Deloitte.

Ciberseguridad

Encuesta 2018 sobre Tendencias de Cyber Riesgos y Seguridad de la Información en Ecuador

Octubre 2018

Índice

Introducción

La evolución de la gestión de Cyber Riesgos y Seguridad de la Información

Deloitte se complace en presentar los resultados del **Estudio 2018 sobre Tendencias en Gestión de Ciber Riesgos y Seguridad de la Información en Ecuador**.

Las organizaciones en Ecuador se encuentran inmersas en un contexto de fuerte desarrollo de negocios digitales y de mayor exposición a las ciber amenazas inherentes a este nuevo contexto de negocios.

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.

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 Ciberseguridad en Ecuador.

Las organizaciones analizadas incluyen los aspectos clave que hacen a la gestión de ciberseguridad.

84 Organizaciones participantes

5 Industrias

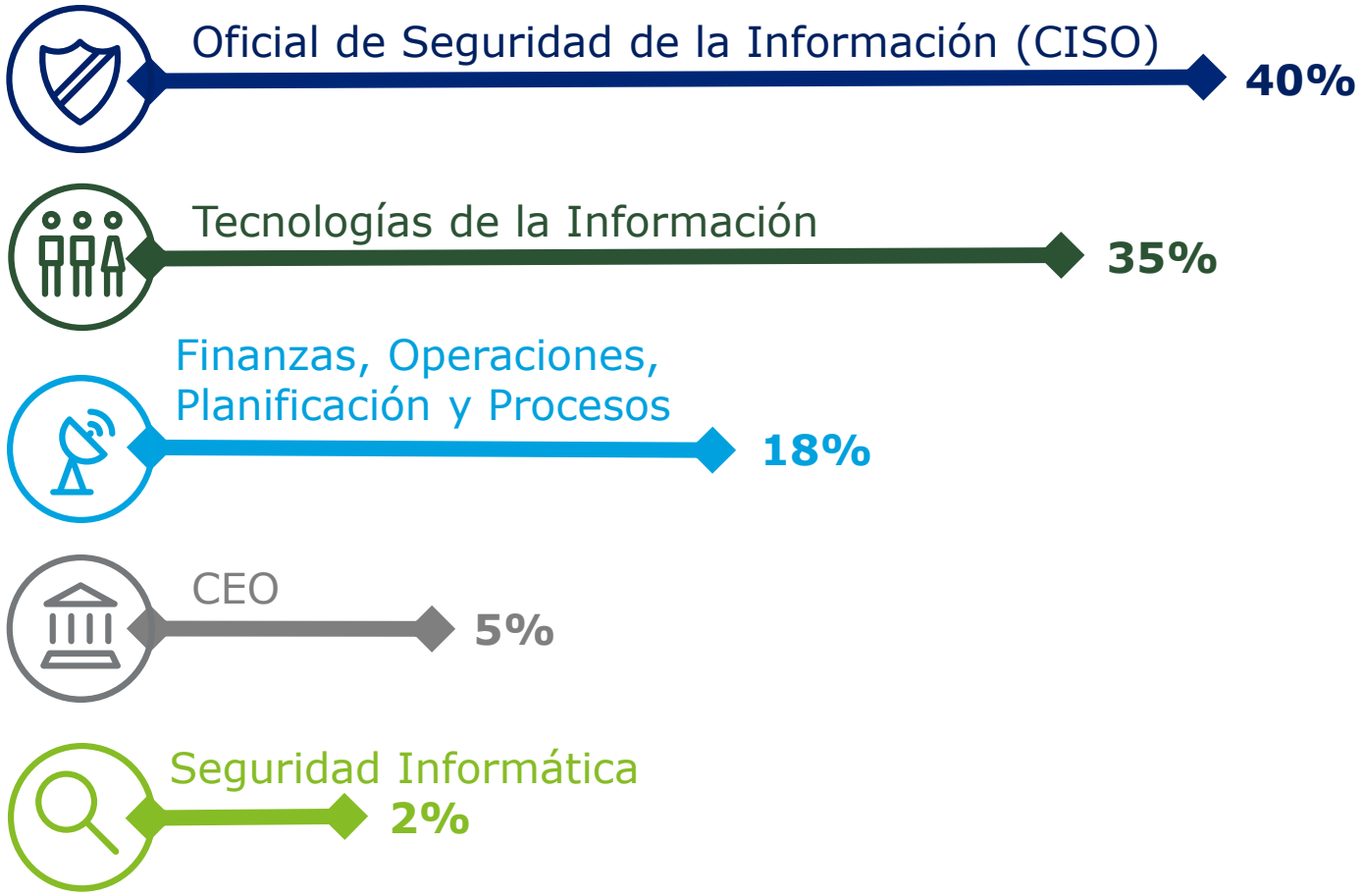
Información general sobre el Estudio

Detalle de industrias y sectores participantes

- Sector Público | **39%**
- Financiero | **27%**
- Consumo | **24%**
- Telecom | **6%**
- Energía | **4%**

Información general sobre el Estudio

Perfil del ejecutivo entrevistado



Información general sobre el Estudio

Proceso de recopilación de la información

Periodo de ejecución

Referencias

Indica la perspectiva de Deloitte

Principales tendencias identificadas

Principales tendencias identificadas

4 de cada 10 organizaciones sufrieron un incidente de seguridad en los últimos 24 meses.

El 70% de las organizaciones afirma no tener certeza de la efectividad de su proceso de respuesta ante incidentes de ciberseguridad.

Perspectiva de Deloitte

D

A pesar de contar con más presupuesto, la tendencia de ciber-ataques se mantiene; por lo cual las empresas deben enfocar sus esfuerzos en actividades de monitoreo que permiten adelantarse o responder de forma más ágil ante un inminente ataque.

A pesar de afirmar que el presupuesto se incrementará para 2019, se mantiene la tendencia de que la principal barrera que enfrentan los CISOs continua siendo la falta de presupuesto y/o de recursos suficientes

Perspectiva de Deloitte

D

Con el incremento de las ciber-amenazas, así como de los requerimientos de negocio, las empresas aún encuentra en el presupuesto su principal obstáculo en la gestión de la ciberseguridad dentro de sus organizaciones.

Principales tendencias identificadas

Apenas 1 de cada de 10 organizaciones cuenta con una estructura de gobierno de seguridad para brindar recursos y administrar las iniciativas de ciberseguridad.

Perspectiva de Deloitte

Contar con un gobierno de seguridad de información constituye un desafío que las organizaciones no han podido resolver aún; los beneficios de contar con el mismo son la alineación estratégica y la retroalimentación con respecto a las iniciativas en ejecución y por iniciar.

5 de cada 10 organizaciones han implementado un programa de concientización en ciberseguridad de los empleados.

Perspectiva de Deloitte

Los procesos y la tecnología constituyen dos pilares fundamentales de la gestión de seguridad de información; pero las personas continúan siendo el eslabón más débil en la cadena de protección de la información empresarial.

Principales tendencias identificadas

Evolución de la gestión de Ciberseguridad

D La función de Gestión de Ciberseguridad está evolucionando hacia un nuevo paradigma que incluye tres componentes centrales y estratégicos: Asegurar, Monitorear y Responder:

Seguro

Se enfoca en la protección de la información que soporta los procesos clave del negocio, implementando controles adecuados para el mismo.

Vigilante

Busca 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 detectar o predecir un ataque a la información.

Resiliente

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

SEGURO

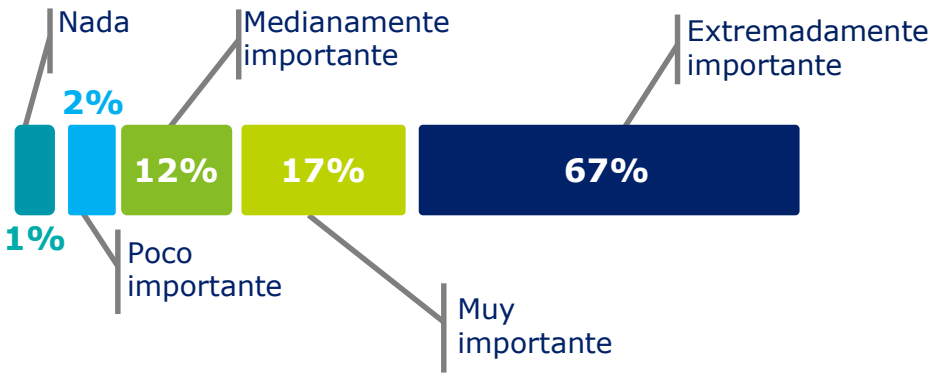
Protección de la Información

Seguro

Vigilante

Resiliente

Importancia de la ciberseguridad en las organizaciones

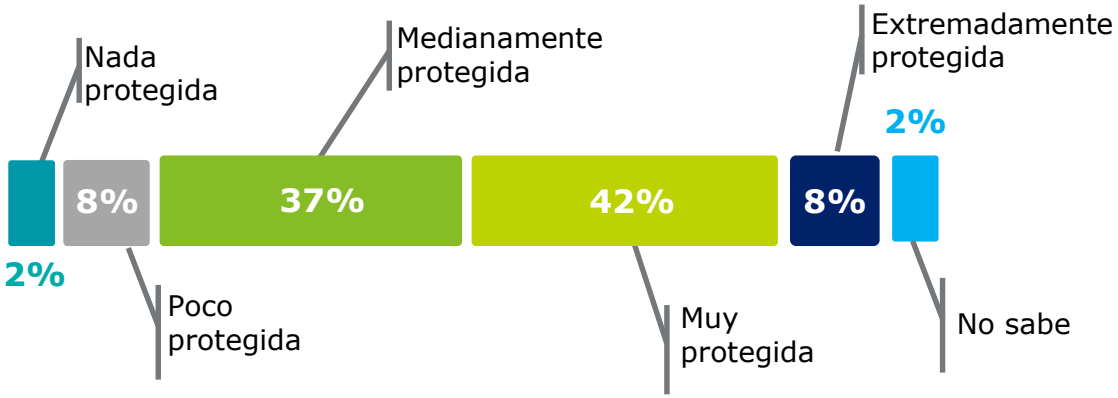


D

Si bien existen industrias donde la regulación o el beneficio que buscan los ciber delincuentes presiona para invertir en seguridad, es notable que un motivo importante sea la reducción del riesgo.

Consecuentemente, tener cuantificados los riesgos y medir su evolución es un requisito clave para una buena gestión.

Nivel de protección - en ciberseguridad - de las organizaciones

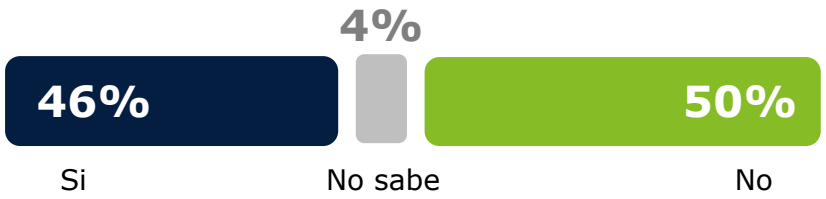


D

Con el pasar de los años, vemos que las organizaciones incrementan su interés y por ende la inversión en ciberseguridad, esto se ve reflejada en la cantidad y calidad de mecanismos de protección de la información en cada una de ellas.

Sin embargo, paralelamente se incrementa también la sofisticación de los ataques, dando como resultado que las organizaciones deban incluir en sus estrategias la velocidad a la cual incrementan el nivel de protección en comparación con la cantidad y capacidad de los ataques.

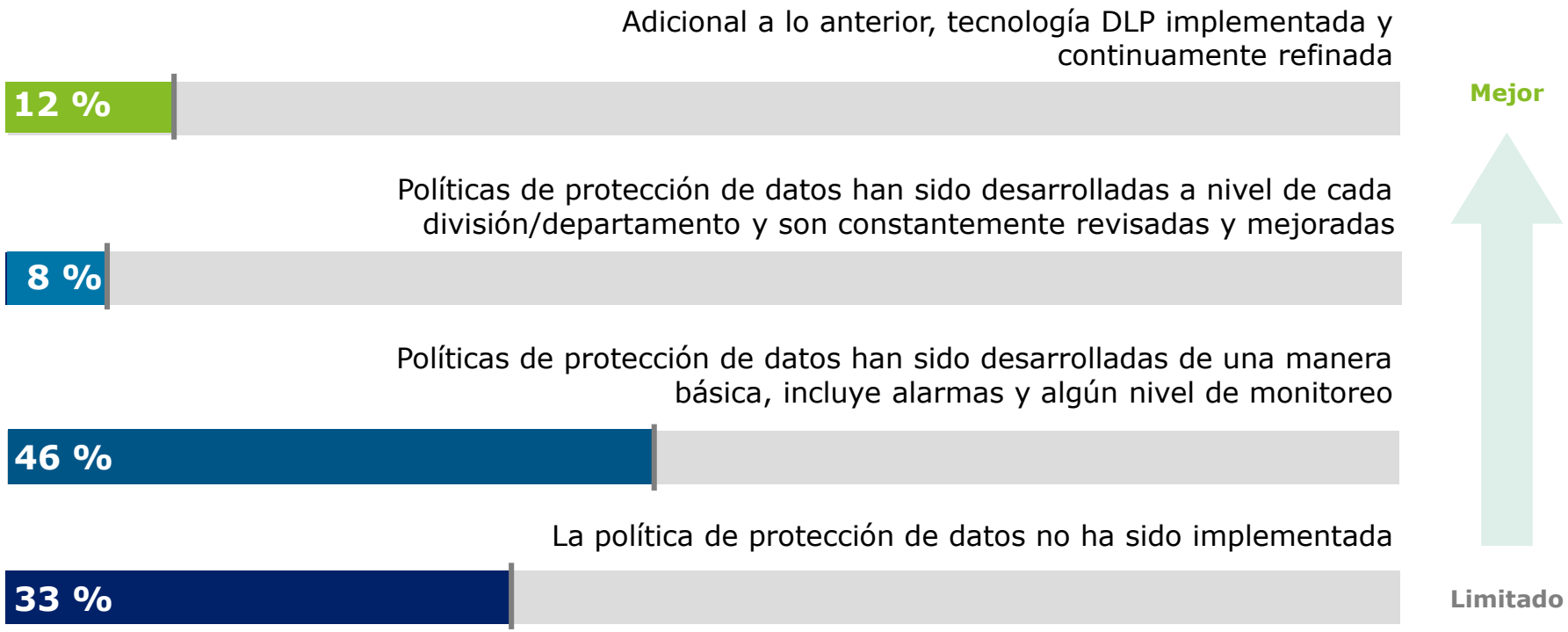
Organizaciones que cuentan con terceros que les proveen servicios administrados de seguridad



D

Transferir los riesgos, simplifica la labor de mitigación y permite enfocar esfuerzos en la organización, sin embargo el riesgo sigue siendo propiedad de la organización, no del tercero, por lo que se debe contar con una adecuada gestión de los servicios provistos.

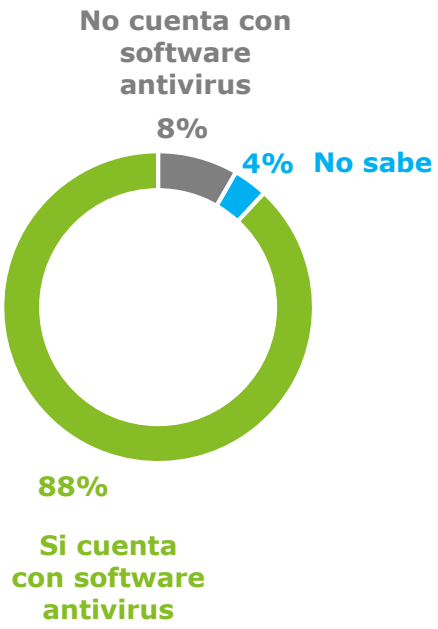
Actividades realizadas por las organizaciones para prevención de pérdida de información

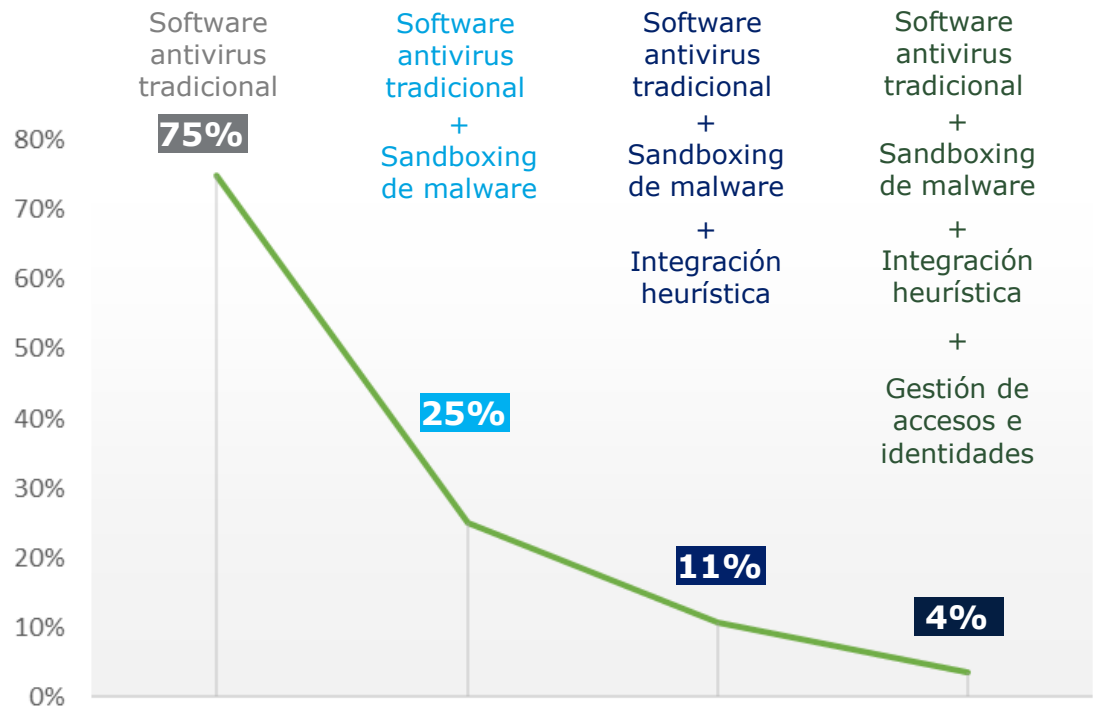


D

Proteger los datos generados como parte de la operación del negocio debe ser una prioridad fundamental a seguir en cada organización, esto se debe a que en los datos radica el futuro de la organización, que debidamente explotada –por la propia organización o por la competencia- puede resultar en el crecimiento o extinción de la organización.

Capacidades tecnológicas de detección y protección de malware implementadas

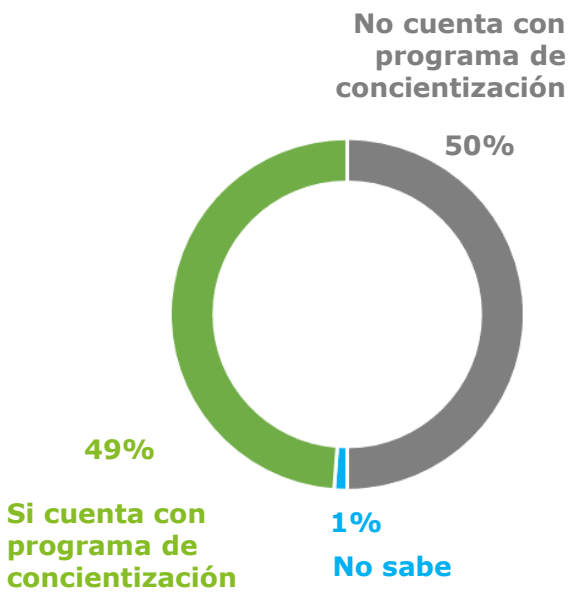


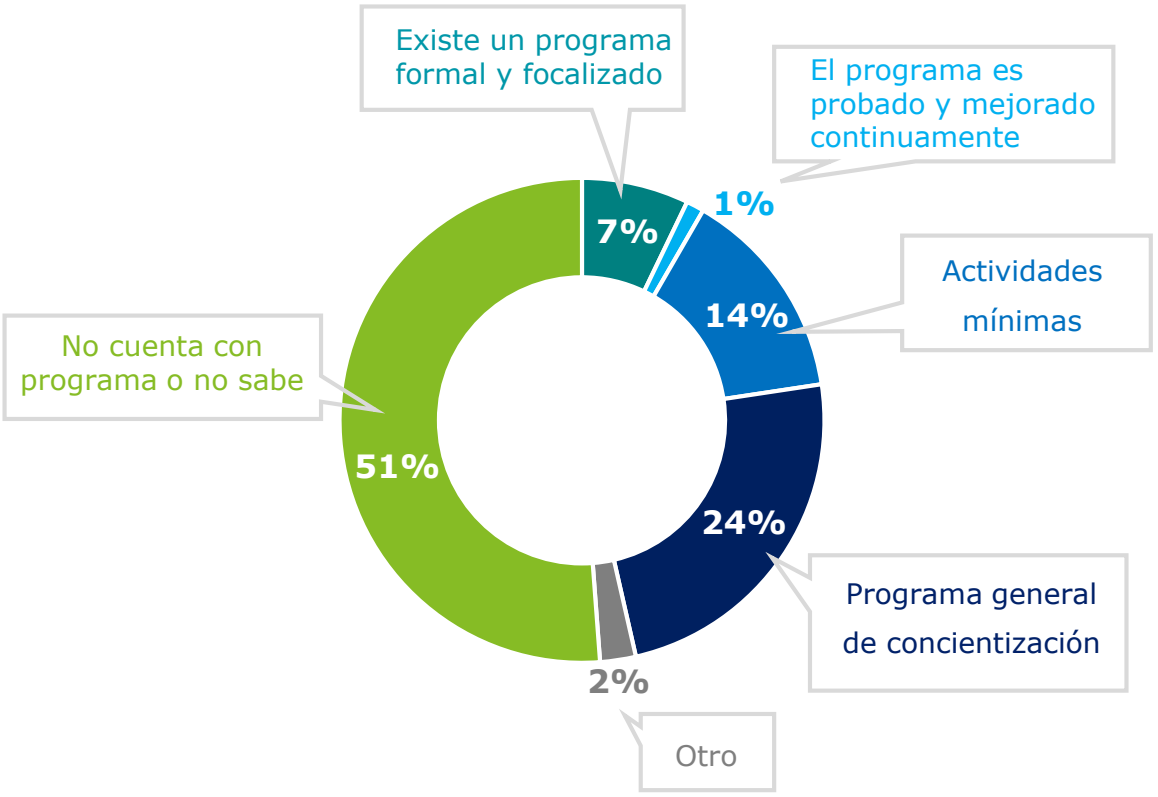


D

La mayoría de las organizaciones aprovechan los beneficios de contar con una herramienta tecnológica para la gestión automática de malware. Por otro lado, hacer frente a los ataques que se van sofisticando con el paso del tiempo, requiere que las organizaciones evolucionen en el mismo sentido, mejorando las capacidades de malware avanzado, análisis heurístico de malware y su integración con los accesos e identidades de los colaboradores.

Programa de concientización sobre amenazas específicas de ciberseguridad



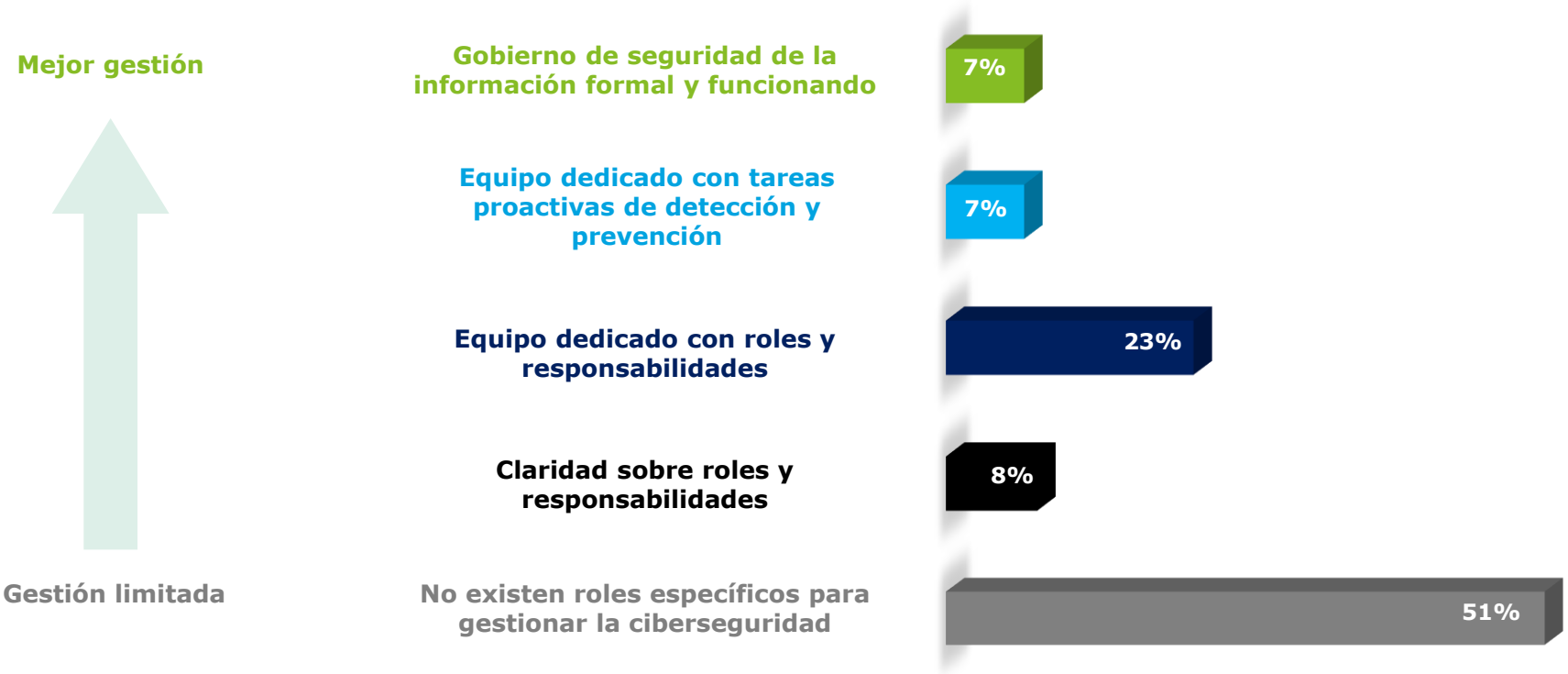


D

El factor humano sigue siendo un factor de vital importancia para la seguridad de la información. Su importancia radica en que resulta una alternativa de entrada a las organizaciones y mediante la cual muchos controles tecnológicos pueden ser burlados.

Concientizarlos sobre la importancia de su rol y su compromiso para con la información seguirá siendo la mejor medida para evitar ser vulnerados, hasta ahora.

Gestión de recursos y conjunto de habilidades asociados a ciberseguridad



D

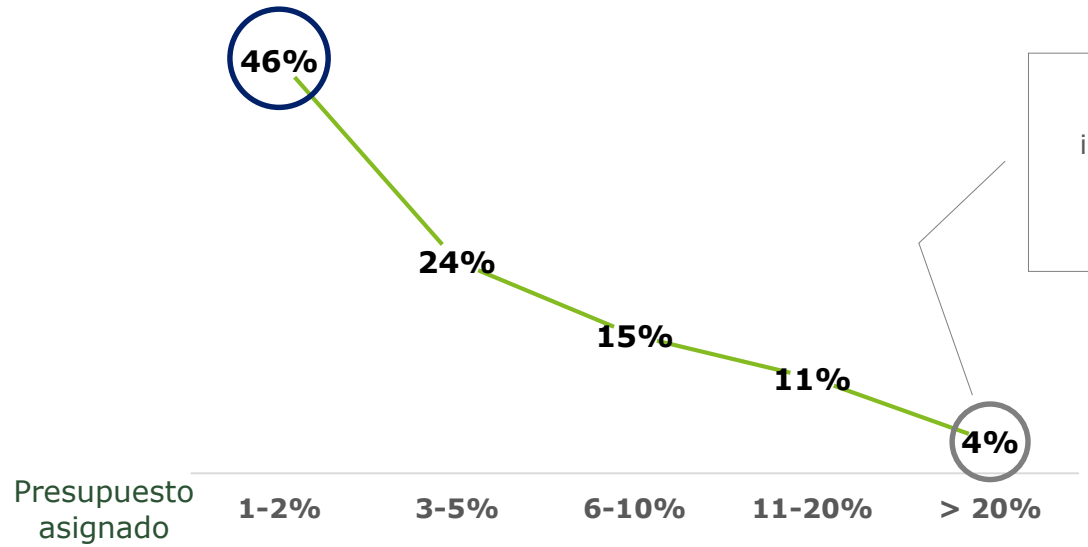
Definitivamente una mejor y más especializada administración de la ciberseguridad habilitará a las organizaciones para tomar decisiones más efectivas y con visión de futuro en el corto, mediano y largo plazo.

La formalización de una estructura de gobierno de seguridad de la información debe contar con los integrantes capaces de tomar decisiones efectivas.

Porcentaje del presupuesto de TI asignado a ciberseguridad

Del 1 al 2% es el presupuesto que la mayoría de las organizaciones asigna a ciberseguridad

Muy pocas organizaciones invierten más del 20% de su presupuesto en ciberseguridad



D

Contar con un presupuesto propio, es un paso fundamental para el crecimiento y madurez de la función de cyber riesgos y seguridad de la información.

El presupuesto debe estar en línea con el apetito de riesgo de la organización.

VIGILANTE

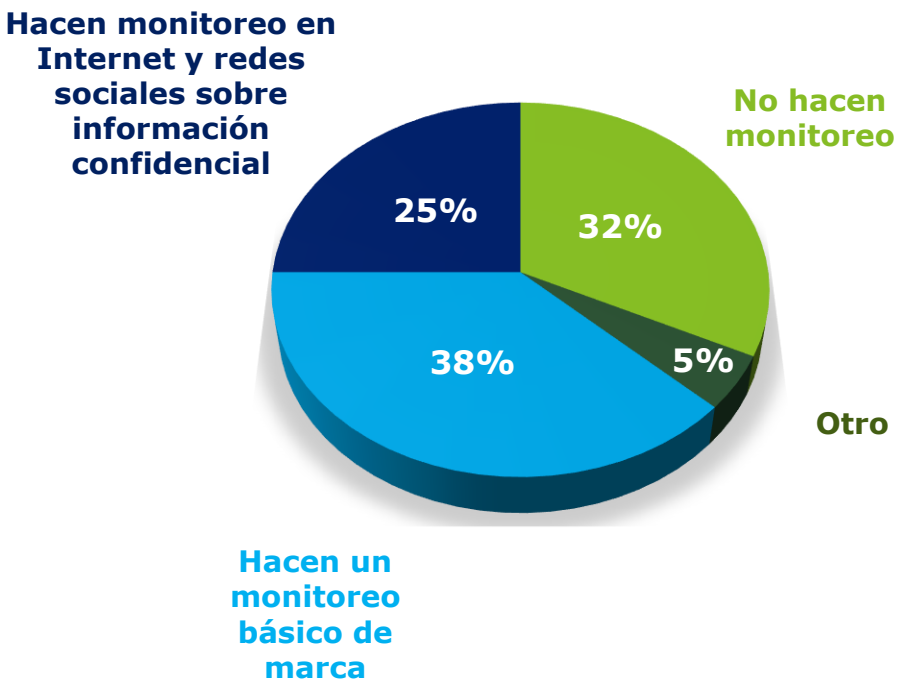
Monitoreo proactivo de amenazas y eventos

Seguro

Vigilante

Resiliente

Monitoreo de información disponible públicamente sobre la marca, su personal, aplicaciones y tecnologías que podrían ser usados en potenciales ataques.

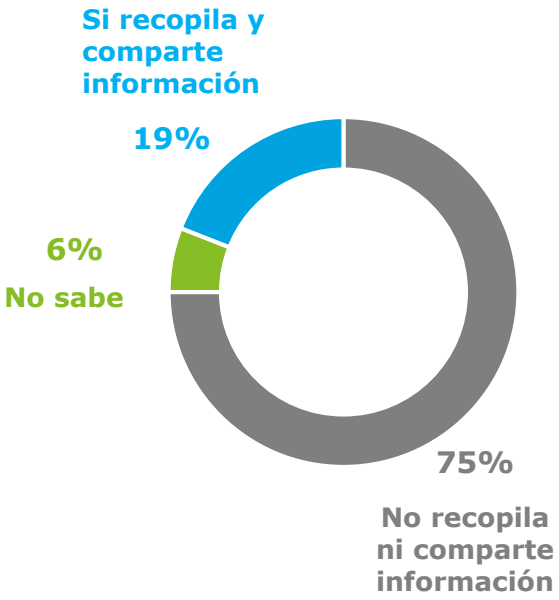


D

El monitoreo de eventos clave de seguridad constituye la base operacional para una adecuada gestión de riesgos y seguridad de la información.

En Ecuador se observa un grado de desarrollo bajo de estas capacidades, casi siempre limitadas a responder reactivamente a lo evidente.

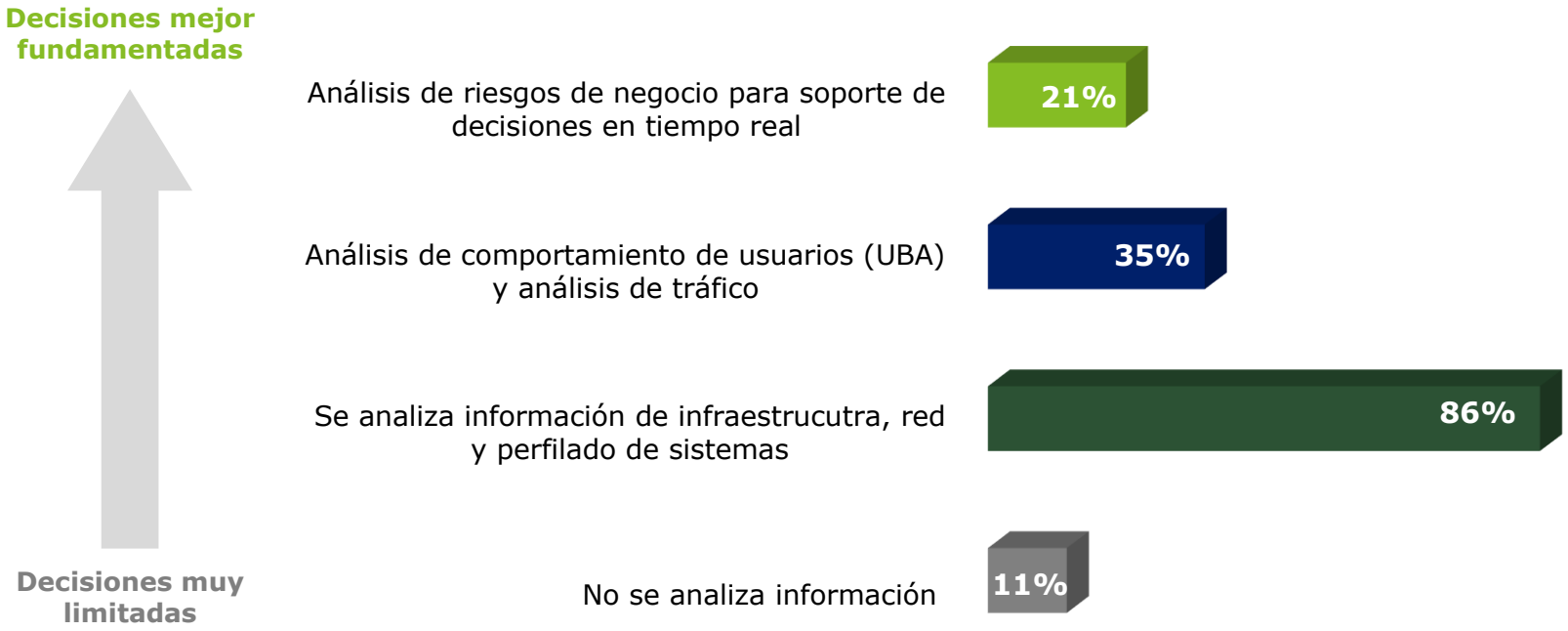
Inteligencia de amenazas



En un ambiente de constante cambio tecnológico y donde el modelo de operación es usualmente 24/7, contar con información actualizada de la situación de riesgos de seguridad resulta una competencia clave a desarrollar por las organizaciones.

En Ecuador aún hay mucho trabajo por recorrer para recolectar, almacenar y compartir información para un análisis de inteligencia de las amenazas existentes.

Análisis de información (Logs de operación)



D

La automatización de los procesos y el empleo de tecnología genera registros de su operación que proporcionan una valiosa fuente de información para re-orientar apropiadamente los esfuerzos de proteger la información de la organización.

Las organizaciones deben recopilar estos registros, analizar tendencias y anomalías y utilizar los resultados para tomar decisiones mejor sustentadas.

Gestión de riesgos de ciberseguridad

Los cambios en configuraciones conllevan a actualizaciones automáticas en el programa de gestión de vulnerabilidades

11%

Existe integración consistente entre el área de seguridad y gestión de riesgos

18%

Existen métricas de ciber riesgos en algunas unidades de negocio especificas definidos y monitoreados

16%

Indicadores clave de ciber riesgos están definidos y son monitoreados

14%

No se ejecutan actividades específicas

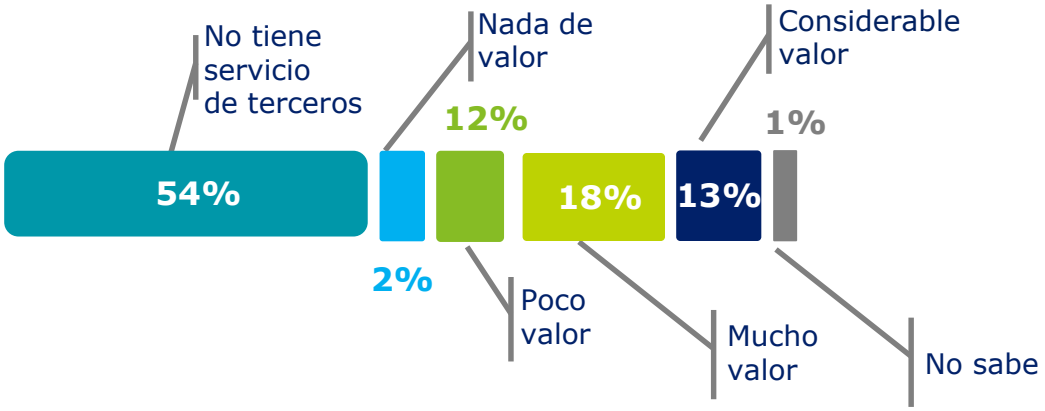
60%

D

Definitivamente la gestión de riesgos ha sido una base ampliamente probada y ha demostrado ser la mejor aproximación para proteger la información de la organización e implementar controles para reducir el impacto negativo.

Controlar el impacto en la operación, imagen, finanzas y regulatorio, puede obtenerse a través de la gestión de riesgos de ciberseguridad.

Desde la perspectiva de las organizaciones, valor que consideran que agrega un tercero con respecto a la protección de su información

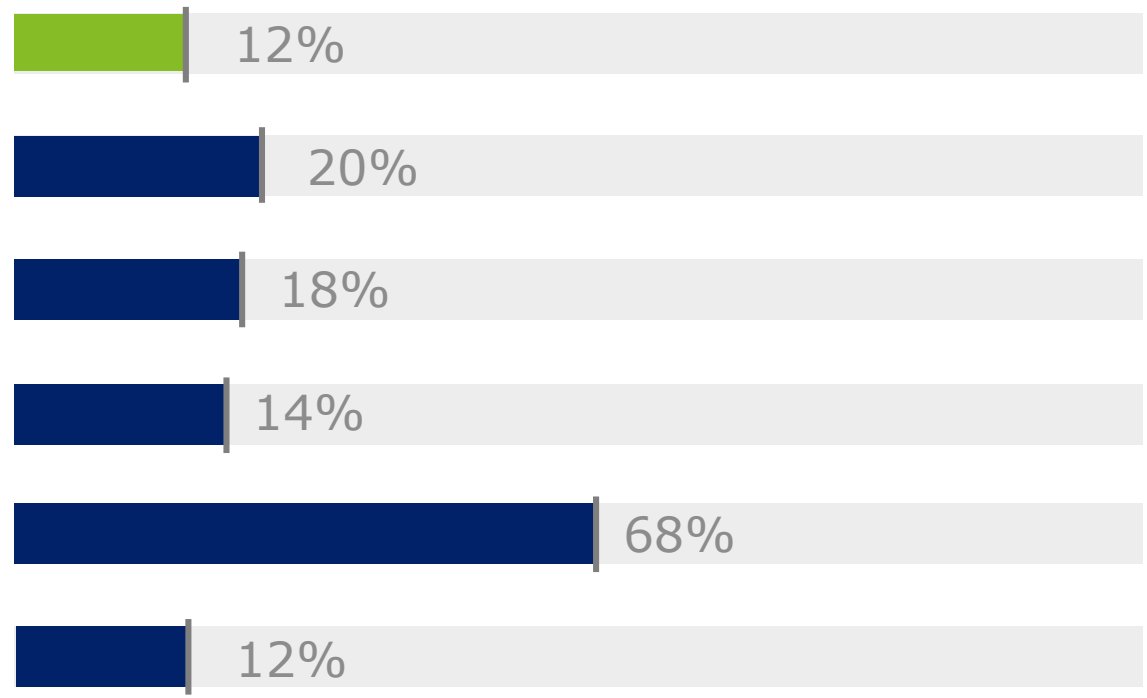


D

Medir el desempeño del servicio provisto por el tercero, en comparación con la meta esperada, permite a las organizaciones valorar al tercero y brinda confianza de que la información está siendo efectivamente protegida.

Adicionalmente, evaluar a los terceros permitirá una certera toma de decisiones respecto a las capacidades del mismo para incrementar el nivel protección según la evolución de los riesgos.

Gestión de los servicios de ciberseguridad ejecutados por un tercero



Procesos de respuesta a incidentes de seguridad son probados con el tercero

Existen procesos para notificar oportunamente incidentes de seguridad por los terceros

Se realiza una revisión periódica de los terceros

Riesgos específicos de ciberseguridad son considerados y evaluados durante la contratación de terceros

Los contratos incluyen cláusulas de confidencialidad de la información

No hay terceros involucrados

D

Proteger la información sigue siendo responsabilidad de la organización aún cuando se decida transferir el riesgo, debido a que el impacto recae finalmente sobre la organización.

En este contexto, las organizaciones deben considerar, además del aspecto legal común de contratar a un tercero, la capacidad tecnológica para hacer frente a riesgos emergentes y mecanismos administrativos como el derecho de auditarlos y su permanente compromiso para comprobar su capacidad de respuesta ante un inminente o materializado incidente de seguridad de la información.

RESILIENTE

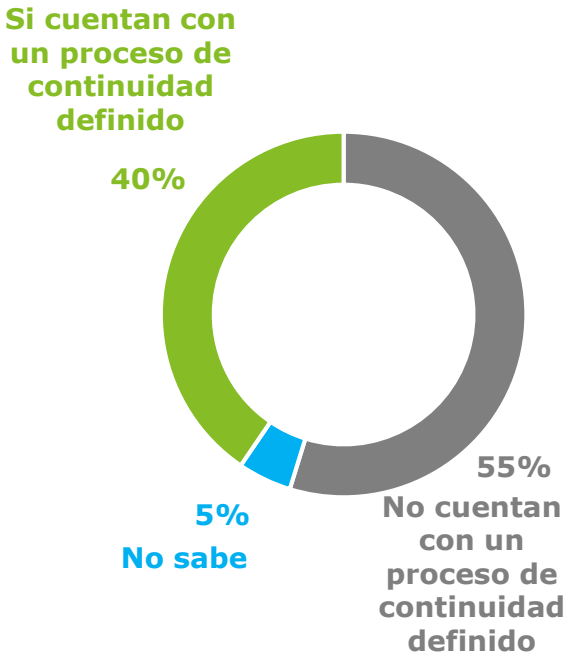
Respuesta rápida ante una disrupción del negocio

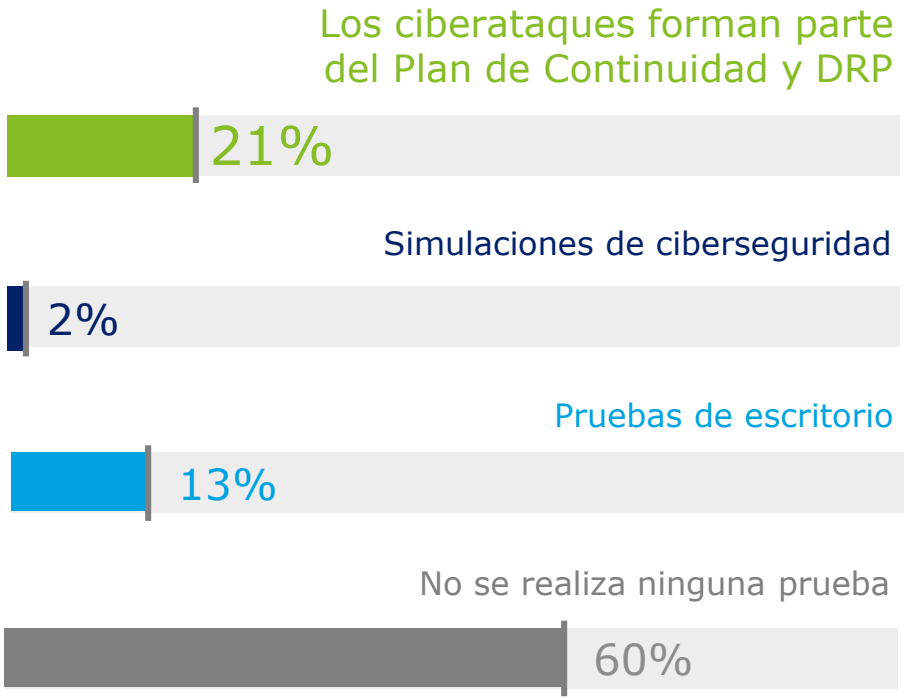
Seguro

Vigilante

Resiliente

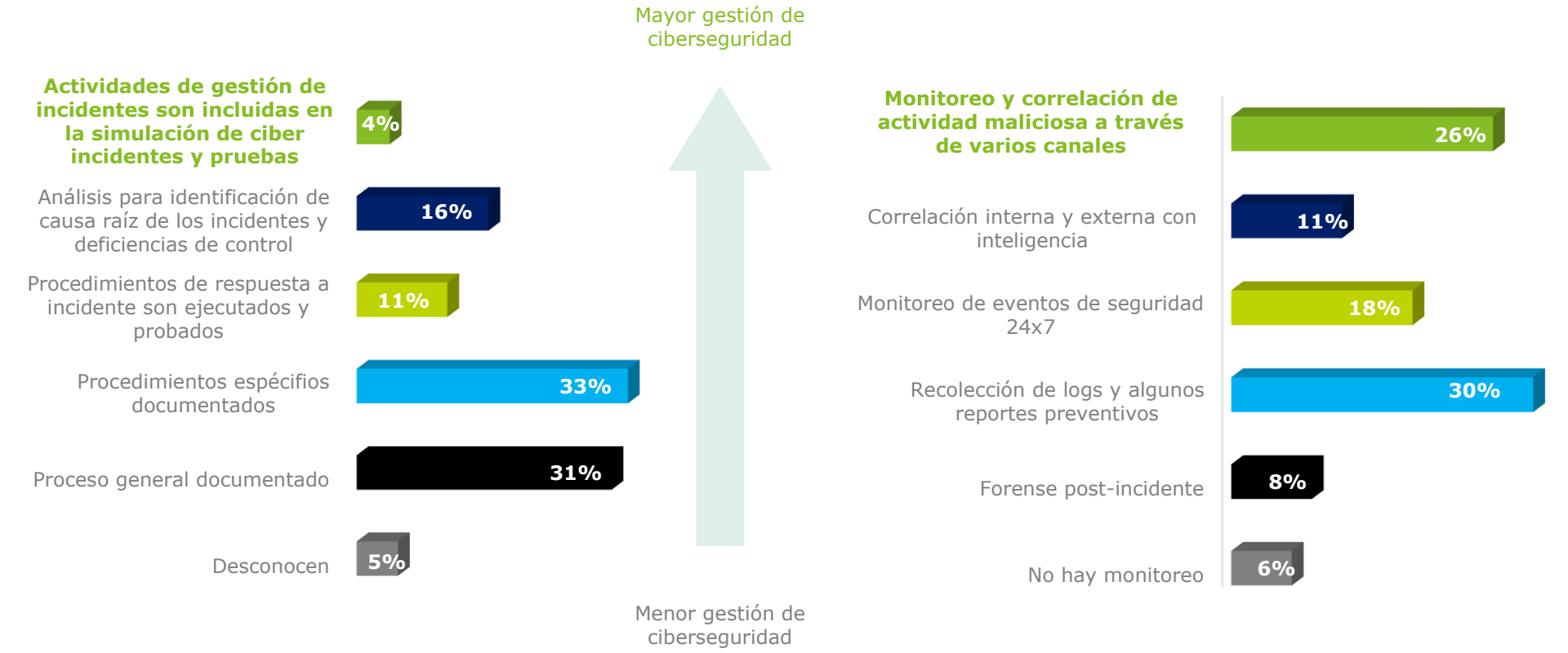
Continuidad de las operaciones





Es evidente que aún falta un gran esfuerzo en las organizaciones para tomar mayores medidas preventivas ante situaciones que comprometan la continuidad operativa. Un pilar importante para concientizarse es, iniciar con un estudio de impacto al negocio (BIA por sus siglas en inglés), el cuál brindará la información necesaria para gestionar los riesgos de no contar con un Plan de Continuidad del Negocio.

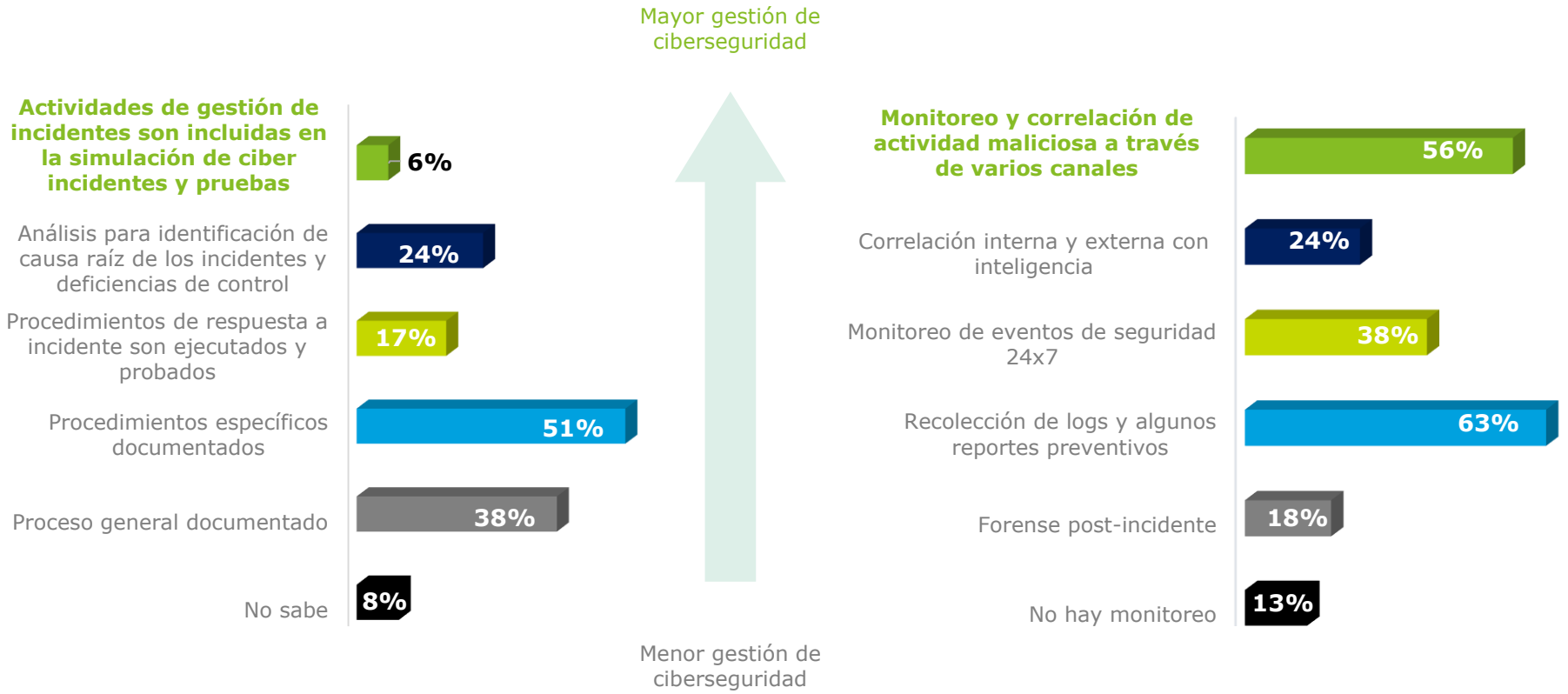
Gestión de incidentes de seguridad de la información



D

Estar preparado para prevenir y atender el mayor número de incidentes de seguridad de la información debe formar parte de los objetivos operativos fundamentales. Administrar todos los incidentes de seguridad soporta la continuidad operativa de las organizaciones y en consecuencia los hablita en el cumplimiento de los objetivos de negocio.

Gestión de incidentes de seguridad de la información

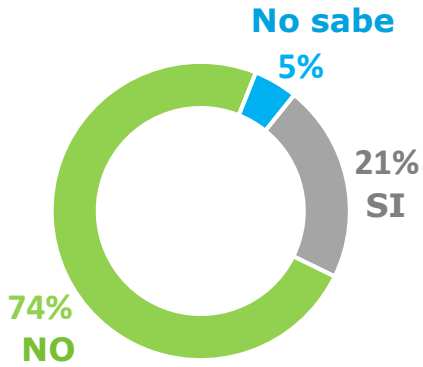


D

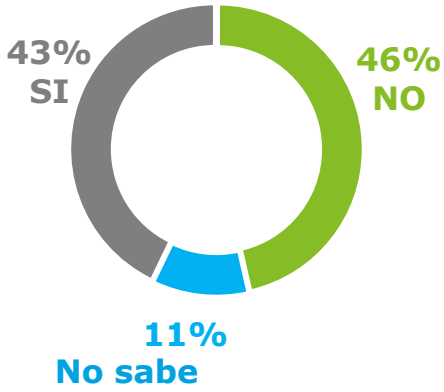
Estar preparado para prevenir y atender el mayor número de incidentes de seguridad de la información debe formar parte de los objetivos operativos fundamentales. Administrar todos los incidentes de seguridad soporta la continuidad operativa de las organizaciones y en consecuencia los hablita en el cumplimiento de los objetivos de negocio.

Incidentes de ciberseguridad

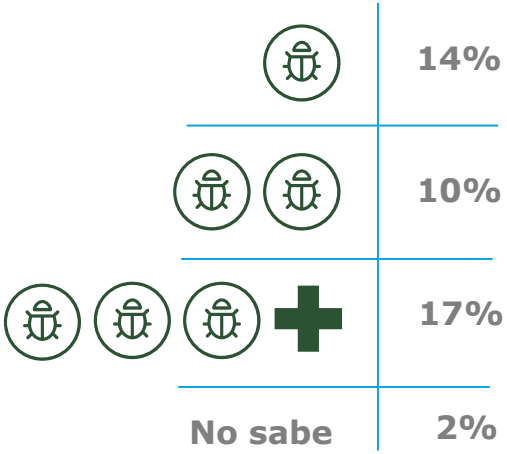
Validan la efectividad del proceso de respuesta a incidentes de ciberseguridad



Tuvieron ciberataques en los últimos 24 meses



Cantidad de ciberataques experimentados en los últimos 24 meses



Contar con una diversidad de puntos estratégicos de detección y contención de ciber ataques es una excelente estrategia de ciberseguridad. Identificando los activos críticos y calcular el impacto en caso de materializarse el riesgo, es un buen punto de partida para iniciar los primeros esfuerzos de protección ante ciber ataques.

Consideraciones finales

Consideraciones finales

1

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

2

Si bien las organizaciones cuentan con un espectro de mecanismos tecnológicos, administrativos y legales para proteger la información, es importante que verifiquen su efectividad a fin de no solo mejorarlo, sino asegurar que funcionarán adecuadamente cuando se requieran.

3

El monitoreo proactivo de la situación de riesgos y el análisis de inteligencia de la información disponible resulta de vital importancia si las organizaciones desean prevenir la materialización de los riesgos latentes y evolucionar a nuevas y mejoradas estrategias de ciberseguridad.

4

Con base en un sustentado conocimiento de las prioridades de la organización, es posible establecer una línea base para prepararse ante disrupciones del negocio y contener los posibles impactos negativos.

Deloitte.

Acerca de Deloitte

Deloitte se refiere a una o más de Deloitte Touche Tohmatsu Limited compañía privada de UK limitada por garantía, y su red de firmas miembro, cada una separada legalmente como entidades independientes. Por favor visite www.deloitte.com/about para una descripción más detallada de la estructura legal de Deloitte Touche Tohmatsu Limited y sus firmas miembro.

Deloitte presta servicios de auditoría, impuestos, consultoría y asesoramiento financiero a organizaciones públicas y privadas de diversas industrias. Con una red global de Firmas miembro en más de 150 países, 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. Más de 244.000 profesionales de Deloitte se comprometen a ser estándar de excelencia.

Esta publicación contiene exclusivamente información general y ninguna de Deloitte Touche Tohmatsu Limited, sus firmas miembro o entidades relacionadas (colectivamente, la "Red Deloitte"), por medio de esta publicación da asesoramiento profesional o de servicios. Antes de dar cualquier decisión o tomar cualquier acción que pueda afectar sus finanzas o negocio, Ud. debe consultar un profesional experto. Ninguna entidad en la Red Deloitte será responsable por cualquier pérdida sustentada por cualquier persona que se refiera a esta publicación.