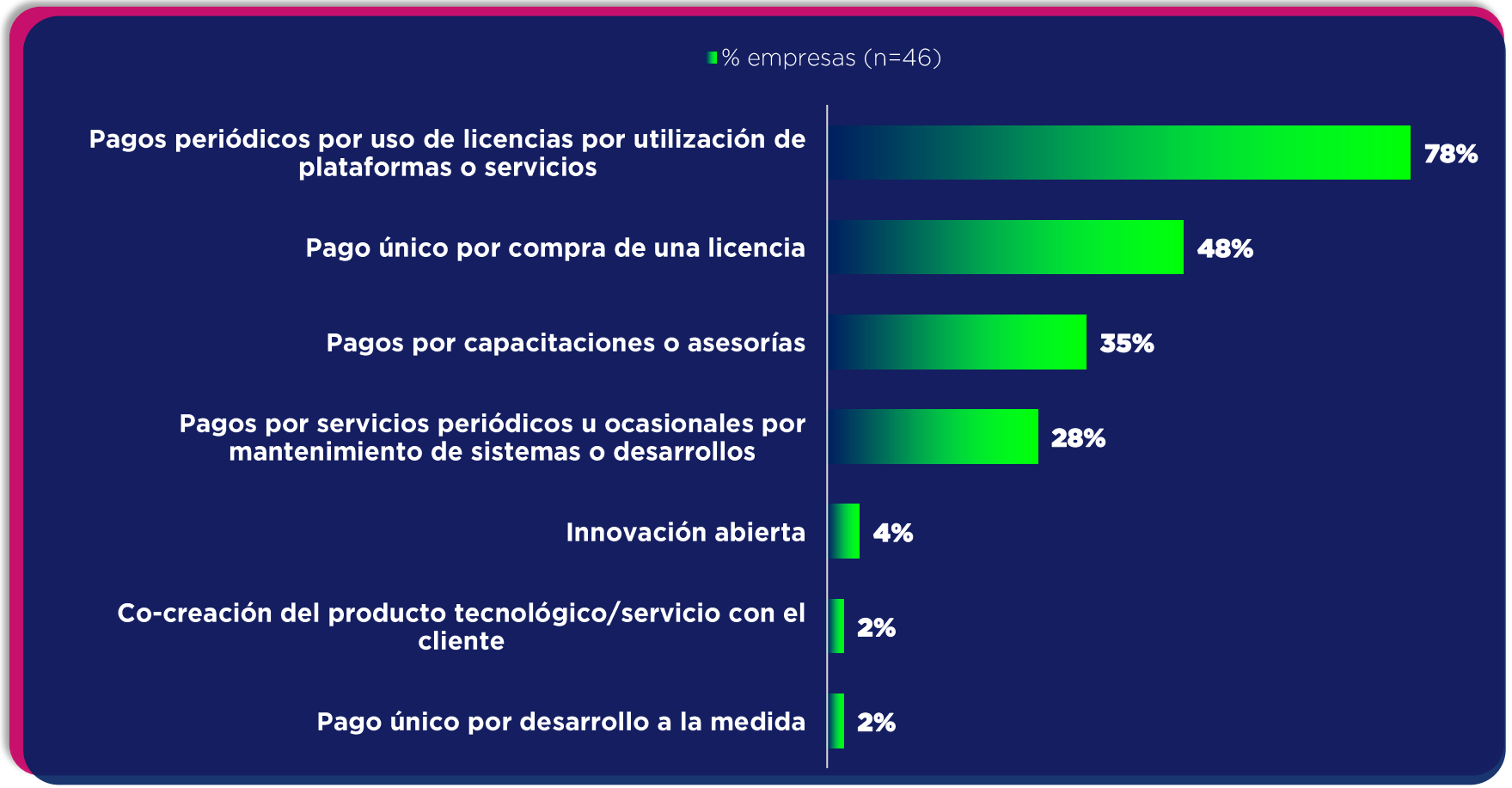
- **94%** de empresas se abastece en el mercado local
- **87%** importa servicios o soluciones del exterior
- **81%** se abastece en el mercado local y por importaciones
- **6%** solamente se abastece mediante importación
- **Ninguna** empresa se abastece solo por el mercado local

Fuente: elaboración propia a partir de datos de encuesta

11. Modelos de negocio con proveedores de ciberseguridad

Los modelos de negocio representan las maneras en los proveedores generan valor para el cliente. Entre las empresas encuestadas, el pago periódico por uso de licencias es el principal modelo para el 78% ellas, es decir, por los derechos de la utilización de productos de seguridad o servicios remotos. Por otra parte, el 48% de empresas realiza pagos únicos por compra de licencia; capacitaciones-asesorías (35%) o por mantenimiento (28%). Para estas empresas, no resultan habituales otros modelos más diferenciados, como la innovación abierta, la co-creación de las soluciones con el cliente o desarrollos a la medida, las cuales resultan normalmente en ámbitos más orientados al valor agregado, al abordaje de proyectos específicos o a nuevos desafíos para la organización.

Modelos de negocio entre las empresas y sus proveedores de ciberseguridad:



Fuente: elaboración propia a partir de datos de encuesta

12. Aspectos de valor agregado solicitado a proveedores de ciberseguridad

Las certificaciones de calidad o del fabricante destacan como los elementos de valor agregado más solicitados por los consumidores de ciberseguridad, es decir, que buscan un nivel de respaldo sobre el desempeño de las soluciones, así como del nivel de protección que puedan proveer. Adicionalmente, la experiencia comprobable resulta clave, así como un adecuado servicio al cliente que normalmente se vincula con el soporte y respuesta ante incidentes de ciberseguridad.

Por encima del promedio

Aspectos clave de valor agregado	% empresas (n=43)
Certificaciones de calidad o del fabricante	**47%**
Experiencia y trayectoria comprobable	**37%**
Servicio al cliente	**16%**
Estabilidad, desempeño y eficiencia	12%
Respaldo y representación en el mercado local	7%
Relación precio-valor	5%
Capacitación y acompañamiento	5%
Cumplimiento de especificaciones técnicas	5%
Innovación y pensamiento creativo	2%
Comprensión de los requerimientos del cliente	2%
Amplio portafolio de los servicios	2%
Garantía	2%

Atributos varios de valor agregado demandados por las empresas:

- ✓ Proveedores contemplados en cuadrante de líderes de Gartner o Forrester Wave
- ✓ Formación y actualización continua del personal especializado.
- ✓ Optimización de los recursos y servicios ofertados.
- ✓ Enfoque en prevención y respuesta; gestión de riesgo; protección de infraestructura.
- ✓ Cumplimiento de especificaciones técnicas y ambientales de acuerdo a la Ley de Contratación Administrativa.
- ✓ Plataforma basada nube, proactiva y probada. SIEM integrado, SaaS, Apis para integración.

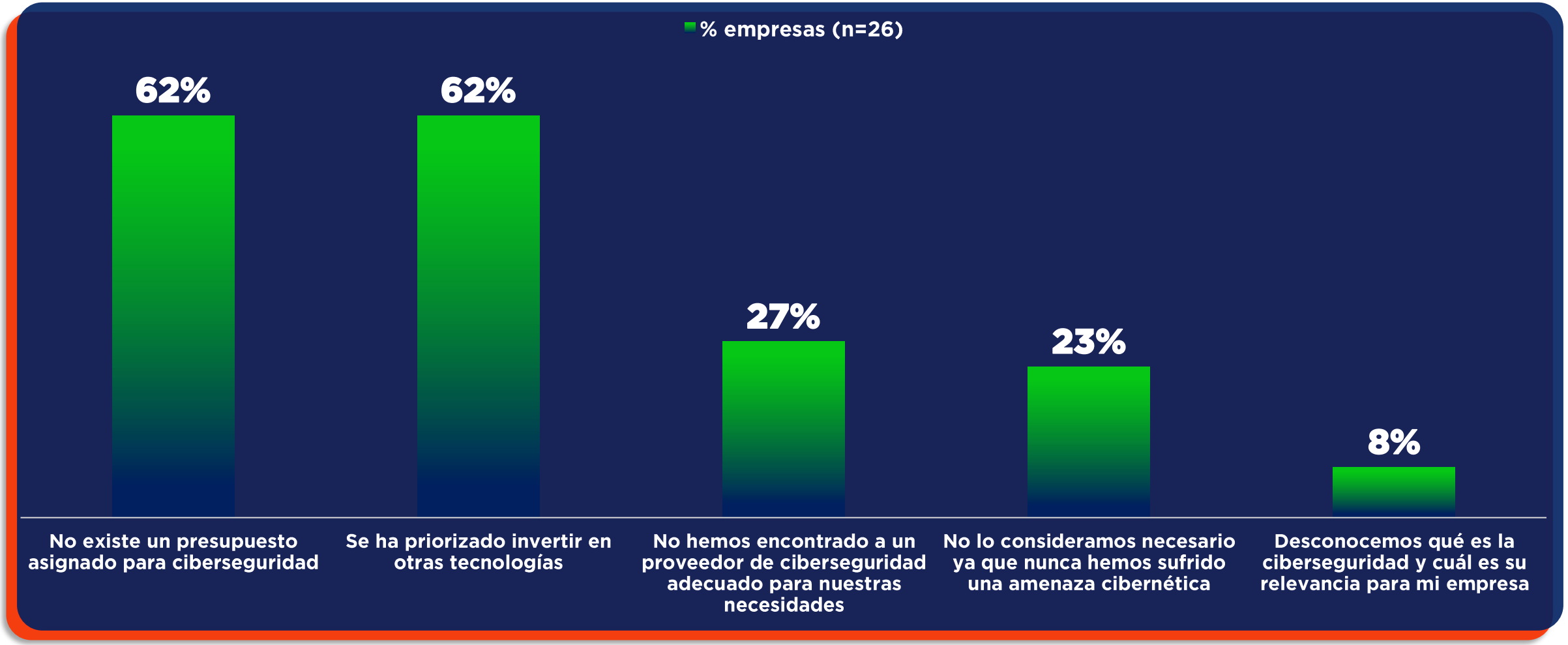
Certificaciones o buenas prácticas solicitadas:

- **Ethical Hacking**
- **Protección de datos**
- **ISO 27001**
- **NIST Framework**

Fuente: elaboración propia a partir de datos de encuesta

13. ¿Qué razones limitan la inversión en ciberseguridad?

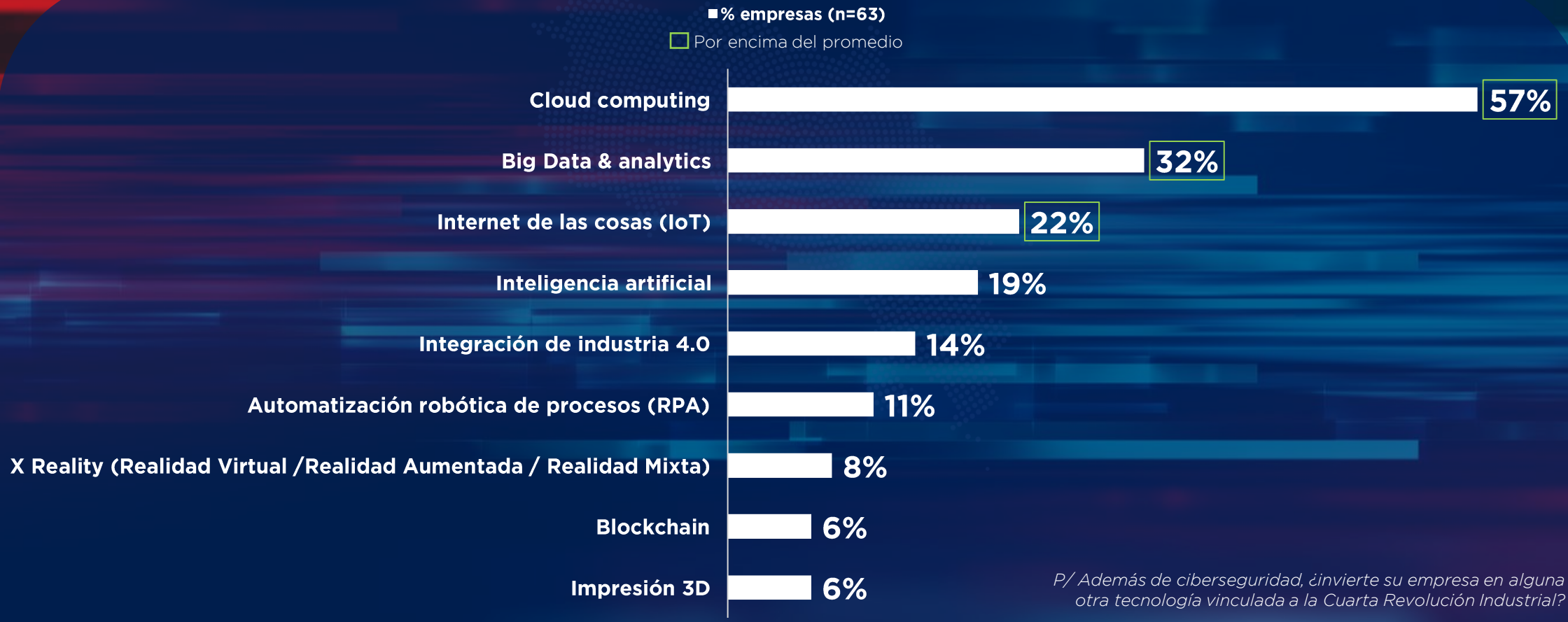
Alrededor de 6 de cada 10 empresas no posee un presupuesto formal asignado a la ciberseguridad, esto significa que sus recursos son variables o se destinan a otras necesidades. En un mismo nivel, las empresas han priorizado invertir en otras tecnologías por encima de la ciberseguridad. Por otra parte, es importante considerar que un 27% de las empresas no han encontrado a un proveedor de ciberseguridad que se ajuste a sus requerimientos, lo cual evidencia oportunidades de acercamiento por parte de la oferta.



Fuente: elaboración propia a partir de datos de encuesta

14. ¿En qué otras tecnologías 4.0 invierten los usuarios de ciberseguridad?

De un total de **10 categorías tecnológicas** vinculadas a la Cuarta Revolución Industrial, **Cloud Computing** destaca como la principal tecnología en la que más empresas invierten (57% de ellas), además de ciberseguridad, al ser Cloud normalmente una plataforma de soporte y respaldo para las soluciones de seguridad. Por otra parte, Big Data (32%) e Internet de las Cosas son las otras dos categorías cuyas tasas están por encima del promedio. Para profundizar en la oferta costarricense de tecnologías 4.0 consulte esta investigación.



P/ Además de ciberseguridad, ¿invierte su empresa en alguna otra tecnología vinculada a la Cuarta Revolución Industrial?

Fuente: elaboración propia a partir de datos de encuesta

CAPÍTULO 2

Necesidades potenciales y principales amenazas de ciberseguridad que han afectado a las empresas

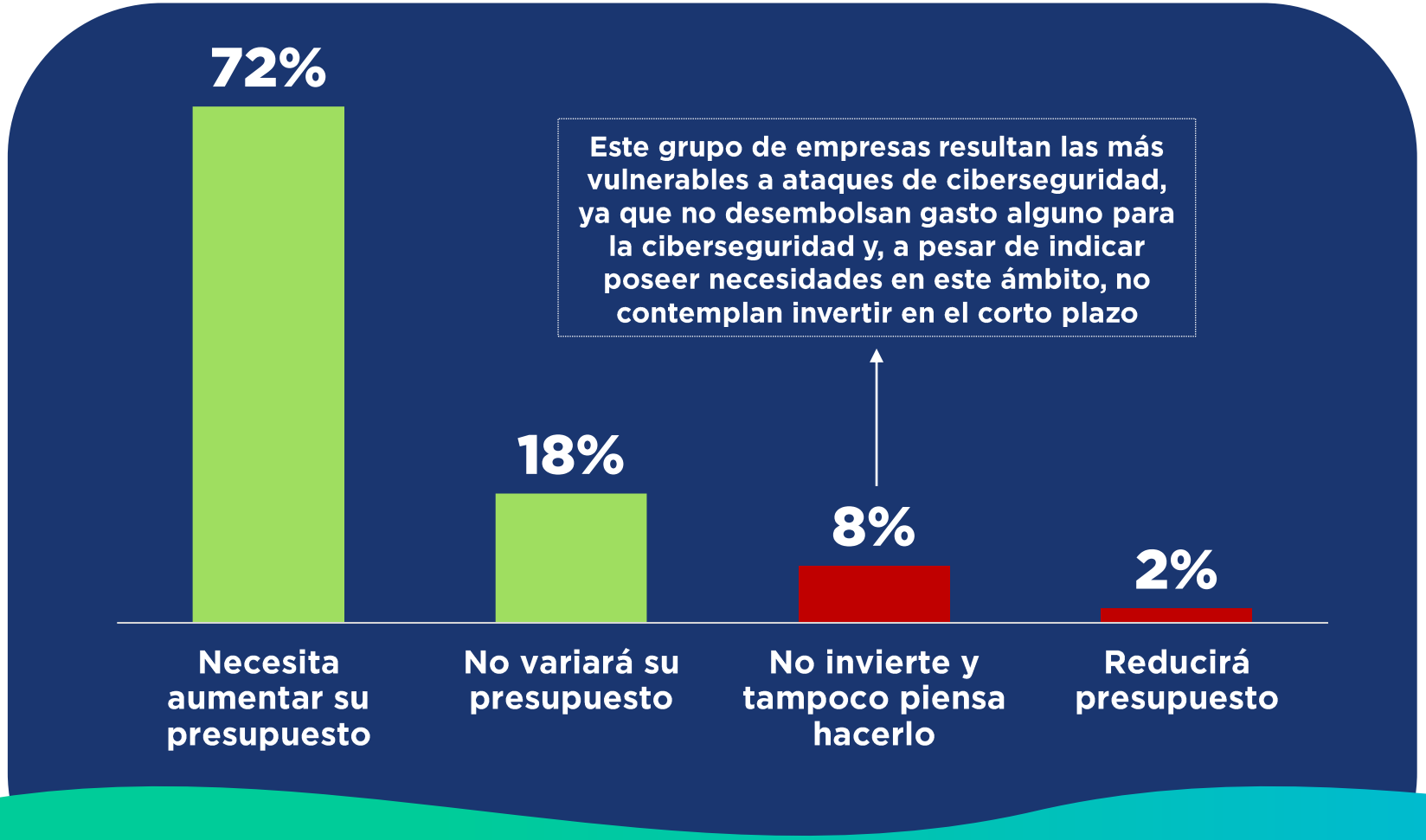
(n=64)

Este capítulo busca comprender las necesidades potenciales que poseen las empresas así como los riesgos a los cuales se han enfrentado. Para ello se abarca el total de la muestra encuestada, es decir, incluyendo también al grupo de empresas que nunca han invertido en ciberseguridad, pero que poseen igualmente necesidades en este ámbito.

15. Perspectivas del gasto en ciberseguridad en el corto plazo

En caso de tener libertad presupuestaria, se solicitó a las empresas considerar todas sus necesidades actuales y potenciales con el fin de determinar las necesidades reales de gasto en el corto. En total, **7 de cada 10 empresas considera necesario incrementar su presupuesto** con el fin de hacer frente a sus requerimientos en ciberseguridad. Por el contrario tan solo el 2% de las empresas planea disminuir su gasto. **Es clave resaltar que un 8% de las empresas nunca ha invertido en ciberseguridad y tampoco planea hacerlo.**

En caso de tener libertad presupuestaria ¿cuáles son las perspectivas de gasto en el corto plazo?
(n=64)



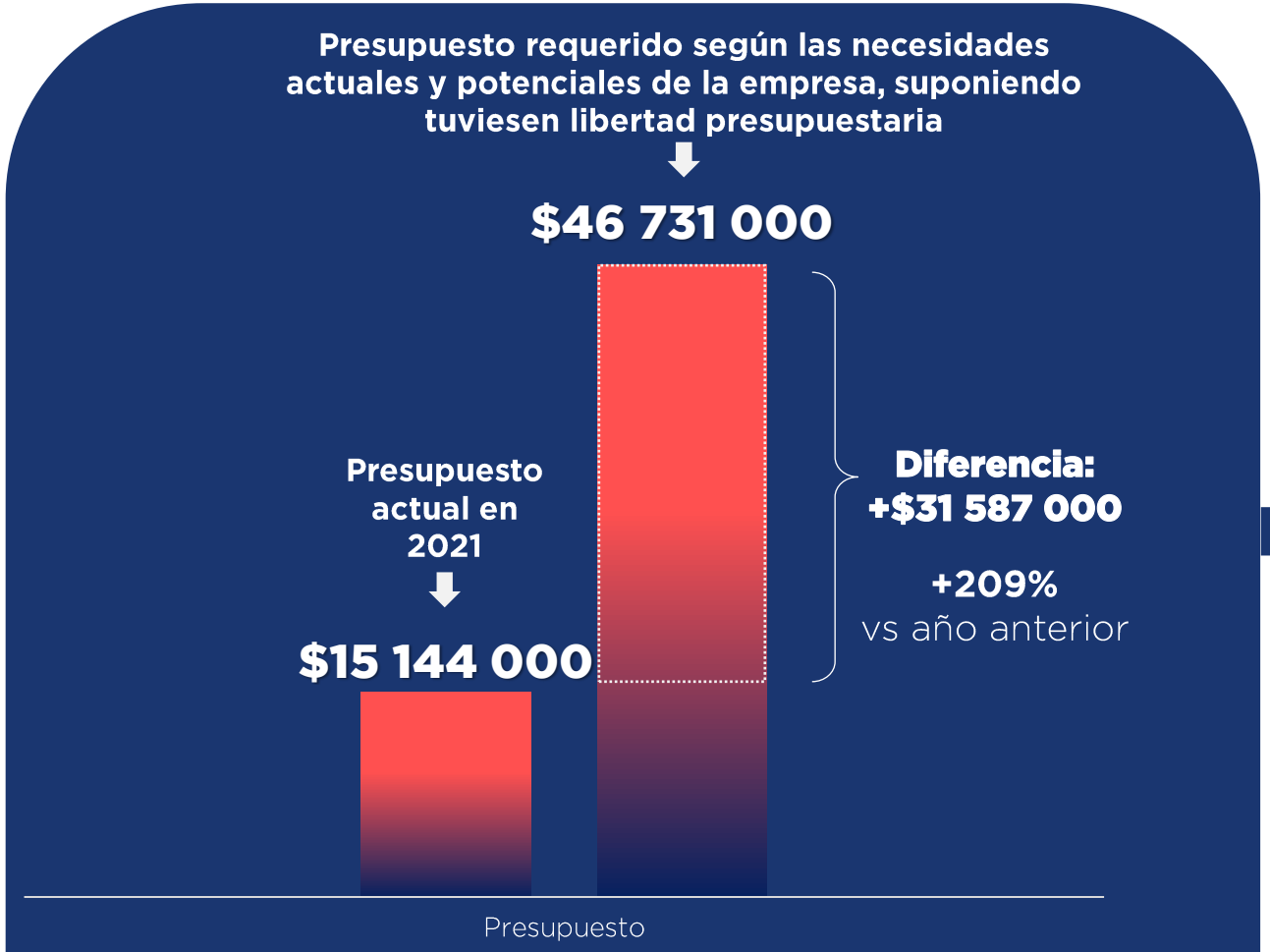
Según tamaño	% empresas (n=64)
Necesita aumentar presupuesto	**72%**
Grande	28%
Pequeña	20%
Mediana	16%
Micro	8%
No variará presupuesto	**18%**
Grande	11%
Pequeña	3%
Mediana	2%
Micro	2%
No invierte y tampoco lo hará	**8%**
Micro	6%
Grande	2%
Pequeña	2%
Reducirá presupuesto	**2%**
Mediana	2%

Fuente: elaboración propia a partir de datos de encuesta

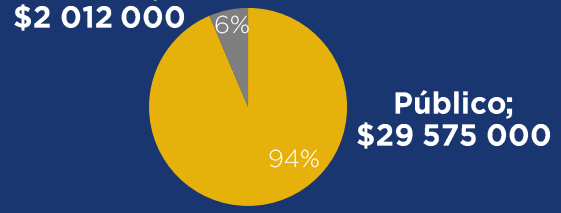
16. De tener libertad presupuestaria, ¿cuál es el valor requerido según necesidades?

Se solicitó a las empresas encuestadas considerar todas sus necesidades actuales y potenciales de ciberseguridad para que determinasen cuál es el presupuesto real que requerirían en el corto plazo para hacer frente a sus necesidades de seguridad. En total, se evidencia que la inversión necesaria debería ser el doble de la actual, no obstante, si se excluye de la muestra a tres empresas con incrementos sustanciales, el presupuesto debería incrementarse solo en **$1,3 millones** (+8,5% con respecto al presupuesto actual).

(n=47)



Distribución del crecimiento en el presupuesto:

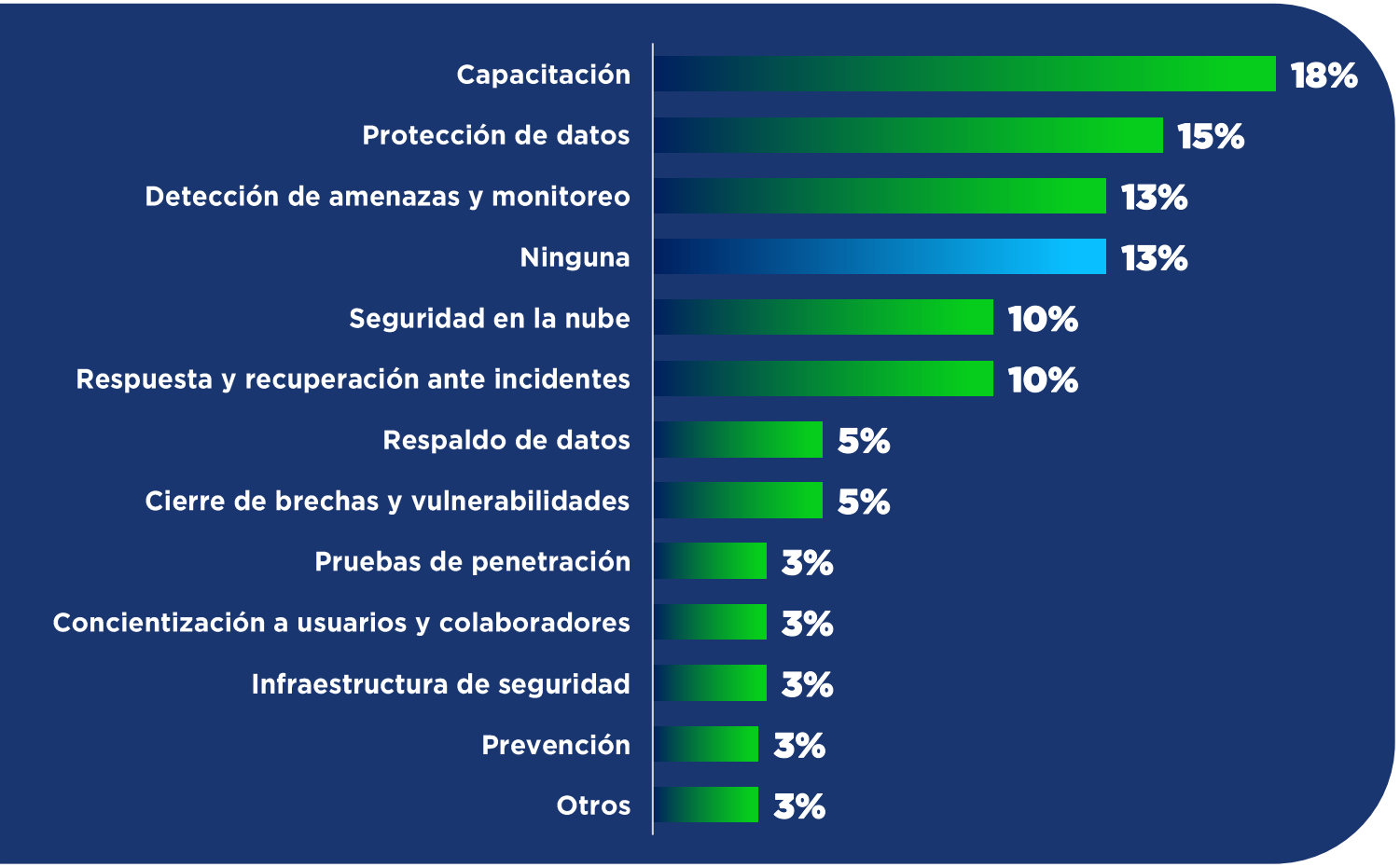


Tamaño	Variación en presupuesto	Distribución según tamaño	
Empresas que invierten (n=35)	$1 442 000	Grande	$950 000
		Pequeña	$367 000
		Mediana	$101 000
		Micro	$24 000
	$29 000 000	Grande (2 empresas)	$29 000 000
Empresas que nunca han invertido (n=12)	$145 000	Grande	$40 000
		Pequeña	$40 000
		Mediana	$35 000
		Micro	$30 000
	$1 000 000	Mediana (1 empresa)	$1 000 000
Total general	**$31 587 000**		

Fuente: elaboración propia a partir de datos de encuesta

17. Necesidades insatisfechas o en las que requieren apoyo las empresas

La capacitación en materia de ciberseguridad es la principal necesidad en la que requieren más apoyo las empresas de esta tecnología, seguido de otras necesidades clave, como la protección de datos (de la organización y de los usuarios); la detección de amenazas y monitoreo; la seguridad en la nube y la respuesta ante incidente (continuidad del negocio). Estas áreas pueden ser consideradas por las empresas oferentes de ciberseguridad para efectos de generar un acercamiento y apoyar a los usuarios.



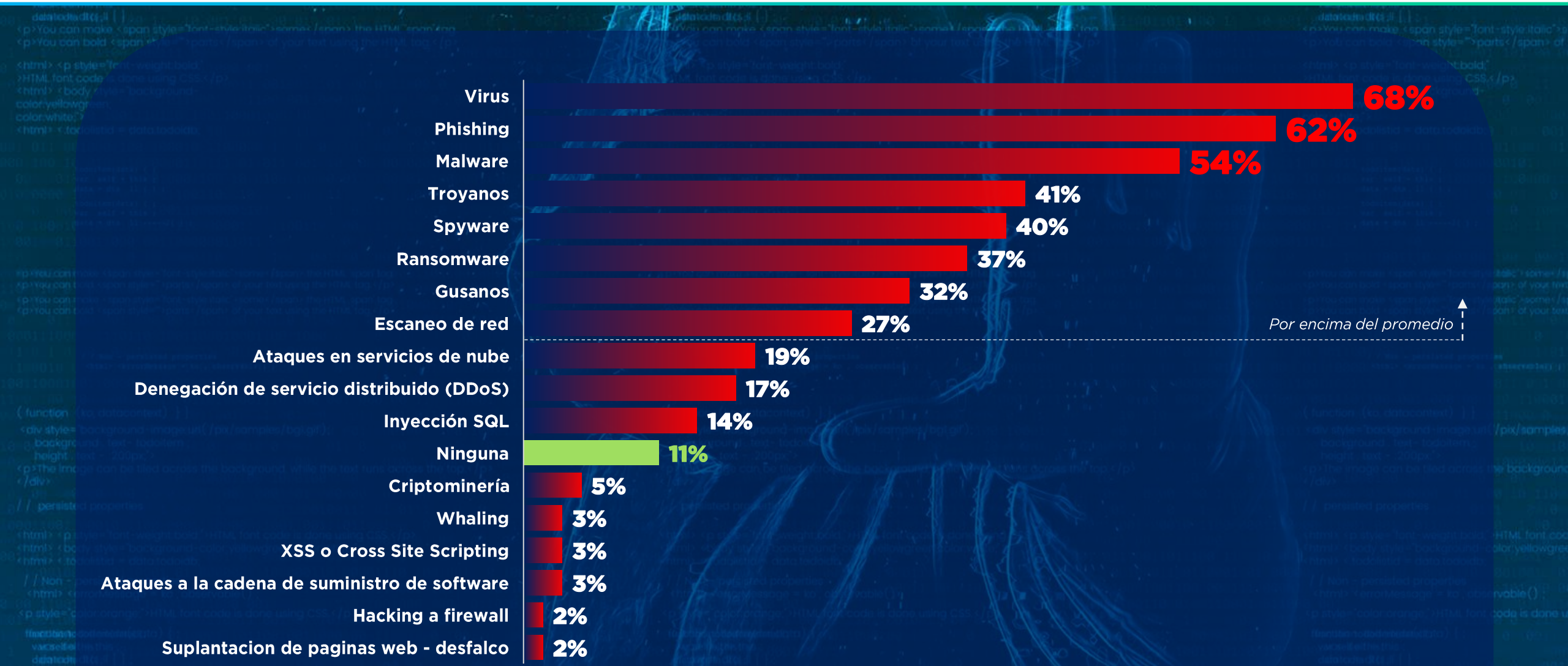
Otras necesidades varias	% empresas
Estabilidad y compatibilidad de sistemas	2%
Gobernanza de ciberseguridad	2%
Seguridad para dispositivos	2%
VPN públicas	2%
Plataforma proactiva SOC + SIEM	2%
Gestión de accesos	2%
Infraestructura de identidad	2%
Consolas de administración centralizadas	2%
Más recurso humano especializado	2%
Penetration testing en dispositivos incrustrados	2%

P/ ¿Cuál considera puede ser la necesidad en ciberseguridad más insatisfecha o en la que más necesita apoyo su empresa?

Fuente: elaboración propia a partir de datos de encuesta

18. Amenazas a las que se han visto expuestas las organizaciones

En total, el 89% de las empresas encuestadas se ha visto afectada por la ciberdelincuencia. Cerca de 7 de cada 10 empresas se ha visto afectadas por virus, una de las infecciones más comunes en el mundo, seguido muy de cerca por phishing (62%) y malware (54%). Con menor participación, destacan otros tipos de ataques que resultan normalmente menos frecuentes, o bien que tienen mayor incidencia según el sector al que pertenezca la empresa, como por ejemplo el Whaling o ataques a la cadena de suministro de software.



Fuente: elaboración propia a partir de datos de encuesta

19. ¿Cuál consideran las organizaciones es su mayor amenaza actual?

La mayoría de empresas considera al **ransomware** como su principal amenaza, lo cual es congruente con el contexto global en donde se estima que este tipo de ataques afectó al **66% de las empresas en el mundo** en 2021, un incremento significativo del **78% con respecto a 2020**. El Ransomware es un software dañino que impide acceder a archivos o sistemas del equipo infectado, dejándolo inutilizable a menos de que la empresa pague por un rescate. El pago promedio global de rescate fue de **$812 mil USD** en 2021.

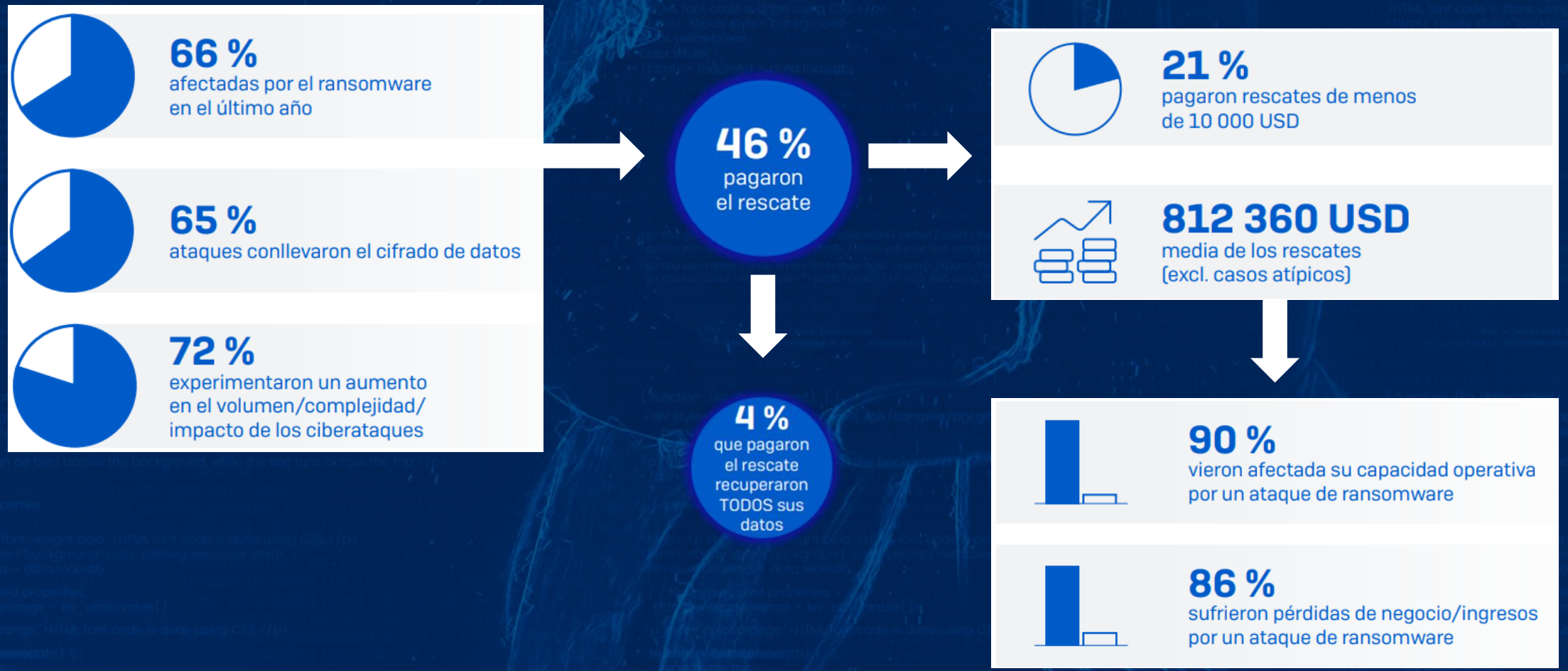
Mayor amenaza	% empresas (n=64)
Ransomware	**20%**
Violación y robo de datos	**18%**
Phishing	**13%**
Ataques a servidores e infraestructura local	9%
Vulneraciones y riesgos generados por los usuarios	9%
Continuidad de los servicios ante ataques	7%
Virus	7%
Malware	7%
Falta de cultura organizacional en ciberseguridad	7%
Vulnerabilidad del software actual	5%
DDoS	4%
Violación de datos en la nube	4%
Nuevas tácticas y tecnologías de ciberataques	4%
Ingeniería social	2%
Inyección SQL	2%
Falta de gobernanza en la empresa	2%
Zero Day	2%
Falta de normas y procedimientos	2%
Ciberseguridad en dispositivos incrustados	2%
Spyware	2%

Por encima del promedio

Fuente: elaboración propia a partir de datos de encuesta

20. Contexto: afectación global por Ransomware en 2021

De acuerdo con una encuesta global de Sophos, referente especializado en ciberseguridad, el Ransomware es una de las amenazas de mayor crecimiento en 2021. Es importante notar que una mayoría de empresas pagó por un rescate (66%), pero tan **solo el 4% de los afectados recuperó la totalidad de los datos secuestrados**. Aunque no se pague por un rescate, las empresas igualmente sufrieron pérdidas económicas y operativa, ya que tardaron en promedio un mes en recuperarse y a un costo de **$1,4 millones de USD**.



Fuente: SOPHOS, "El estado del Ransomware 2022" (n=5600; 31 países)

CAPÍTULO 3

Características de la oferta costarricense de ciberseguridad

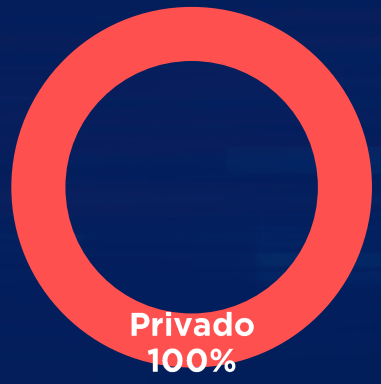
(n=14)

Este capítulo analiza a las empresas locales que desarrollan servicios y soluciones tecnológicas de ciberseguridad, para lo cual se aplicó una versión de encuesta diferenciada, a la medida de esta población.

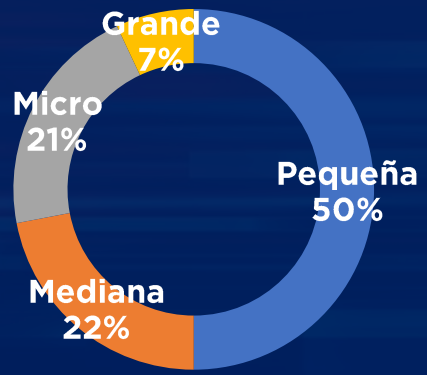
Perfil de participantes: se encuestó a un total de 14 empresas costarricenses que desarrollan ciberseguridad, la mayoría con un perfil PYME (el 93% de la muestra) y empresas grandes en menor medida.

Cantidad total de encuestados:	14 empresas
Perfil de participantes:	• CEO – **57%** • CISO – **36%** • CTO – **7%**

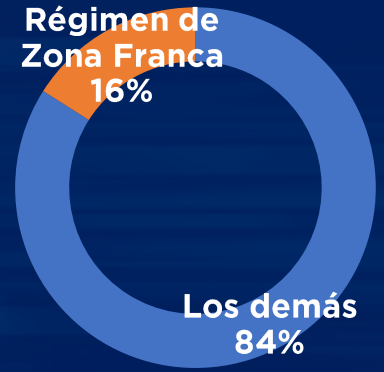
Según naturaleza:



Según tamaño:



Según clientes:



Solamente opera desde Costa Rica

71%

Posee también sucursal en otro mercado

29%

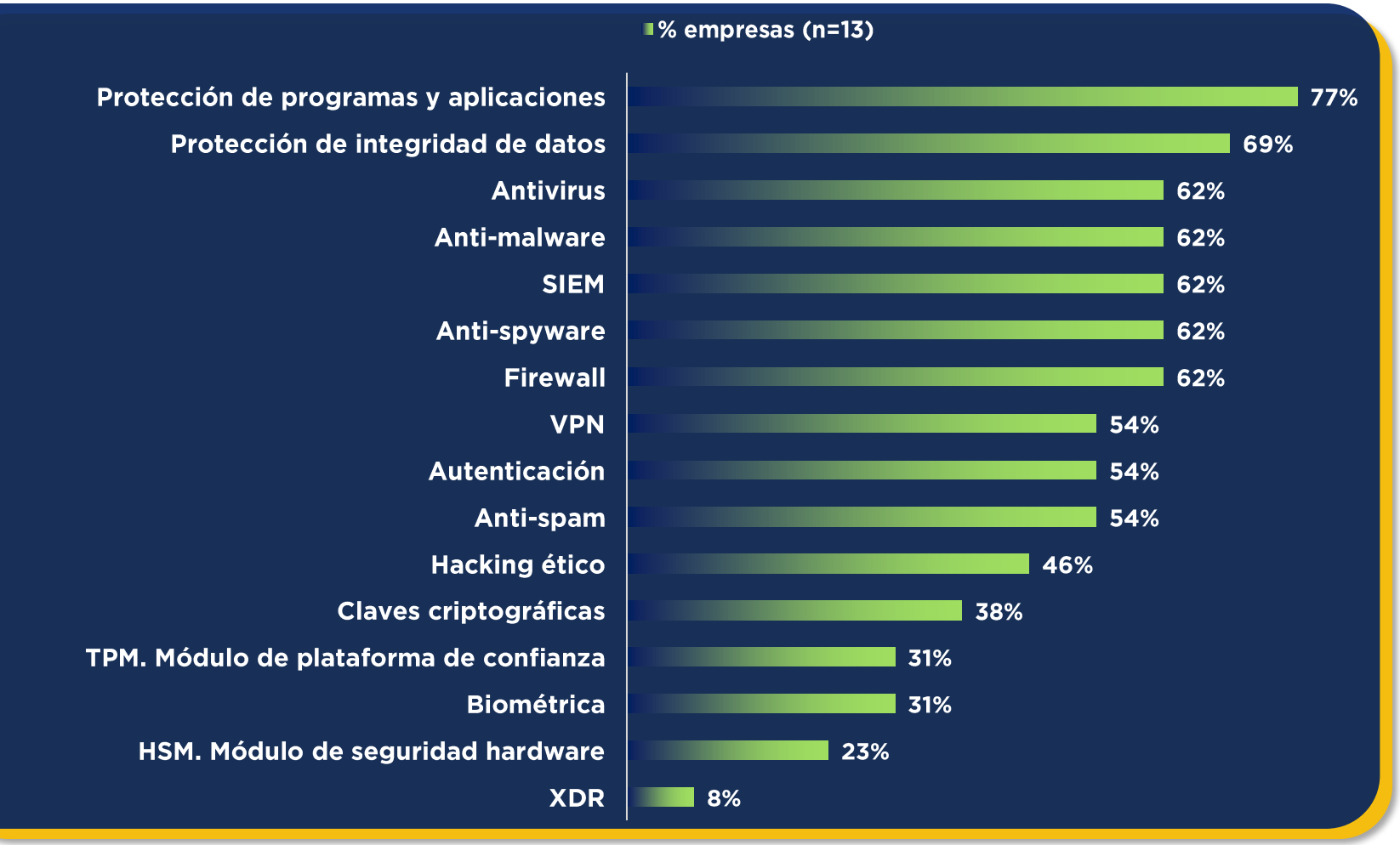
Estados Unidos, Panamá, Guatemala, Puerto Rico, República Dominicana

Fuente: elaboración propia a partir de datos de encuesta

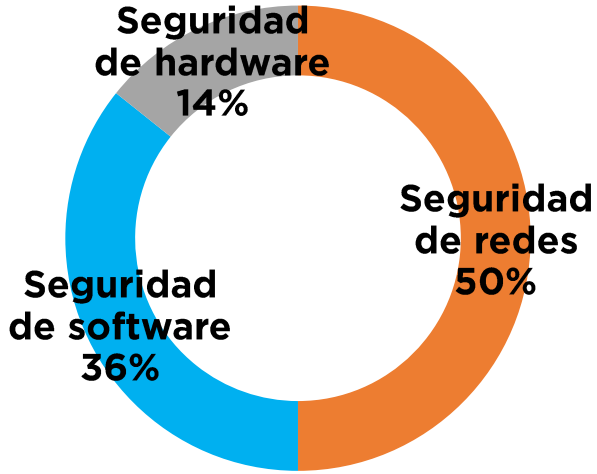
21. ¿Cuál es la categoría de seguridad más demandada por sus clientes?

La seguridad de red es la categoría de ciberseguridad más demandada entre los clientes de este grupo de empresas oferentes (50% de ellas); seguido de seguridad de software (36%) y de hardware (14%). De manera más específica, el 77% de este sector atiende protección de programas y aplicaciones; el 69% la protección de la integridad de datos y un 62% en soluciones basadas en antivirus, antimalware, antispyware y SIEM.

Principales soluciones de ciberseguridad ofertadas (2021)



Principales categorías de soluciones de ciberseguridad demandadas
(2021; n=14)



Fuente: elaboración propia a partir de datos de encuesta

22. Oferta de productos de ciberseguridad

Principales productos de ciberseguridad ofertados

(2021; n=14)

Descripción de la solución	% empresas (n=14)
Fortinet	21%
Antivirus varios	14%
Cynet 360	
Microsoft Azure	7%
NGFW (Next-Generation Firewall)	7%
Anti-malware	7%
Atvise SCADA	7%
VPNs	7%
Carbon Black (End Point Security)	7%
Citrix (App Security)	7%
Pfsense	7%
Cleafy (Fraud Prevention)	7%
CloudFlare (DDoS and App Security)	7%
Vmware (Microsegmentacion)	7%
Cymylate (Breach and Attack Simulation)	7%
WhatchGuard	7%
Cyrebro (SOC-SIEM)	7%
MDR (Managed Detection and Response)	7%

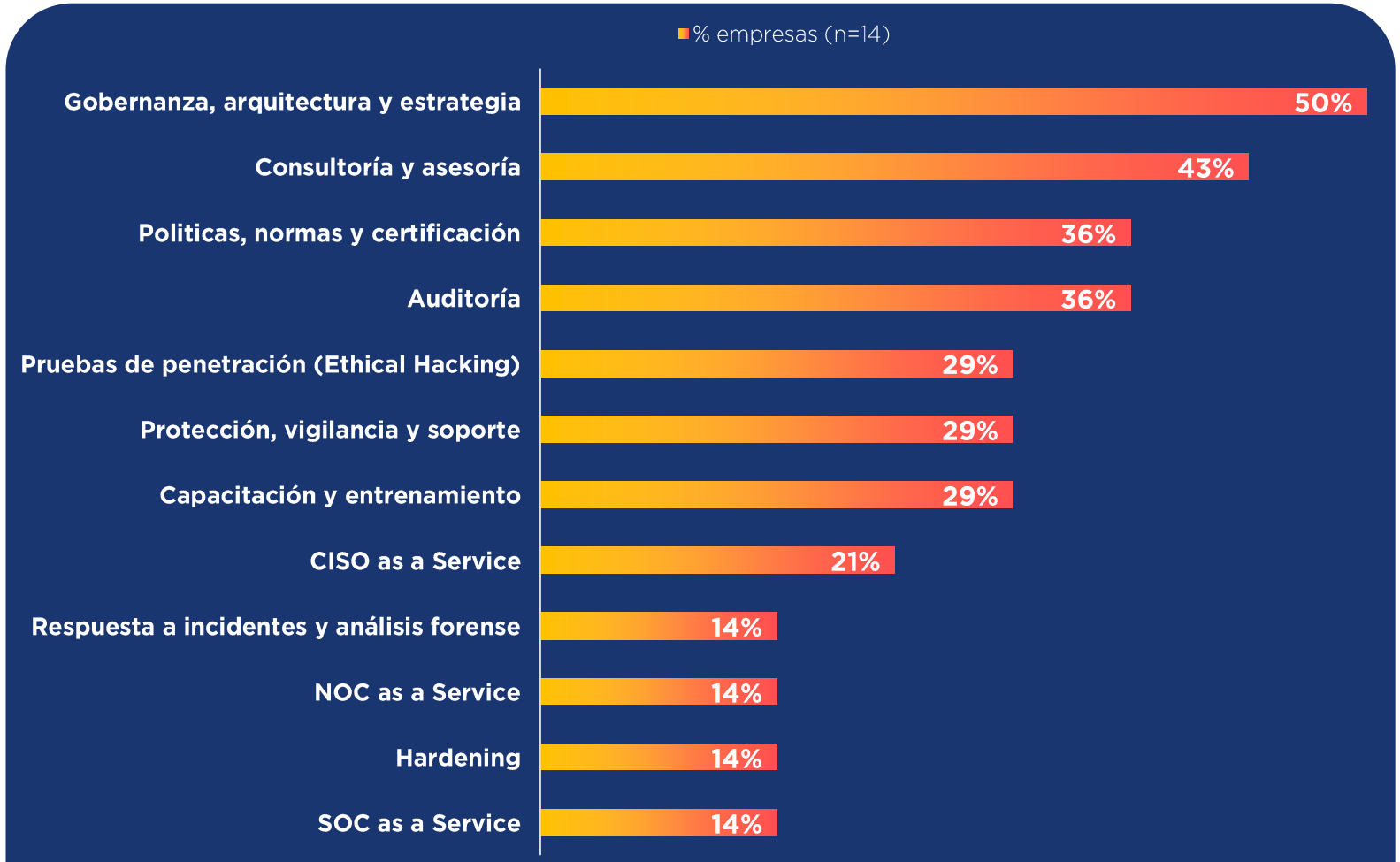
Descripción de la solución	% empresas (n=14)
Darktrace (IA/ML Detection)	7%
Mikrotik	7%
Defender cloud	7%
Oracle Solutions	7%
Ping Identity (IDM)	7%
DNSEC	7%
EDR (Endpoint Detection Response)	7%
Tenable (Vulnerability Management)	7%
Teramind (DLP y Productiviy)	7%
Imperva (Data and App security)	7%
Vnode	7%
Industrial-Shields	7%
Webs-8000	7%
Jace-8000	7%
Alert-8000	7%
Kaspersky	7%

P/ ¿Qué porcentaje de sus ventas de seguridad informática es resultado de la comercialización de productos de ciberseguridad?

Fuente: elaboración propia a partir de datos de encuesta

22. Oferta de servicios de ciberseguridad

Principales servicios de ciberseguridad ofertados (2021)



Otros servicios	% empresas
Pruebas de concepto	7%
Gestión de Proyectos TI (PMTIaaS)	7%
Autenticación	7%
Control de contenido	7%
Secure Coding	7%

Fuente: elaboración propia a partir de datos de encuesta

23. Principal especialización o diferencial de la oferta de ciberseguridad

Especialización principal de la empresa	% empresas (n=14)
Penetration Testing (Hacking ético)	14%
Seguridad de redes	14%
Ciberseguridad en redes industriales y operativas (de dispositivos IoT)	7%
Capacitación	7%
Infrastructura segura multinube para red IT & OT	7%
CISO as a Service	7%
Plataforma SOC (SIEM integrado)	7%
Protección de Identidades	7%
Seguridad ofensiva	7%
Estrategia de ciberseguridad basada en auditoría y diagnóstico	7%
Autentificación	7%
Infraestructura tecnológica	7%
Total general	**100%**

Fuente: elaboración propia a partir de datos de encuesta

Consideraciones clave

1. **Prevención vs respuesta:** el abordaje de seguridad de las empresas es mayormente preventivo, con poca preparación en acciones de respuesta y recuperación ante incidentes. Si se considera que el 89% de las empresas ha estado expuesta a ataques, es claro que las estrategias de continuidad del negocio resultan tan importantes como las preventivas, donde solo el 55% ha implementado acciones al respecto.

2. **Vulnerabilidad centrada en la micro empresa:** casi un 10% de las empresas no solo nunca ha invertido en ciberseguridad, sino que tampoco considera necesario hacerlo en el corto plazo, la mayoría de ellas de tamaño micro/pequeña. Más que una limitante de presupuesto, refleja pobre cultura organizacional y desconocimiento sobre la relevancia de la ciberseguridad.

3. **Ransomware es la principal preocupación:** casi 4 de cada 10 empresas costarricenses se va visto afectada, que está además entre los de mayor crecimiento en el mundo (+78% en 2021 vs año anterior). Considerando la tendencia global, es una posibilidad que más empresas locales o Gobierno resulten expuestas, ante lo cual destaca aún más la importancia de contar con planes de continuidad del negocio y recuperación ante desastres señalada anteriormente.

4. **Mitad de empresas son soft-users:** el 45% de empresas ha implementado entre 1 a 4 categorías de soluciones de ciberseguridad estratégica, es decir, son usuarios parciales o poco intensivos de seguridad digital, comparado con el 29% de empresas que han implementado a cabalidad entre 9 a 12 categorías (heavy-users). Por otra parte, según soluciones utilizadas, destacan entre las más empleadas aquellas básicas y habituales para las empresas, es decir, paquetes de antivirus, firewall, anti-malware o VPNs; pero una muy baja participación de otras más exhaustivas y especializadas, como XDR (23% de empresas), Zero Trust (17%) o SASE (15%), entre otros.

5. **Ciberseguridad compite en presupuesto con otras tecnologías 4.0:** entre las limitantes para el gasto en ciberseguridad, el 62% de empresas ha priorizado invertir en otras tecnologías. Cloud Computing, Big Data e IoT son las tres principales en las que más gastan las empresas, en complemento a ciberseguridad.

Caracterización del uso y necesidades potenciales de *ciberseguridad*

en empresas costarricenses

Erick J. Apuy
Dirección de Inteligencia Comercial
Mayo 2022