Deloitte.

ESCUELA BANCARIA DE GUATEMALA

Tendencias en Cyber Riesgos y Seguridad de la Información

Estudio de Tendencias en Latinoamérica 2016

Agosto 2016

Agenda

1. Introducción al Estudio de Deloitte sobre Cyber Riesgos y Seguridad de la Información en Latinoamérica en 2016
2. Resumen de las Tendencias Identificadas
3. Principales Resultados y Hallazgos
4. Conclusiones Finales

Introducción al Estudio

Introducción al Estudio de Deloitte sobre Cyber Riesgos y Seguridad de la Información en Latinoamérica en 2016

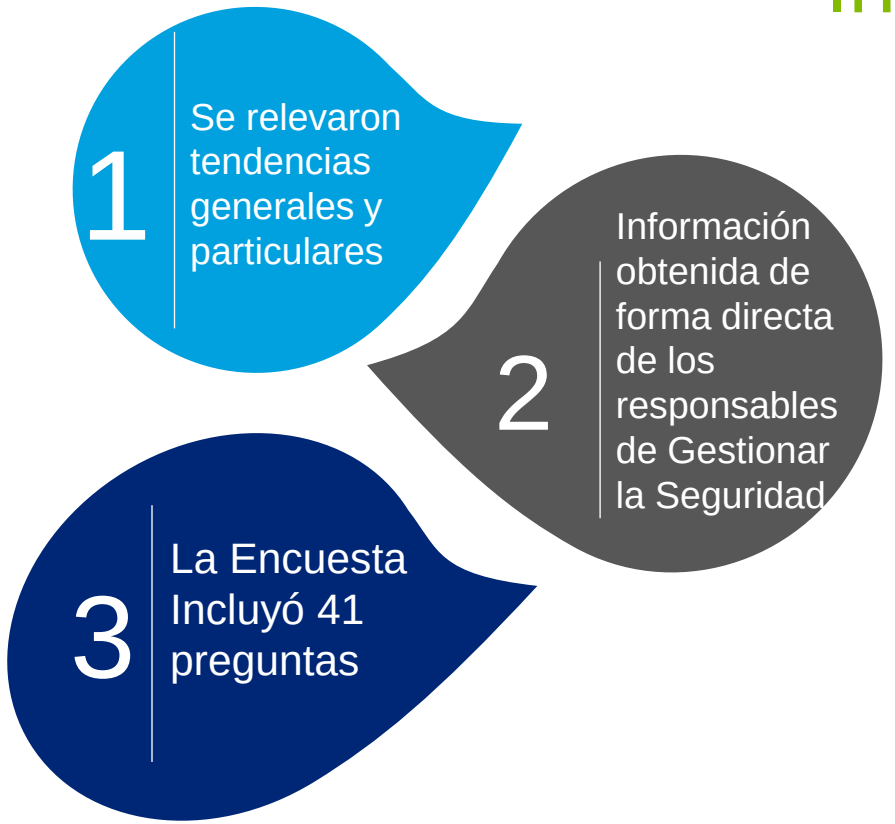
Iniciativa Regional que permite identificar las tendencias en Cyber Riesgos y Seguridad de la Información

- Realizado entre Enero y Abril de 2016.
- Reuniones y Entrevistas con CISOs, Líderes y responsables de gestionar Cyber Riesgos y Seguridad de la Información de organizaciones de múltiples industrias.
- Las organizaciones participantes reciben un reporte de benchmarking personalizado

El Estudio 2016 en números

89/ **Organizaciones participantes**

14/ **Países**



Gobierno

Presupuesto e Inversiones

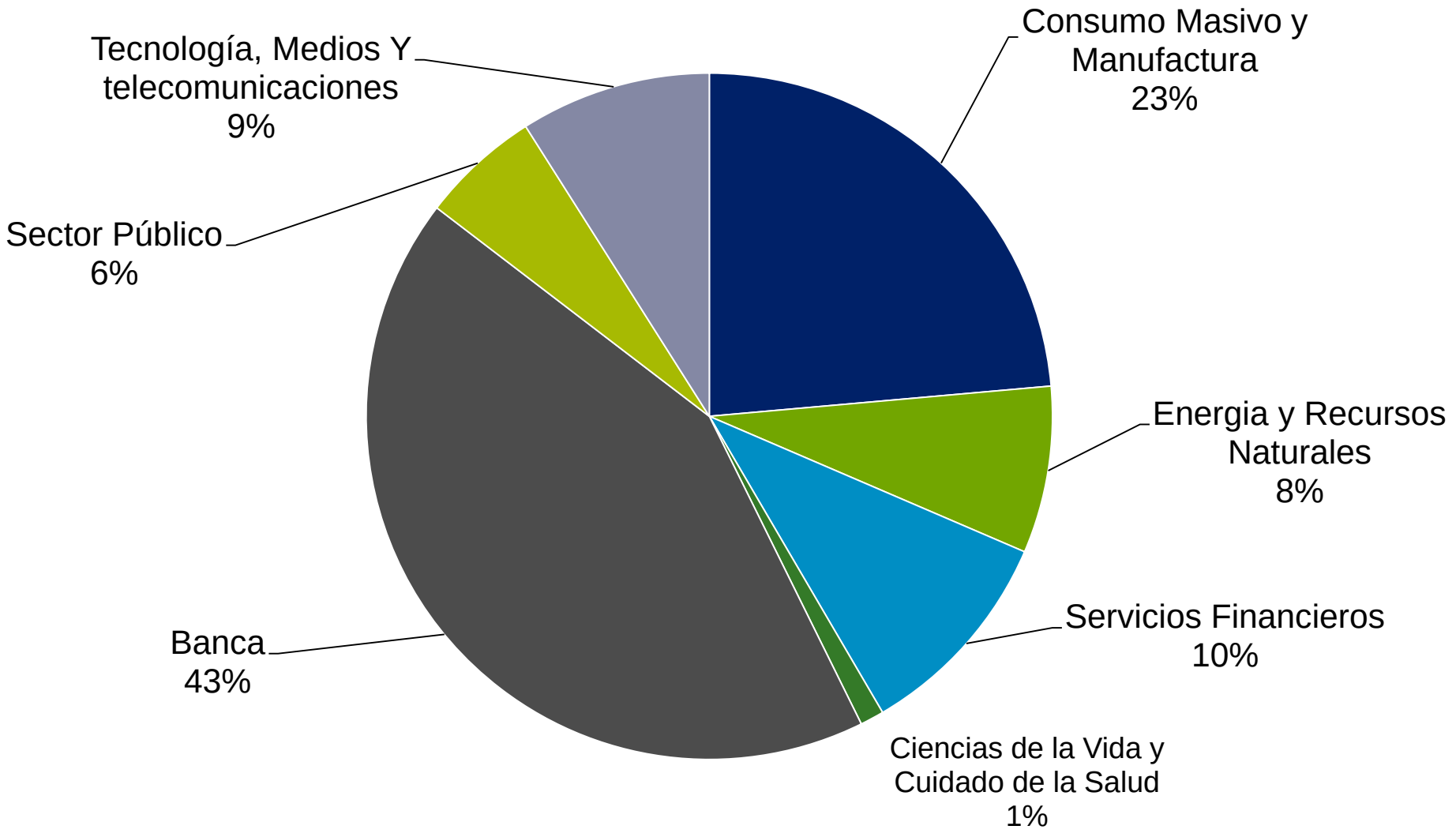
Amenazas

SOC

Tecnologías

Mejores Prácticas

Industrias y Sectores Económicos Participantes



Resumen de las Tendencias Identificadas

Principales Tendencias

1. 4 DE CADA 10 ORGANIZACIONES SUFRIERON UNA BRECHA DE SEGURIDAD EN LOS ULTIMOS 24 MESES

   MENOS DEL 20% DE LAS ORGANIZACIONES CUENTAN CON UN SOC (Security Operation Center)

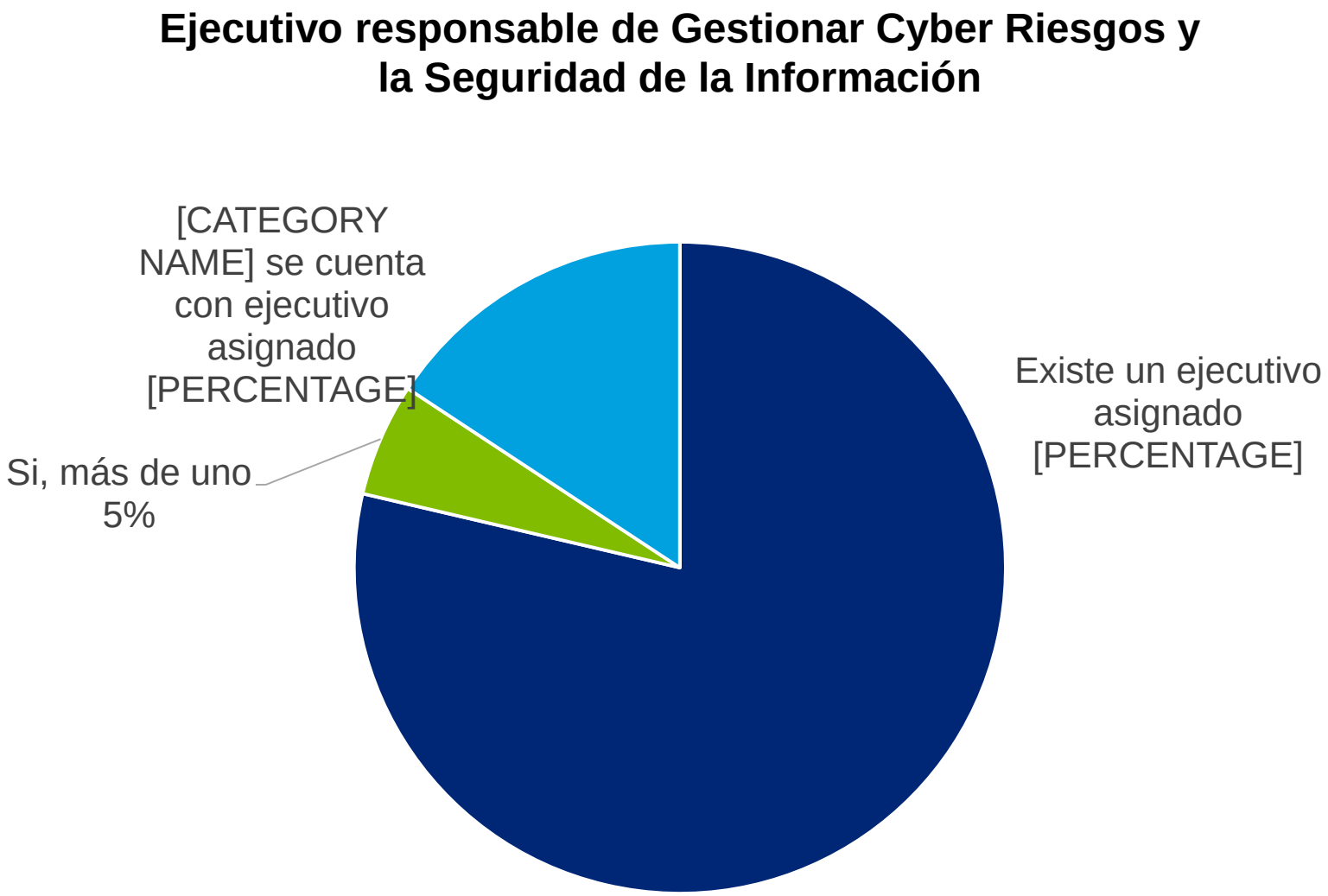
2. A PESAR DE QUE LAS ORGANIZACIONES INCREMENTAN SUS PRESUPUESTOS, LA PRINCIPAL BARRERA QUE ENFRENTAN LOS CISOs SIGUE SIENDO LA FALTA DE PRESUPUESTO Y/O DE RECURSOS SUFICIENTES

3. MENOS DEL 10% DE LAS ORGANIZACIONES CUENTAN CON INDICADORES (KPIs) Y/O TABLERO DE GESTION INTEGRAL DE RIESGOS DE SEGURIDAD

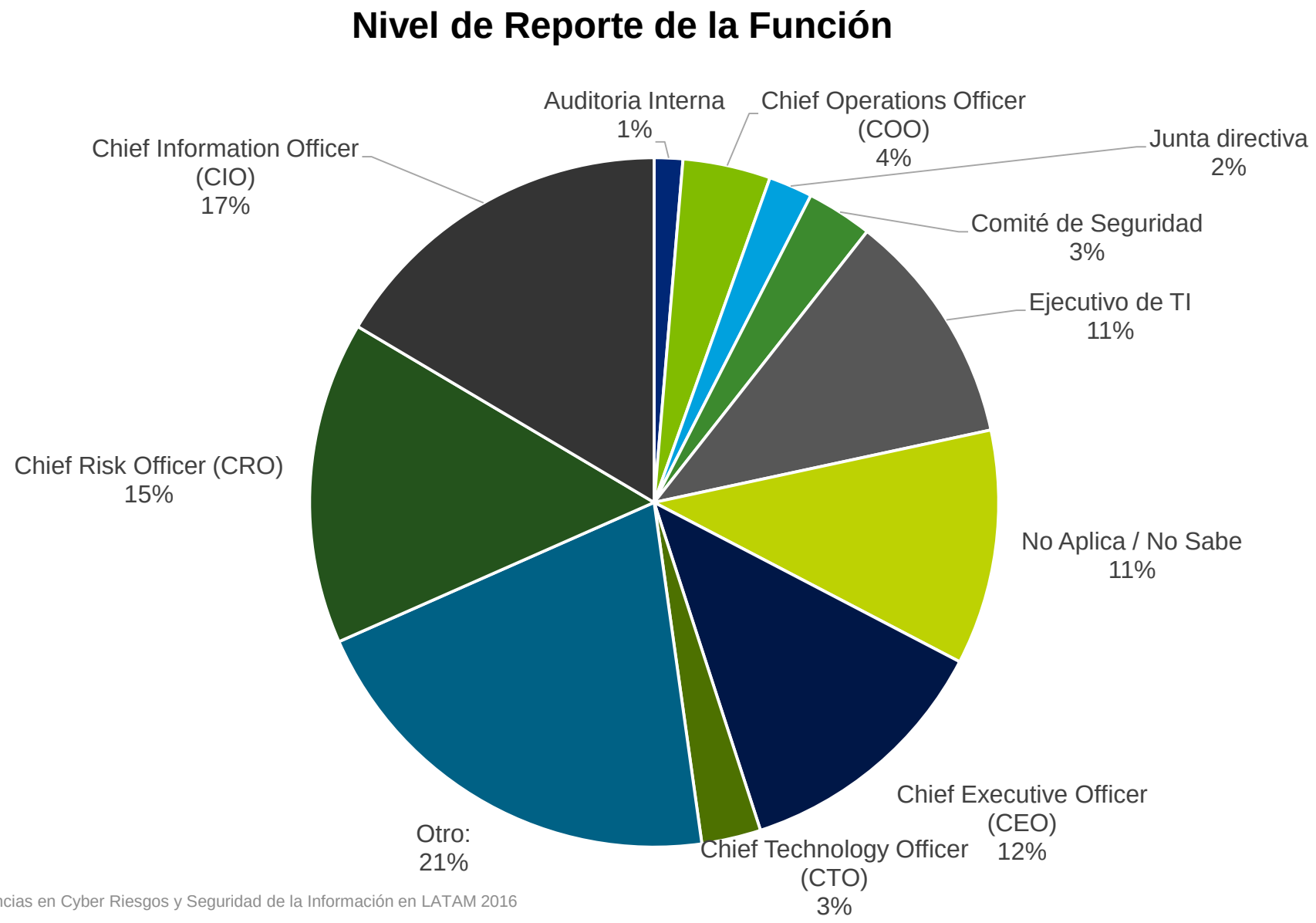
4. LA CAPACITACIÓN Y CONCIENTIZACIÓN ES LA INICIATIVA DE SEGURIDAD QUE MAYOR CANTIDAD DE ORGANIZACIONES EJECUTARAN EN 2016

Principales Resultados y Hallazgos

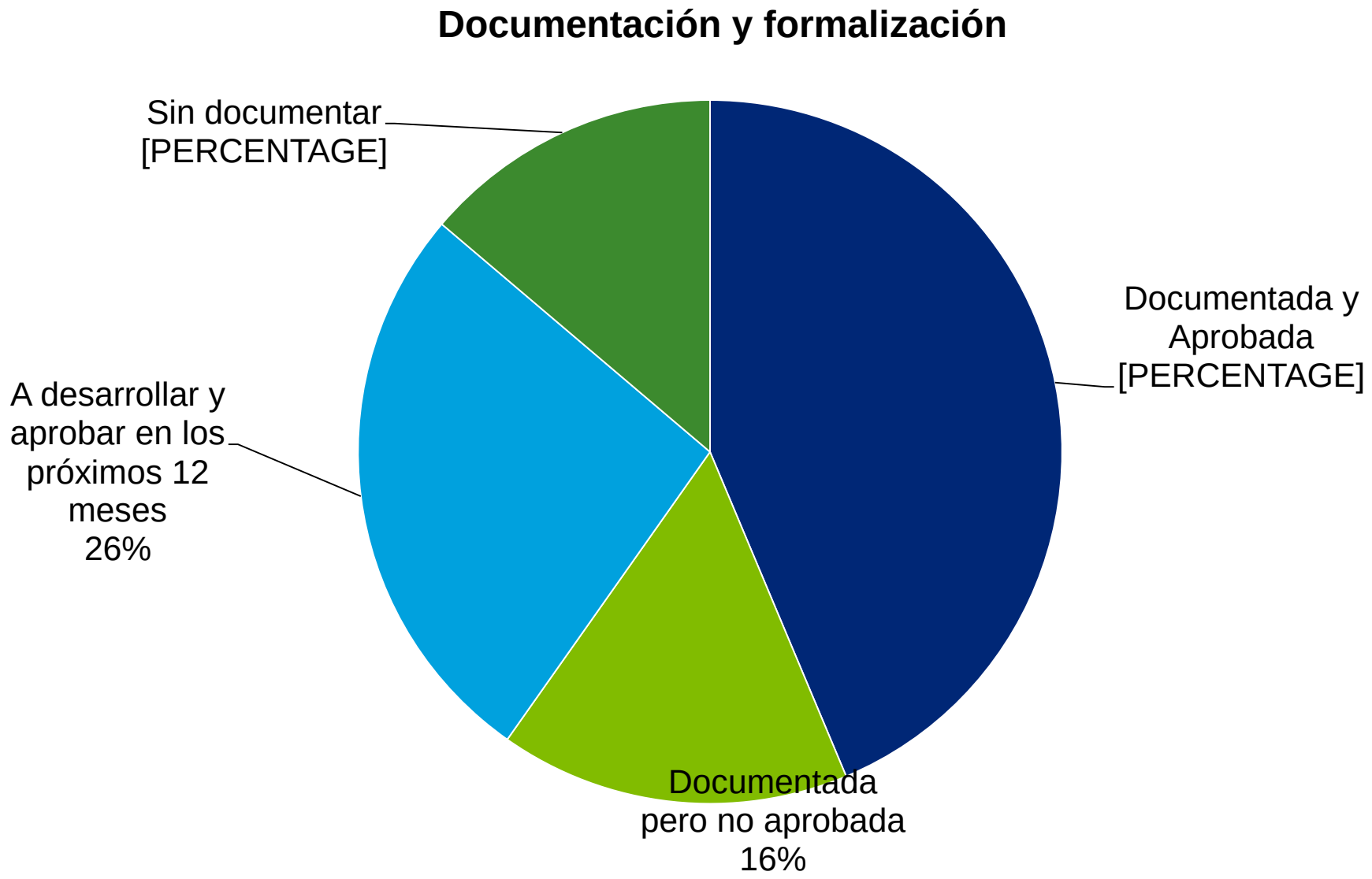
Conformación del área de Seguridad de la Información



Conformación del área de Seguridad de la Información (cont.)



Estrategia de Cyber Riesgos y Seguridad de la Información



Principales obstáculos y barreras que enfrenta el CISO

#1/ Falta de Presupuesto y/o Recursos Suficientes (50%)

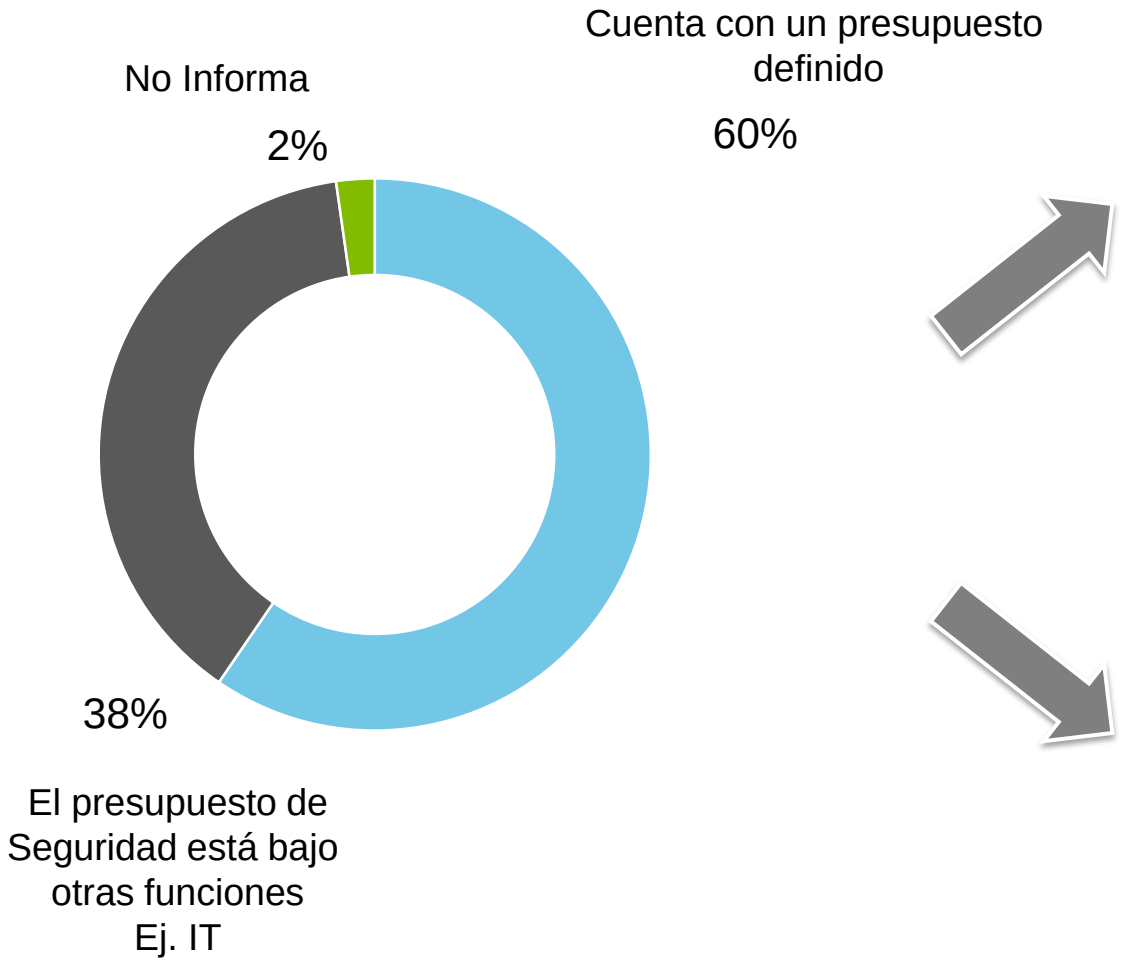
#2 / Falta de Visibilidad y/o Influencia en la Organización (37%)

- Menos del 25% de las Organizaciones consideran que la complejidad de las amenazas hace más difícil gestionar la seguridad
- Sólo un 15% considera que las nuevas tecnologías dificultan la gestión de seguridad

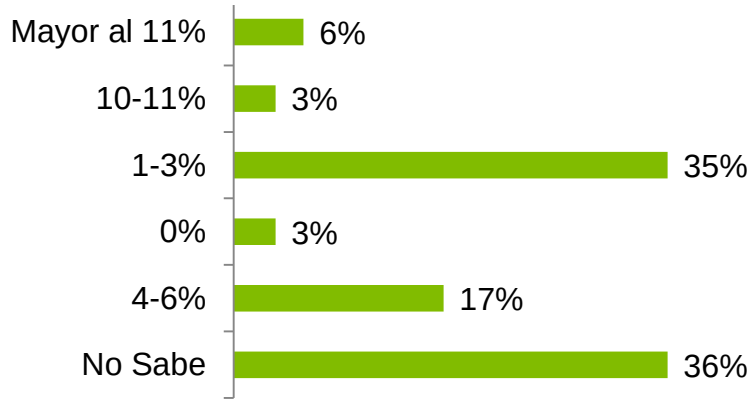
Responsabilidades del CISO

+ 50%

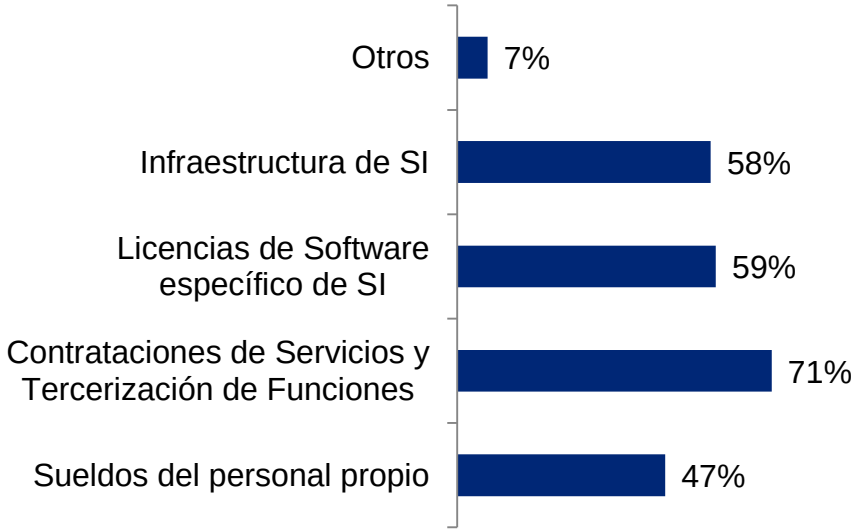
Presupuesto de Seguridad de la Información



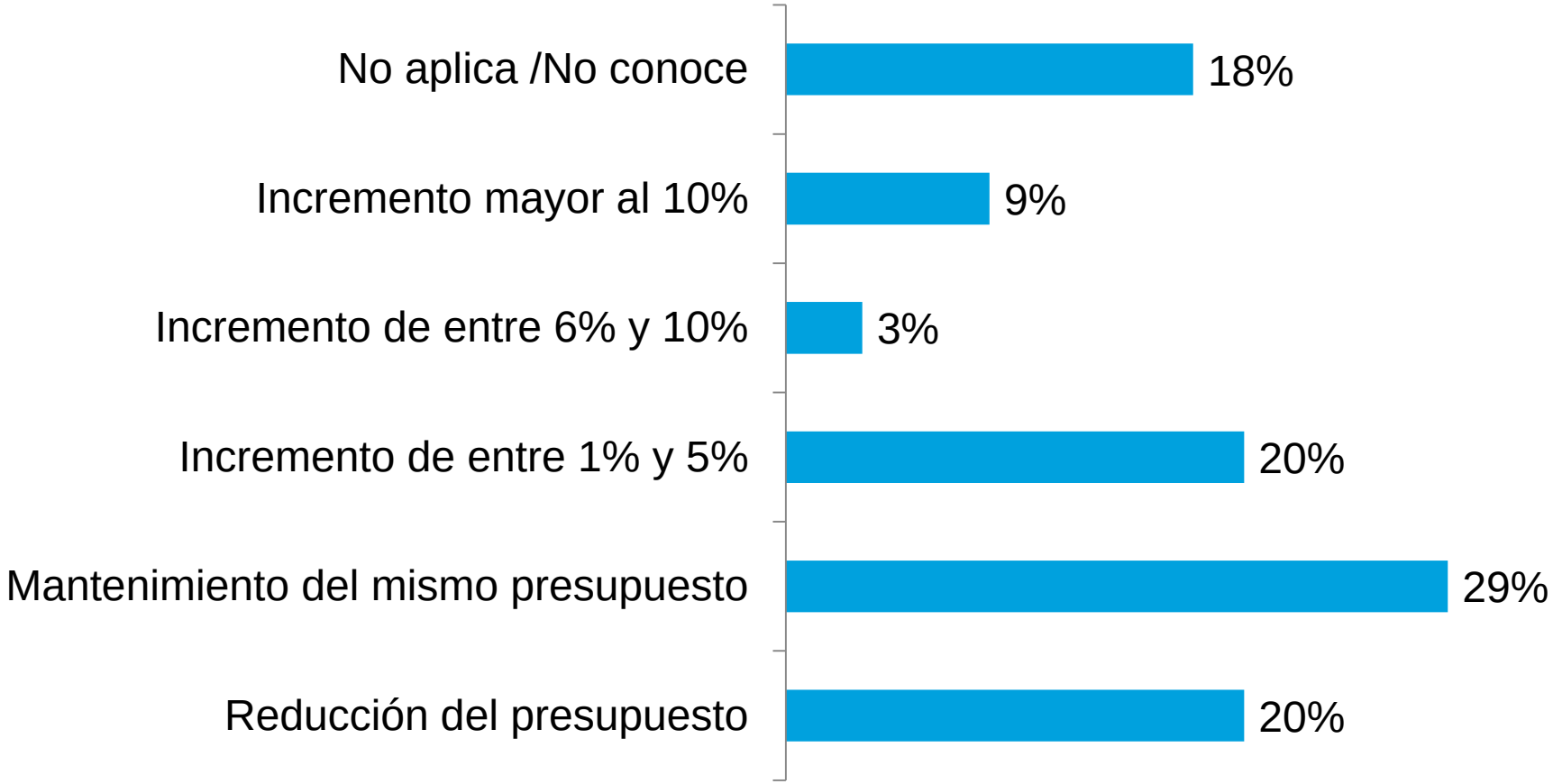
Presupuesto de SI en relación al % Presupuesto TI



Distribución del presupuesto



Evolución del Presupuesto respecto 2015



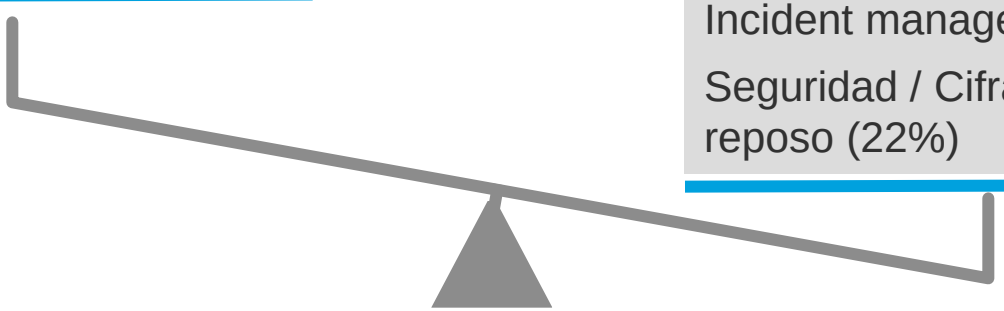
Principales iniciativas para el 2016

1. Capacitación y concientización en Seguridad de la Información
2. Gobierno de Seguridad de la Información (SI)
3. Alineación de la SI con el negocio
4. Protección de datos sensibles
5. Generación de indicadores, medición y reporte de SI

Tecnologías de Seguridad

Más Utilizadas

- Antivirus (100%)
- Firewalls (99%)
- Antispam (82%)
- Anti spyware (71%)
- Filtro de contenido (60 %)
- Sistema de Detección o Prevención de Intrusos (IDS/IPS) (64%)
- Vulnerability management (52%)
- Network access control (42%)

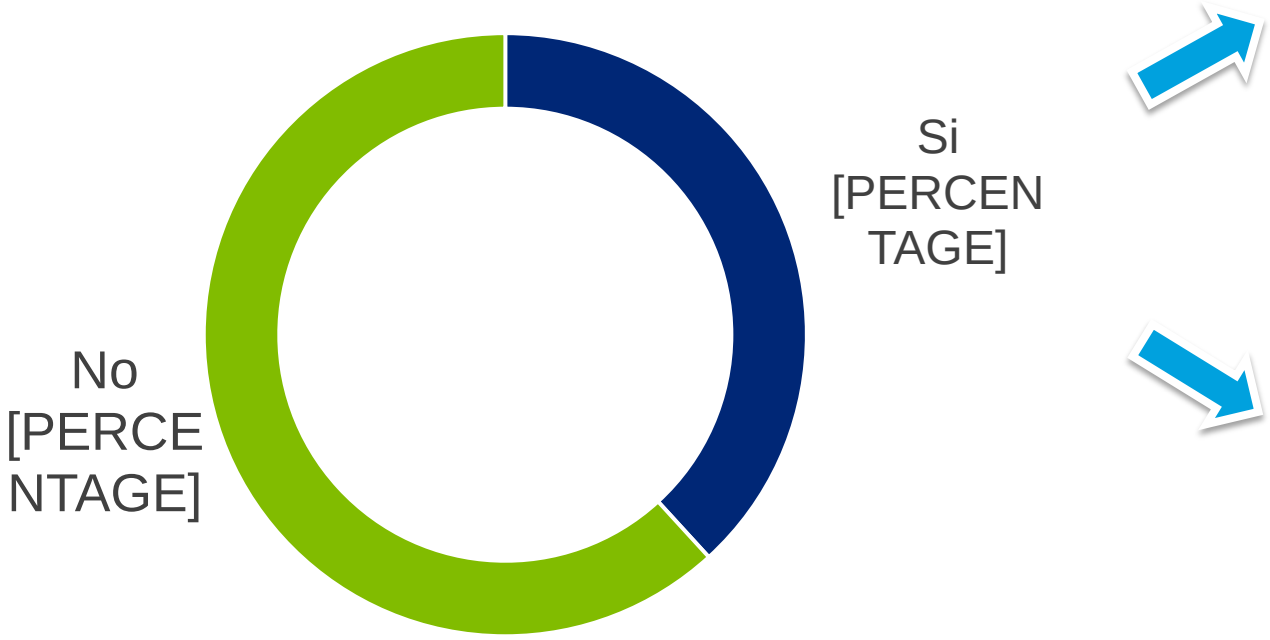


Menos Utilizadas

- Administración de identidades federada (12%)
- Cifrado de almacenamiento / dispositivos móviles (17%)
- Enterprise Single Sign On (19%)
- Incident management workflow (22%)
- Seguridad / Cifrado de datos en reposo (22%)

Brechas de Seguridad

Ha sufrido una brecha externa y/o interna de seguridad en los últimos 24 meses?



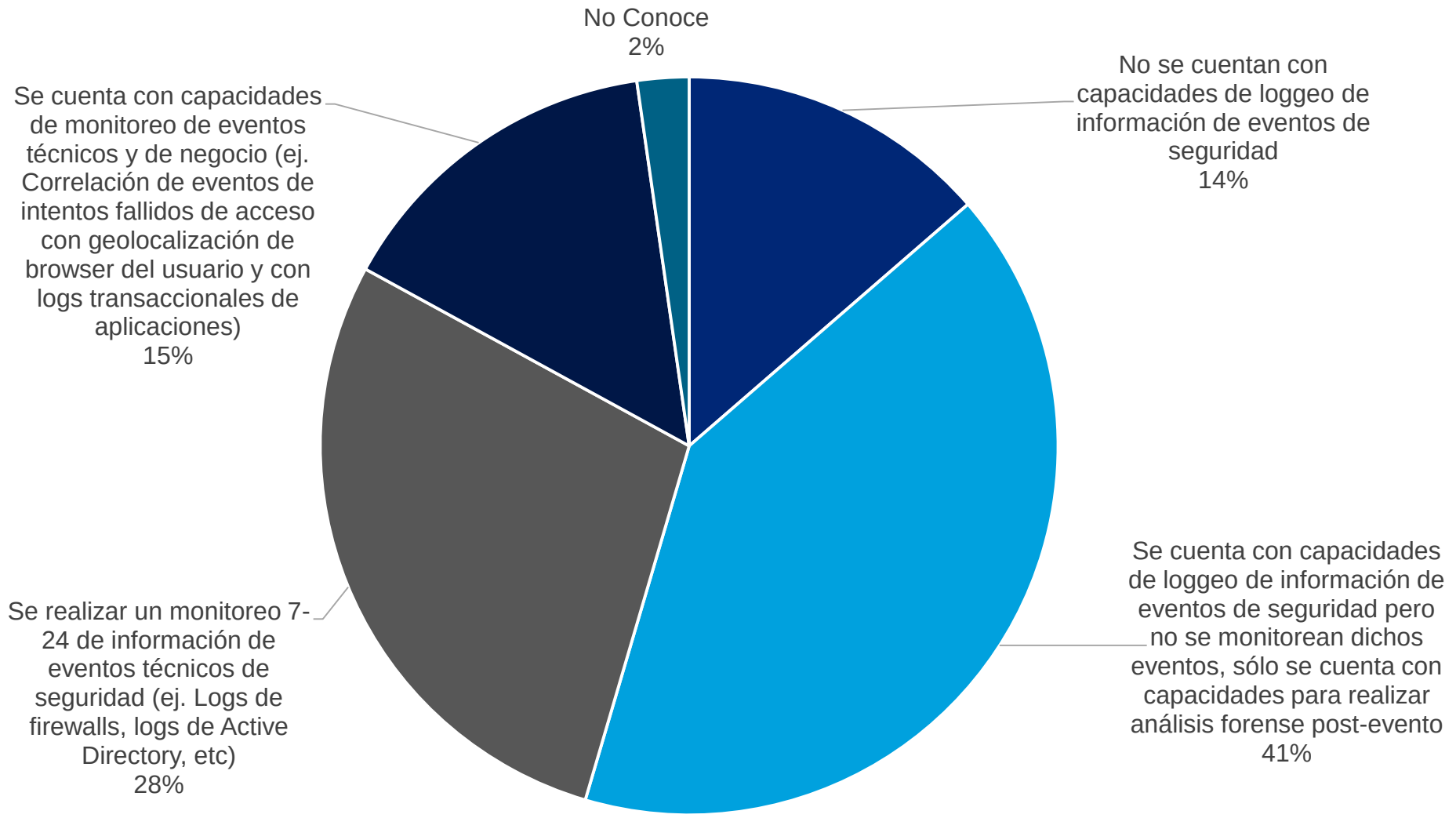
Vectores:

- Software malicioso (malware, troyano, virus, ransomware) que ingresa desde fuera de la organización
- Incidente causados por un ataque físico (ej. laptop robada)
- Incidente de seguridad ocasionado por un empleado (utilización de privilegios excesivos)

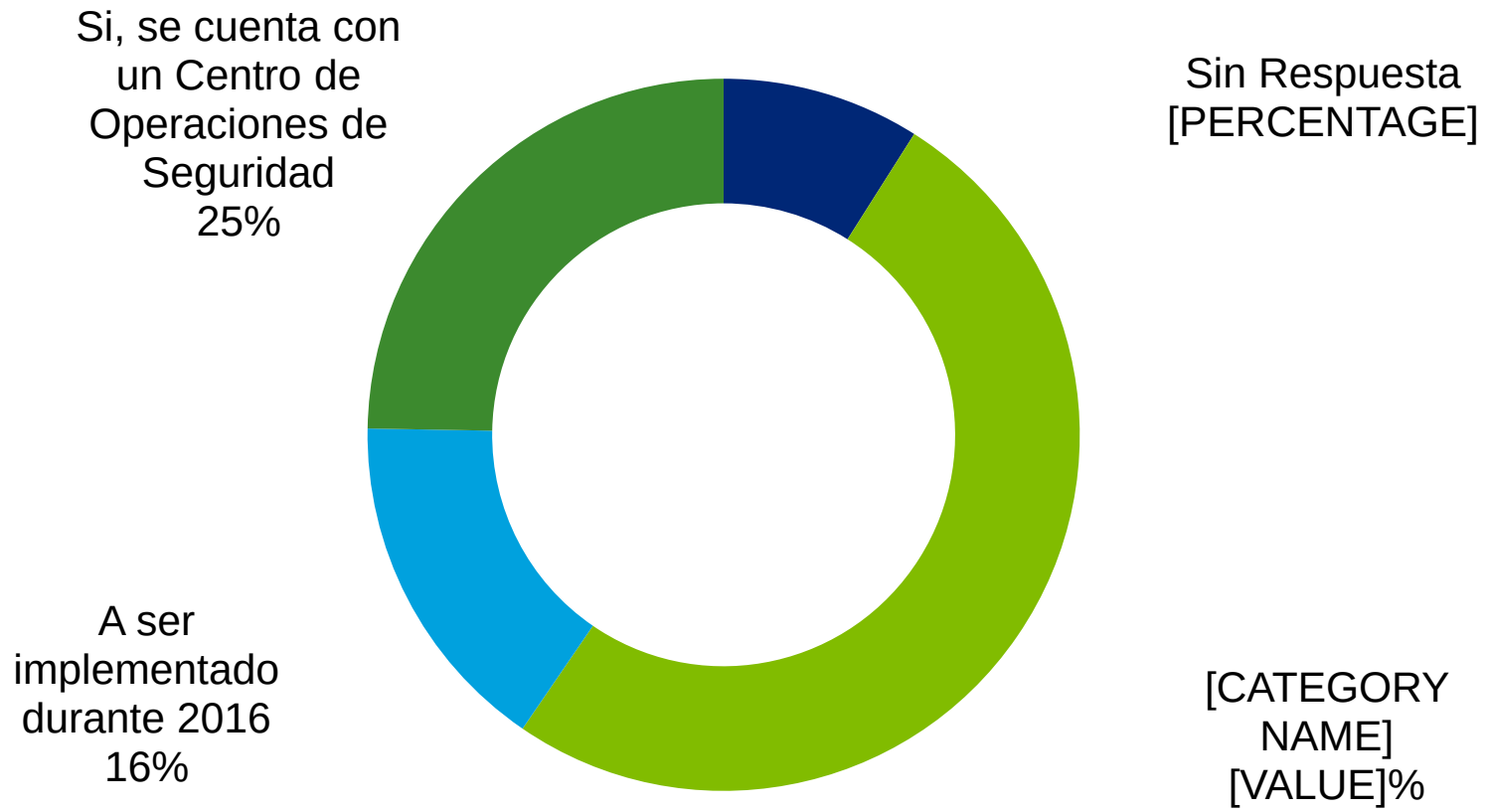
Impacto Económico/Financiero:

- La mayoría *No sabe o No aplica* (+57%)
- Para aquellos que han evaluado, el 38% informa que el incidente no ha tenido impacto financiero
- El 20% sufrió perdidas inferiores a los USD 250,000 y un 5% pérdidas superiores a dicho monto.

Capacidades de Monitoreo y Respuesta ante Incidentes



Utilización de un SOC (“Security Operation Center”)

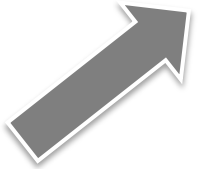


Debilidades en Controles de Seguridad – Hallazgos de Auditoría

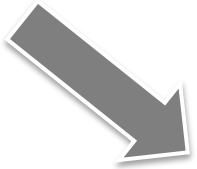
Prácticas de Administración de Usuarios y Accesos

Protección de Datos Personales

+80% de las Organizaciones deben cumplir con regulaciones o leyes de protección de datos personales



Sólo la mitad han asignado recursos con dedicación a proteger datos personales



1 de cada 4 organizaciones han sufrido brechas de seguridad con impacto en datos personales

Conclusiones Finales

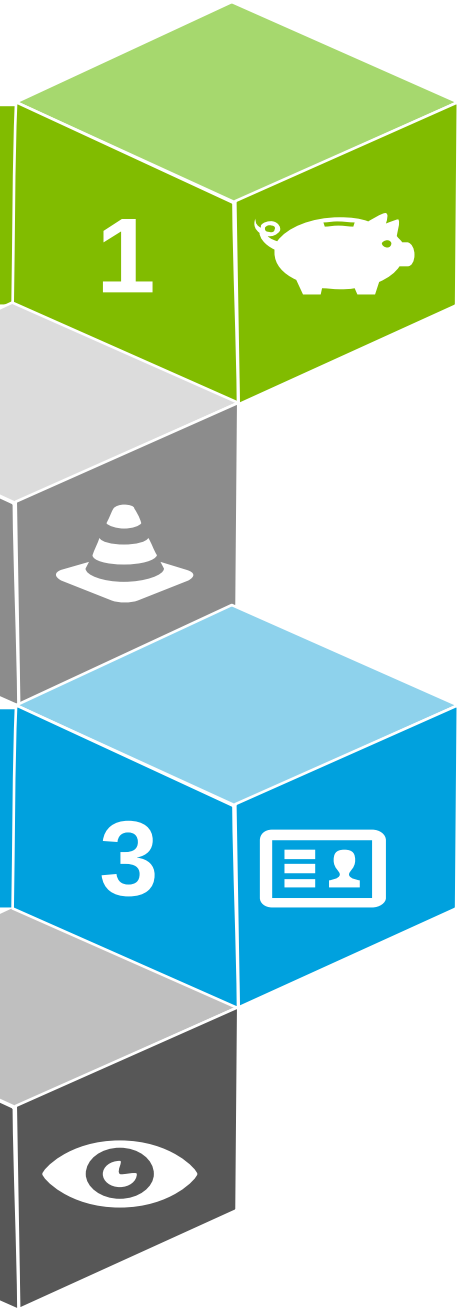
Consideraciones finales

Si bien existe conciencia sobre la importancia de la seguridad de la información, los CISOs en América Latina aún luchan por convencer a la organización para que inviertan en Seguridad

Los CISOs en Latinoamérica tienen bastante claridad y acuerdo en el alcance de sus responsabilidades y procesos. En ese alcance generalmente no se incluye la seguridad física ni la continuidad de negocio.

En un contexto de nuevas y más sofisticadas cyber amenazas, las Auditorías de Seguridad siguen identificando debilidades básicas de seguridad en segregación de funciones y administración de usuarios. Estos aspectos continúan siendo un área a mejorar por los CISOs

El desarrollo de capacidades para monitorear y responder a las cyber amenazas representa una necesidad urgente, las organizaciones aún se encuentran en un estado temprano de madurez en prácticas de Monitoreo y SOC



Muchas Gracias!!

Deloitte.

Acerca de Deloitte

Deloitte presta servicios profesionales en auditoría, impuestos, consultoría y asesoramiento financiero a organizaciones públicas y privadas de diversas industrias. Con una red global de firmas miembro en 140 países, Deloitte brinda su experiencia y profesionalismo de clase mundial para ayudar a sus clientes a alcanzar el éxito desde cualquier lugar del mundo en el que éstos operen.

Los 165.000 profesionales de la Firma están comprometidos con la visión de ser modelo de excelencia; están unidos por una cultura de cooperación basada en la integridad y el valor excepcional a los clientes y mercados, en el compromiso mutuo y en la fortaleza de la diversidad. Disfrutan de un ambiente de aprendizaje continuo, experiencias retadoras y oportunidades de lograr una carrera en Deloitte. Sus profesionales están dedicados al fortalecimiento de la responsabilidad empresarial, a la construcción de la confianza y al logro de un impacto positivo en sus comunidades.

Deloitte se refiere a Deloitte Touche Tohmatsu -asociación suiza- y a su red de firmas miembro, cada una como una entidad única e independiente. Por favor, vea en www.deloitte.com/about la descripción detallada de la estructura legal de Deloitte Touche Tohmatsu y sus Firmas miembro.