

Seguridad sin fronteras

Resultados de la Encuesta Global de
Seguridad de la Información

Marzo de 2011

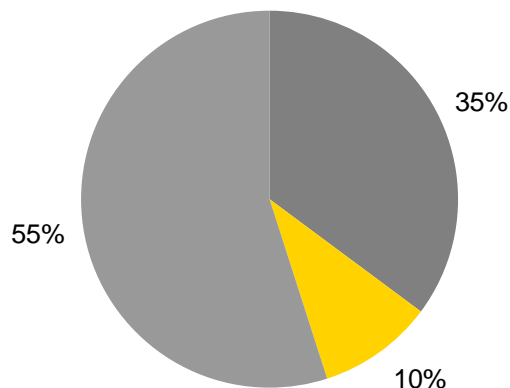


Inversión y retos

1. ¿Cuál de las siguientes declaraciones describe mejor la inversión anual de su organización en seguridad de la información?



Encuesta México

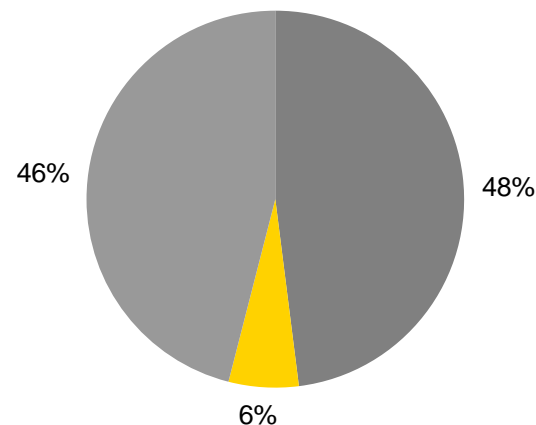


- Incremento en el porcentaje del total de gastos
- Disminución del porcentaje del total de gastos
- Relativamente constante del total de gastos

Resultados

Un 35% de las organizaciones planean incrementar su inversión en seguridad de la información y 55% la mantendrá. Es importante señalar que únicamente 10% de los participantes recortará su inversión en el tema.

Encuesta Global



- Incremento en el porcentaje del total de gastos
- Disminución del porcentaje del total de gastos
- Relativamente constante del total de gastos

Nuestra perspectiva

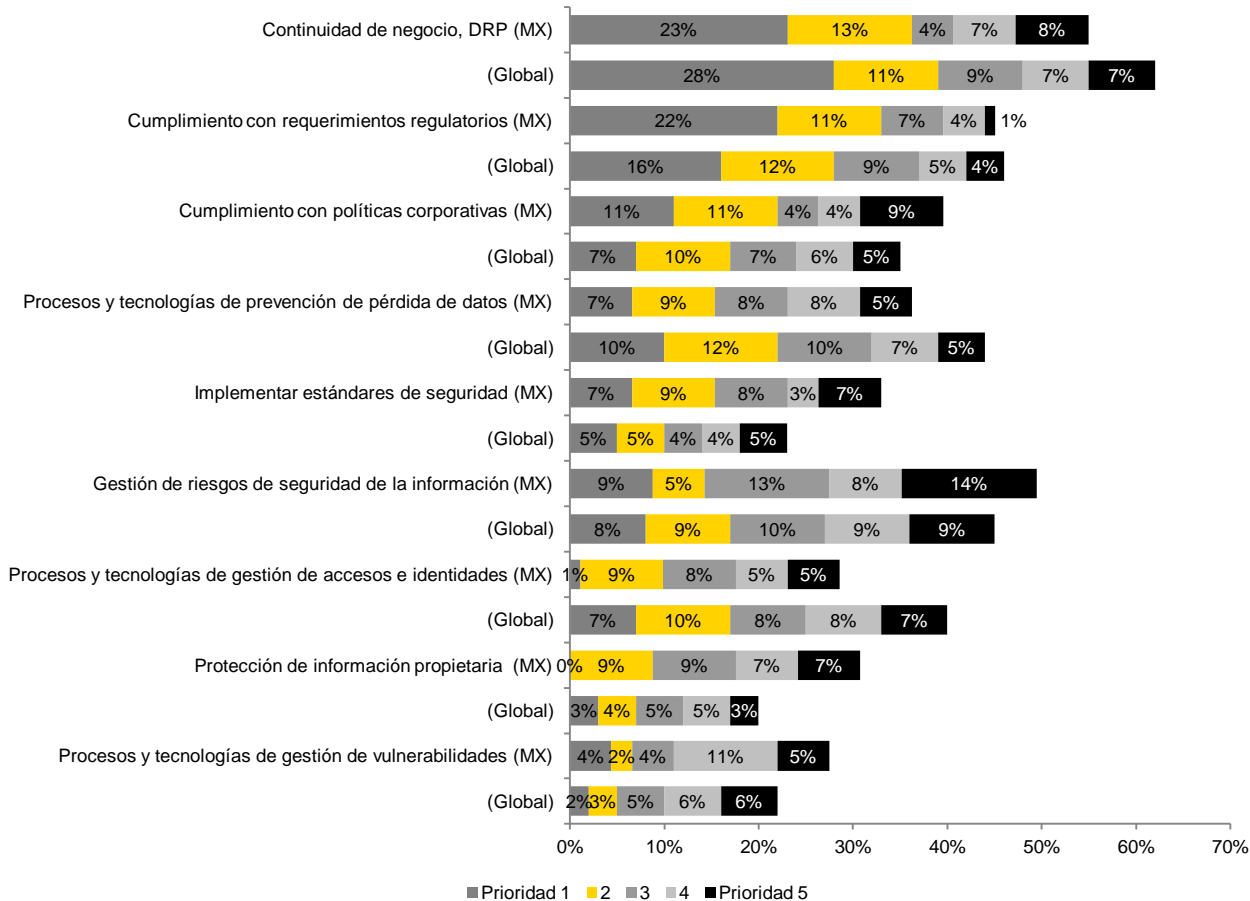
Aun cuando los efectos de la crisis económica no han desaparecido por completo, notamos un compromiso elevado de las organizaciones por reforzar su seguridad evitando disminuir la inversión que han venido realizando.

2. Por favor indique sus cinco principales prioridades de seguridad de la información para los siguientes 12 meses



Resultados

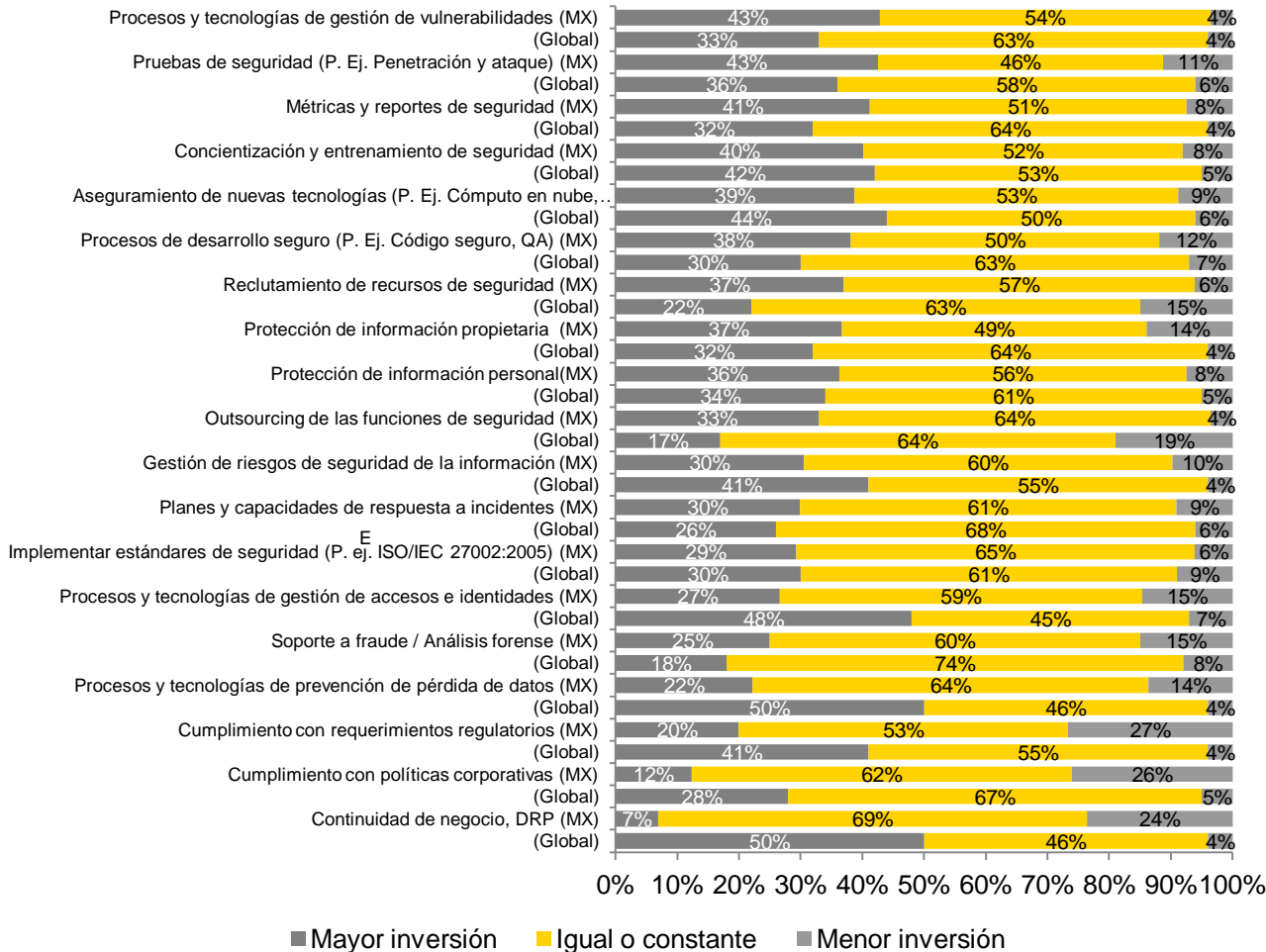
La prioridad para 2011 es:
 1. Continuidad de negocio
 2. Cumplimiento con requerimientos regulatorios
 3. Cumplimiento con políticas corporativas



Nuestra perspectiva

Adicional a los temas recurrentes, 2011 es un año en el que el cumplimiento regulatorio toma especial relevancia debido a la entrada en vigor de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

3. Comparado con el año previo, ¿su organización planea invertir más, menos o relativamente lo mismo en las siguientes actividades?



Resultados

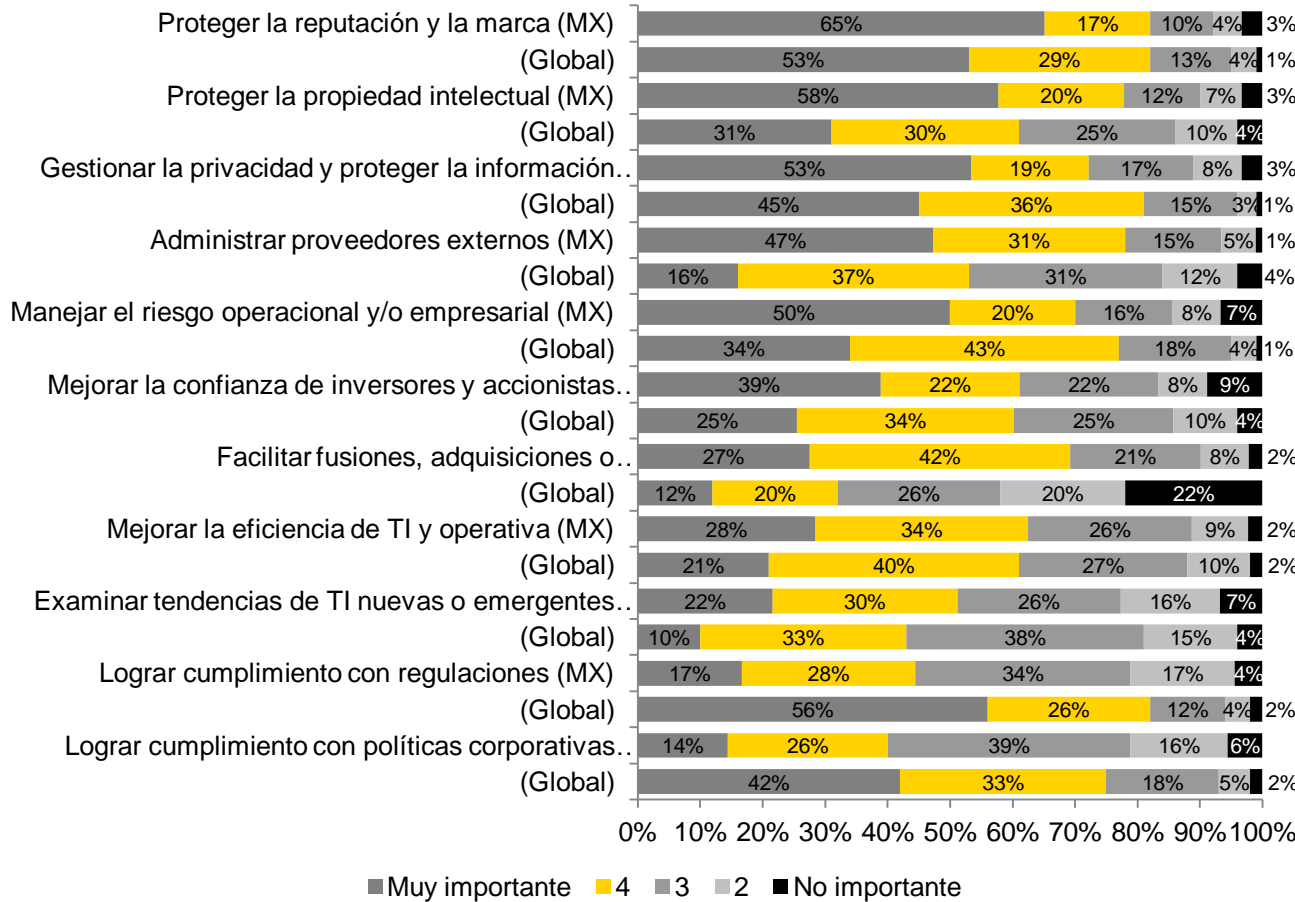
Las áreas de mayor inversión son:

1. Procesos y tecnologías de gestión de vulnerabilidades
2. Pruebas de seguridad
3. Métricas y reportes de seguridad

Nuestra perspectiva

Mientras que la tendencia global es la inversión en temas de continuidad de negocio y procesos y tecnologías de protección de pérdida de datos; en México las organizaciones continúan invirtiendo en procesos relacionados con seguridad informática sin involucrar temas relacionados con el negocio.

4. ¿Qué tan importante es la seguridad de la información como soporte de las siguientes actividades en su organización?



Resultados

Las actividades principales que soportan los procesos de seguridad de la información son:

1. Proteger la reputación y la marca
2. Proteger la propiedad intelectual
3. Privacidad y protección de información

Nuestra perspectiva

Como en años pasados, la protección de la reputación y la marca es un tema prioritario que soporta Seguridad de la Información. Es interesante señalar que evidentemente debido a la entrada en vigor de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, la privacidad y protección de información se convierte en un tema preferente.

5. ¿Qué tan significativas son las siguientes consecuencias de la pérdida o robo de información para su organización?

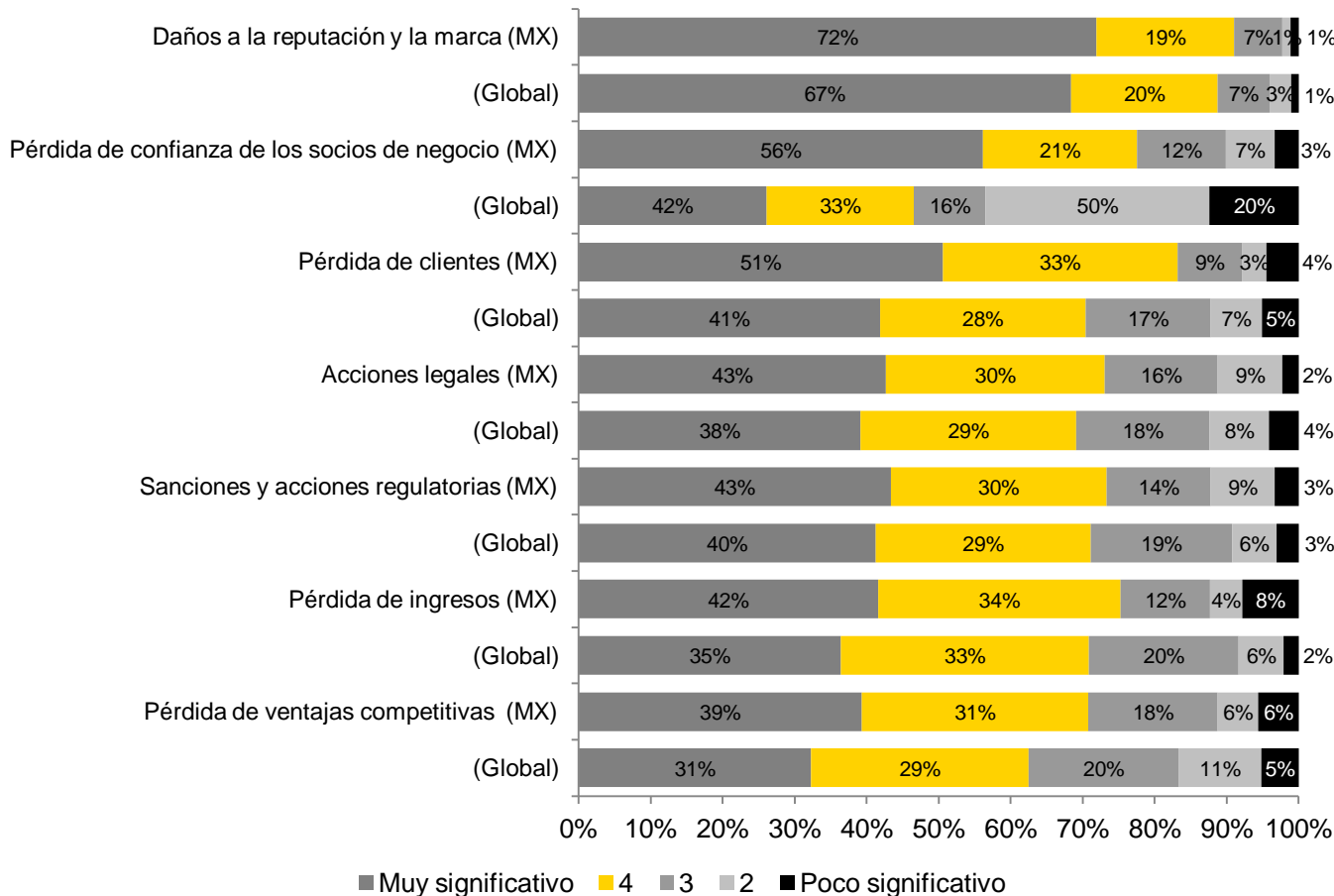


Resultados

El 72% de los encuestados considera muy significativo el daño a la reputación y la marca por la pérdida de la información. Mientras que la pérdida de confianza de socios de negocio y la pérdida de clientes son consecuencias muy significativas para los negocios.

Nuestra perspectiva

Aunque los daños a la reputación y la marca y la pérdida de confianza han sido temas recurrentes, hoy las organizaciones se enfrentan a un habilitador primordial para robustecer la importancia de ambos temas; considerando las sanciones y penas que la Ley establece por incumplimiento.

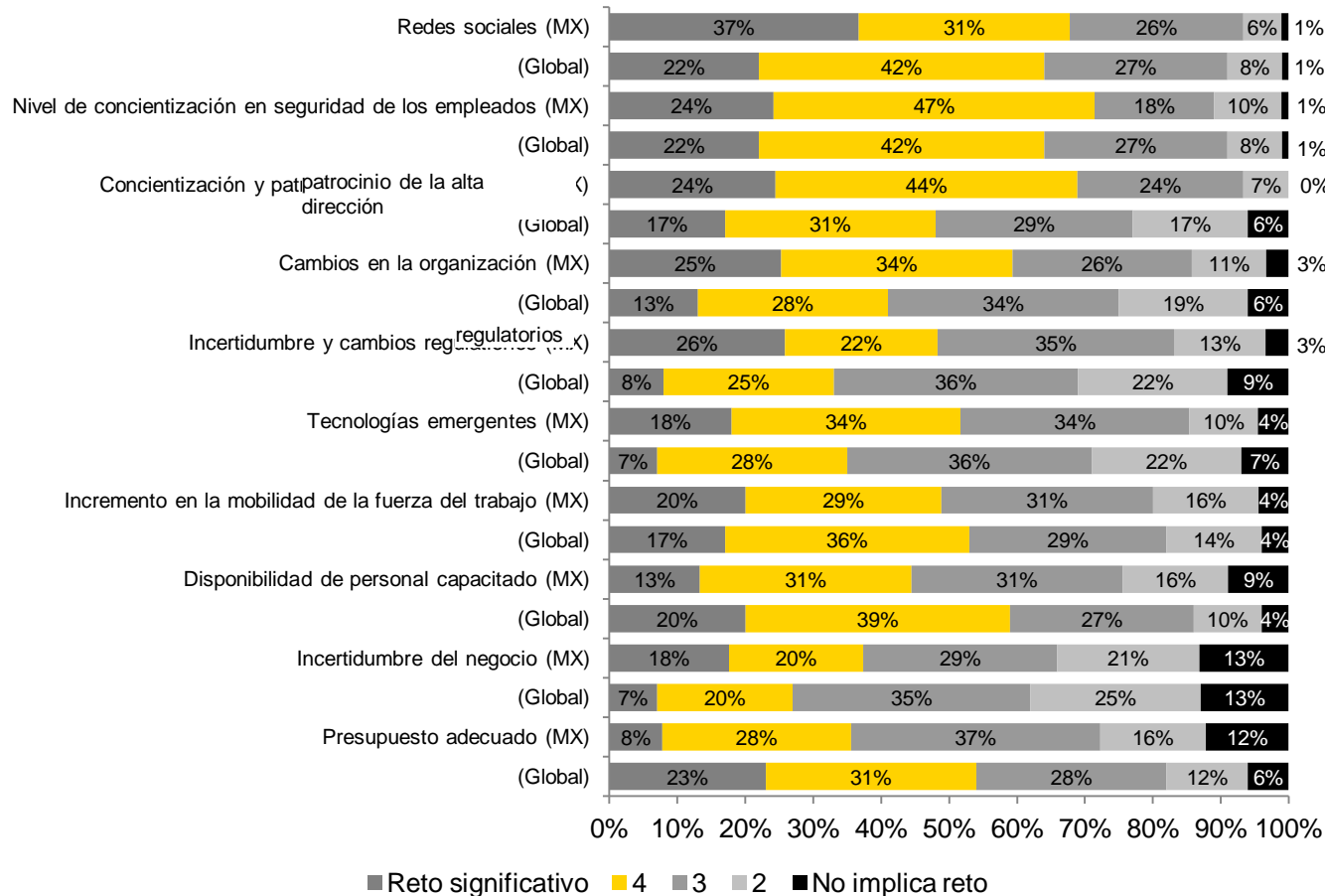


6. ¿Qué nivel de reto implica la entrega efectiva de las siguientes iniciativas de seguridad de la información dentro de su organización?



Resultados

El mayor reto es percibido en las redes sociales, que 68% de los encuestados lo coloca en los primeros dos lugares. Es interesante observar que para los encuestados los cambios regulatorios alcanzan solo 48% en nivel de reto, por debajo del cambio organizacional.



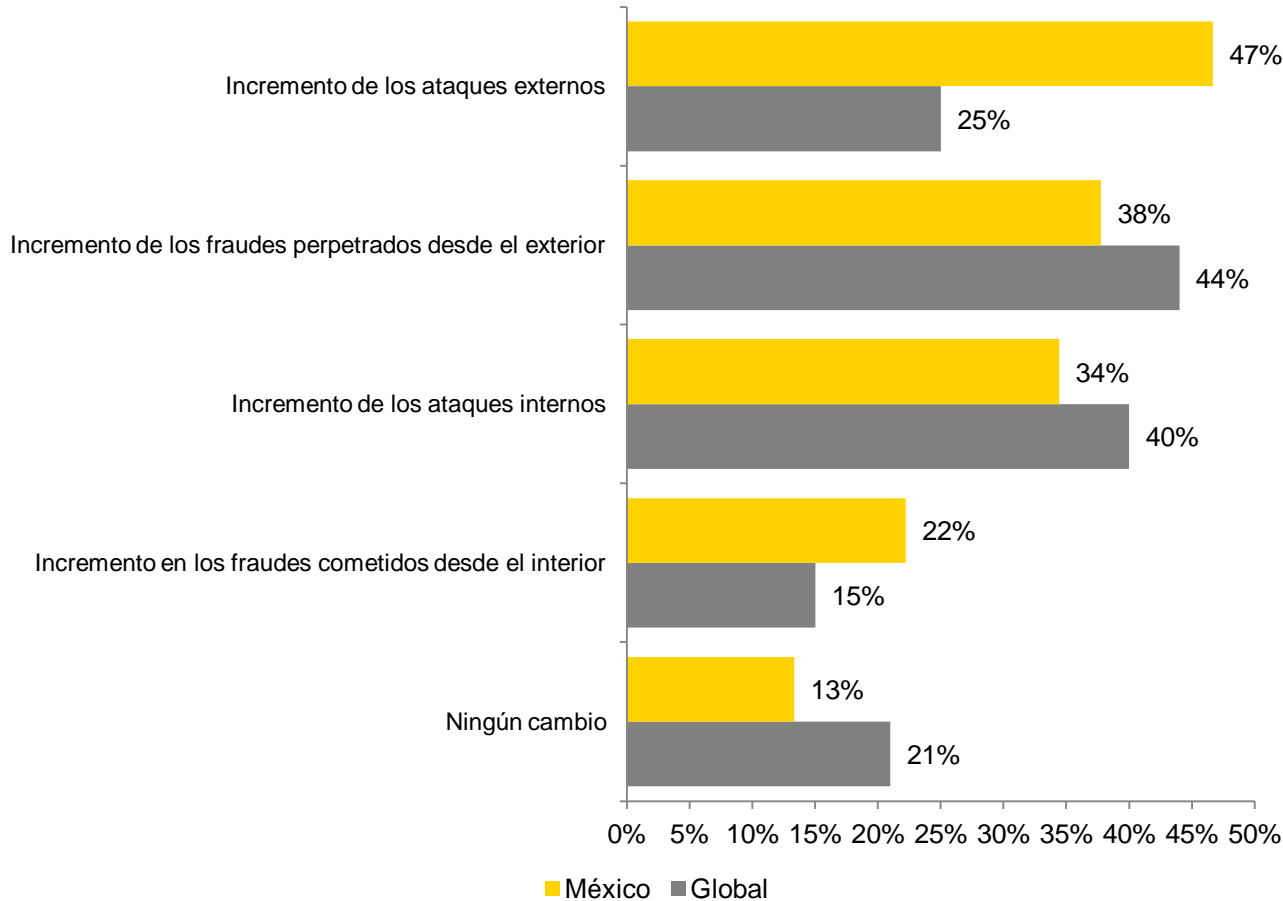
Nuestra perspectiva

El reto más importante tanto a nivel global como en México son las redes sociales. Además es importante apuntar que a pesar de la entrada en vigor de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y todo lo que ésta implica, son pocas las organizaciones que señalan como un reto importante esta iniciativa.



Amenazas y riesgos

7. Considerando el ambiente económico actual, ¿ha percibido cambios en las amenazas que enfrenta su organización?



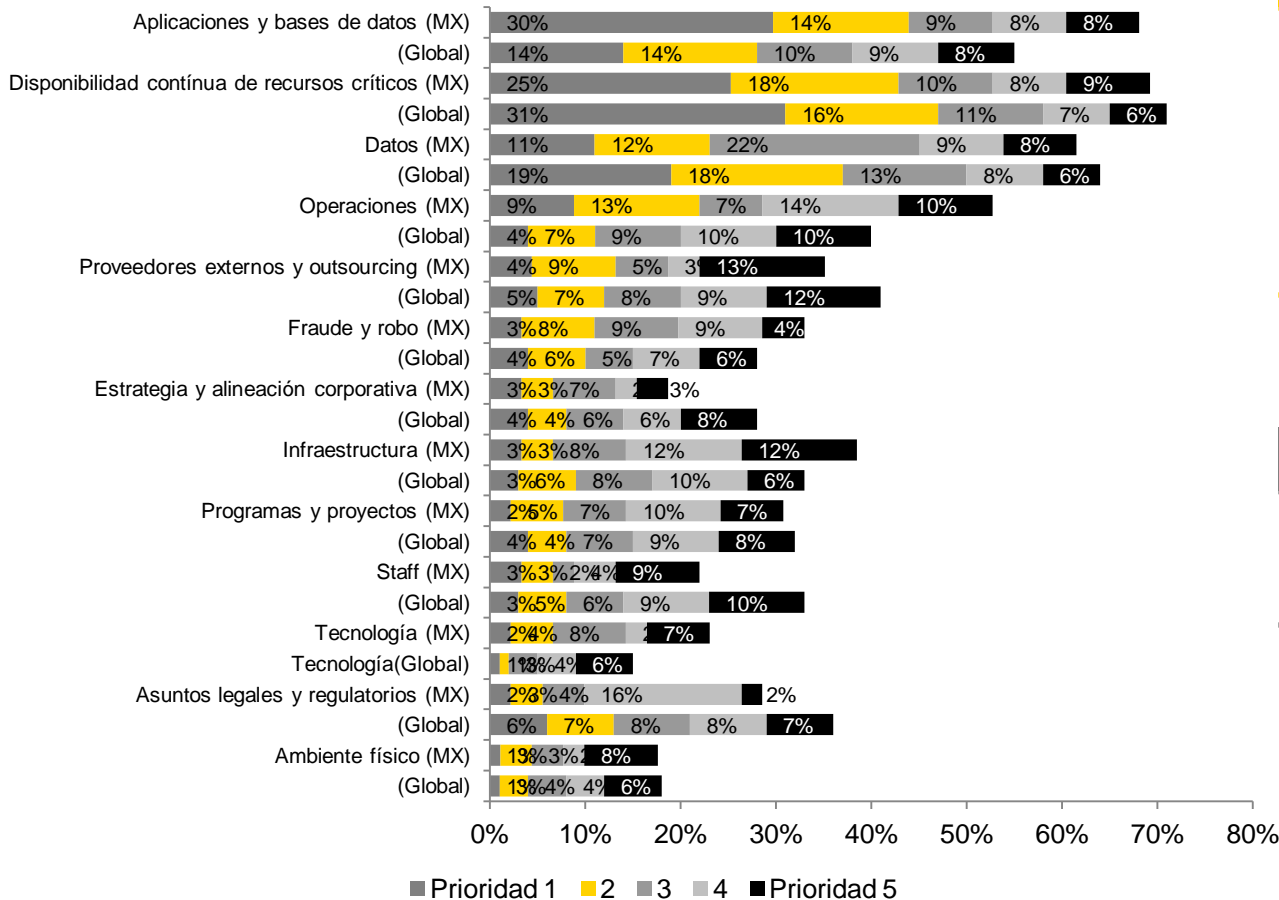
Resultados

Hay una percepción muy fuerte de que los ataques y los fraudes se han incrementado desde el exterior.

Nuestra perspectiva

El creciente negocio de la delincuencia cibernética ha aumentado en forma significativa los intentos de ataque y fraude que vienen del exterior, sin embargo, no debemos descuidar el interior de nuestras organizaciones por esta razón.

8. De la siguiente lista, ¿cuáles son las cinco principales áreas de riesgo derivado del uso de sistemas informáticos en su organización?



Resultados

De manera consistente con las prioridades de Seguridad de la Información, las áreas de riesgo son:

- Aplicaciones y bases de datos
- Disponibilidad continua de recursos críticos
- Datos

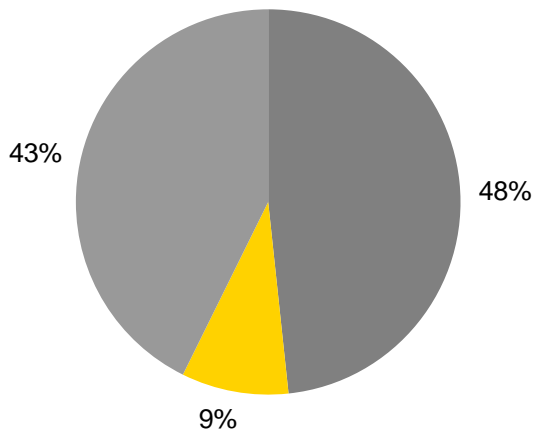
Nuestra perspectiva

Las organizaciones empiezan a poner especial énfasis en las áreas de mayor riesgo para el negocio.

9. En relación con sus cinco principales áreas de riesgo, ¿cuál de las siguientes frases describe mejor la inversión total planeada por su organización en los siguientes 12 meses?



Encuesta México

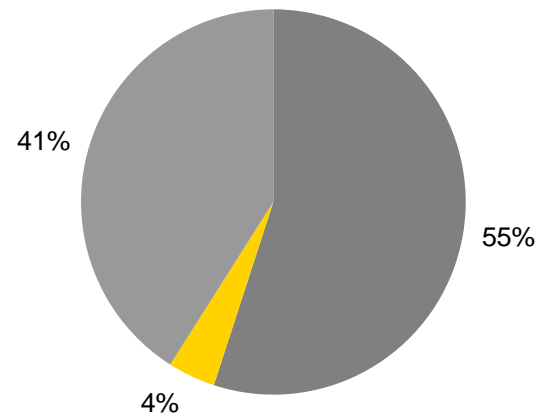


- Incrementar el nivel de inversión planeado
- Reducir el nivel de inversión planeado
- Mantener relativamente constante el nivel de inversión planeado

Resultados

Una de cada dos organizaciones encuestadas planea incrementar el nivel de inversión para atender las áreas de mayor riesgo y solo 9% planea reducirlo.

Encuesta global



- Incrementar el nivel de inversión planeado
- Reducir el nivel de inversión planeado
- Mantener relativamente constante el nivel de inversión planeado

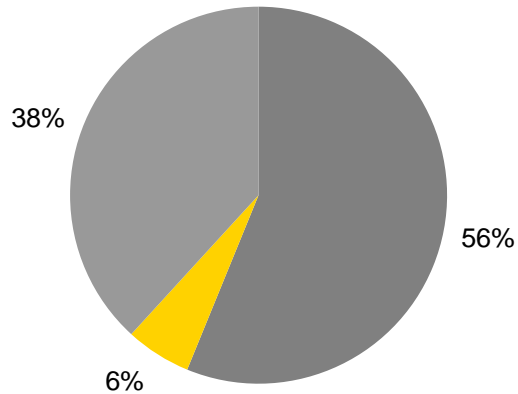
Nuestra perspectiva

Aunque es alentador que las organizaciones estén incrementando o manteniendo su nivel de inversión para mitigar y atacar los principales riesgos que les preocupan, es importante que esta inversión se base en análisis bien elaborados y procesos implementados de manera correcta.

10. Dadas las tendencias actuales hacia el uso de redes sociales, cómputo en nube y dispositivos personales móviles en las organizaciones, ¿percibe cambios en el ambiente de riesgos que enfrenta su organización?



Encuesta México

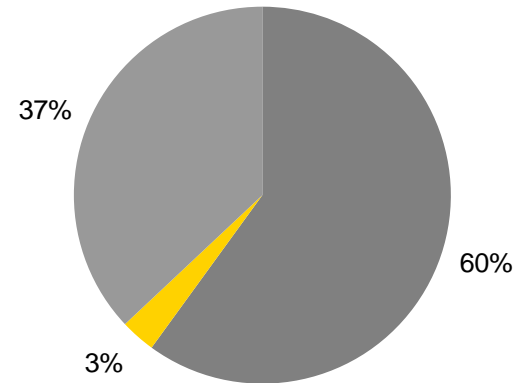


- Sí incremento en el nivel de riesgo
- No, disminución en el nivel de riesgo
- Nivel de riesgo relativamente constante

Resultados

El 56% de los encuestados considera las redes sociales, el cómputo en nube y móvil como factores que incrementan el riesgo dentro de las organizaciones.

Encuesta Global

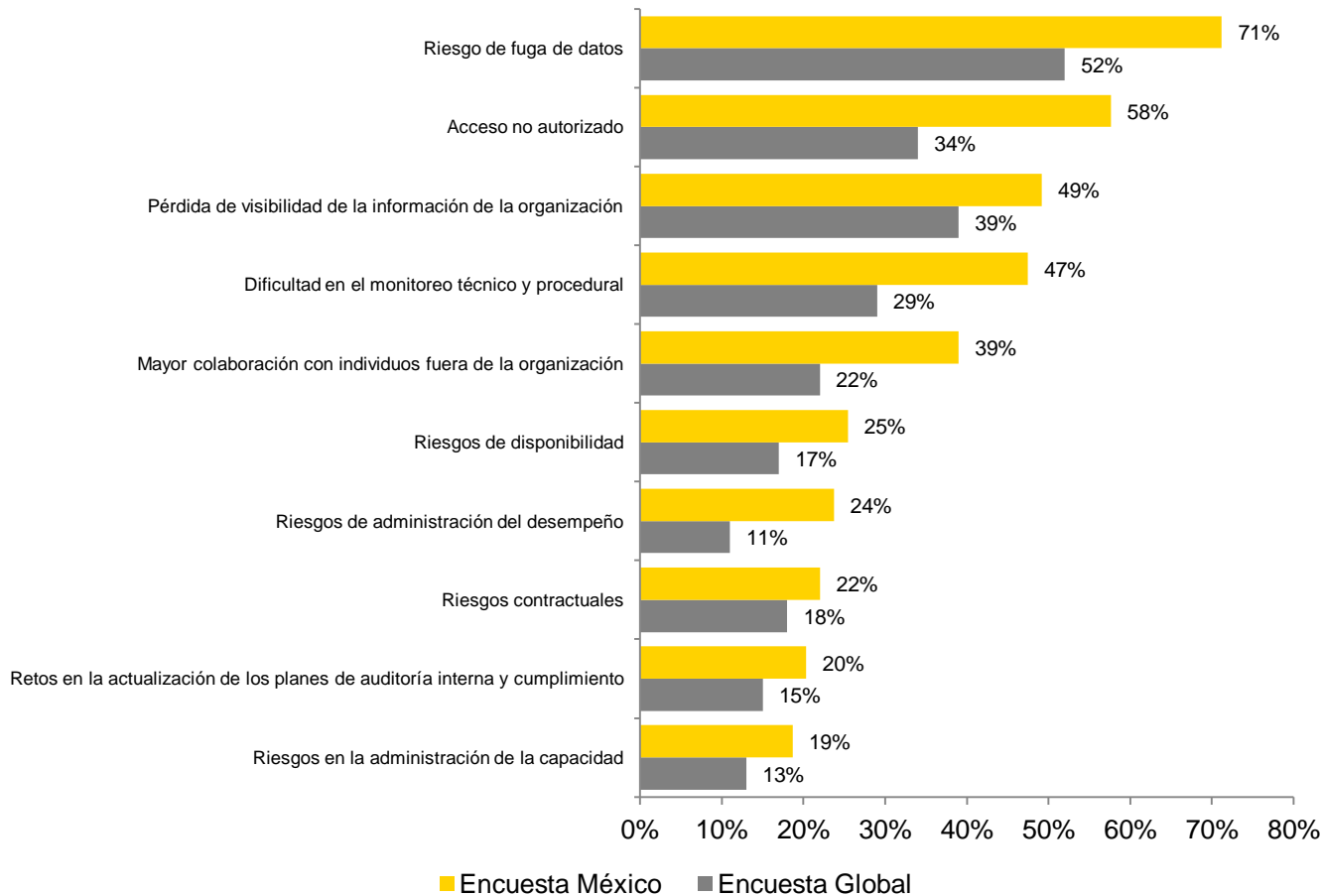


- Sí incremento en el nivel de riesgo
- No, disminución en el nivel de riesgo
- Nivel de riesgo relativamente constante

Nuestra perspectiva

Son factores que incrementan nuestro mapa de riesgos, de tal forma que no podemos permanecer pasivos ante éstos. Es necesario que como mínimo entendamos los diversos riesgos que trae su uso, modifiquemos las políticas de uso de sistemas de información de forma adecuada y capacitemos a nuestro personal sobre las amenazas que enfrentan.

10a. ¿Cuál de los siguientes riesgos ha identificado dadas las tendencias actuales del uso de redes sociales, cómputo en nube y dispositivos personales móviles?



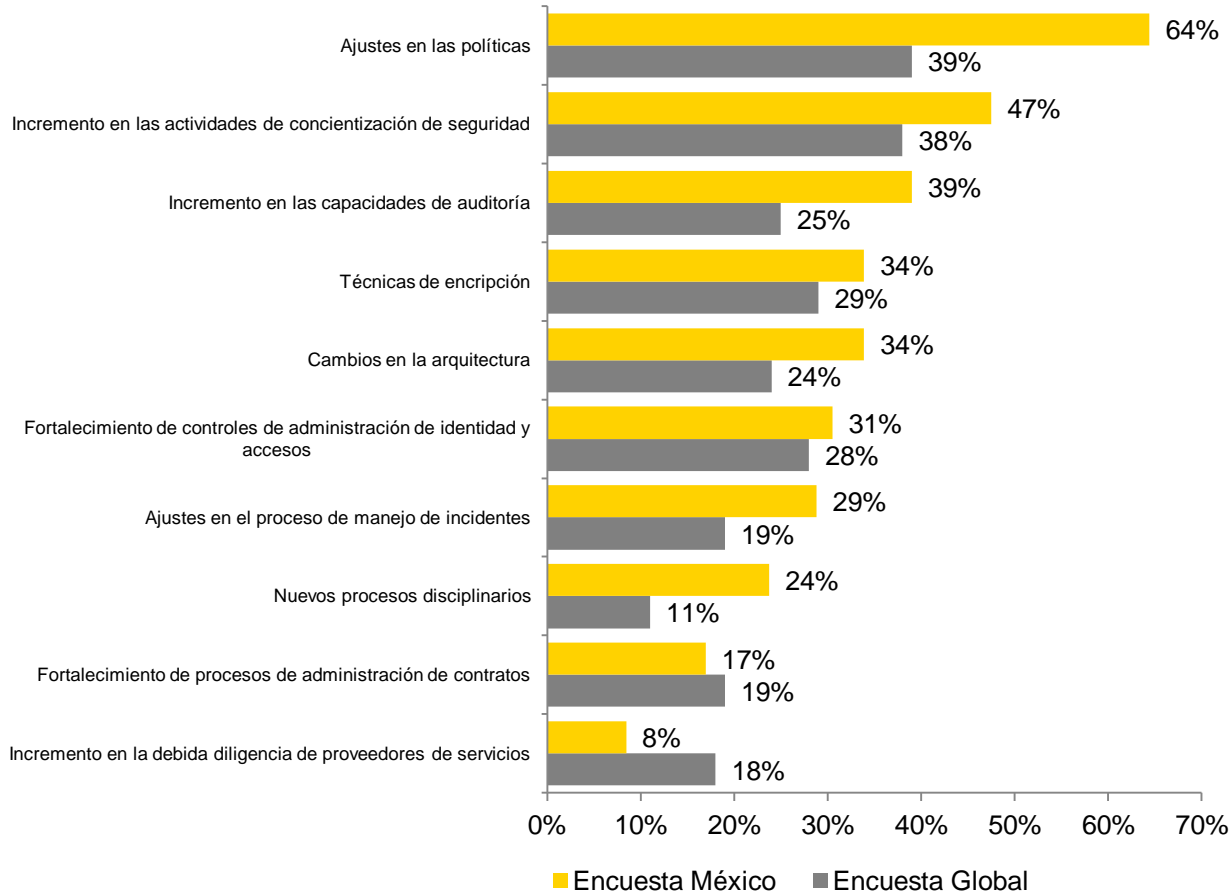
Resultados

Los nuevos riesgos o aquellos que han escalado en prioridad son encabezados por la fuga de datos, el acceso no autorizado y las múltiples formas en las que la información puede salir de la organización.

Nuestra perspectiva

Existe un rezago importante en el manejo de los riesgos generados por las tendencias actuales, ya que el riesgo de fuga de datos, acceso no autorizado y pérdida de visibilidad de la información, superan los 10 puntos porcentuales respecto a la tendencia global.

10b. ¿Cuáles de los siguientes controles ha implementado para mitigar los riesgos derivados del uso de redes sociales, cómputo en nube y dispositivos personales móviles?



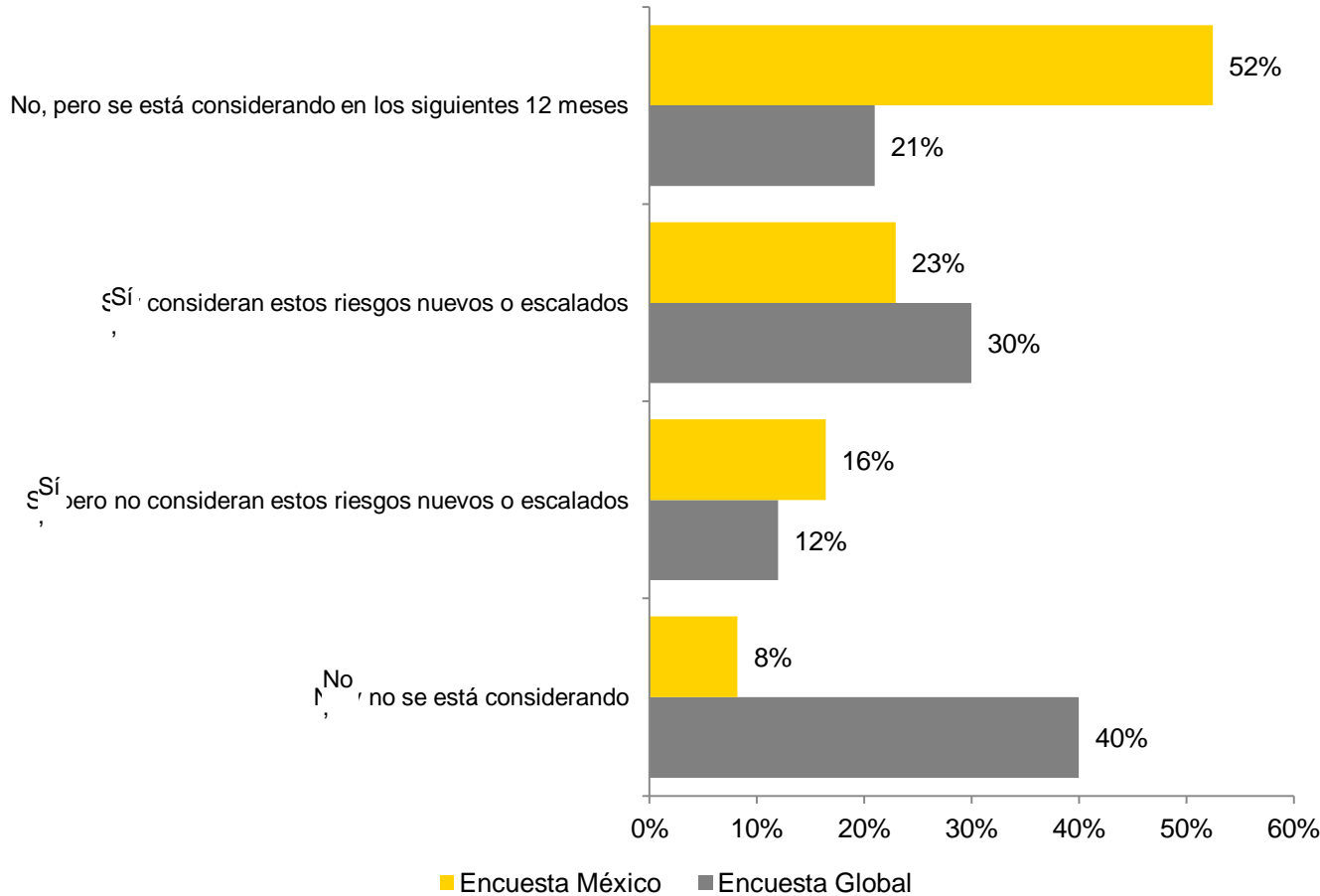
Resultados

Ajuste en políticas, concientización y políticas de auditoría, son los principales controles implementados para mitigar riesgos derivados de redes sociales, cómputo en nube y dispositivos personales móviles.

Nuestra perspectiva

Es importante considerar que además de llevar a cabo ajustes en las políticas existentes y controles detectivos, será de vital importancia establecer los controles preventivos necesarios.

10c. ¿Cuenta con un programa de administración de riesgos de TI establecido que maneje estos riesgos derivados del uso de redes sociales, cómputo en nube y dispositivos personales móviles?



Resultados

Únicamente 23% de las organizaciones ha tomado medidas contra estos nuevos riesgos y las tiene implementadas, 52% de nuestros encuestados lo tiene considerado para los siguientes 12 meses.

Nuestra perspectiva

Aunque el uso de cómputo en nube está dentro del control de TI y el cómputo móvil lleva algunos años implementado, el uso de redes sociales ha aumentado exponencialmente en los últimos dos años y cada vez es más difícil regularlo. Es necesario ser más rápidos en dar respuesta a estas problemáticas crecientes.

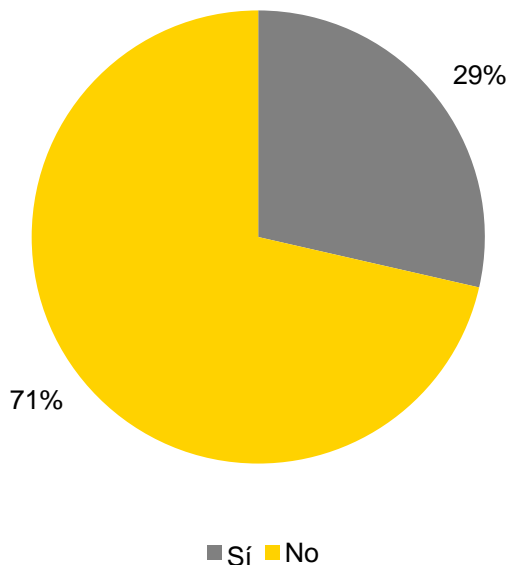


Herramientas y tecnología

11. ¿Su organización usa alguna tecnología específica para soportar el proceso de administración de riesgos?



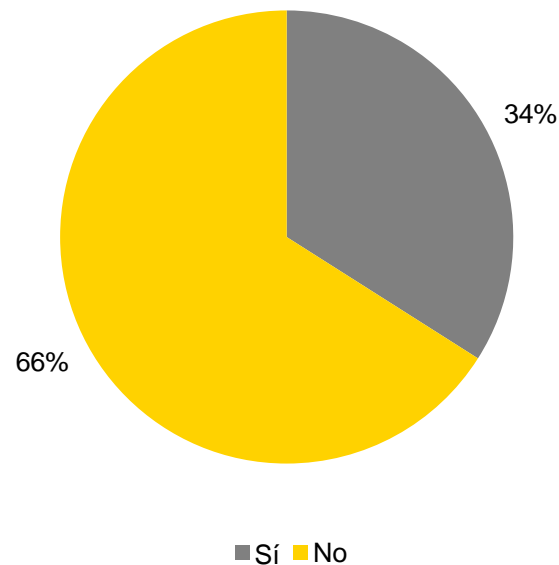
Encuesta México



Resultados

El 29% de las organizaciones encuestadas cuenta con tecnología que soporte su proceso de gestión de riesgos.

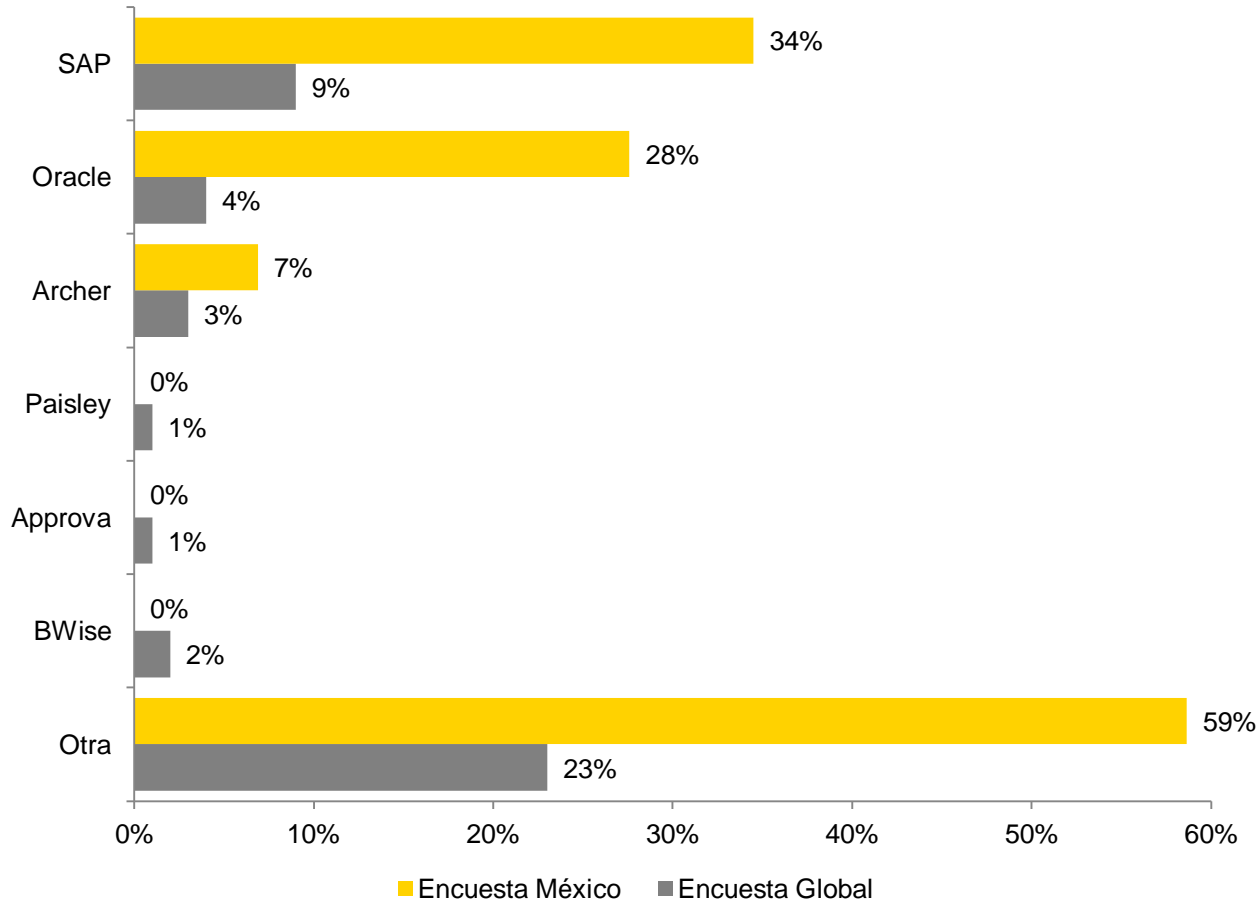
Encuesta Global



Nuestra perspectiva

Las soluciones de GRC pueden ayudar a automatizar su proceso, pero sin la asesoría adecuada para soportarlas pueden ser inversiones que no aporten en la gestión de los riesgos que enfrentamos.

11a. ¿Cuál de las siguientes tecnologías de gobierno, riesgo y cumplimiento (GRC) utiliza su organización?



Resultados

SAP y Oracle fueron identificados como los principales jugadores en tecnología GRC implementada en las organizaciones encuestadas.

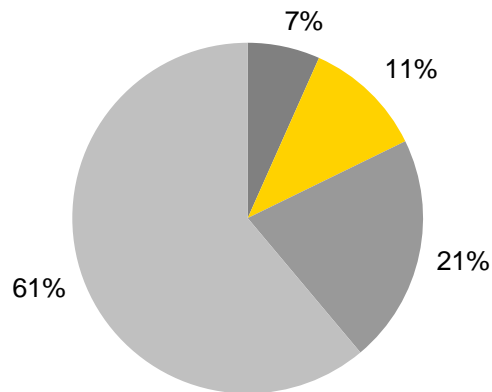
Nuestra perspectiva

Difícilmente un solo fabricante cubrirá todas las necesidades de gestión de riesgos de una organización, por lo que se están adoptando soluciones híbridas que se complementan entre sí.

12. ¿Su organización usa actualmente soluciones entregadas por medio de cómputo en nube?



Encuesta México

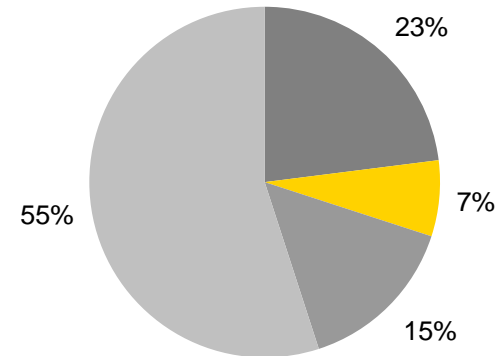


- Sí, actualmente en uso
- Sí, en evaluación
- No, pero con planes de uso en los próximos 12 meses
- No, y sin planes de uso en los próximos 12 meses

Resultados

Un 7% de las organizaciones encuestadas utiliza soluciones de cómputo en nube, 32% está evaluándolas o planeando utilizarlas en los próximos 12 meses.

Encuesta Global

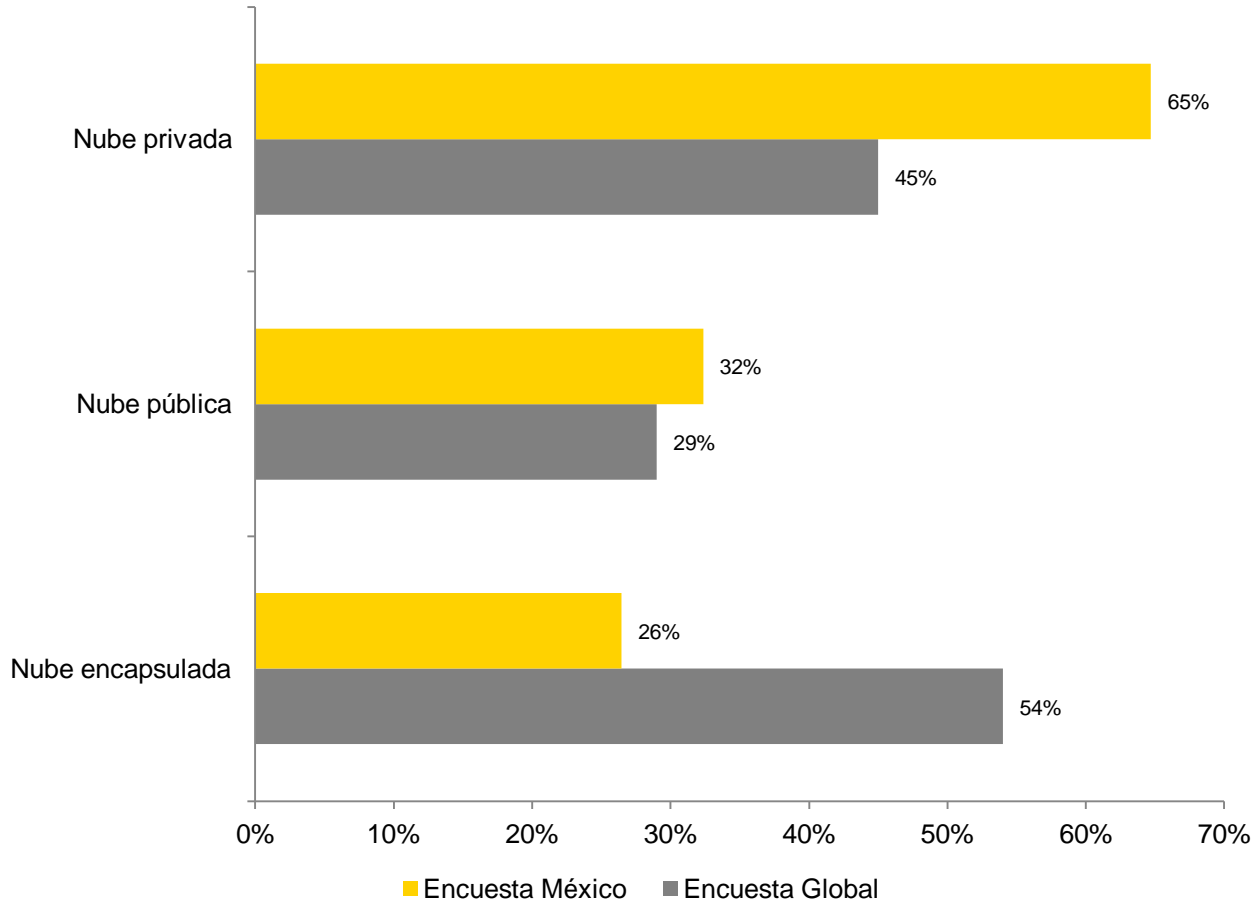


- Sí, actualmente en uso
- Sí, en evaluación
- No, pero con planes de uso en los próximos 12 meses
- No, y sin planes de uso en los próximos 12 meses

Nuestra perspectiva

Hay una baja adopción del cómputo en nube en nuestro país, probablemente derivado del poco conocimiento que tenemos de los riesgos que traen consigo estas soluciones y las implicaciones legales de contar con ellas.

12a. ¿Qué clase de tecnología de cómputo en nube utiliza o planea utilizar?



Resultados

De aquellos que utilizan cómputo en nube, 65% lo hace a través de nubes privadas.

Nuestra perspectiva

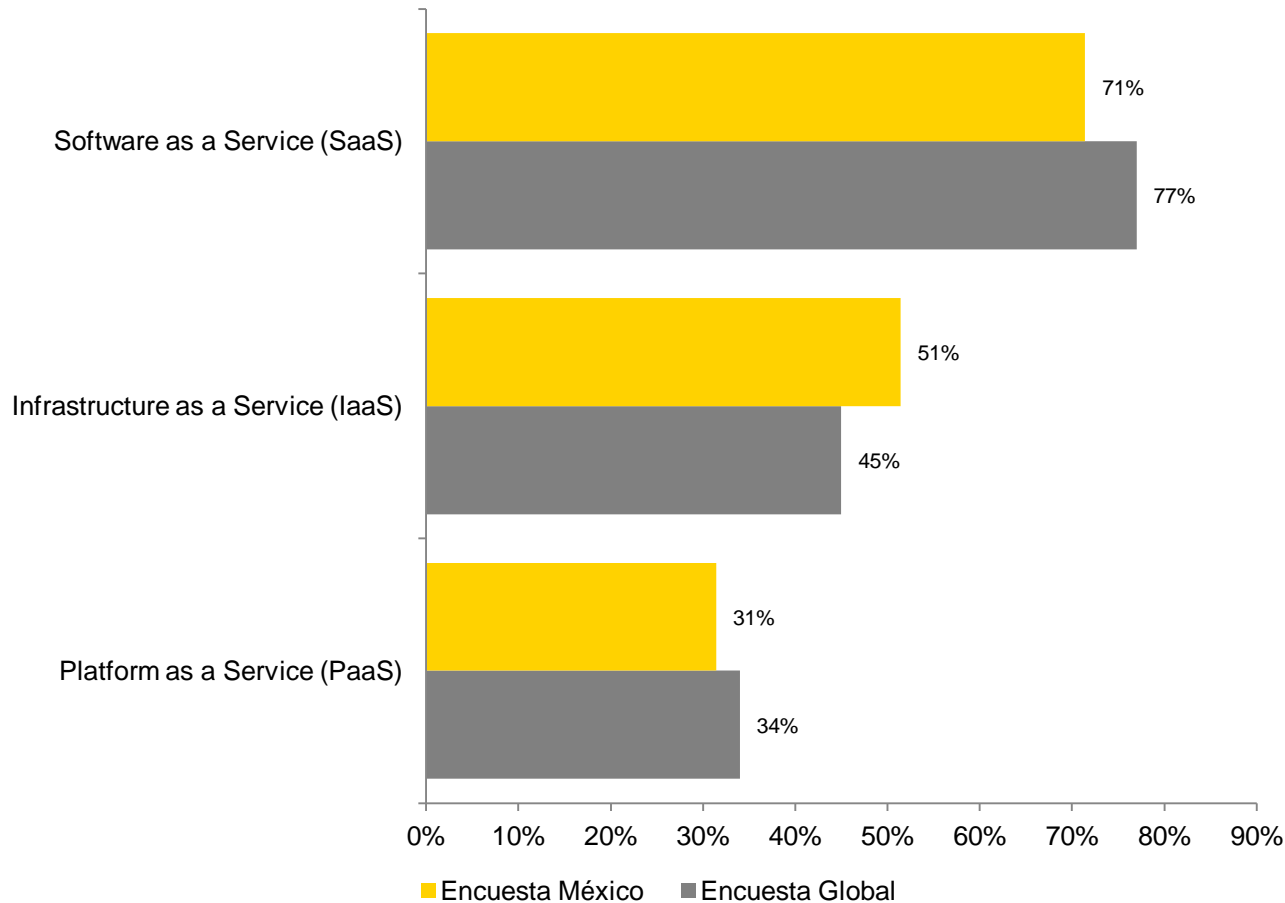
En línea con un problema de confianza, es usual que utilicemos tecnología que privilegie nuestra sensación de privacidad. Sin embargo, es importante basar nuestra noción de seguridad en un análisis y evaluación de riesgos.

12b. ¿Qué clase de servicio de nube está utilizando o planea utilizar?



Resultados

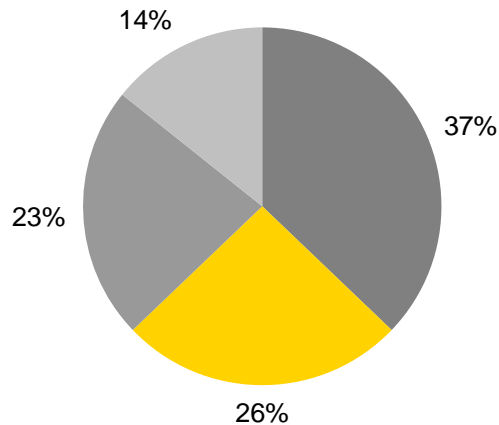
Entre las organizaciones que utilizan servicios de cómputo en nube, los más populares son Software as a Service (71%) e Infrastructure as a Service (51%).



12c. ¿Incrementaría su confianza en los proveedores de servicio de cómputo en nube, si cuentan con algún tipo de certificación externa?



Encuesta México

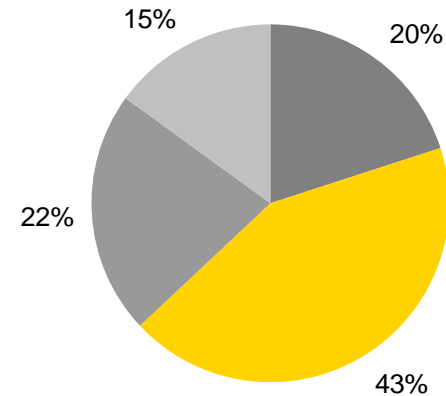


- Sí en cualquier caso
- Sí pero solo si está basada en un estándar reconocido
- Sí pero solo, si la entidad certificadora puede demostrar la acreditación
- No

Resultados

El 37% de los encuestados respondió afirmativamente que una certificación independiente les ayudaría a incrementar el nivel de confianza en servicios de cómputo en nube.

Encuesta Global



- Sí en cualquier caso
- Sí pero solo si está basada en un estándar reconocido
- Sí pero solo, si la entidad certificadora puede demostrar la acreditación
- No

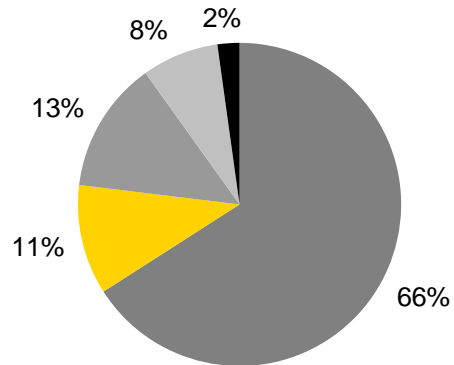
Nuestra perspectiva

Existen certificaciones basadas en estándares reconocidos que pueden ayudar a mejorar nuestra confianza, sin embargo, también es posible realizar evaluaciones por nuestra cuenta que aclaren el panorama del riesgo que representa entregar nuestra operación a un tercero.

13. ¿Su organización usa actualmente tecnologías de virtualización?



Encuesta México

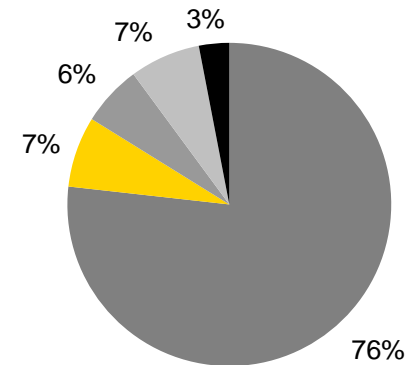


- Sí
- Ítem, planeada en los próximos 12 meses
- No, en evaluación
- No, y no planeada en los próximos 12 meses
- No aplica

Resultados

Dos terceras partes de las organizaciones utilizan virtualización dentro de su infraestructura y 11% adicional tiene planeado implementarla en los siguientes 12 meses.

Encuesta Global



- Sí
- Ítem, planeada en los próximos 12 meses
- No, en evaluación
- No, y no planeada en los próximos 12 meses
- No aplica

Nuestra perspectiva

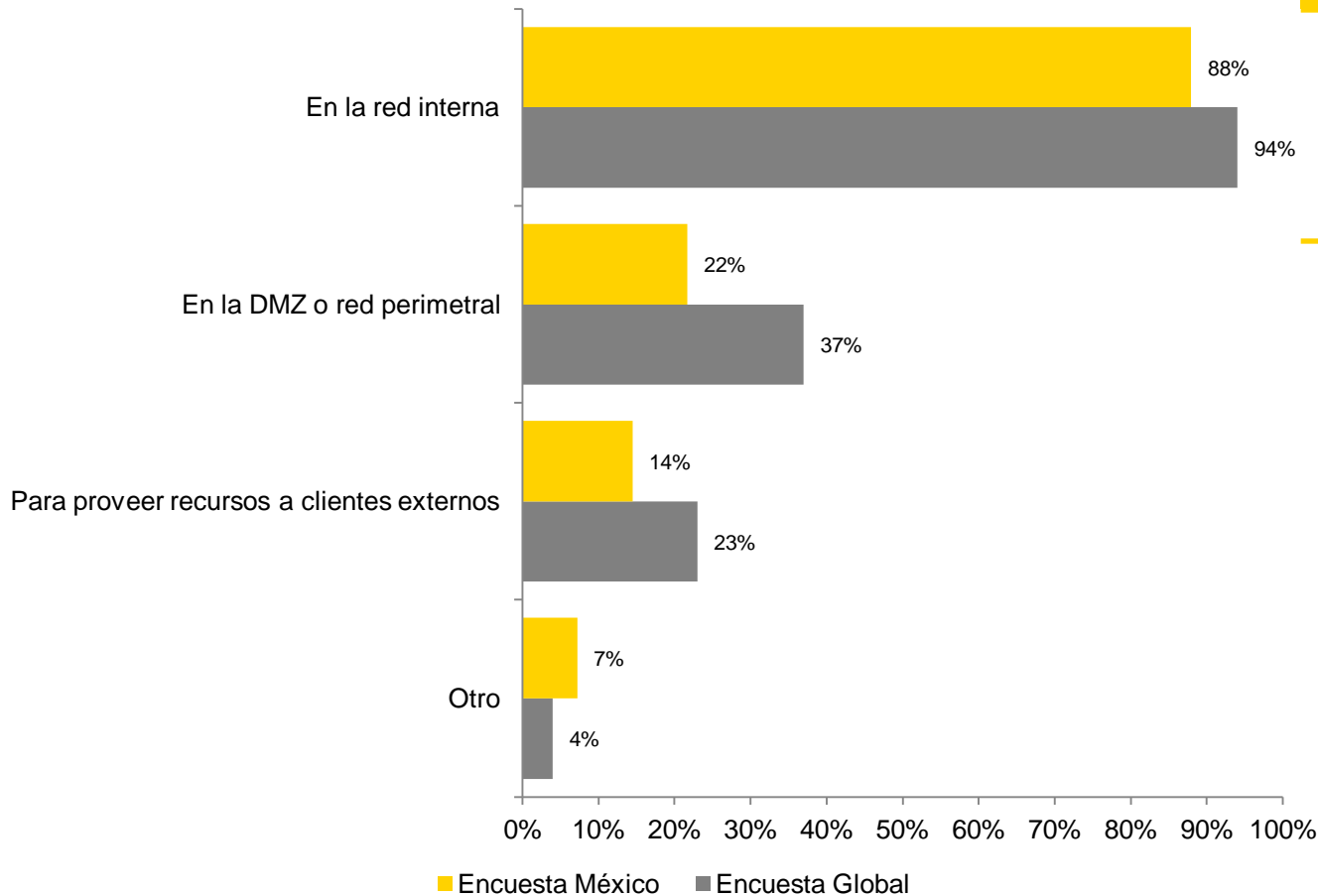
Por su enorme ventaja de costo-beneficio, la virtualización se ha adoptado en forma rápida en los últimos cinco años. Sin embargo, ¿estamos seguros de estar tomando en cuenta los riesgos asociados y de estar aplicando controles adecuados en los procesos de administración de nuestros equipos virtuales?

13a. ¿En qué ambiente utiliza o pretende utilizar virtualización?



Resultados

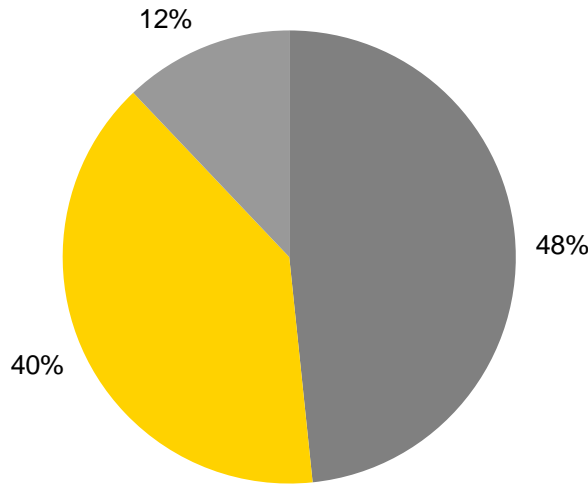
El 88% de los usuarios de virtualización hace uso de esta tecnología en la red interna, mientras que su uso para otros ambientes es bajo.



14. ¿Su organización cuenta con un programa específico de administración de accesos e identidades que mitigue los riesgos asociados con los derechos de acceso a sus datos y sistemas?

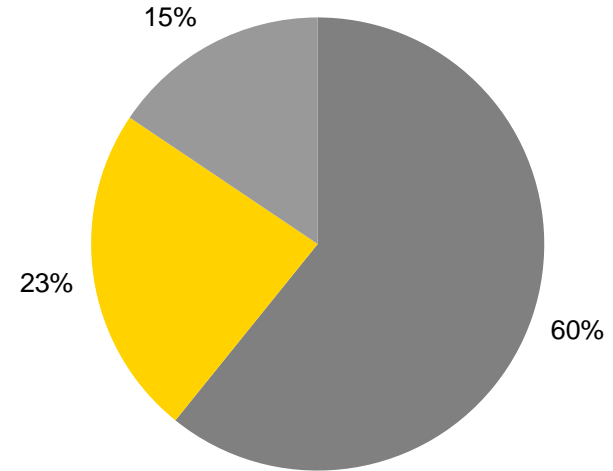


Encuesta México



■ Sí ■ Planeado en los siguientes 12 meses ■ No, y no planeado

Encuesta Global



■ Sí ■ Planeado en los siguientes 12 meses ■ No y no planeado

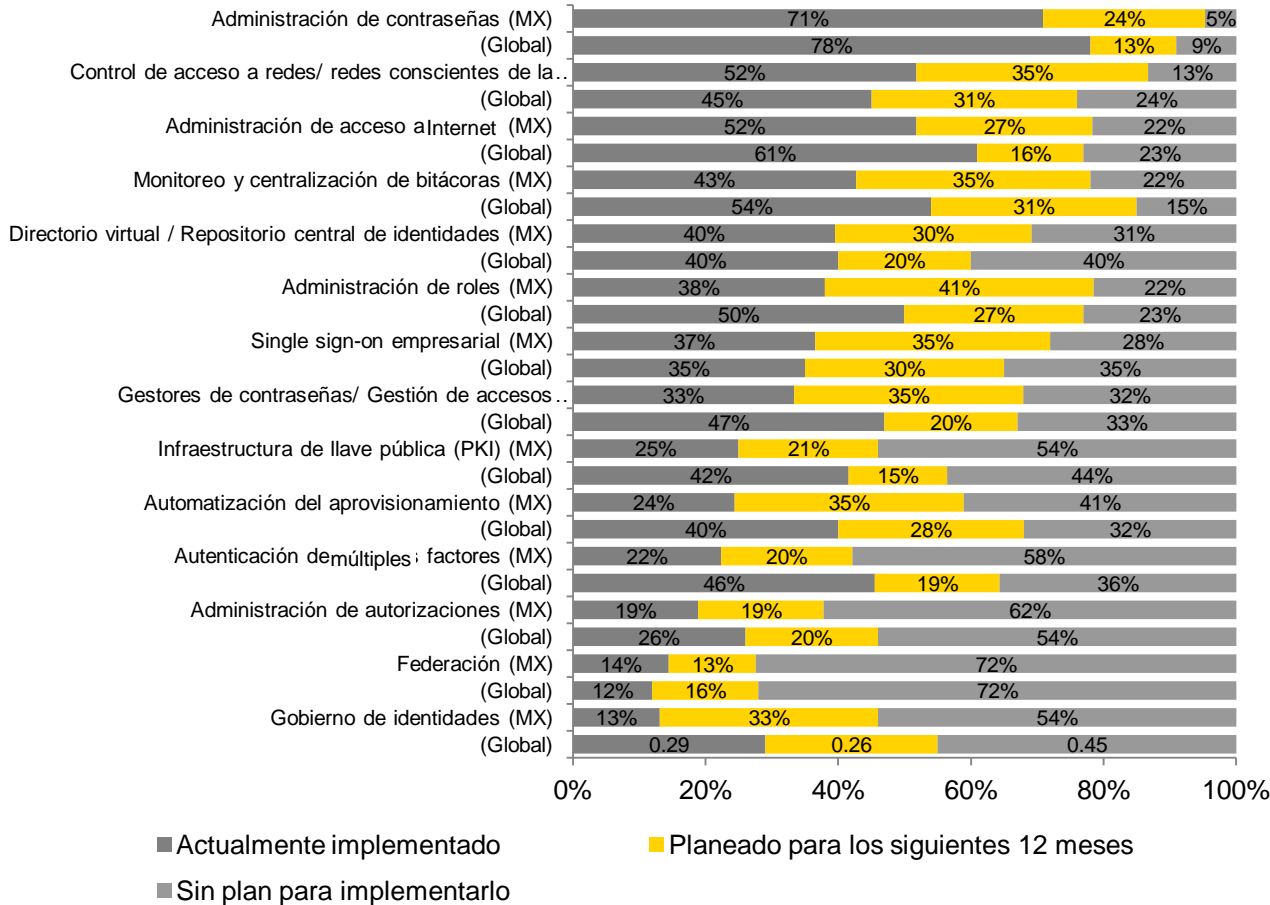
Resultados

Casi la mitad de los encuestados cuenta con alguna tecnología que los ayude a administrar identidades.

Nuestra perspectiva

Debido a la creciente preocupación por mantener la confidencialidad de la información, el control de identidades y accesos ha tomado gran relevancia. Casi 90% de las organizaciones contará en los próximos 12 meses con programas de administración que les ayuden controlar las identidades y los privilegios.

15. ¿Cuáles de las siguientes tecnologías de administración de accesos e identidades han sido implementadas o están por implementarse en su organización?



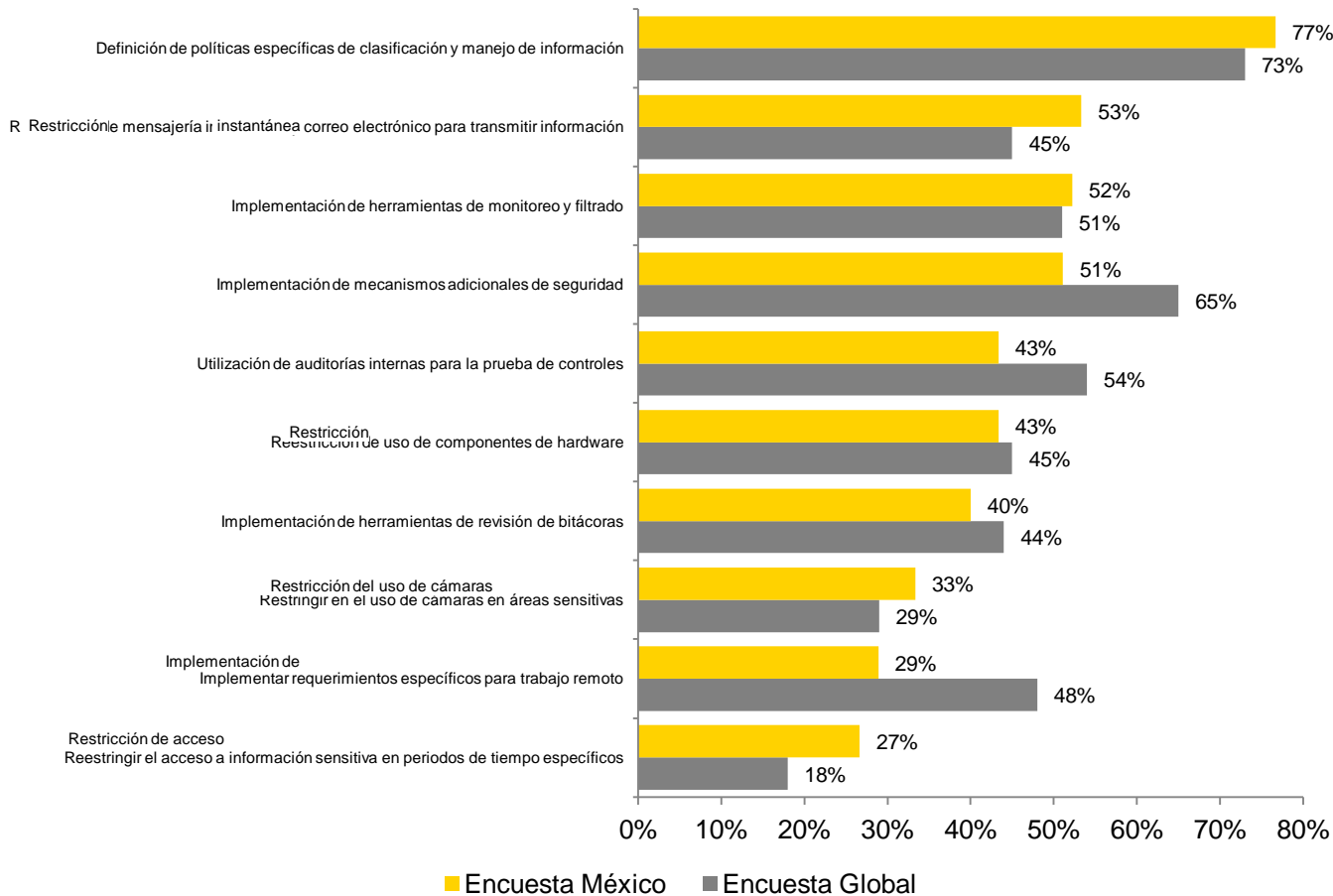
Resultados

Administración de contraseñas, control de acceso a redes y administración de acceso a internet figuran como las principales tecnologías implementadas en México.

Nuestra perspectiva

¿Se han tomado en cuenta los procesos que sirven de base de las tecnologías implementadas o próximas a implementarse?
 ¿El control está siendo una carga muy pesada para sus usuarios?
 ¿Su estrategia está alineada a los procesos de negocio o está interfiriendo con éstos?

16. ¿Cuál de las siguientes acciones ha tomado su organización para controlar la fuga de datos e información sensible?



Resultados

El 77% de los participantes ha reforzado sus políticas de clasificación de información, mientras que 53% se ha enfocado a bloquear la salida de información por correo y mensajería instantánea.

Nuestra perspectiva

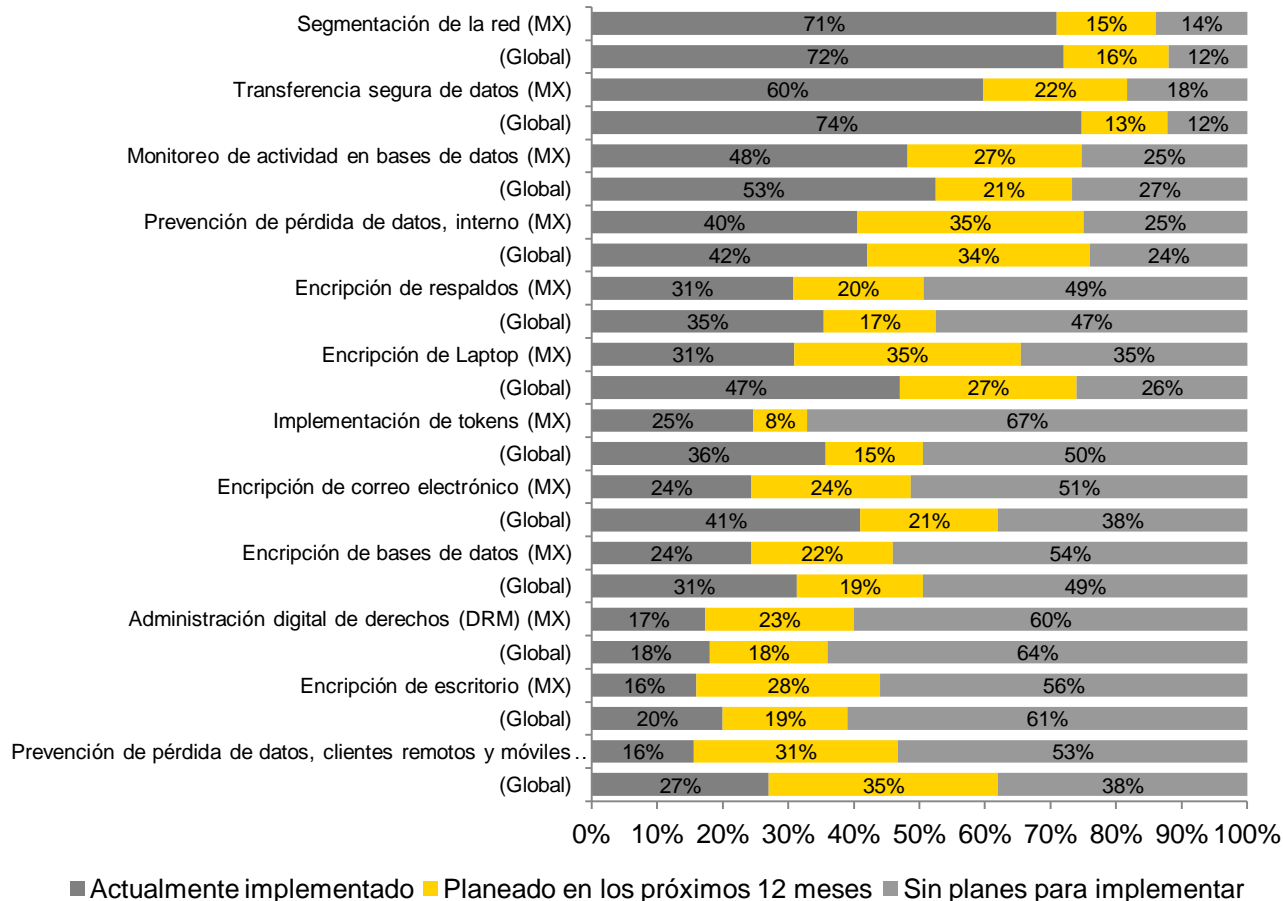
Los controles técnicos no son suficientes si nuestros colaboradores no están proporcionalmente conscientes de su papel primordial en los procesos de protección de datos y no asumen esta responsabilidad.

17. ¿Cuáles de las siguientes tecnologías de protección de datos tiene o planea implementar en su organización?



Resultados

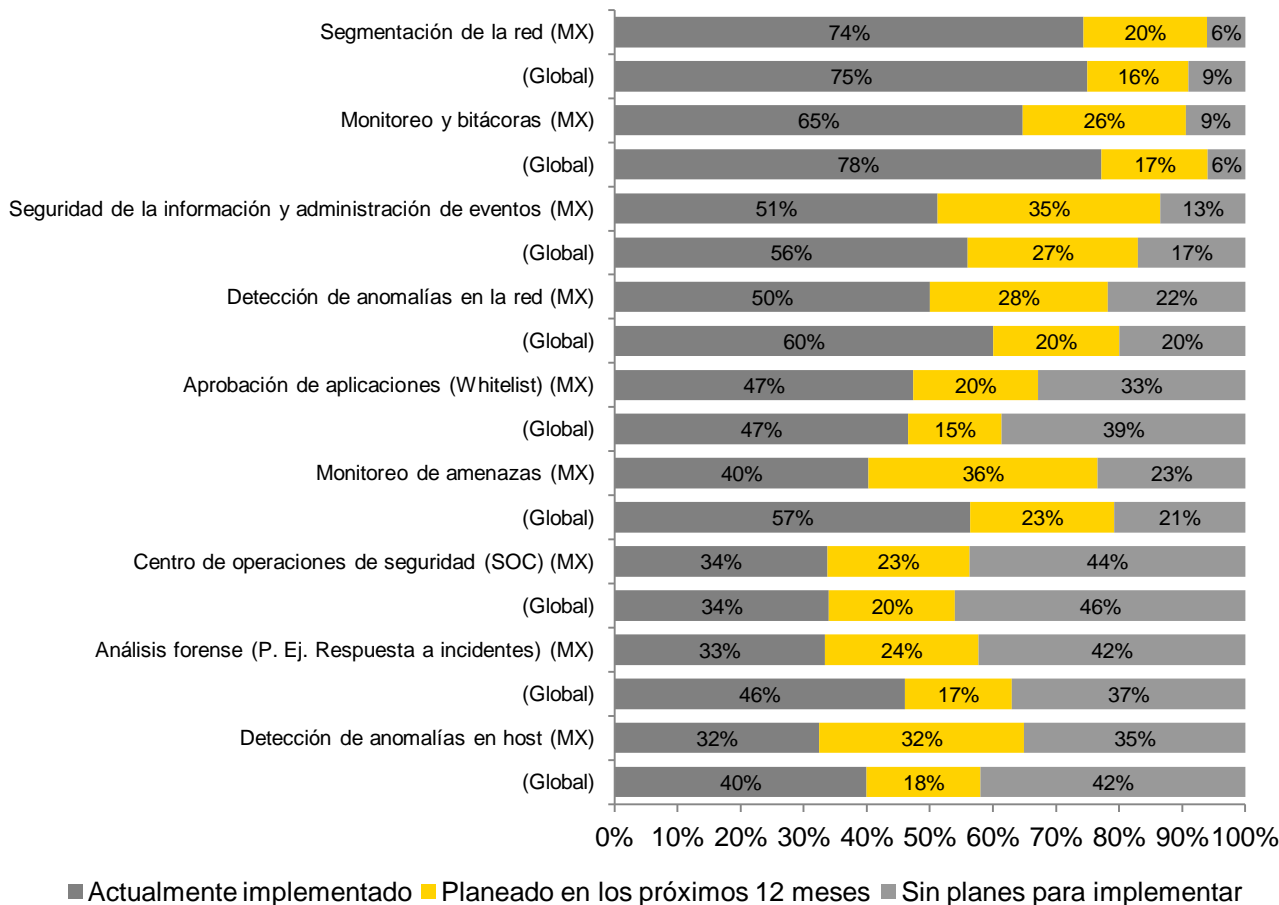
El principal enfoque está en segmentación de red (71%), transmisión segura de red (60%) y monitoreo en bases de datos (48%).



Nuestra perspectiva

La correcta implementación de estas tecnologías ayudará a mejorar nuestra postura de seguridad, pero aquellas que ya están en uso deben ser evaluadas constantemente para verificar que están contribuyendo a mitigar los nuevos riesgos de la organización.

18. ¿Cuáles de las siguientes (tecnologías / procesos) han sido implementadas en su organización para prevenir, detectar o reaccionar ante ataques externos?



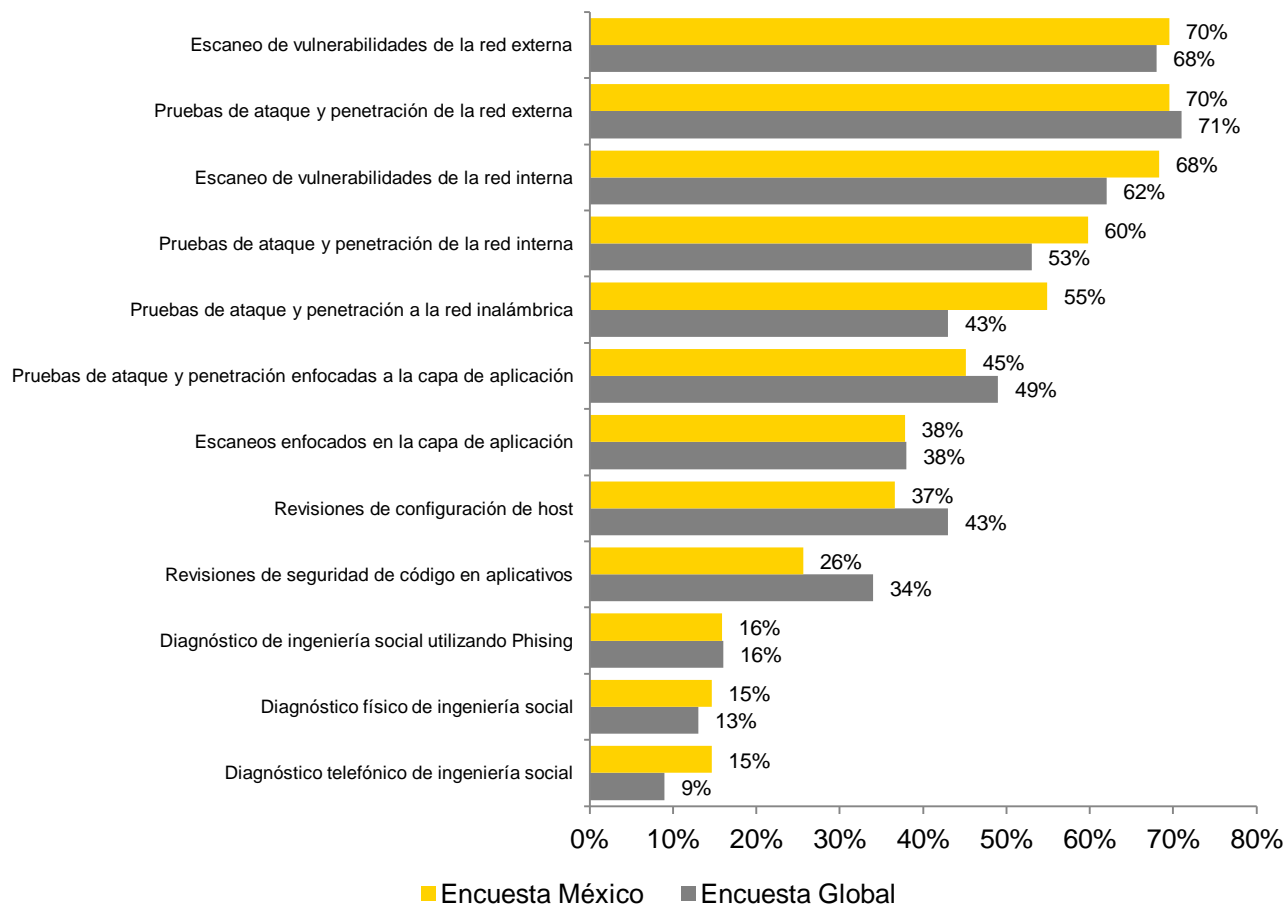
Resultados

Para ayudar con la prevención y detección de ataques externos se han implementado principalmente segmentación de la red, monitoreo de bitácoras y procesos de seguridad de información.

Nuestra perspectiva

Adicional a la aplicación de procesos o tecnologías, ¿mantenemos al tanto a los colaboradores de la organización de los riesgos que enfrentan y cómo evitarlos?

19. ¿Qué tipos de diagnósticos o pruebas técnicas de seguridad serán realizadas en su organización en el transcurso del año?



Resultados

Las principales pruebas que las organizaciones encuestadas aplican en sus ambientes son:

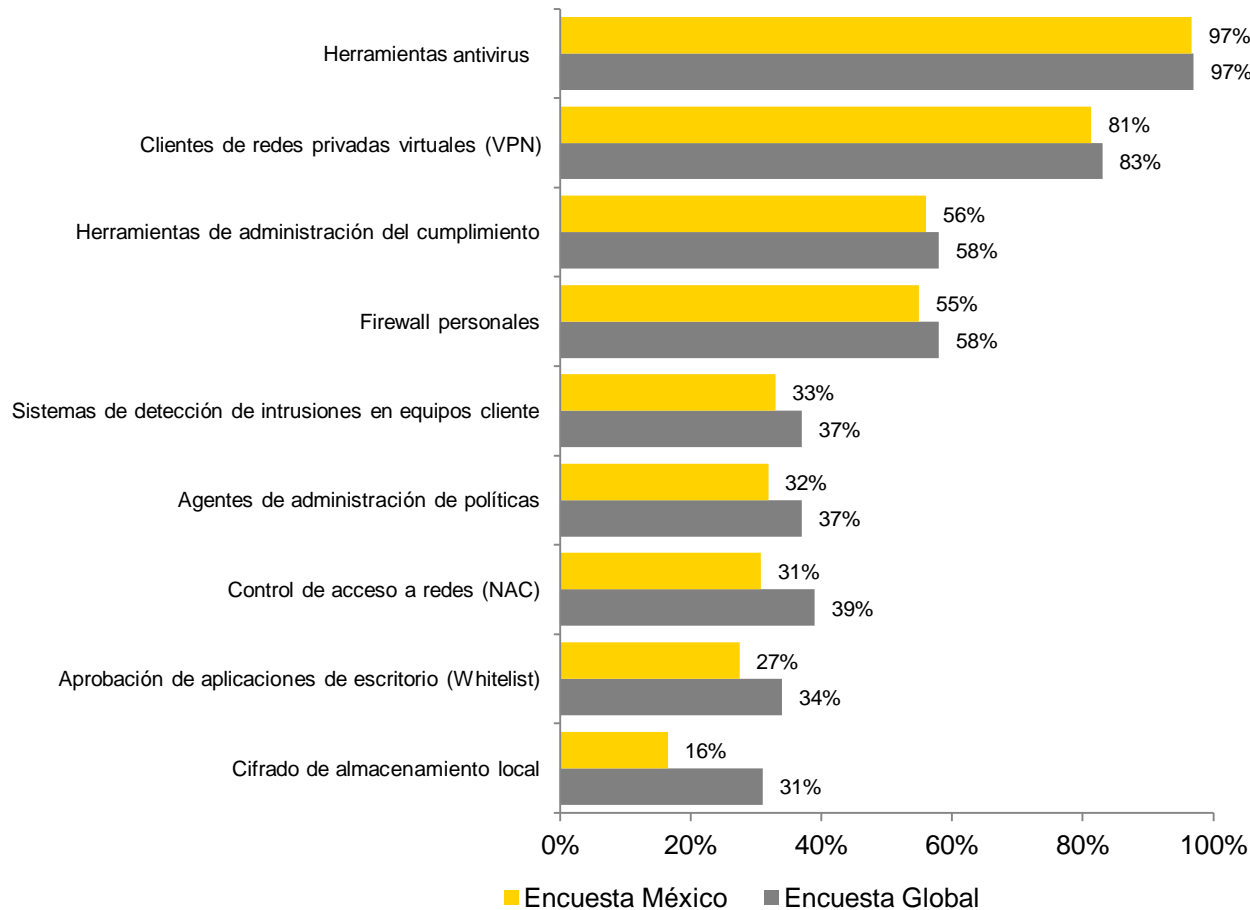
1. Escaneo de vulnerabilidades de la red externa
2. Pruebas de ataque y penetración de la red externa
3. Escaneo de vulnerabilidades de la red interna

Nuestra perspectiva

¿Cuenta con una metodología adecuada para la realización de estas pruebas?

¿Se da seguimiento apropiado a los hallazgos recibidos como resultado?

20. ¿Cuál de los siguientes tipos de seguridad en equipos cliente ha implementado su organización para proveer protección adicional a computadoras de escritorio o dispositivos móviles?



Resultados

En equipos cliente observamos un uso casi generalizado de herramientas antivirus (97%), alto uso de clientes de VPN (81%) e incremento en el uso de herramientas de cumplimiento técnico.

Nuestra perspectiva

La implementación de estas tecnologías debe ir acompañada de un seguimiento y monitoreo constante. Es necesario escuchar las alertas que nos pueden estar enviando, pues es probable encontrar oportunamente posibles ataques antes de que sean exitosos.

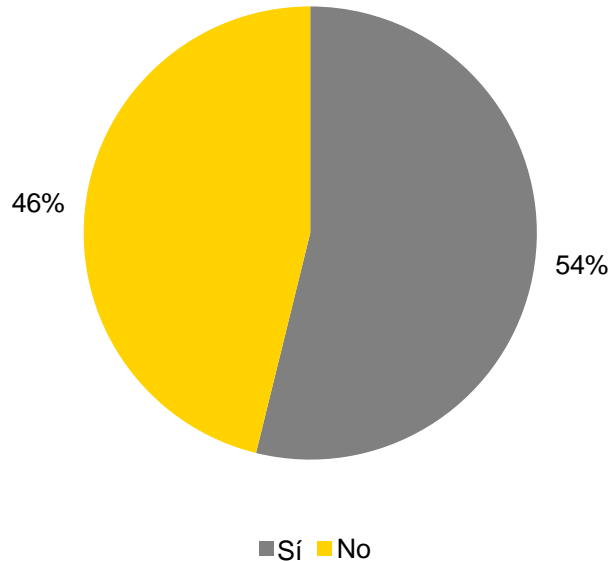


Gobierno y control

21. ¿Su organización cuenta con una estrategia documentada de seguridad de la información para los próximos uno a tres años?



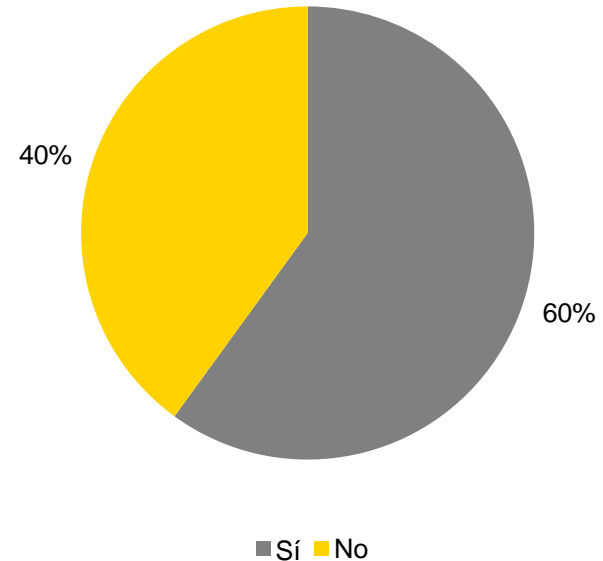
Encuesta México



Resultados

Más de la mitad de las organizaciones encuestadas cuenta con un plan a mediano o largo plazo de seguridad de la información.

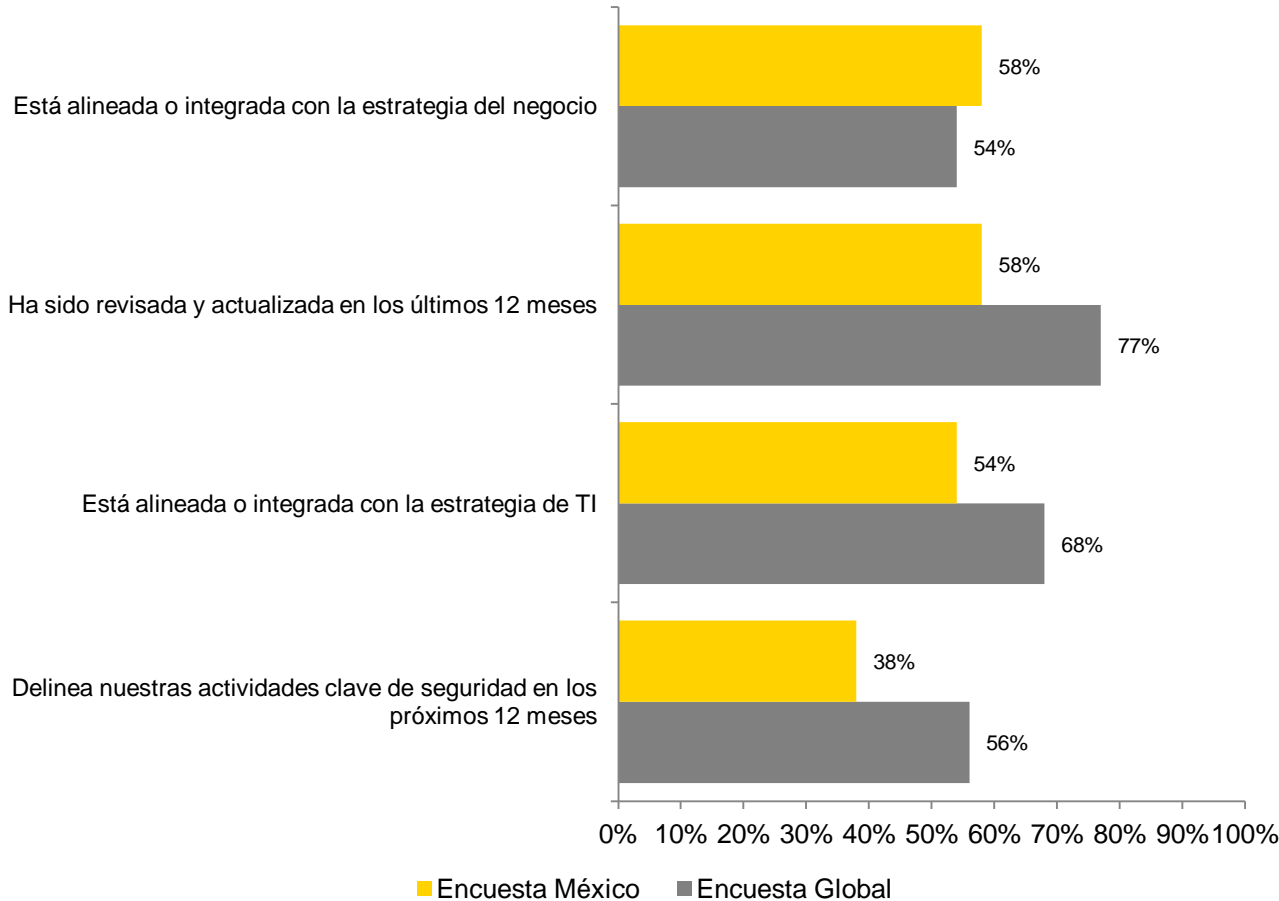
Encuesta Global



Nuestra perspectiva

Aquellas organizaciones que no cuentan con una estrategia de seguridad de la información, ¿están enfocando sus esfuerzos en la dirección correcta, ¿están cumpliendo con las expectativas y necesidades del negocio?, ¿están preparándose para cumplir con los cambios regulatorios?

21a. En relación a su estrategia de seguridad de la información:



Resultados

La mayoría de las organizaciones alinea la estrategia de seguridad de la información con la del negocio y la de TI, y la han revisado en los últimos 12 meses.

Nuestra perspectiva

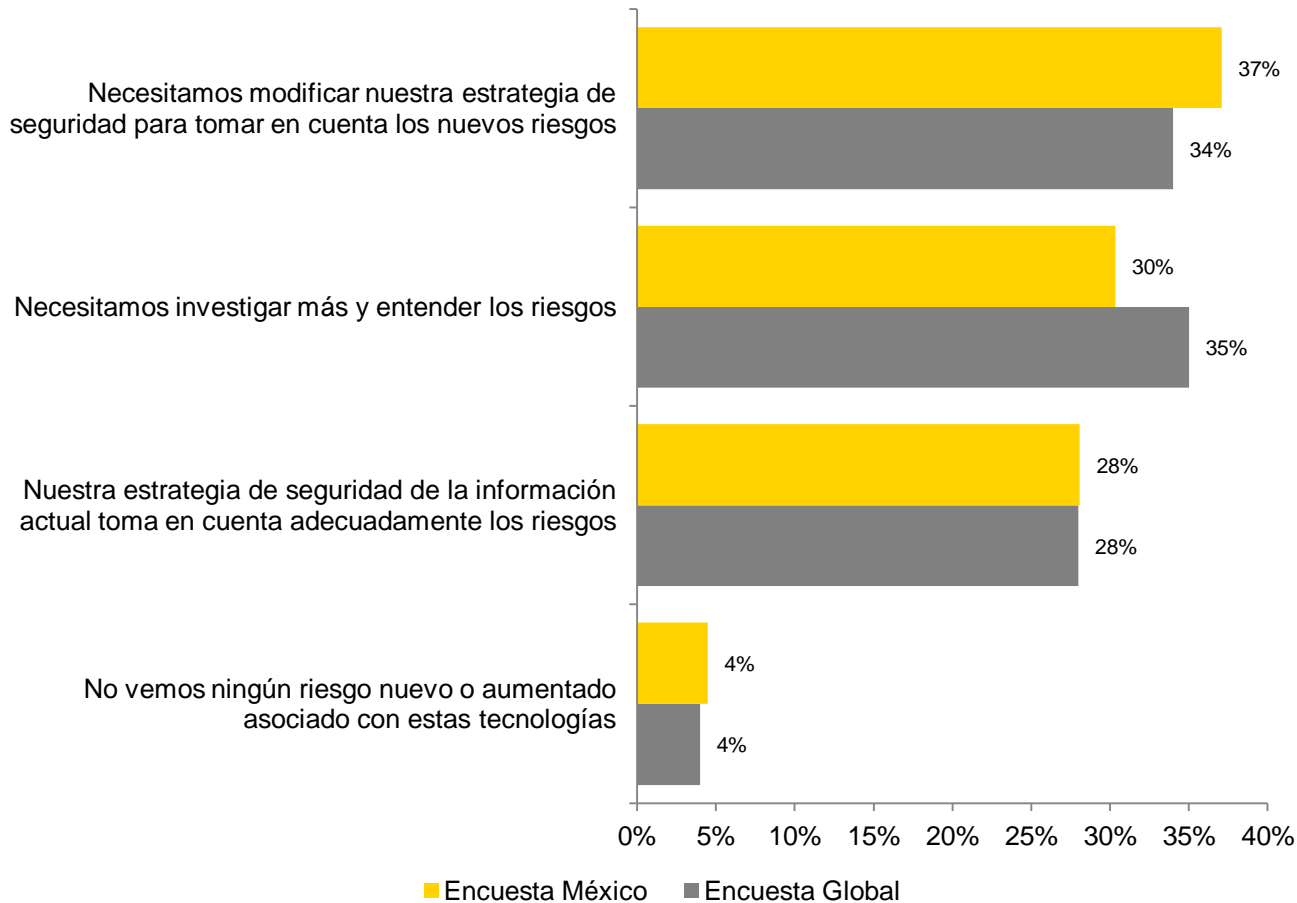
Es importante alinear las estrategias de seguridad y TI con la de la organización para que respondan adecuadamente a las necesidades de ésta. Es vital mantenerla actualizada para reflejar los nuevos riesgos que aparecen a diario y hacer que defina actividades clave para que sea un documento vivo.

22. ¿Cuál de las siguientes declaraciones describe mejor su estrategia de seguridad respecto a los riesgos asociados al creciente uso de redes sociales, dispositivos móviles o cómputo en nube?

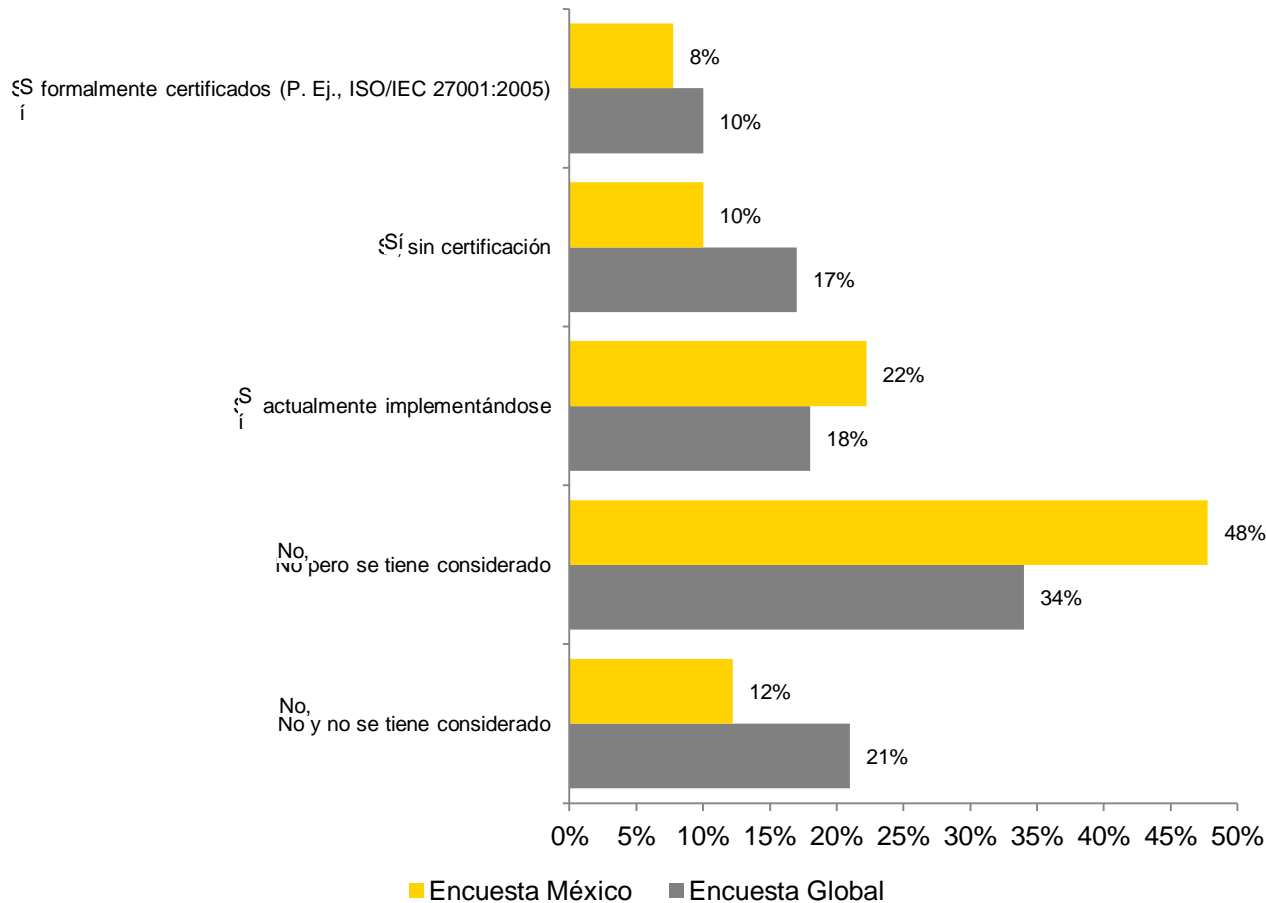


Resultados

Únicamente 28% de las organizaciones ha tomado en cuenta dentro de su estrategia los riesgos derivados del uso de cómputo en nube, dispositivos móviles y redes sociales, 67% aún está investigando o reconoce que debe modificarla.



23. ¿Su organización ha implementado un sistema de gestión de seguridad de la información que contemple la administración general de ésta?



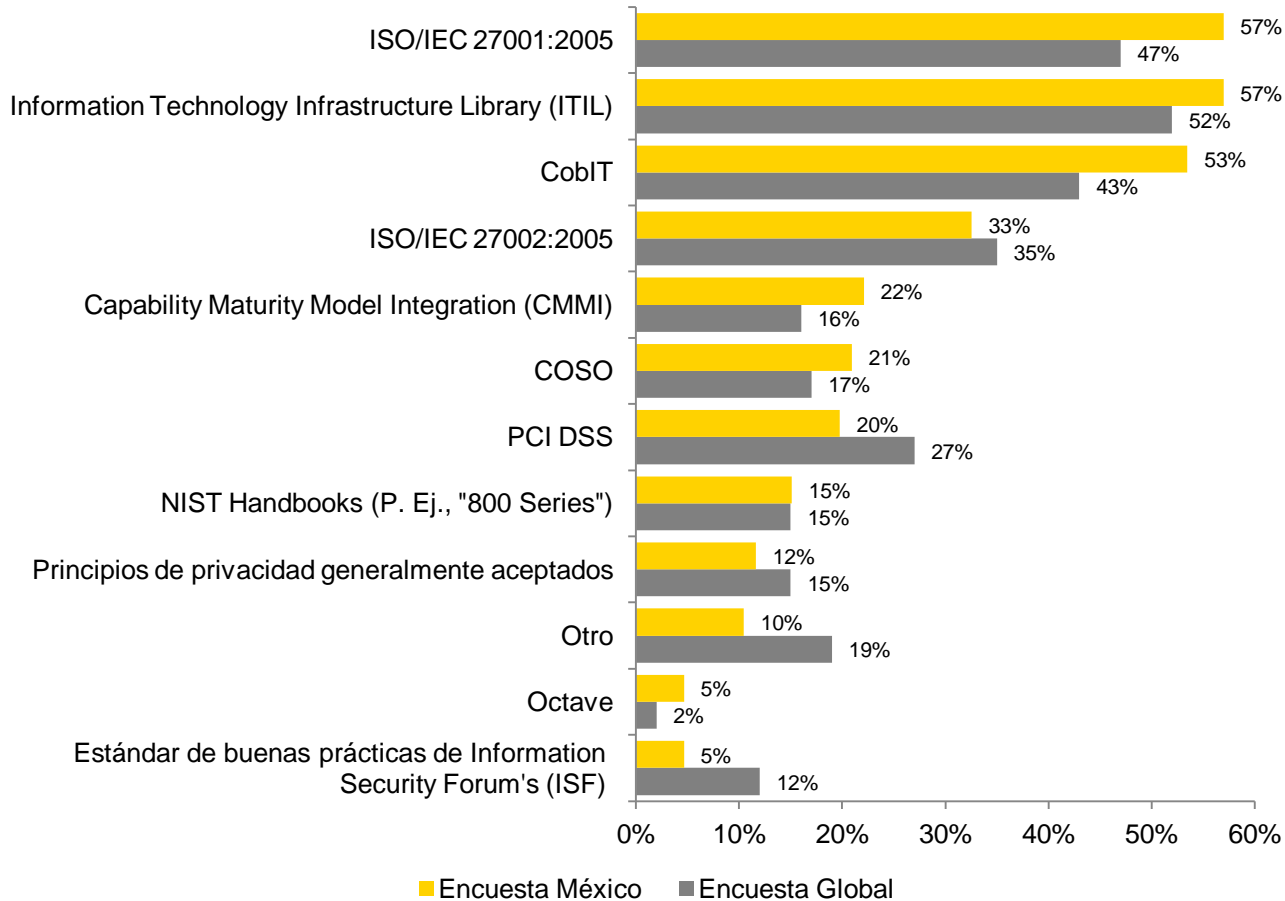
Resultados

Solo 8% de los encuestados cuenta con una certificación formal de un sistema de gestión de seguridad de la información. Se observa una fuerte tendencia del resto de los participantes a implementar y/o certificar su sistema.

Nuestra perspectiva

Aun cuando un sistema de gestión nos ayuda a fundar bases sólidas para la seguridad de la información en la organización, la certificación *per se* no garantiza que seamos seguros, sino el adecuado seguimiento de las políticas y procesos que se definan.

24. De la siguiente lista de estándares o mejores prácticas de seguridad de la información, ¿cuáles está utilizando su organización?



Resultados

Los principales estándares y mejores prácticas utilizados por las organizaciones son ISO/IEC 27001:2005, ITIL y CobIT; más de la mitad de las organizaciones utiliza al menos uno de éstos.

Nuestra perspectiva

Aunque es un avance importante utilizar ITIL y CoBIT sabemos que éstos no son estándares de seguridad, por lo que es necesario implementar adicional a ellos controles específicos de seguridad en la organización. Además es muy importante contar también con políticas de desarrollo seguro para minimizar el riesgo derivado de la fabricación de software para la operación de la organización.

25. ¿Cómo evalúa su organización la calidad y efectividad de la seguridad de la información?



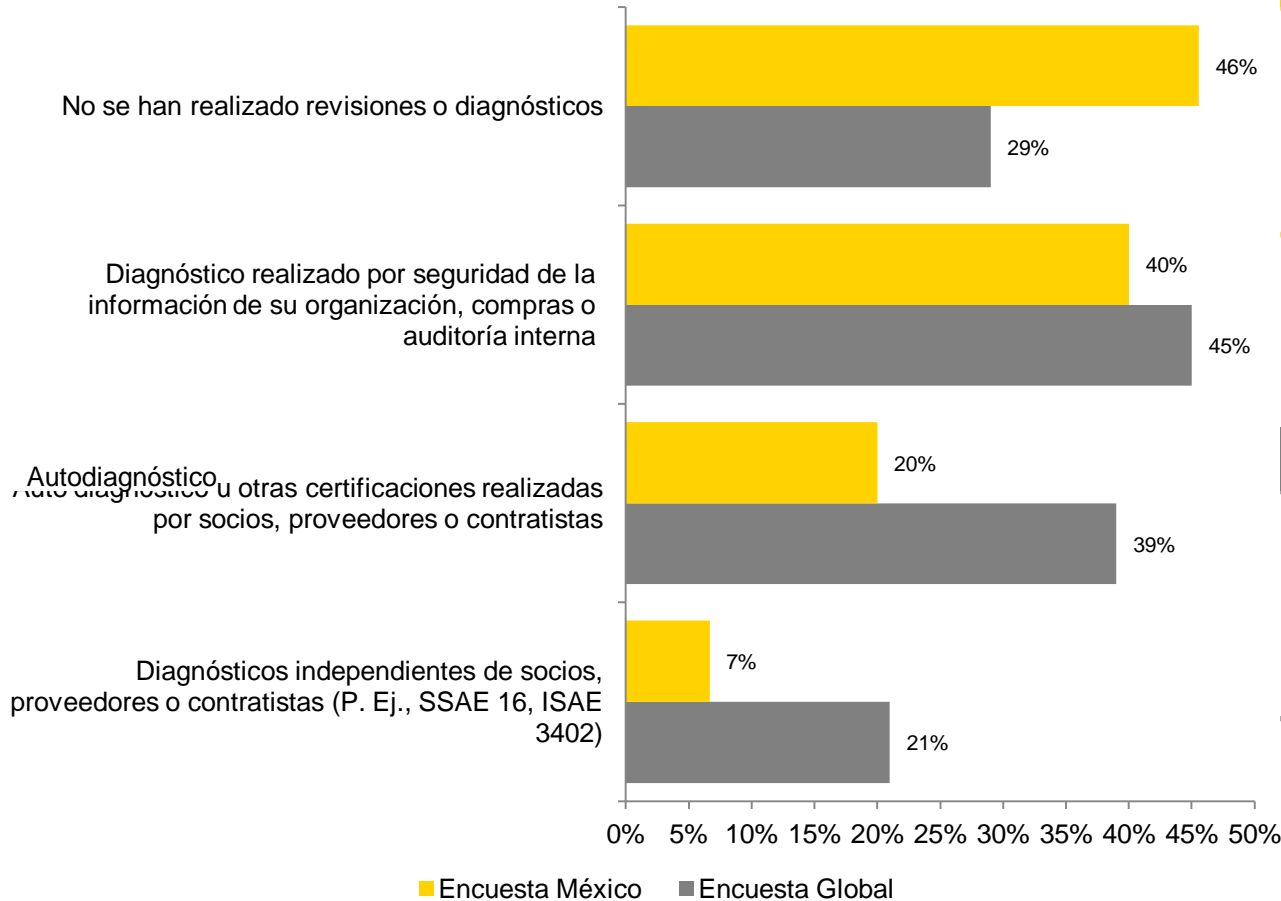
Resultados

Los principales métodos para evaluar la seguridad de la información en las organizaciones son: diagnósticos de auditoría interna, externa y autoevaluaciones de TI o seguridad informática.

Nuestra perspectiva

Las auditorías periódicas deben considerar la atención a riesgos nuevos o escalados como los que hemos discutido. También es importante evaluar el conocimiento que tienen los colaboradores de la organización de las políticas para entender el grado de entendimiento de los esfuerzos de concientización.

26. ¿Cómo se asegura de que sus socios externos, proveedores o contratistas estén protegiendo la información de su organización?



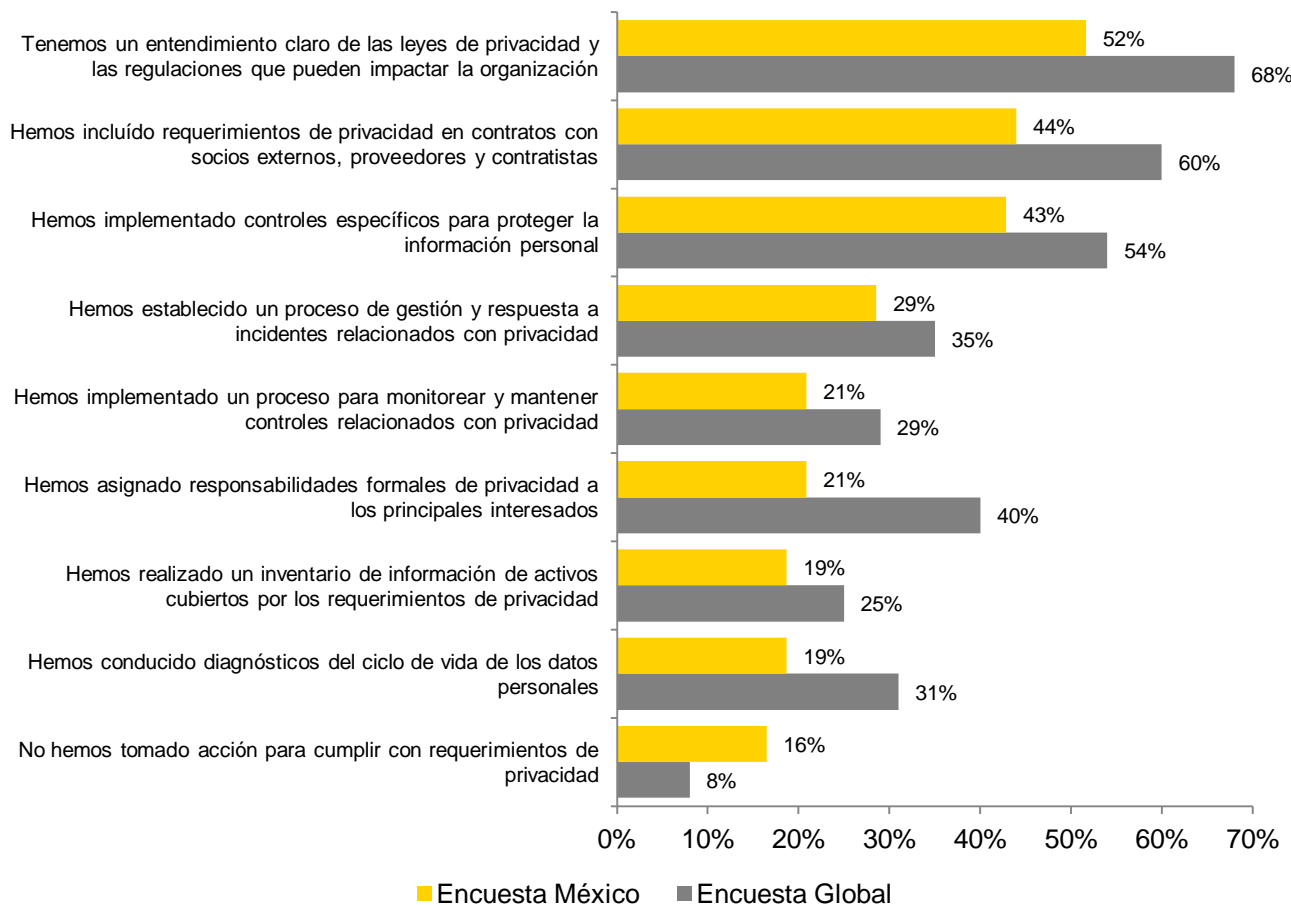
Resultados

Casi la mitad de las organizaciones no evalúa a los terceros que intervienen en la operación. Únicamente 7% utiliza diagnósticos basados en estándares reconocidos.

Nuestra perspectiva

El riesgo de los terceros involucrados en nuestra operación puede resultar transferido a la organización si no se tienen esquemas iguales o mejores de atención a incidentes.

27. ¿Cuál de las siguientes declaraciones puede ser hecha por su organización en relación a la privacidad de datos?



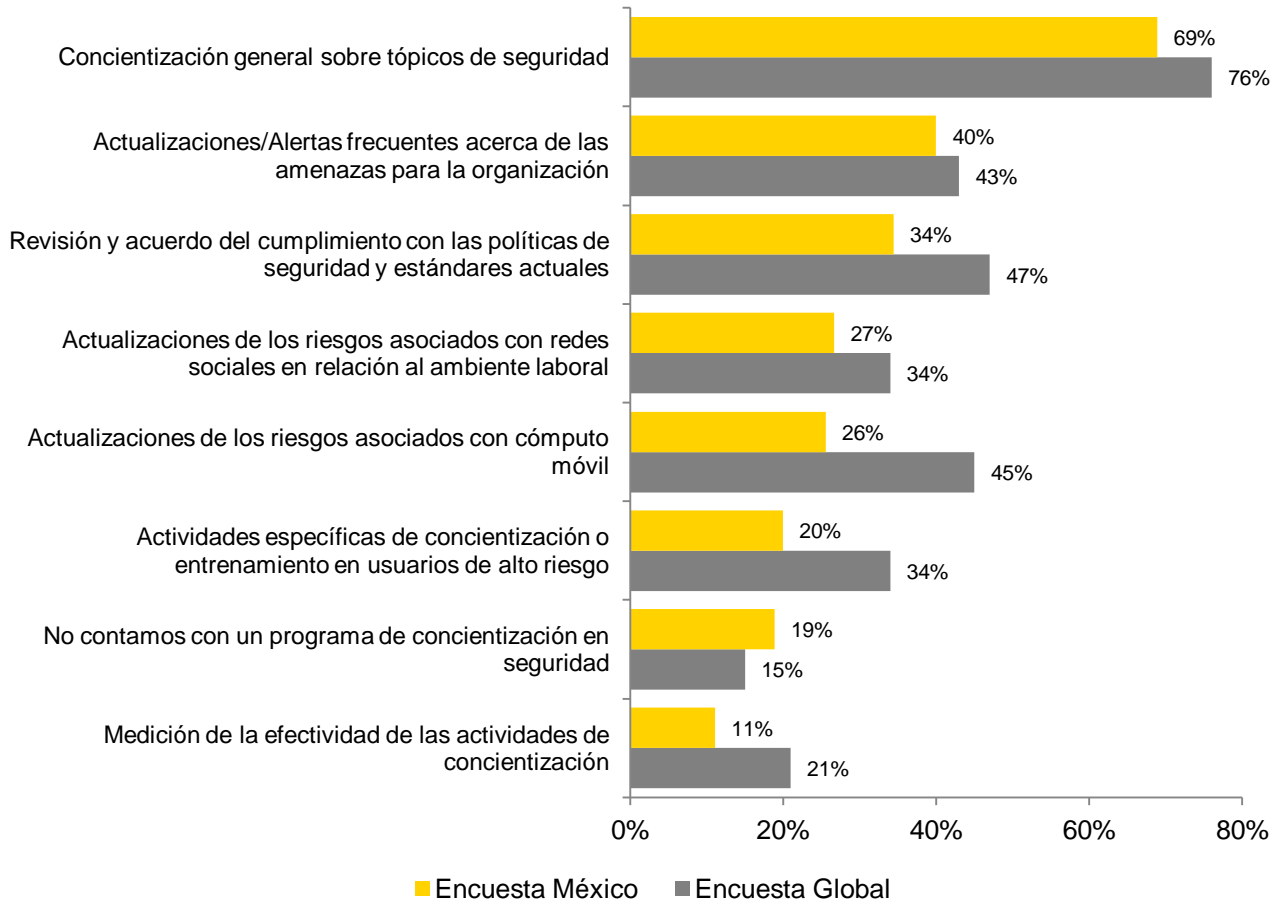
Resultados

Solo la mitad de las organizaciones encuestadas tiene un entendimiento claro de las regulaciones de privacidad de datos y ha tomado medidas al respecto.

Nuestra perspectiva

La entrada en vigor de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares marcará la primera vez para muchas organizaciones en que estarán sujetas a esquemas de cumplimiento regulatorio. Es necesario entender las implicaciones de esto en nuestra operación y las relaciones que mantenemos con terceros.

28. ¿Qué elementos están cubiertos actualmente en el programa de concientización de su organización?



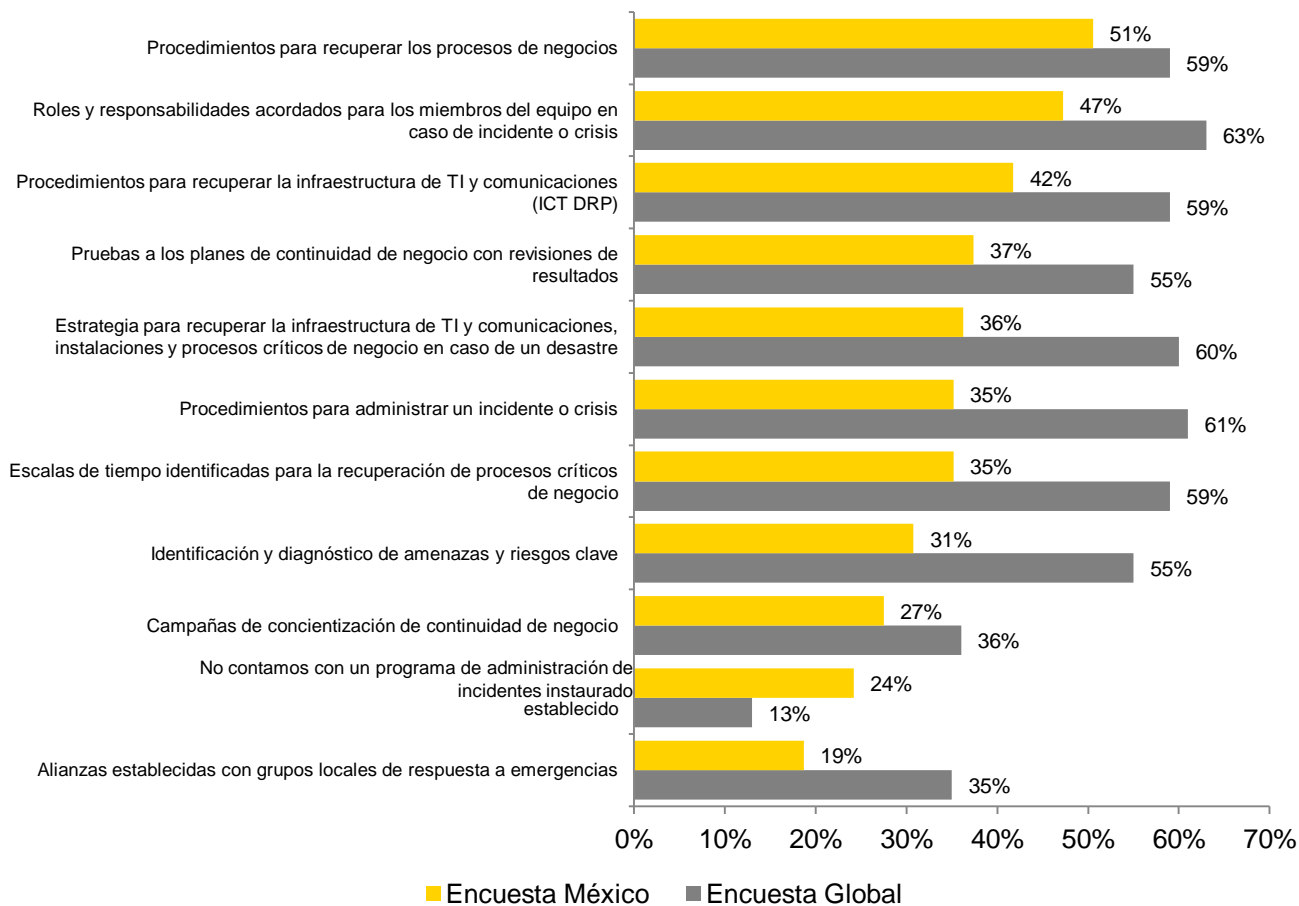
Resultados

Las principales actividades de concientización se centran en tópicos de seguridad (69%), alertas frecuentes de amenazas (40%) y revisión de las políticas y estándares (34%). El 20% de las organizaciones de nuestro país no cuenta con un programa de concientización.

Nuestra perspectiva

Es necesario mantener este tipo de programas para convertir a los colaboradores de la organización en la primera línea de defensa de la misma.

29. ¿Cuál de los siguientes elementos está incluido en el programa de continuidad de negocio de su organización?



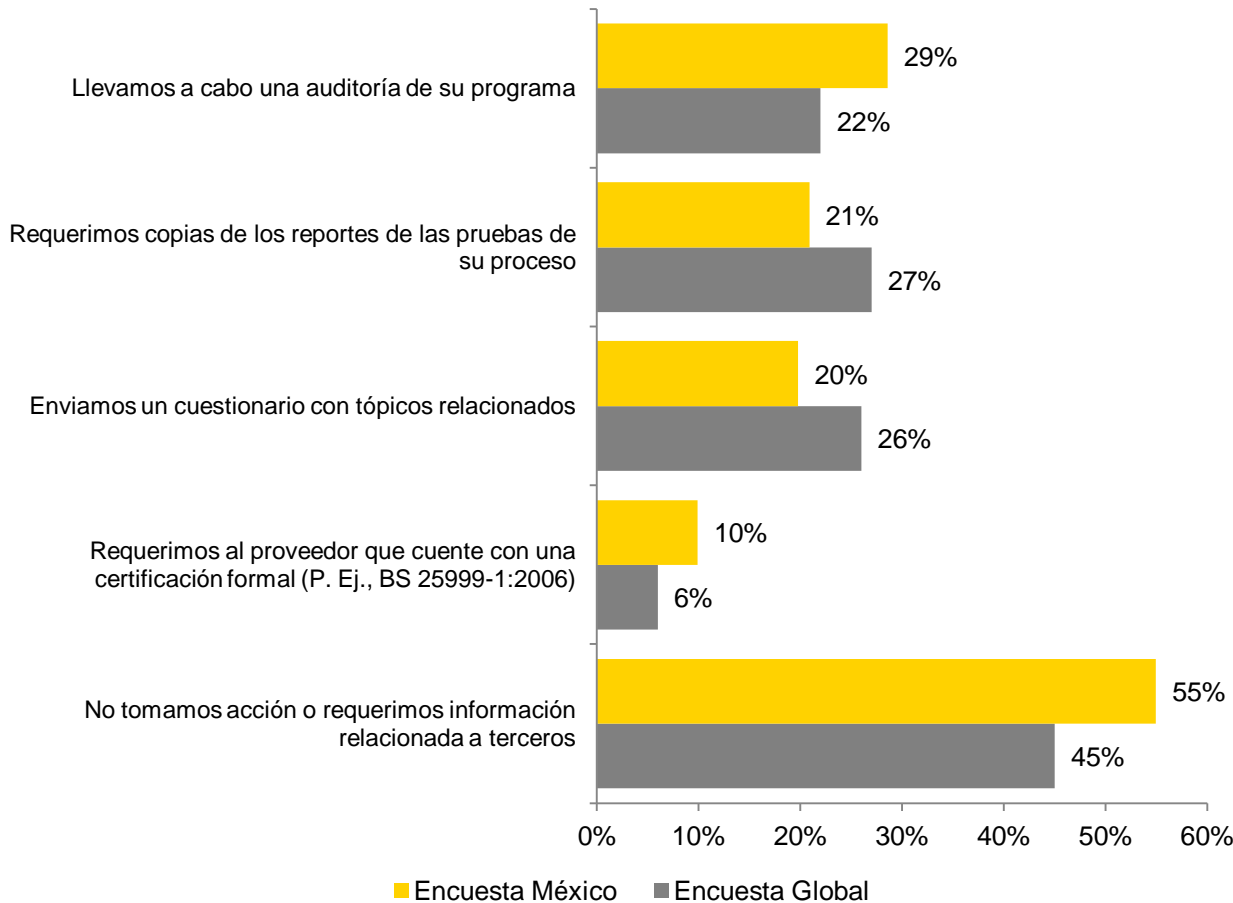
Resultados

Una de cada cuatro organizaciones no cuenta con un programa de administración de incidentes.

Nuestra perspectiva

Existen múltiples estudios que demuestran que un incidente que ponga en riesgo la continuidad de negocio por un periodo prolongado puede poner en peligro su viabilidad. Es necesario que no tomemos a la ligera el tema y reforzemos los programas ya establecidos.

30. ¿Cómo evalúa la capacidad de administración de continuidad de negocio de terceros?



Resultados

La mitad de los encuestados no requiere que los terceros que intervienen en su operación cuenten con programas de continuidad de negocio.

Nuestra perspectiva

Existen reportes que pueden ser exigidos a su proveedor de servicios que evalúen su postura de continuidad de negocio, que le brinden certeza de la elección que está realizando y le eviten adquirir riesgos innecesarios. Es ineludible exigir a los terceros involucrados en la operación que cuenten con sus propios programas de continuidad.

The background of the slide is a dense, repeating pattern of question marks. The question marks are rendered in a stylized, hand-drawn or sketch-like font, with varying sizes and orientations, creating a sense of movement and inquiry. A solid yellow horizontal bar is positioned in the upper right quadrant, containing the word 'Preguntas' in a bold, black, sans-serif font.

Preguntas

Ernst & Young

Aseguramiento | Asesoría | Fiscal | Legal | Transacciones

Acerca de Ernst & Young

Ernst & Young es un líder global en aseguramiento, asesoría de negocios, servicios fiscales, legales y transaccionales. A nivel global, nuestros 141,000 profesionales están unidos por los mismos valores y un compromiso sólido con la calidad. Marcamos la diferencia al ayudar a nuestra gente, clientes y comunidades a lograr su potencial.

Para mayor información por favor visite www.ey.com/mx

© 2011 Mancera, S.C.

Integrante Ernst & Young Global

Derechos reservados

Ernst & Young se refiere a la organización global de firmas miembro conocida como Ernst & Young Global Limited, en la que cada una de ellas actúa como una entidad legal separada. Ernst & Young Global Limited no provee servicios a clientes.

NUESTRAS OFICINAS	CLAVE	TELÉFONO	NUESTRAS OFICINAS	CLAVE	TELÉFONO
AGUASCALIENTES	449	912-82-01	MEXICALI	686	568-45-53
CANCÚN	998	884-98-75	MÉXICO, D.F.	55	5283-13-00
CHIHUAHUA	614	425-35-70	MONTERREY	81	8152-18-00
CIUDAD JUÁREZ	656	648-16-10	NAVOJOA	642	422-70-77
CIUDAD OBREGÓN	644	413-32-30	PUEBLA	222	237-99-22
CULIACÁN	667	714-90-88	QUERÉTARO	442	216-64-29
GUADALAJARA	33	3884-61-00	REYNOSA	899	929-57-07
HERMOSILLO	662	260-83-60	SAN LUIS POTOSÍ	444	825-72-75
LEÓN	477	717-70-62	TIJUANA	664	681-78-44
LOS MOCHIS	668	818-40-33	TORREÓN	871	713-89-01
MÉRIDA	999	926-14-50	VERACRUZ	229	922-57-55

