Deloitte.

La Evolución de la Gestión de Ciber-Riesgos y Seguridad de la Información

Encuesta 2016 sobre Tendencias de Ciber-Riesgos y Seguridad de la Información en Latinoamérica

Julio 2016

Índice

Introducción

La Evolución de la Gestión de Ciber-Riesgos y Seguridad de la Información

Deloitte se complace en presentar los resultados del **Estudio 2016 sobre Tendencias en Gestión de Ciber-Riesgos y Seguridad de la Información en Latinoamérica**.

Las Organizaciones en Latinoamérica se encuentran inmersas en un contexto de fuerte desarrollo de negocios digitales y de mayor exposición a las ciberamenazas inherentes a este nuevo contexto de negocios.

En los resultados obtenidos revela que si bien hay una consolidación de la función de gestión de ciber-riesgos y seguridad de la información, los ejecutivos responsables de administrar la seguridad de la información consideran que aún no cuentan con recursos suficientes y son conscientes que tienen un largo camino por recorrer.

Dentro de los aspectos que presentan mayores desafíos para las organizaciones en Latinoamérica se destaca la implementación de capacidades de monitoreo de riesgos y de respuesta ante incidentes, y brechas de seguridad de la información. Esto resulta de relevancia considerando que 4 de cada 10 organizaciones han sufrido una brecha de seguridad en los últimos 24 meses.

El camino para convertirse en una organización adaptada a los ciber-riesgos actuales debe iniciarse a partir de la toma de conciencia y la concientización de los niveles ejecutivos de la organización sobre las ciber-amenazas propias del nuevo ambiente digital de negocios. Comprender el nivel de exposición y qué se puede hacer para mejorar es el primer paso que los Ejecutivos de gestionar los ciber-riesgos deben dar.

Lo invitamos a recorrer el presente documento donde encontrará un resumen de las principales tendencias de ciber-riesgos y seguridad de la información identificadas, y el detalle de los aspectos clave identificados según las respuestas recibidas de las organizaciones participantes.

Información General sobre el Estudio

Objetivo y Alcance del Estudio

El Estudio tiene por objetivo identificar las tendencias en materia de gestión de Ciber-Riesgos y Seguridad de la Información en Latinoamérica

Las áreas alcanzadas incluyen los aspectos clave que hacen a la gestión de ciber-riesgos y seguridad de la información.

Las organizaciones participantes reciben resultados personalizados comparando sus prácticas de gestión de ciber-riesgos y seguridad de la información contra las tendencias relevadas.

89/ **Organizaciones participantes**

13/ **Países**

7/ **Industrias / Sectores**

Gobierno y Estrategia

Presupuesto e Inversiones

Amenazas

Mejores Prácticas

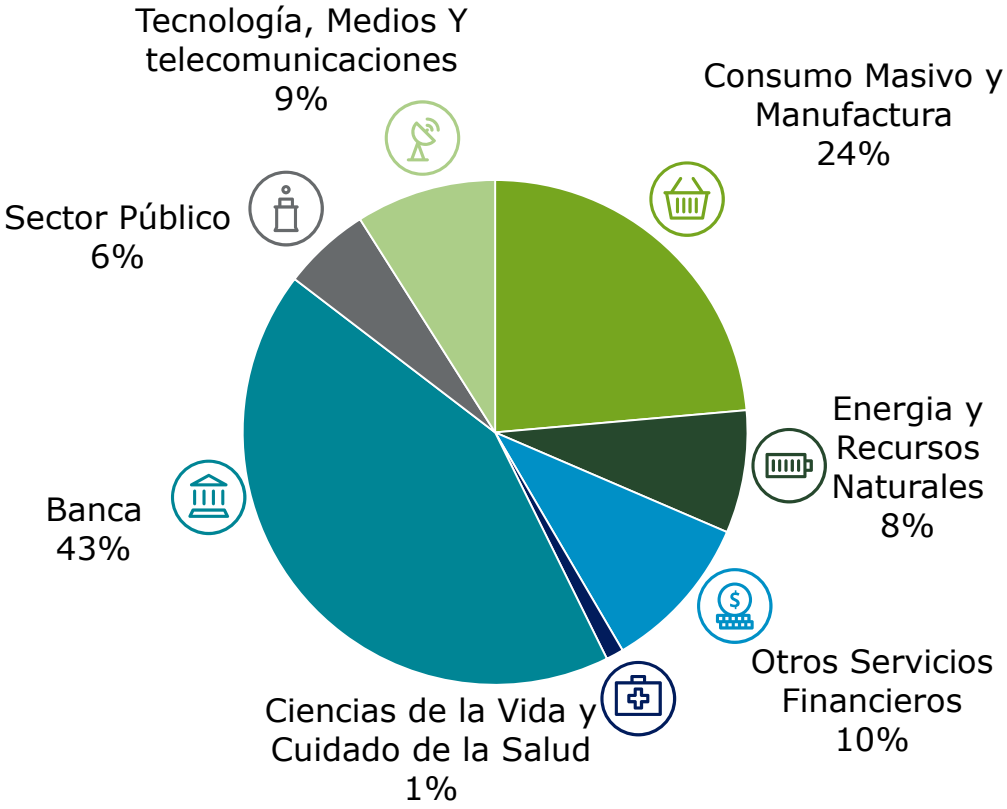
Tecnologías

SOC

Información General sobre el Estudio

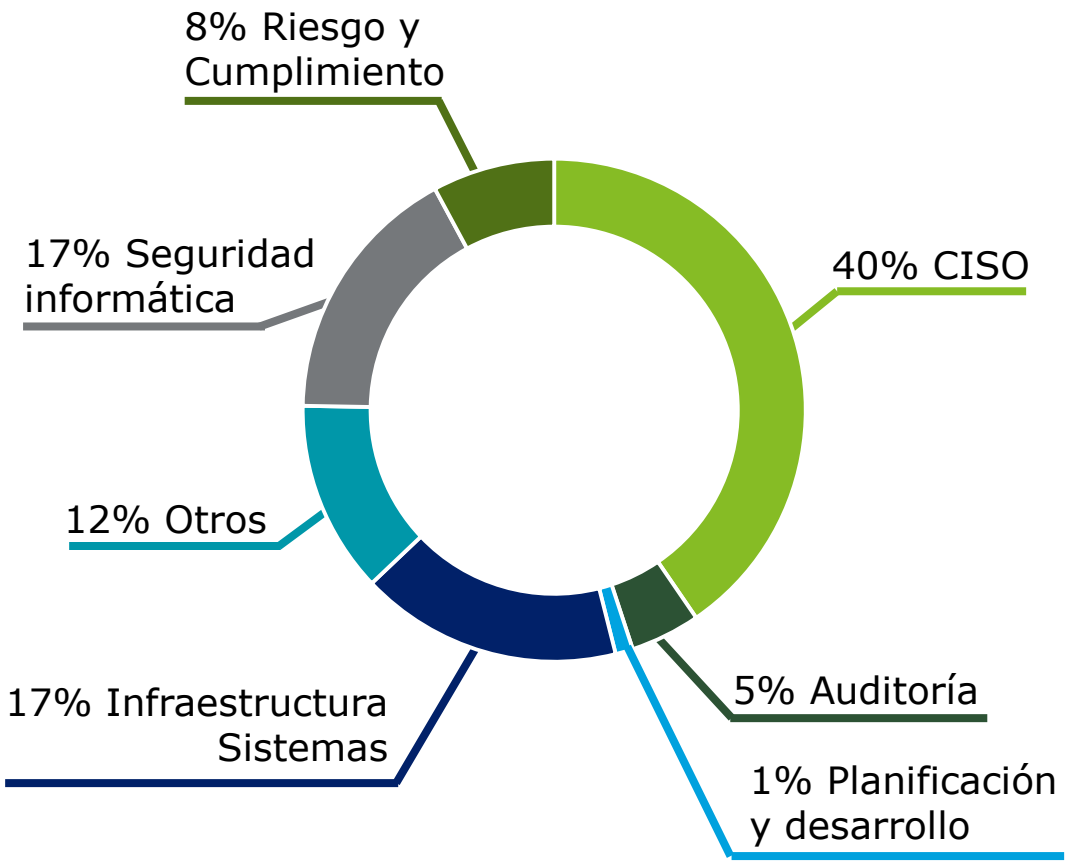
Detalle de Países e Industrias Participantes

Argentina
Chile
Colombia
Costa Rica
Ecuador
El Salvador
Guatemala
México
Nicaragua
Panamá
Perú
Republica Dominicana
Uruguay



Información General sobre el Estudio

Perfil del Ejecutivo Entrevistado



Proceso de recopilación de la información

Se llevó a cabo durante los meses de Enero y Mayo de 2016, recopilando la información y tendencias mediante entrevistas con CISOs y otros ejecutivos a cargo de la gestión de ciber-riesgos y seguridad de la información.

Se utilizó un cuestionario con 41 preguntas de distintos temas referentes a Ciber-Riesgos y Seguridad.

Referencias

Indica la perspectiva de Deloitte

Principales Tendencias Identificadas

Resumen de las Principales Tendencias Identificadas

Principales Tendencias Identificadas

La perspectiva de Deloitte

1 2 3 4

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)

D

Siguiendo la tendencia relevada en años anteriores y a pesar del aumento de la inversión en seguridad de la información, las organizaciones continúan sufriendo brechas de seguridad.

En este contexto, resulta crítico que la inversión no sólo se destine a implementar medidas de protección sino también a mejorar las capacidades de monitoreo y respuesta ante incidentes, aspecto que sigue siendo un pendiente significativo que tienen las organizaciones en Latinoamérica.

1 2 3 4

A PESAR DE CONTAR CON MAYOR PRESUPUESTO, LA PRINCIPAL BARRERA QUE ENFRENTAN LOS CISOs SIGUE SIENDO LA FALTA DE PRESUPUESTO Y/O DE RECURSOS SUFICIENTES

D

La visibilidad de la problemática de ciber-riesgos y seguridad de la información continúan en aumento, con funciones de Seguridad de la Información consolidadas y con incrementos en los presupuestos.

Según la visión de los ejecutivos de ciber-riesgos y seguridad de la información, aún existe déficit de recursos y presupuestos para poder cubrir las necesidades y requerimientos del negocio.

Principales Tendencias Identificadas

La perspectiva de Deloitte

MENOS DEL 10% DE LAS ORGANIZACIONES CUENTAN CON UN TABLERO CON INDICADORES (KPIs) QUE PERMITA EVALUAR LA GESTION DE CYBER RIESGOS Y DE SEGURIDAD DE LA INFORMACIÓN

Contar con indicadores clave (KPI) de la gestión de ciber-riesgos y seguridad de la información constituye un desafío que los ejecutivos no han podido resolver aún.

Como contraparte del aumento de los presupuestos y de la visibilidad de la seguridad de la información, las organizaciones necesitan contar con indicadores que permitan entender el nivel de riesgo al que están expuestas y la calidad de la gestión. Asimismo, estos indicadores deben ser no sólo para facilitar la propia gestión del Área sino fundamentalmente para ser comprendidos por el negocio.

LA CAPACITACIÓN Y CONCIENTIZACIÓN ES LA INICIATIVA DE SEGURIDAD QUE MAYOR CANTIDAD DE ORGANIZACIONES EJECUTARAN DURANTE 2016

Los ejecutivos de ciber-riesgos y seguridad de la información perciben la importancia de capacitar y concientizar a los distintos usuarios.

Un aspecto que se destaca es la concientización a los niveles ejecutivos de la organización, de forma tal de lograr un entendimiento de los riesgos. Gran parte del tiempo del ejecutivo de ciber-riesgos y seguridad de la información se debe dedicar comunicar a sus pares, a la Alta Gerencia y a los Accionistas sobre esta problemática y así lograr adecuada visibilidad y apoyo en la ejecución de los programas.

Principales Tendencias Identificadas

Evolución de la Gestión de Ciber-Riesgos y Seguridad de la Información

La función de Gestión de Ciber-Riesgos y Seguridad de la Información está evolucionando hacia un nuevo paradigma que incluye tres componentes centrales y estratégicos: Asegurar, Monitorear y Responder

Be SECURE

Aseguramiento y Protección de los Activos de Información

Significa enfocarse en la protección de los activos de información críticos que soportan los procesos claves del negocio, implementando medidas y procesos de gestión adecuados al negocio

Be VIGILANT

Monitoreo Proactivo de Amenazas y Eventos

Significa establecer una cultura en toda la organización que permita estar atentos a las amenazas y desarrollar la capacidad de detectar patrones de comportamiento que puedan indicar o incluso predecir un ataque a activos críticos.

Be RESILIENT

Respuesta Rápida ante la Ocurrencia de una Brecha de Seguridad

Significa tener la capacidad de controlar rápidamente el daño y movilizar los recursos necesarios para minimizar el impacto, incluyendo costos directos y disrupción del negocio, así como también daños a la reputación y a la marca.

Resultados Detallados

Secure

Aseguramiento y Protección de los Activos de Información

¿Cuenta su organización con un ejecutivo responsable de gestionar los ciber-riesgos y la seguridad de la información (CISO – Chief Information Security Officer o similar)?

La función de seguridad de la información está muy consolidad en Latinoamérica, incluyendo todo tipo de industrias y organizaciones de distintos tamaños.

¿A quién reporta el CISO?

La ubicación y nivel de reporte de la función de ciber-riesgos y seguridad de la información es altamente dependiente del nivel de madurez, requisitos regulatorios y tamaño de la organización. La tendencia general es el reporte fuera del área de TI, siendo así en más del 65% de las organizaciones encuestadas.

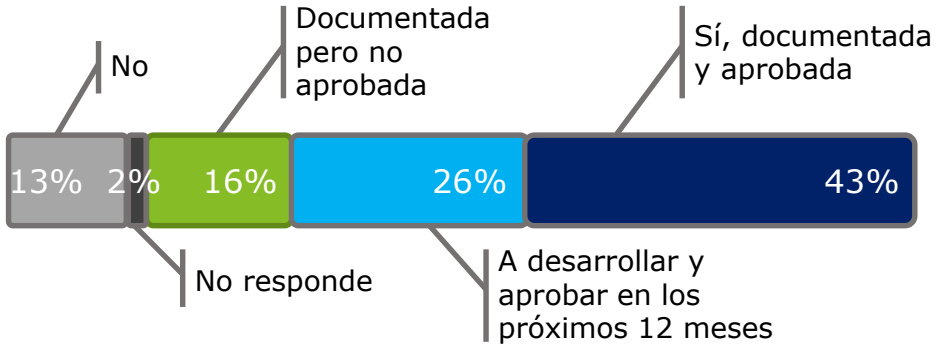
¿Qué áreas y/o funciones de gestión de ciber-riesgos y seguridad de la información se encuentran dentro de las responsabilidades del CISO?

D

El alcance de actividades y procesos desarrollados por la Función de Ciber-Riesgos y Seguridad es bastante consistente en las organizaciones de Latinoamérica. Existen funciones básicas como Gobierno de la Seguridad (Marco Normativo, Políticas, Procedimientos y Estándares), Monitoreo de Eventos, Respuesta Ante Incidentes, Administración de Vulnerabilidades, Administración de Accesos que deben ser parte del alcance de la Función.

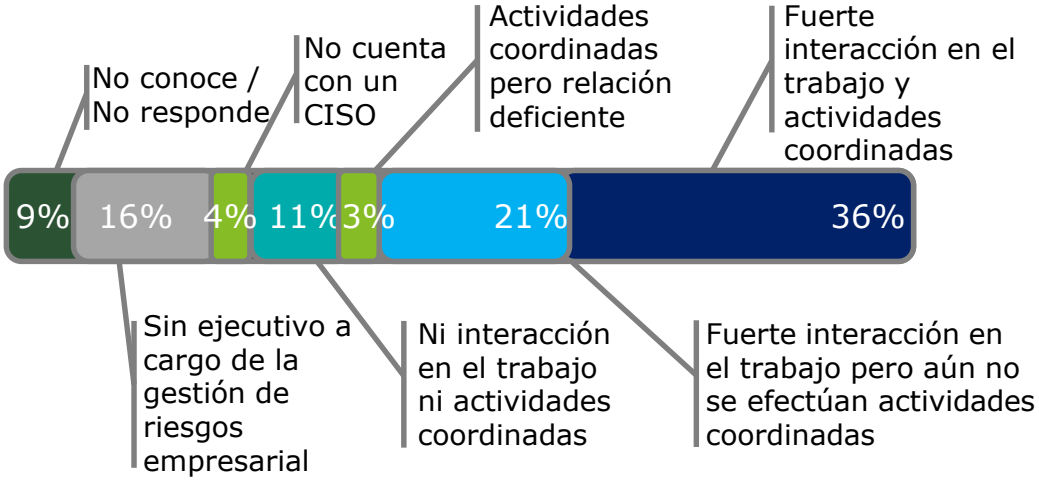
Se destaca que la Continuidad de Negocios y la Recuperación Tecnológica mayoritariamente no forman parte de los procesos liderados por el CISO, a pesar de ser la DISPONIBIDAD uno de los tres atributos clave de la gestión de seguridad de la información junto con la CONFIDENCIALIDAD y la INTEGRIDAD DE LA INFORMACION.

¿Tiene su organización una estrategia de ciber-riesgos y seguridad de la información documentada y aprobada?



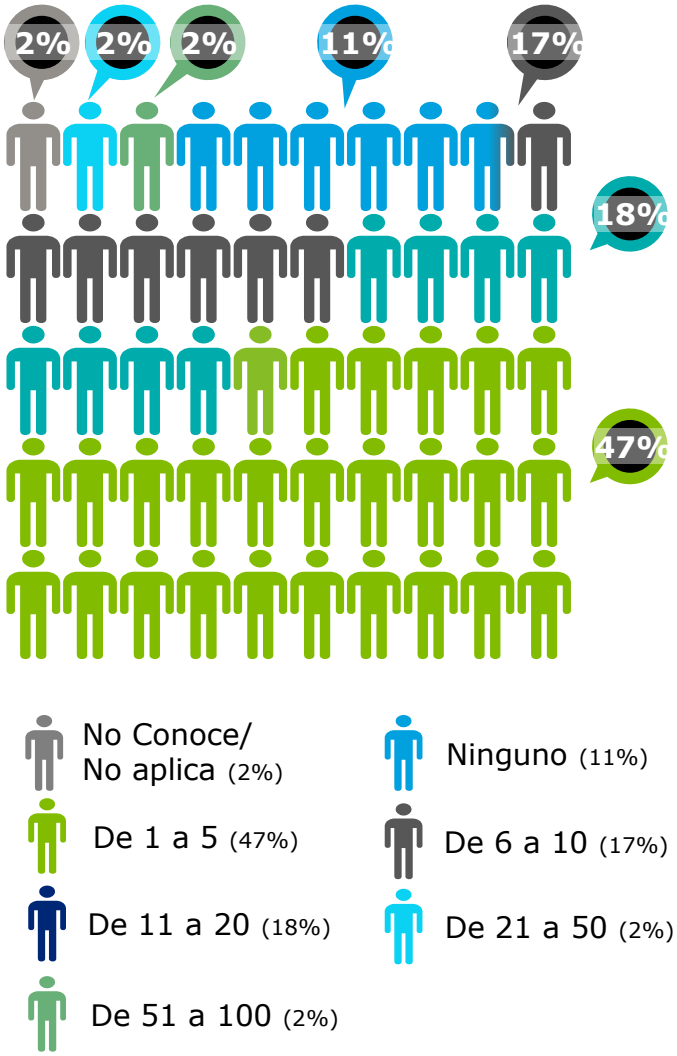
Contar con una Estrategia definida simplifica la gestión, permite ganar visibilidad en la organización y alinear los recursos con las necesidades de negocio.

¿Cuál es la relación entre el CISO y el ejecutivo responsable de la administración del riesgo empresarial?



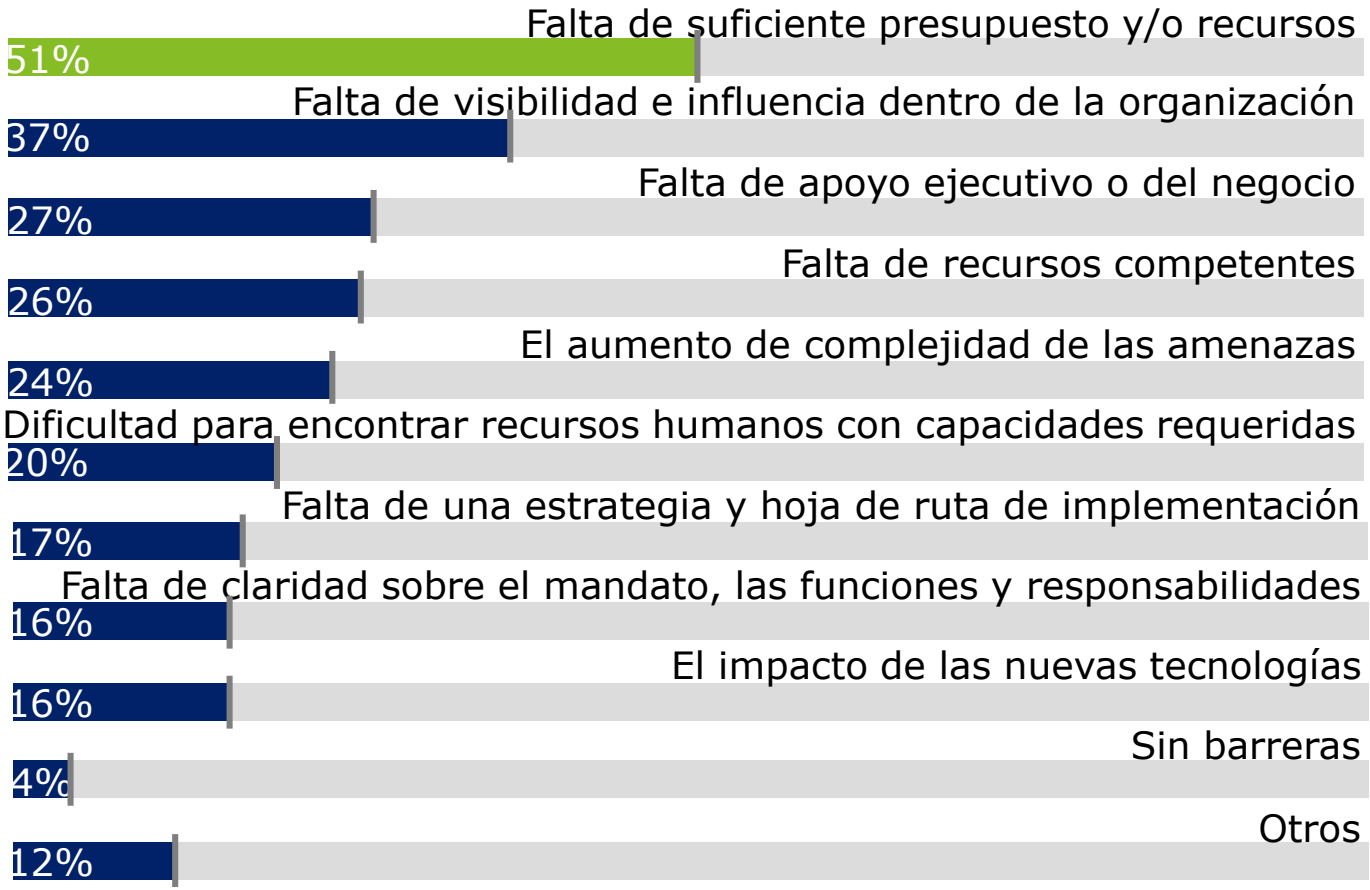
Existe una tendencia creciente a alinear la gestión de ciber-riesgos y seguridad de la información con el proceso general de administración de riesgos de la organización. Este alineamiento es clave para que la inversión en seguridad de la información sea adecuadamente percibida por el Negocio.

¿Cuántos profesionales dedicados a gestión ciber-riesgos y seguridad de información tiene su organización?



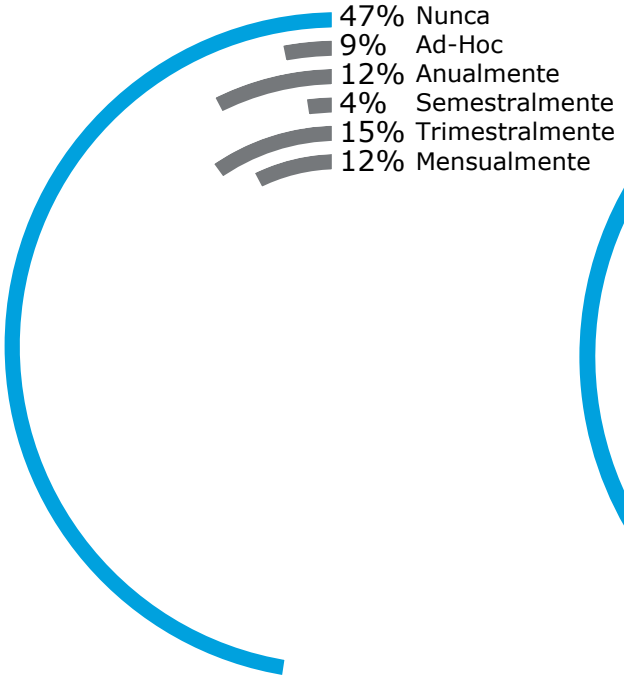
El tamaño y cantidad de recursos humanos dedicados la gestión de ciber-riesgos y seguridad de la información está altamente relacionado con el tamaño de la organización, cuan regulada sea la industria donde la organización opera y fundamentalmente el alcance y actividades que desarrolle el Área. No existe de antemano una cantidad correcta de recursos, dependerá de los aspectos clave anteriormente mencionados.

¿Cuáles son los principales obstáculos que enfrenta para desarrollar su estrategia y programa de ciber-riesgos y seguridad de la información?

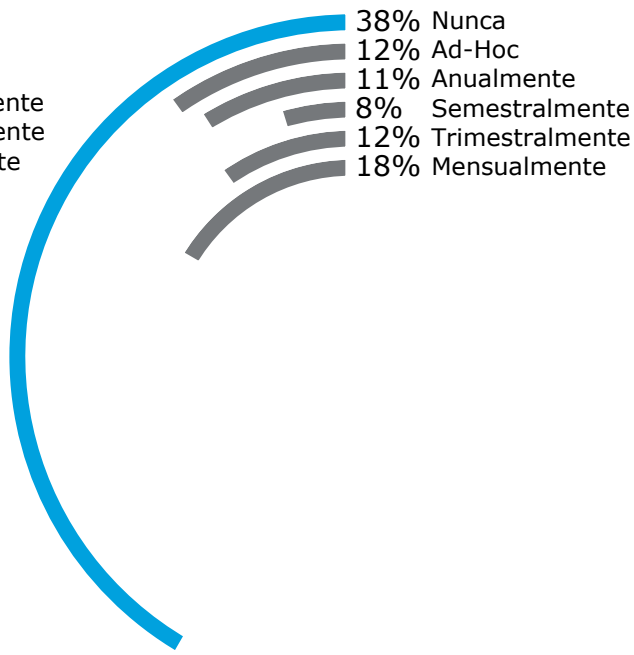


La mitad de los ejecutivos de ciber-riesgos y seguridad de la información consideran que no cuentan con recursos suficientes para llevar adelante su gestión. Se debe considerar que este aspecto puede responder a diversas razones, como la madurez de la gestión, la necesidad de profundizar la concientización a los niveles ejecutivos sobre estos riesgos o incluso que el nivel de riesgo existente no fue adecuadamente evaluado y/o comunicado dentro de la organización. Por otra parte, los CISOs no observa que las nuevas tecnologías generen desafíos significativos.

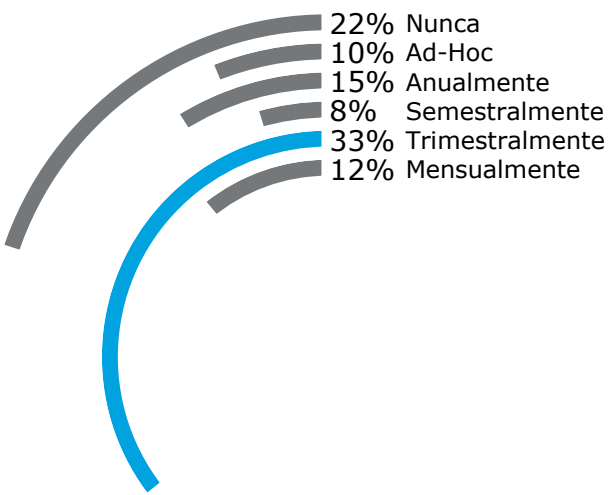
¿Con qué frecuencia Ud. proporciona un informe sobre la situación de ciber-riesgos y seguridad a las principales autoridades de su organización?



Junta Directiva / Directorio



CEO

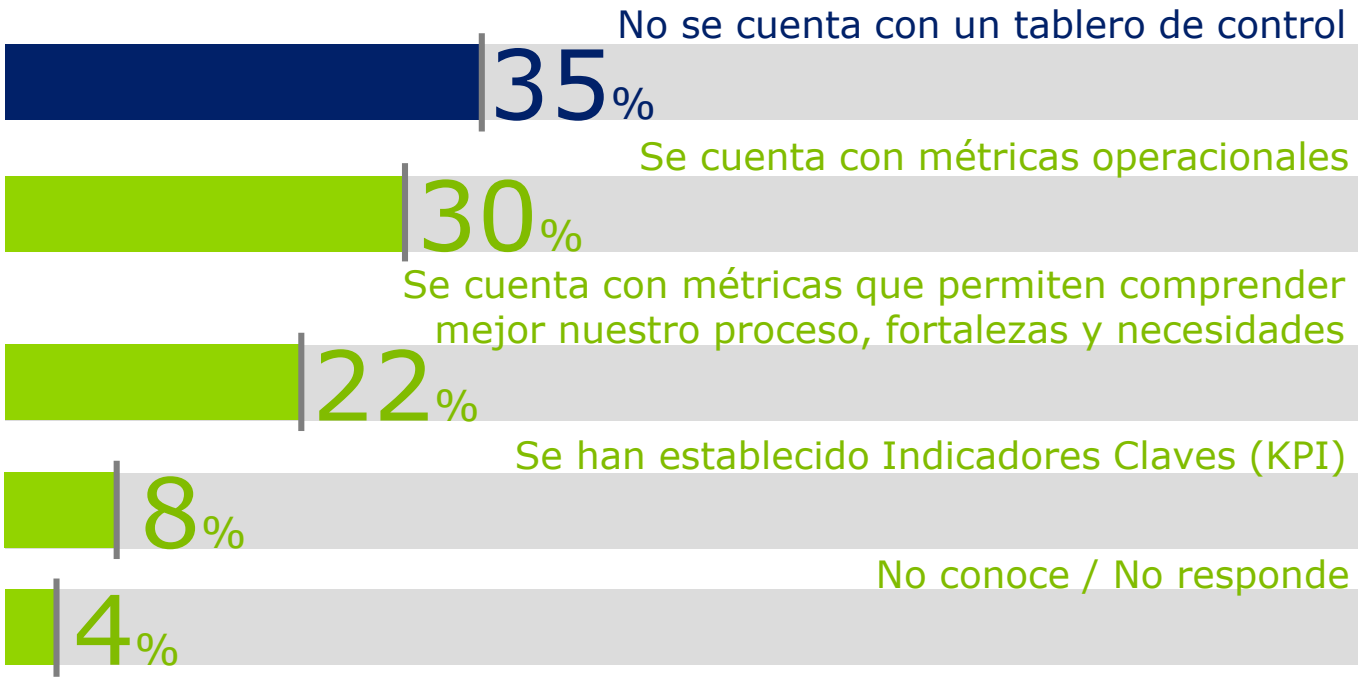


Alta Dirección y/o Comité Ejecutivo

D

El reporte a los máximos niveles ejecutivos de la organización comienza a ser un elemento clave en la gestión que desarrollan los CISOs. Se requiere definir un formato y frecuencia de dicho reporte que sea relevante para los niveles ejecutivos y para el negocio, con enfoque proactivo de comunicación sin esperar a la ocurrencia de una brecha para ser "conocido" dentro de los niveles ejecutivos de la organización.

Describa su tablero de control (dashboard) de Ciber-Riesgos y Seguridad de la Información



A medida que la gestión de ciber-riesgos y seguridad de la información madure y que las organizaciones destinen mayores presupuestos, será clave para los CISOs poder medir el estado de situación, contando para ello con indicadores clave de gestión que permitan interactuar con el negocio y presentar los resultados y éxitos de la gestión realizada.

El desarrollo de estos indicadores deberá servir para entender cómo impacta la seguridad en los procesos clave del negocio.

¿Su organización ha definido un presupuesto específico aplicado a la gestión de Ciber-Riesgos y Seguridad de la Información?

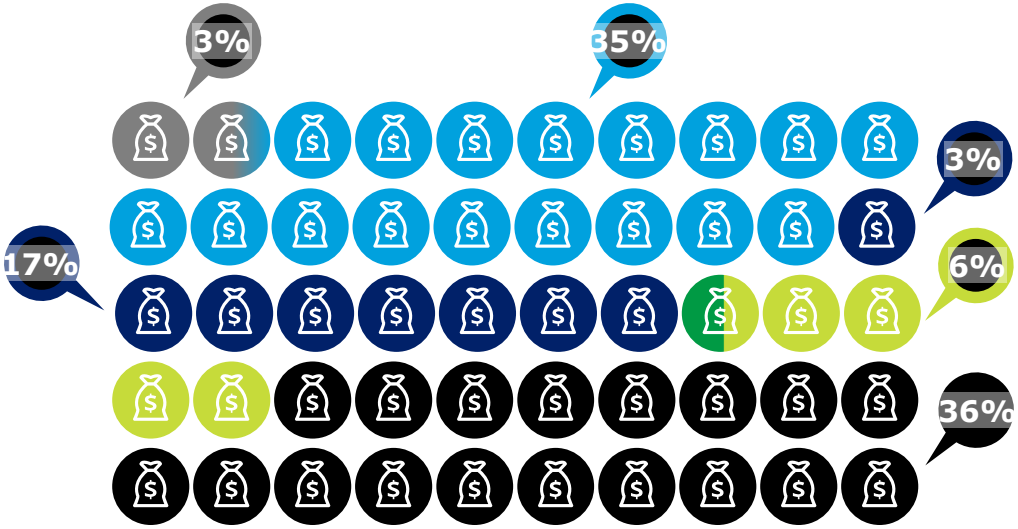
¿Que aspectos, inversiones y gastos están incluidos en su presupuesto de Ciber-Riesgos y Seguridad de la Información?

- 46% Sueldos de Personal Propio
- 70% Servicios y Tercerización de Funciones
- 57% Licencias de Software específico
- 56% Infraestructura

Contar con un presupuesto propio, administrado por el CISO, es un paso fundamental para el crecimiento y madurez de la función de ciber-riesgos y seguridad de la información.

Los ítems a incluir en el presupuesto deben considerar todos los elementos necesarios para una adecuada gestión.

¿Cuánto representa el presupuesto dedicado a Ciber-Riesgos y Seguridad de la Información y en relación con el presupuesto total destinado a TI?

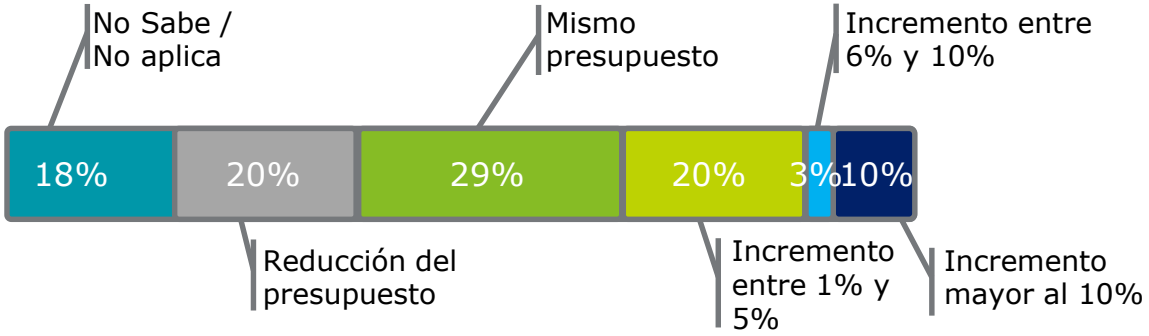


- Sin presupuesto (3%)
- 1%-3% (35%)
- 4%-6% (17%)
- 10%-11% (3%)
- Mayor al 11% (6%)
- No Sabe / No responde (36%)

La referencia con el presupuesto de TI permite entender cómo evoluciona el presupuesto destinado a la función de ciber-riesgos y seguridad de la información.

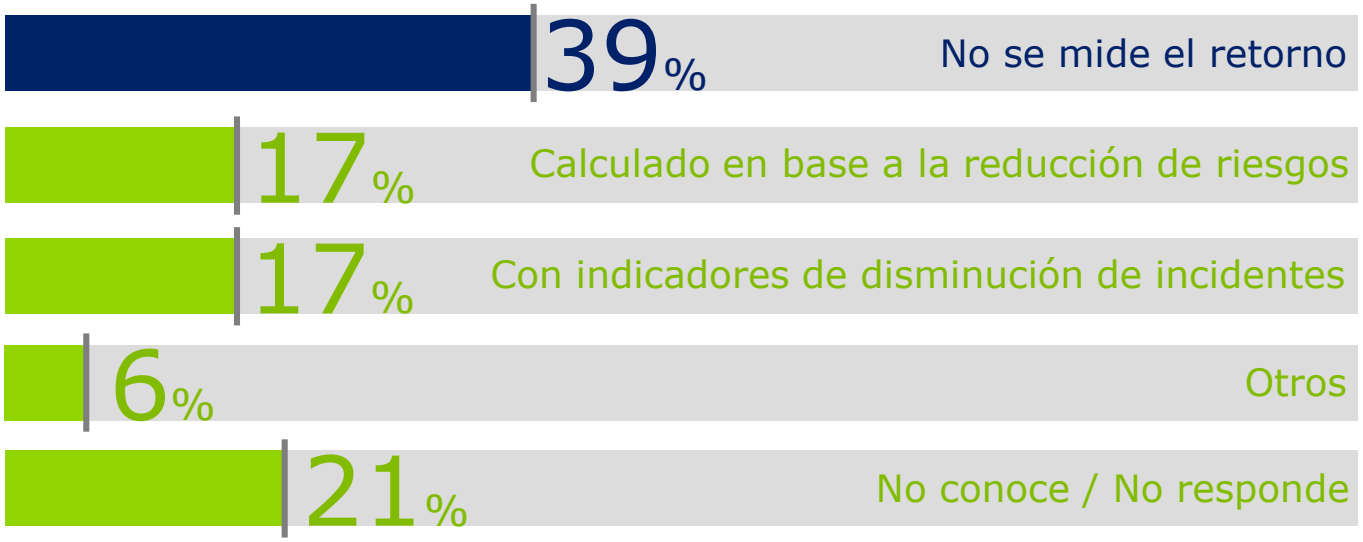
Si bien existe un porcentaje correcto, es deseable que la inversión en ciber-riesgos y seguridad de la información no sea inferior al 3% del presupuesto de TI. En las industrias más maduras el porcentaje supera el 10%.

¿Cuál será la evolución del presupuesto de Ciber-Riesgos y Seguridad de la Información en 2016 en comparación con el presupuesto de 2015?



Por primera ver en los últimos 5 años un número importante de organizaciones no incrementa o directamente reduce el presupuesto destinado a ciber-riesgos y seguridad de la información. Se observó que en muchos casos, las organizaciones han realizado inversiones significativas en tecnologías que están empezando a implementar y capitalizar para lograr reducción de riesgos.

¿Cómo mide su organización el retorno de la inversión en Ciber-Riesgos y Seguridad de la Información?



Otros:

- Por cantidad de pérdidas
- ADHoc por control gestión
- Mediante matriz de Riesgos TIC
- Mediante índice de eficiencia

D

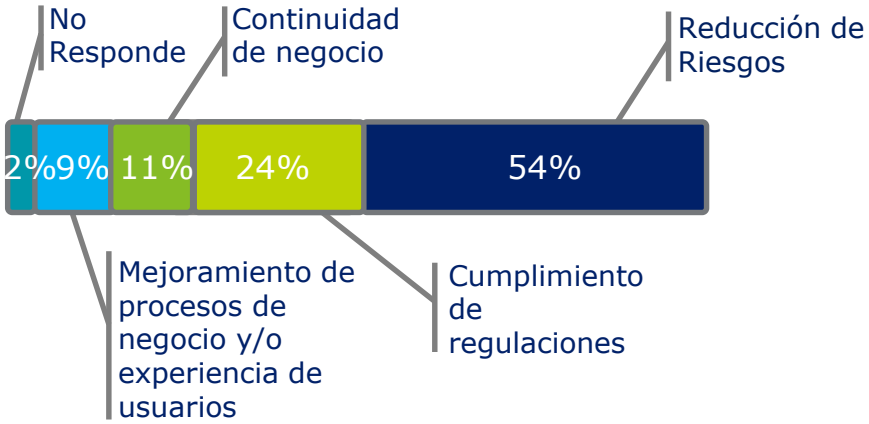
En línea con la falta de tableros e indicadores de gestión, muchas organizaciones no cuentan con una valoración del retorno de inversión en seguridad. Los CISOs podrán justificar las inversiones brindando visibilidad sobre la efectividad de las mismas basándose en indicadores relevantes para el negocio.

Cinco principales iniciativas de Ciber-Riesgos y Seguridad de la Información para el 2016

1. Capacitación y concientización en Ciber-Riesgos y Seguridad de la Información
2. Gobierno de Ciber-Riesgos y Seguridad de la Información
3. Alineamiento con el negocio
4. Protección de información sensible
5. Generación de indicadores, medición y reporte

No sorprende que las iniciativas que mayor cantidad organizaciones están encarando durante 2016 incluyan aspectos muy relacionados con el negocio y con las prácticas de gestión que requieren mayor desarrollo por encontrarse en niveles de madurez más incipientes.

Identifique el principal driver de negocio que se utiliza para priorizar las iniciativas de Ciber-Riesgos y Seguridad de la información en su Organización



D

Si bien existen industrias donde la regulación presiona para invertir en seguridad, es saludable que el principal motivo para invertir sea la reducción del riesgo. Consecuentemente, tener cuantificados los riesgos y medir su evolución es un requisito clave para una buena gestión.

Califique las siguientes amenazas según la probabilidad de ocurrencia que Ud. entiende tienen en su Organización

- Abuso de los privilegios de acceso a información por parte de usuarios internos
- Errores y omisiones en el uso de los sistemas de información por usuarios que deriven en incidentes de seguridad
- Robo de información por atacantes internos
- Amenazas avanzadas persistentes (APT) / Malware generadas por atacantes externos
- Ataques externos explotando vulnerabilidades en plataformas/aplicaciones
- Fraude financiero
- Riesgos sistémicos
- Ataques coordinados
- Amenazas resultantes de la adopción de nuevas tecnologías
- Robo de información por atacantes externos
- Ataques externos explotando vulnerabilidades en la red móvil
- Amenazas por la convergencia de redes sociales y las plataformas online dentro de la red corporativa
- Diversidad de interpretaciones culturales con respecto al comportamiento respecto a SI
- Espionaje industrial o de Estado

D

Las organizaciones deben documentar su mapa de amenazas y utilizarlo como uno de los elementos clave en la planificación de su estrategia de ciber-riesgos y seguridad de la información.

¿Cómo administra los riesgos resultante de interconectar redes y sistemas tradicionales de tecnología informática con otro tipo de redes?

La Seguridad será tan fuerte como lo sea cada uno de sus eslabones. Las Organizaciones que cuentan con redes no informáticas (ej. Industriales) deben ver la seguridad y su protección como un todo para evitar incidentes sobre sus procesos de negocio críticos.

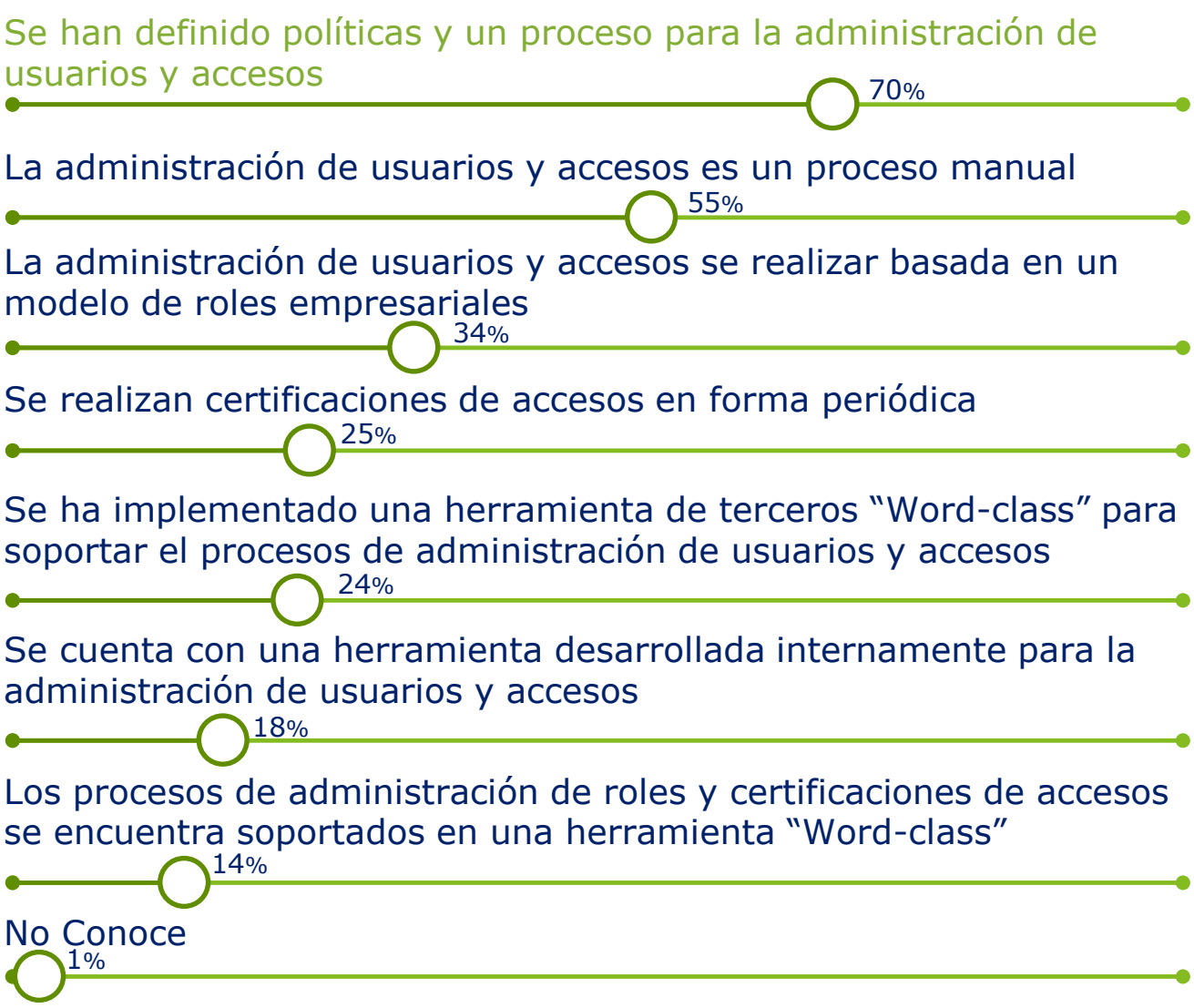
¿Cómo describe la adopción de las siguientes tecnologías de seguridad en su organización?

Implementado en más del 80% de la organización	
Antivirus	98%
Firewalls	96%
Spam filtering solutions	88%
Anti spyware software	80%
Intrusion Detection and/or Prevention Systems	72%
Content filtering/monitoring	67%
Vulnerability management	58%
Network access control	55%
Anti phishing solutions	53%
Email authentication	52%

A implementar en 2016	
Data loss prevention technology	28%
File encryption for mobile devices	24%
Encrypted storage devices	20%
Identity Management and User Provisioning	20%
Vulnerability management	19%

Existen tecnologías de seguridad que hoy constituyen un elemento básico de gestión. Avanzar en las tecnologías que permiten alinear la implementación de seguridad con los requerimientos de negocio constituye el nuevo desafío para los CISOs.

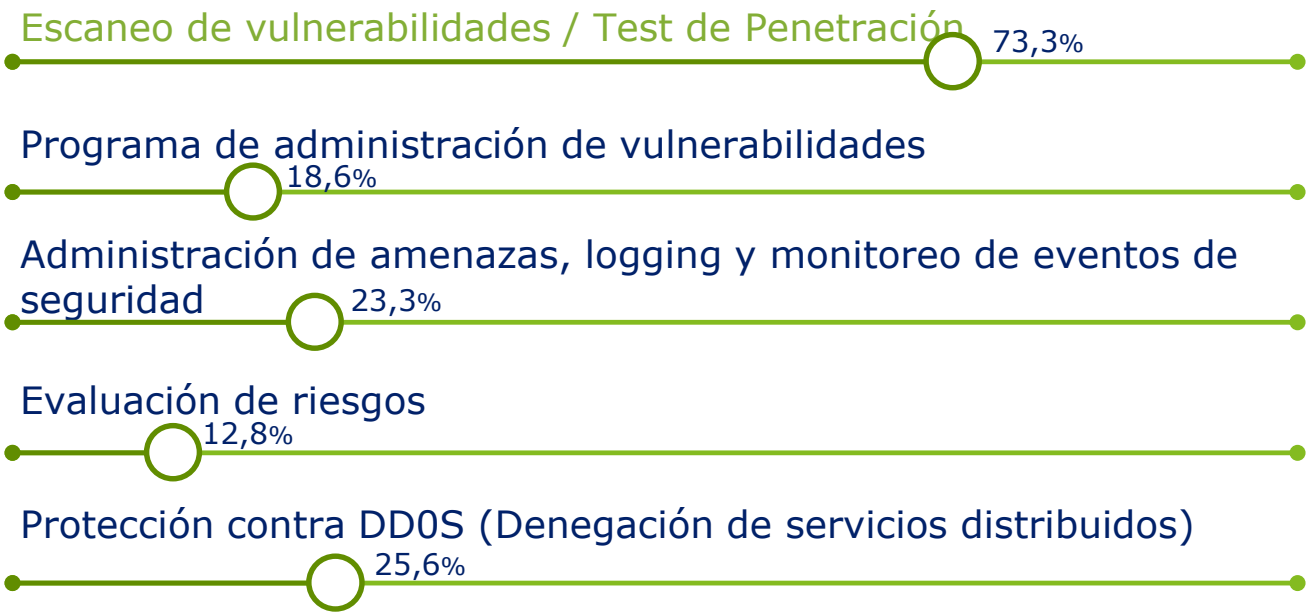
Describa su proceso de administración de usuarios y accesos a recursos de información



D

Entendido como uno de los procesos básicos de gestión de seguridad, la administración de usuarios y accesos continúa siendo un proceso que la mayoría de las organizaciones realizan manualmente con bajo nivel de servicio y propensión al error. Implementar procesos automatizados y basados en herramientas world-class constituye un aspecto prioritario en el camino de la madurez de la gestión de ciber-riesgos y seguridad de la información.

¿Su organización terceriza alguna de las siguientes funciones de gestión de Ciber-Riesgos y Seguridad de la Información?



Otros:

- Filtrado de contenido web
- Filtrado de correo electrónico
- Servicios de administración de accesos e identidades
- Infraestructura de seguridad
- Soporte legal / forense
- Servicios de evaluación y cumplimiento regulatorio/normativo
- Centro de operaciones de seguridad (SOC)
- Por política interna no terceriza servicios de seguridad

D

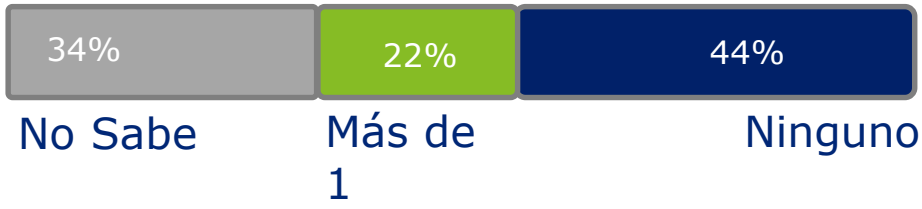
A medida que la gestión de ciber-riesgos y seguridad de la información alcanza mayor nivel de madurez, los CISOs pueden evaluar opciones de tercerización que permitan lograr mayor eficacia y eficiencia en su gestión.

Los CISOs están considerando la tercerización como una herramienta para alcanzar mayor madurez en algunos procesos de gestión y para complementar las capacidades internas con que cuentan, sin perder el control de la operación.

¿Se encuentra su organización alcanzada por alguna regulación o ley de privacidad y protección de datos personales?

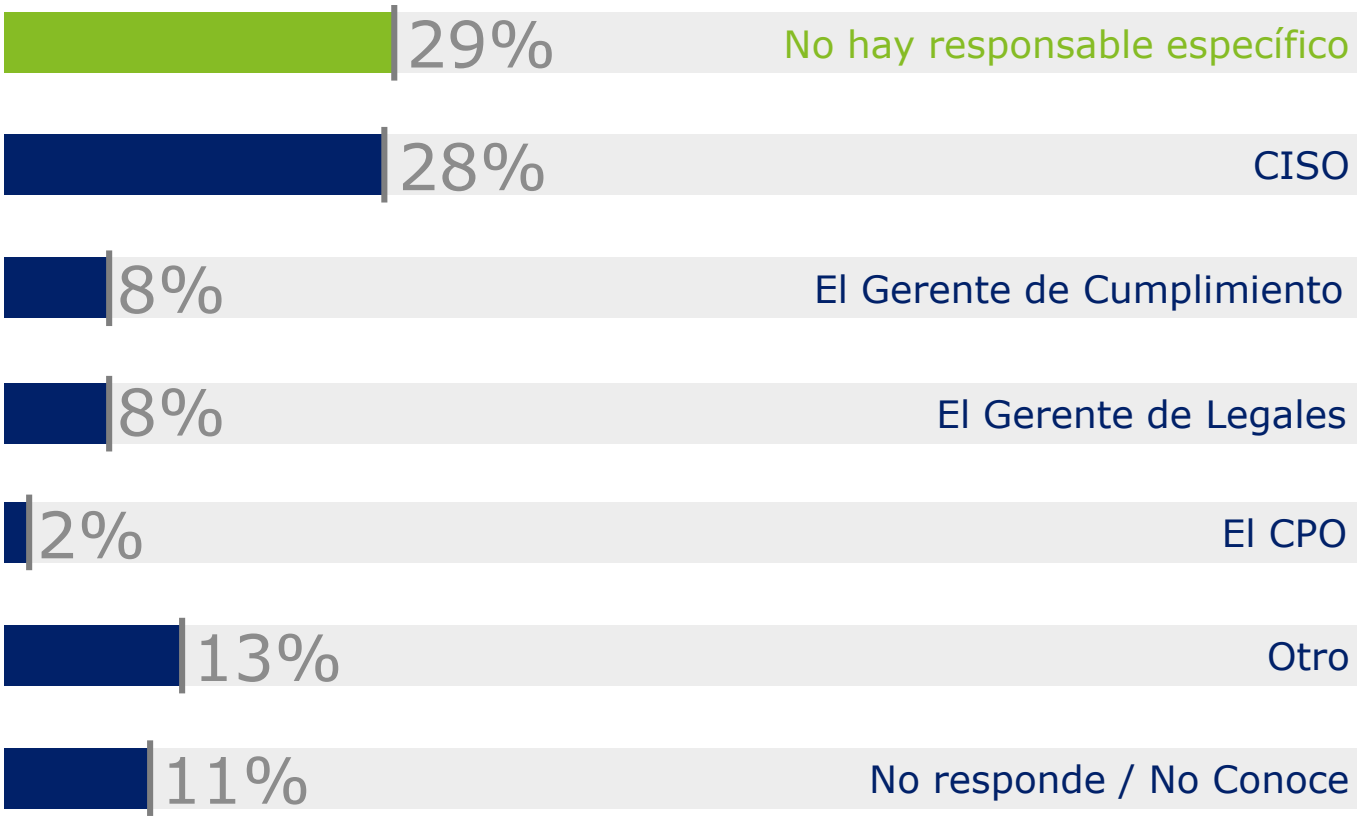
Latinoamérica ha avanzado mucho en materia de protección de datos personales, siendo este un requisito muy consistente a lo largo de los distintos países.

¿Cuántos incidentes específicos de privacidad sufrió su organización en los últimos 24 meses?



La capacidad de identificación de incidentes que involucren pérdida de confidencialidad de datos personales es una materia pendiente para las organizaciones en Latinoamérica.

¿Quién tiene a cargo la responsabilidad de los temas de Privacidad y Protección de Datos Personales en su Organización?



No existe una tendencia homogénea en la asignación de responsabilidad sobre el cuidado de los datos personales. De cualquier forma, es el CISO el responsable de esta gestión de forma mucho más habitual que otros ejecutivos de la organización.

¿Qué medidas ha implementado su organización para cumplir con los requisitos de protección de privacidad y datos personales?

D

Existen distintas medidas y acciones que las organizaciones pueden y deben tomar para proteger la privacidad de los datos personales que administran.

Para hacer que esta gestión sea efectiva es imprescindible contar con el inventario de los datos personales administrados y definir medidas de protección correspondientes. En general se observa que en Latinoamérica aún no se han desarrollado capacidades suficientes de identificación y clasificación de información que permitan garantizar la privacidad de los datos personales y el cumplimiento de requisitos al respecto.

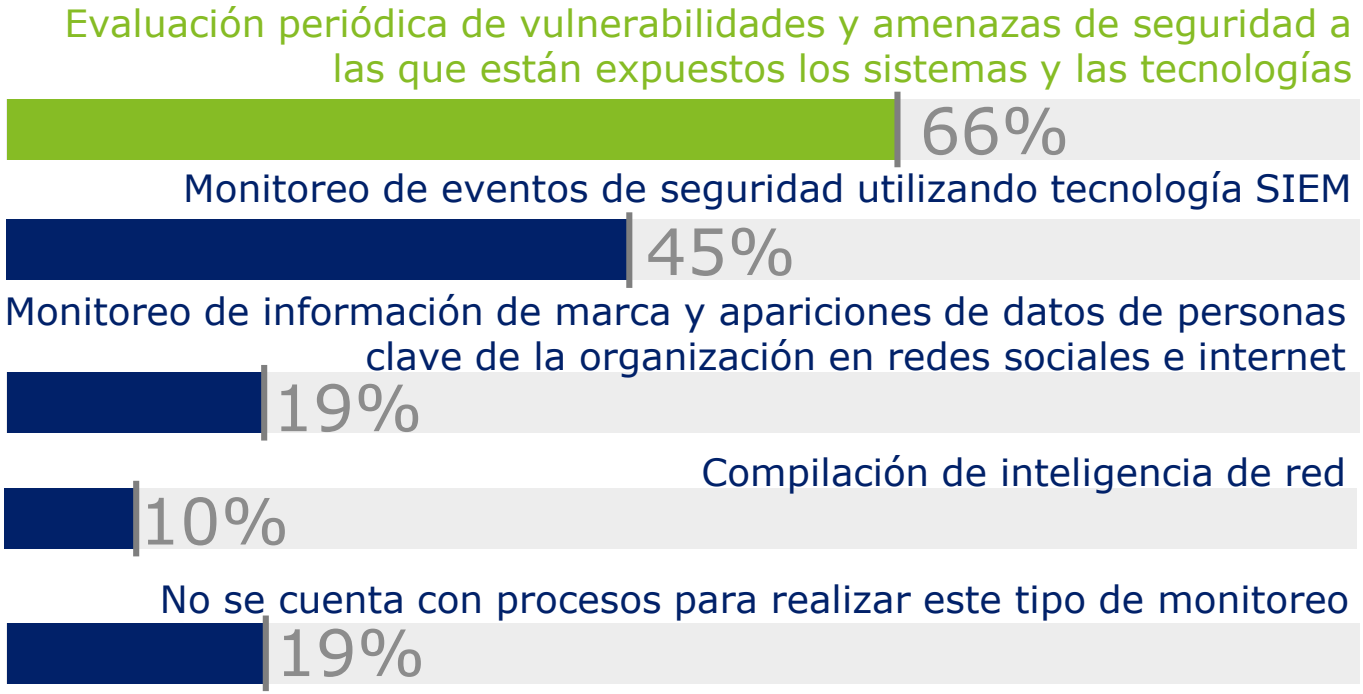
¿Cuándo comparte datos personales con terceros para ejecutar procesos de negocio, cómo se asegura el cumplimiento de requisitos de privacidad y adecuado uso de los datos personales por ese tercero?

La gestión de seguridad sobre terceros involucrados en los procesos de negocio, incluyendo la protección de datos personales, constituye un aspecto sobre el cual las organizaciones en Latinoamérica tienen un largo camino aún por recorrer.

Vigilant

Monitoreo Proactivo de Amenazas y Eventos

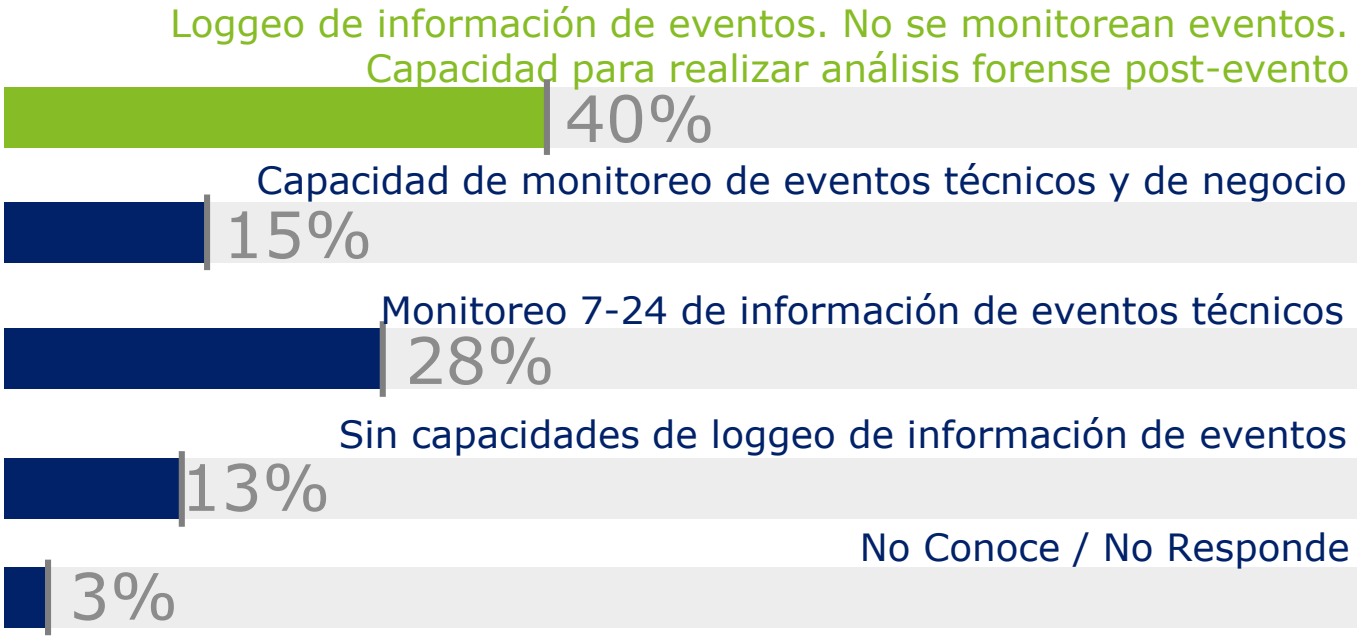
¿Qué procesos y/o tecnologías tiene implementados su Organización para monitorear y evaluar las ciber-amenazas y riesgos de seguridad de la información a los que está expuesta?



D

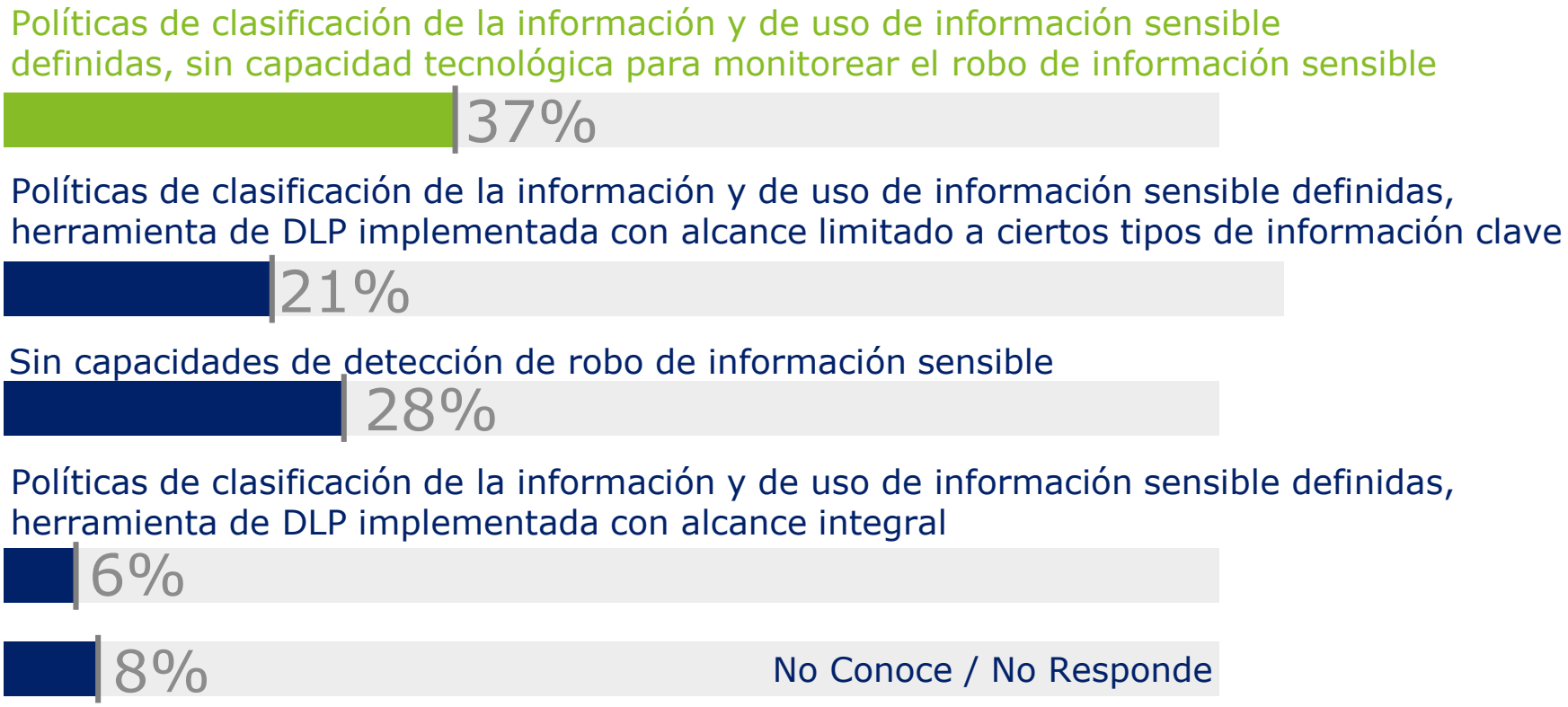
En un ambiente de constante cambio tecnológico y donde modelo de operación que usualmente es 7x24, contar con capacidades de monitoreo de la situación de riesgos de seguridad resulta una competencia clave a desarrollar por las organizaciones.
Se observa que en Latinoamérica estas capacidades en muchos casos son inmaduras o muy lejos de alcanzar los niveles que podrían entenderse como óptimos para el estado de riesgo actual.

¿Qué nivel de capacidades ha desarrollado su Organización para monitorear los eventos de seguridad?



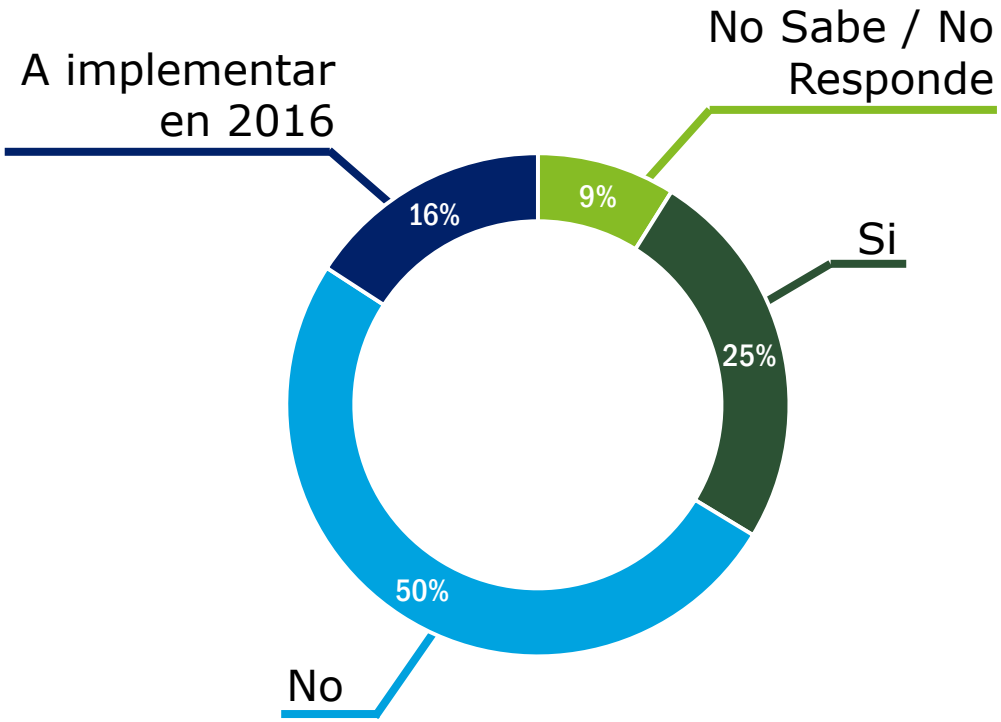
El monitoreo de eventos clave de seguridad constituye la base operacional para una adecuada gestión de ciber-riesgos y seguridad de la información.
En Latinoamérica se observa un grado de desarrollo bajo de estas capacidades, casi siempre limitadas a responder reactivamente para explicar que pasó.

¿Qué nivel de capacidades ha desarrollado su Organización para monitorear el robo de información sensible?



Siendo la protección de información sensible una de las iniciativas prioritarias para las organizaciones en 2016, se observa que esta prioridad responde al bajo nivel de madurez que existe en Latinoamérica para gestionar este riesgo.

¿Cuenta con un Centro de Operaciones de Seguridad (SOC)?

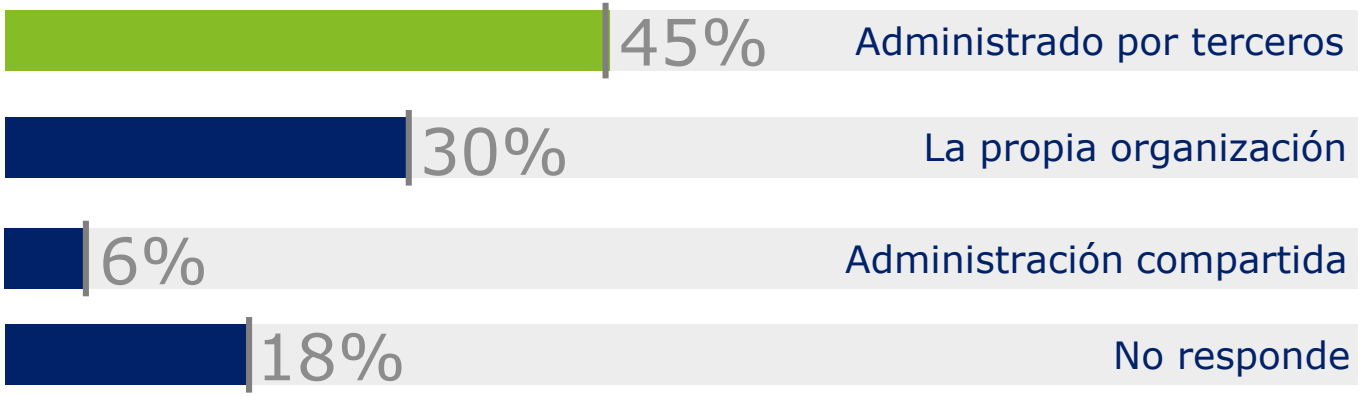


La implementación de un Centro de operaciones de Seguridad (SOC, por sus siglas en ingles) constituye una estrategia clave para lograr eficacia y eficiencia en el monitoreo de riesgos y en la respuesta adecuada ante los incidentes que tarde o temprano las organizaciones van a sufrir.
En Latinoamérica, contar con este tipo de recurso es la excepción, más que la norma. Definitivamente los CISOs deben analizar y avanzar en una estrategia de SOC para poder hacer frente a los desafíos actuales pero mayormente a los futuros, tanto a nivel de amenazas como en lo que refiere a dar respuesta a niveles ejecutivos de la organización sobre el estado de situación de ciber-riesgos y a la certeza en confirmar que la seguridad de la información no fue comprometida.

¿Qué capacidades tiene implementadas en el Centro de Operaciones de Seguridad (SOC)?

Los servicios de SOC implementados en Latinoamérica en su gran mayoría atacan los aspectos básicos del monitoreo de seguridad, existiendo un amplio margen para optimizar y desarrollar dichos servicios.

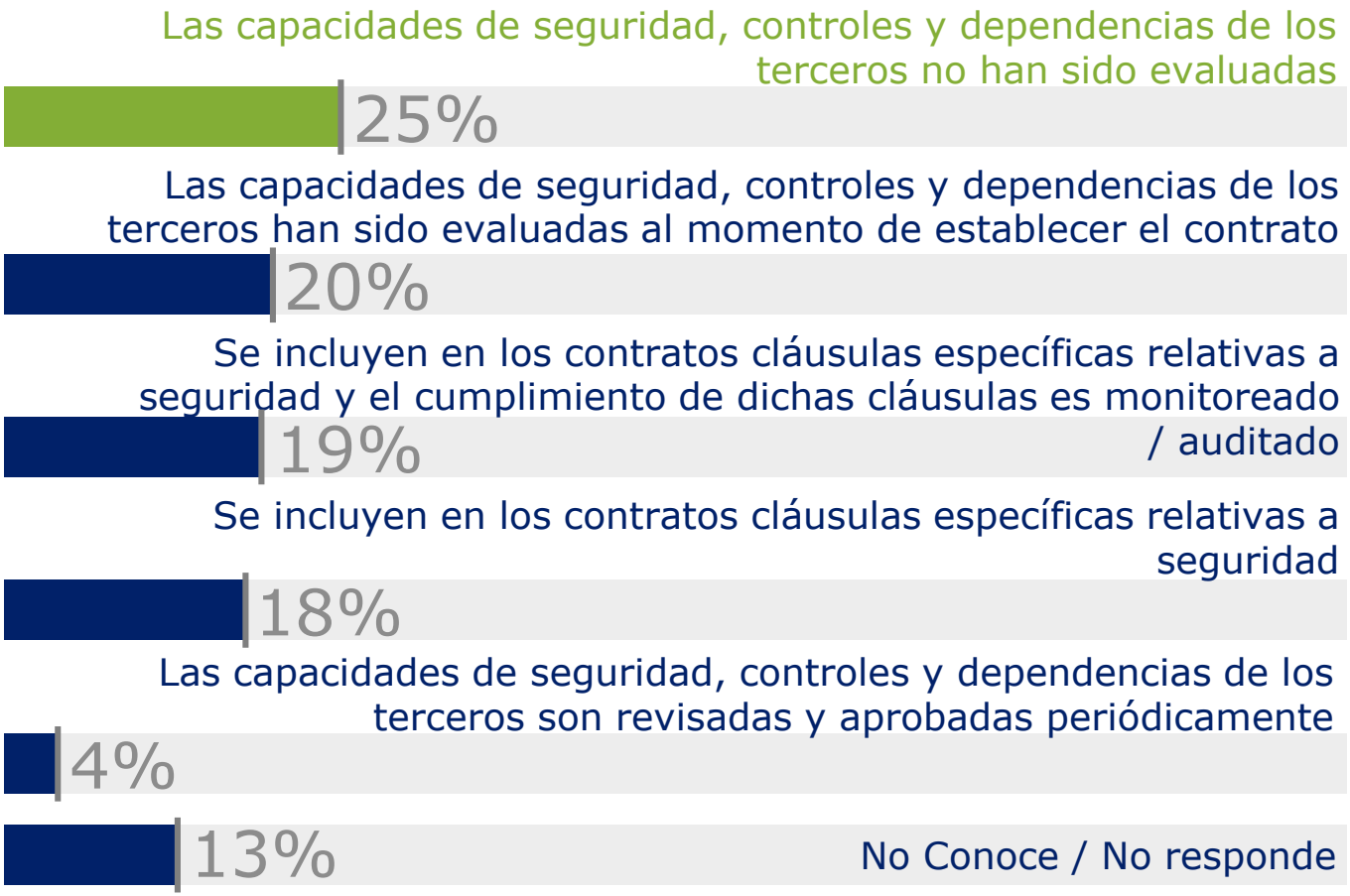
¿Quién es responsable por su Centro de Operaciones de Seguridad (SOC)?



D

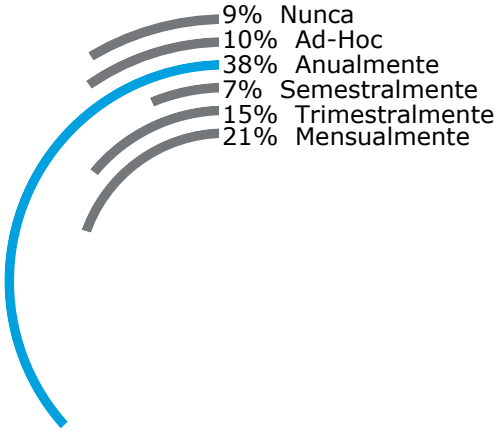
En la definición de su estrategia de SOC, la organización debe analizar los distintos modelos de operación posibles definiendo aquel que mejor se adapte a sus requisitos y a las capacidades con que cuenta internamente.

¿Cómo administra y monitorea la seguridad de terceros con los cuales su Organización hace negocio y/o terceriza parte de sus procesos de negocio?

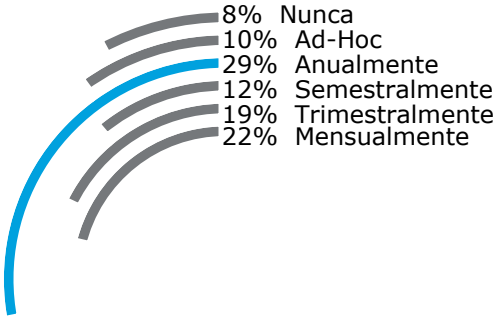


Siendo la interacción y colaboración con terceros una estrategia creciente que utilizan las organizaciones para dar valor, se observa que las organizaciones necesitan imperiosamente mejorar sus capacidades de análisis y gestión de los ciber-riesgos y de la seguridad de la información que afecten a sus terceros socios de negocio.

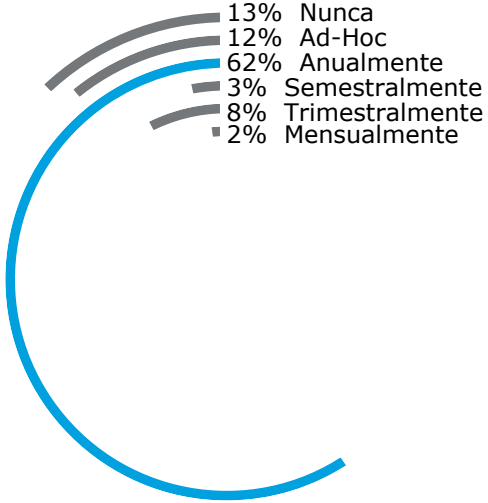
¿Con qué frecuencia Ud. realiza evaluaciones sobre el nivel de riesgo y vulnerabilidad de sus activos de información?



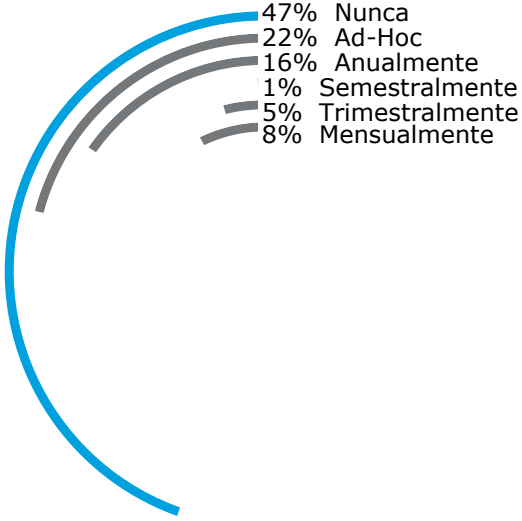
Escaneo de vulnerabilidades externas



Escaneo de vulnerabilidades internas



Pruebas de Ethical Hacking / Penetration Testing

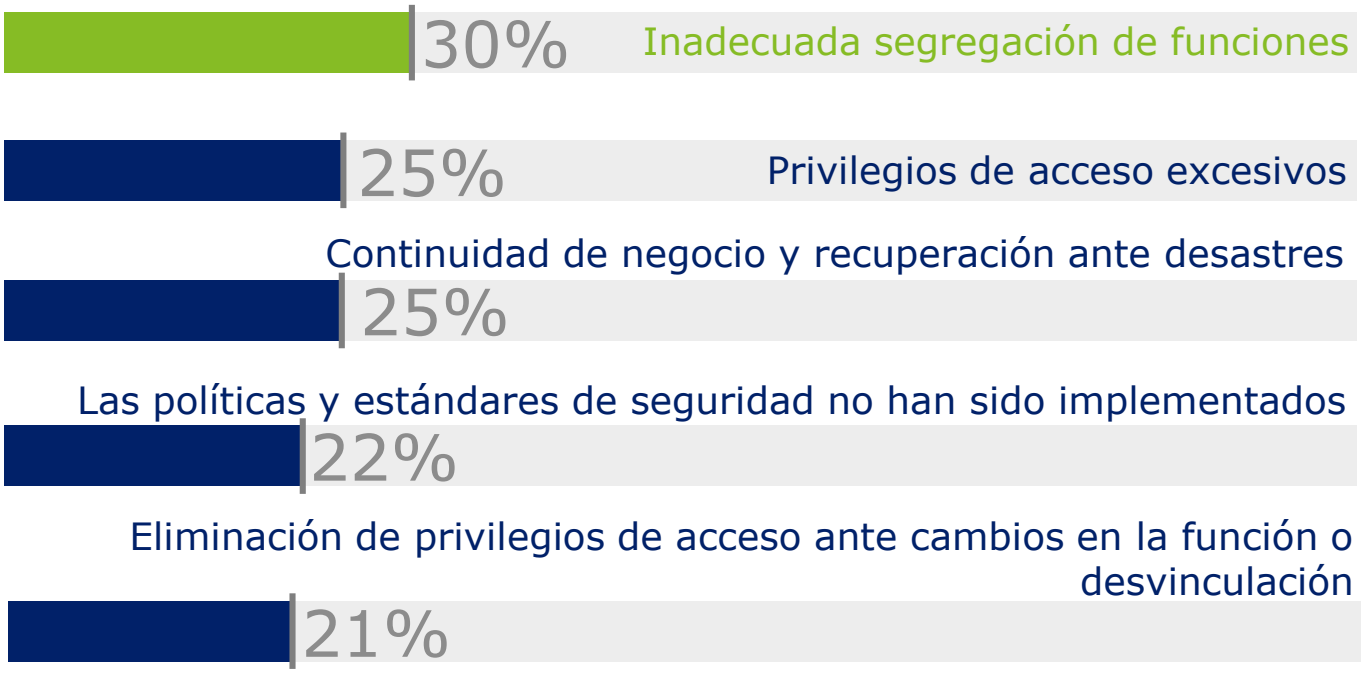


Auditoría de Código Fuente

D

Se observa un gap en las prácticas de revisión del estado de riesgos de seguridad implementadas por las Organizaciones en Latinoamérica, siendo que los riesgos a evaluar requieren una frecuencia mucho mayor de testeos. Particularmente se observa un gap significativo en la revisión de código fuente, considerando que las vulnerabilidades en código son puerta principal para intrusiones y ataques.

¿Cuáles fueron las cinco principales observaciones de auditoría, interna o externa, relacionados con Ciber-Riesgos y Seguridad de la Información en su organización en los últimos 12 meses?



D

Las Auditorias realizadas sobre la situación de ciber-riesgos y seguridad de la información continúan identificando debilidades sobre procesos y cuestiones estructurales de la gestión de seguridad. Los CISOs aún tienen aspectos básicos de la gestión por resolver, especialmente en todo lo referente a gestión de accesos y usuarios

Por otra parte, a medida que las Auditorías se hagan más sofisticadas y especializadas, es posible que se identifiquen nuevas oportunidades de mejora sobre aspectos hoy no cubiertos por las auditorías.

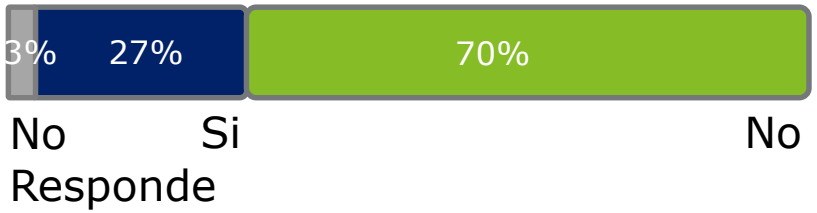
Resilient

Respuesta Rápida ante la Ocurrencia de una Brecha de Seguridad

¿Su organización ha experimentado una brecha de seguridad externa durante los últimos 24 meses?

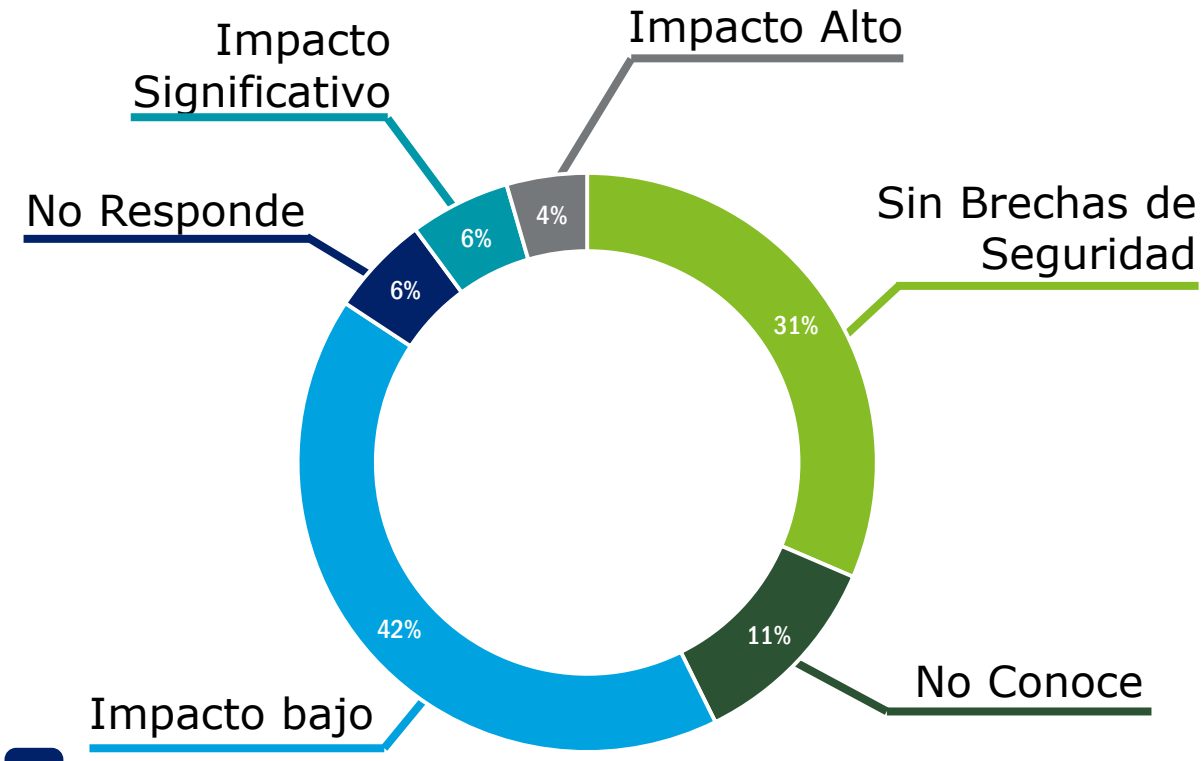
Las brechas de seguridad generadas por atacantes externos continúan siendo las de mayor ocurrencia en las Organizaciones de Latinoamérica.

¿Su organización ha experimentado una brecha de seguridad interna durante los últimos 24 meses?



La formulación de las estrategias y la implementación de capacidades para gestionar ciber-riesgos y seguridad de la información debe partir de la base de que las brechas de seguridad tarde o temprano se materializarán.
El objetivo es minimizar la probabilidad de ocurrencia y el impacto para el negocio.

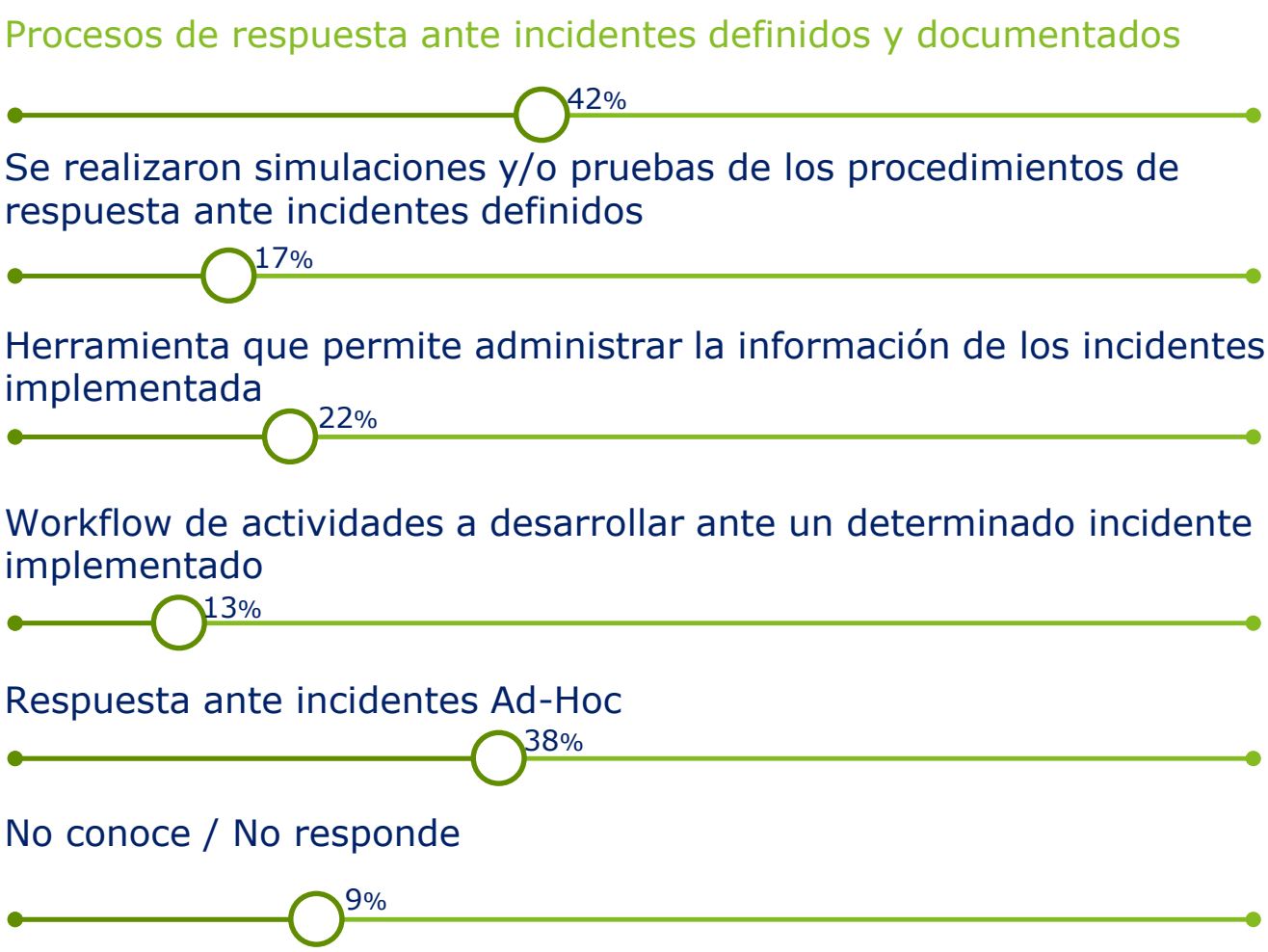
¿Cómo clasificaría la severidad/impacto de las brechas de seguridad sufridas por su organización en los últimos 24 meses?



1 de cada 10 organizaciones sufrieron brechas de seguridad de impacto alto y/o significativo, con pérdidas económicas superiores a U$S 250.000, más las perdidas reputacionales o por daño de imagen.

Se observa que existen organizaciones que al no contar con capacidades adecuadas para monitorear su situación de seguridad pueden sufrir incidentes y no percibirlos o identificar niveles de compromiso inferiores a los que realmente sufrieran.

¿Qué capacidades de respuesta a incidentes de Ciber-Riesgos y Seguridad de la información ha desarrollado su organización?



D

Casi 4 de cada 10 organizaciones no cuenta con capacidades, herramientas ni procedimientos específicos para responden ante una brecha de seguridad.

Por otra parte, sólo 1 de cada 4 Organización ha implementado tecnología y procesos para responder de forma ordenada y rápida ante la ocurrencia de una brecha de seguridad.

Consideraciones Finales

Consideraciones Finales

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

1

Los CISOs 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.

2

En un contexto de nuevas y más sofisticadas ciber-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.

3

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

4

Acerca de Deloitte

A cerca de Deloitte

Deloitte se refiere a una o más de las firmas miembro de Deloitte Touche Tohmatsu Limited, una compañía privada del Reino Unido limitada por garantía ("DTTL"), su red de firmas miembro, y sus entidades relacionadas. DTTL y cada una de sus firmas miembro son entidades únicas e independientes y legalmente separadas. DTTL (también conocida como "Deloitte Global") no brinda servicios a los clientes. Una descripción detallada de la estructura legal de DTTL y sus firmas miembros puede verse en el sitio web www.deloitte.com/about.

Deloitte presta servicios de auditoría, impuestos, consultoría, asesoramiento financiero y servicios relacionados a organizaciones públicas y privadas de diversas industrias. Con una red global de Firmas miembro en más de 150 países y territorios, Deloitte brinda sus capacidades de clase mundial y servicio de alta calidad a sus clientes, aportando la experiencia necesaria para hacer frente a los retos más complejos del negocio. Los más de 225.000 profesionales de Deloitte están comprometidos a generar impactos que trascienden.

La práctica de **CYBER RISK SERVICES** de Deloitte ayuda a las organizaciones a ejecutar sus estrategias de negocio, brindando soporte para el gerenciamiento de los riesgos asociados al desarrollo de negocios en el entorno digital y competitivo existente hoy en día.

Con más de 10000 expertos en ciber-riesgos y seguridad de la información a nivel global, **Deloitte es líder indiscutido en consultoría en ciber-riesgos y seguridad de la información.**

Nuestro Portafolio de Servicios es el más amplio y completo del mercado, con capacidades locales, regionales y globales puestas al servicio de nuestros clientes.

En **Latinoamérica contamos con más de 500 profesionales y expertos en ciber-riesgos y seguridad de la información, centros de ciber-inteligencia y de prestación de servicios propios localizados en la región**, adaptados a las necesidades y riesgos locales y regionales.

Para más información visite www.Deloitte.com/cyber

Contactos

Gerardo Herrera Perdomo
Partner
Risk Advisory Leader
geherrera@deloitte.com

Christiam Garratt
Partner
Risk Advisory
cgarratt@deloitte.com

Edson Villar
Gerente
Risk Advisory
edvillar@deloitte.com

Andrés Gil
Partner
Risk Advisory Leader – Región LATCO (Latina American Countries Organization)
angil@deloitte.com

Deloitte.

Este material y la información contenida en el mismo son emitidos por Deloitte & Touche S.R.L. y tienen como propósito proporcionar información general sobre un tema o temas específicos y no constituyen un tratamiento exhaustivo de dicho tema o temas.

Por lo tanto, la información contenida en este material no intenta conformar un asesoramiento o servicio profesional en materia contable, impositiva, legal o de consultoría. La información no tiene como fin ser considerada como una base confiable o como la única base para cualquier decisión que pueda afectar a ustedes o a sus negocios. Antes de tomar cualquier decisión o acción que pudiera afectar sus finanzas personales o negocios, deberán consultar a un asesor profesional calificado.

Este material y la información contenida en el mismo están emitidos tal como aquí se presentan. Deloitte & Touche S.R.L. no efectúa ninguna manifestación o garantía expresa o implícita con relación a este material o a la información contenida en el mismo. Sin limitar lo antedicho, Deloitte & Touche S.R.L. no garantiza que este material o la información contenida en el mismo estén libres de errores o que reúnan ciertos criterios específicos de rendimiento o de calidad. Deloitte & Touche S.R.L. expresamente se abstiene de expresar cualquier garantía implícita, incluyendo sin limitaciones garantías de valor comercial, propiedad, adecuación a un propósito particular, no-infracción, compatibilidad, seguridad y exactitud.

La utilización que ustedes hagan de este material y la información contenida en el mismo es a vuestro propio riesgo, y ustedes asumen plena responsabilidad y el riesgo de pérdidas resultantes de tal empleo. Deloitte & Touche S.R.L. no será responsable por ningún perjuicio especial, indirecto, incidental o contingente, derivado como consecuencia de su utilización, o de orden penal o por cualquier otro perjuicio que ocurriere, sea en una acción relacionada con un contrato, norma, agravio (incluida, sin limitaciones, una acción por negligencia) o de otro tipo, relacionado con la utilización de este material y la información contenida en el mismo.

Si alguna parte de los párrafos anteriores no resultara aplicable por cualquier razón que fuere, el resto de lo manifestado será, no obstante, aplicable.

www.deloitte.com/pe

Deloitte se refiere a Deloitte Touche Tohmatsu, una asociación suiza, o a una o más integrantes de su red de firmas miembros, cada una de las cuales constituye una entidad separada e independiente desde el punto de vista legal. Una descripción detallada de la estructura legal de Deloitte Touche Tohmatsu y sus firmas miembros puede verse en el sitio web www.deloitte.com/pe.