Deloitte.

Ciber Riesgos y Seguridad de la Información en América Latina & Caribe

Tendencias 2019

Reporte Colombia

Risk Advisory
Abril 2019

Cyber

La Evolución de la Gestión de la Seguridad de la Información

Deloitte se complace en presentar los resultados del **Estudio sobre Tendencias en Gestión de Ciber Riesgos y Seguridad de la Información en América Latina y Caribe** (AL&C)

Las Organizaciones en AL&C 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.

Wilmar Castellanos

Colombia Cyber Risk Services Leader

Índice

Introducción

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 América Latina

El foco incluyó el análisis de las tendencias emergentes a partir de la transformación y digitalización de los negocios

150 **Organizaciones participantes**

12 **Países**

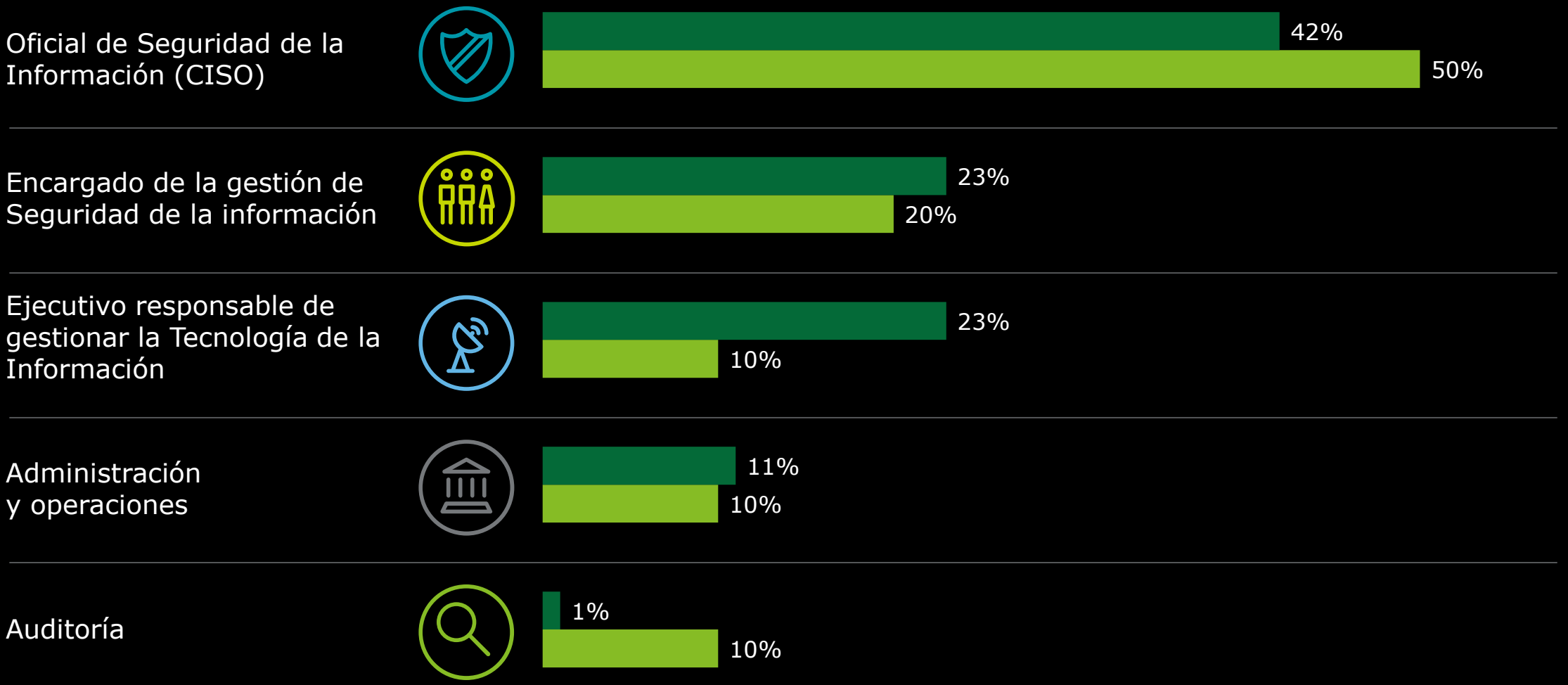
7 **Industrias / Sectores**

Información General sobre el Estudio

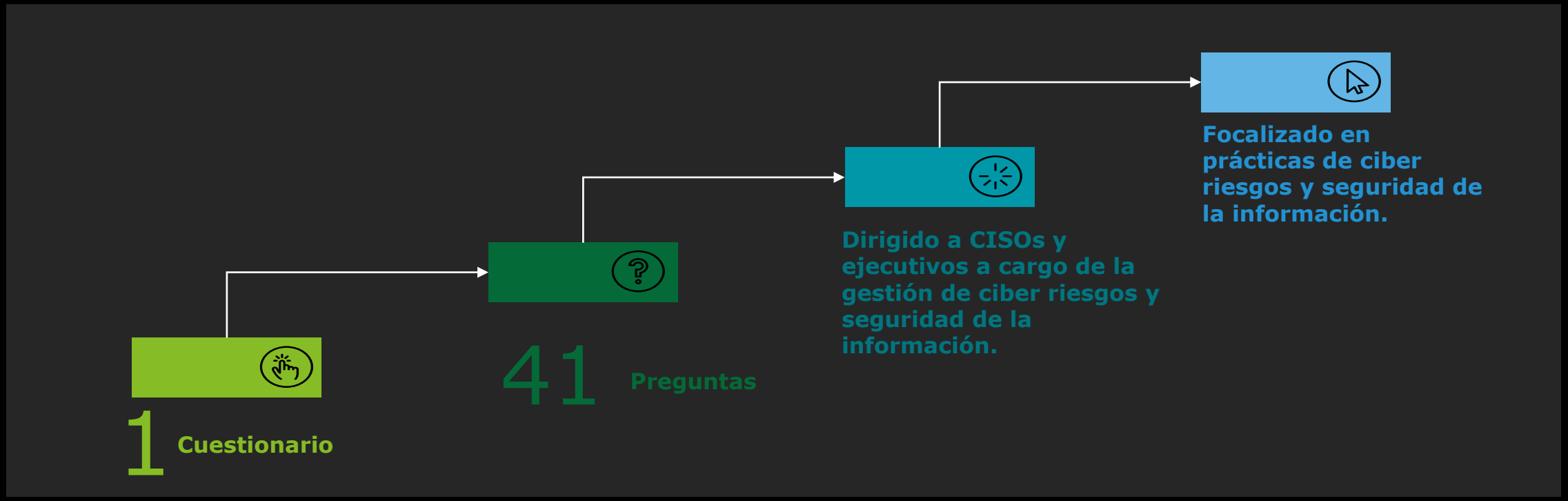
Objetivo y Alcance del Estudio

	LATAM	Colombia
Financiero	44.7%	30%
Manufactura	10.7%	30%
Tecnología, Telecomunicaciones y medios	10.6%	0%
Servicios	10%	20%
Petróleo, Gas y minería	10%	10%
Otros	8%	10%
Sector Público	6%	0 %

Información General sobre el Estudio
Perfil del Ejecutivo Entrevistado



Información General sobre el Estudio
Proceso de recopilación de la información



D Indica la perspectiva de Deloitte

Julio 2018 — **Octubre 2018**

Principales tendencias identificadas

Principales tendencias identificadas

4 de cada 10 organizaciones sufrieron un **incidente de ciber 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 ciber seguridad y **sólo un 3% realiza simulaciones** para probar sus capacidades efectivas de respuesta ante un evento ciber

D

Siguiendo la tendencia mostrada 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, aspecto que sigue siendo un pendiente significativo que tienen las organizaciones en AL&C.

Las organizaciones en América Latina están **incrementando sus presupuestos** dedicados gestionar ciber riesgos y seguridad de la información

El 89% de las organizaciones le asigna una **importancia muy alta a la gestión de ciber riesgos** en un contexto cada vez más digital de los negocios

D

La problemática de ciber riesgos y seguridad de la información y riesgos 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, sus organizaciones ven a esta función como un área clave en el contexto actual de digitalización de los negocios y de amenazas emergentes.

Principales tendencias identificadas

Las organizaciones cuentan con **capacidades limitadas** de monitoreo de ciber seguridad e inteligencia de amenazas.

Sólo un 31% de las Organizaciones realiza inteligencia de amenazas y comparte información con otras organizaciones.

D

Las Organizaciones en AL&C están en un estado inicial en lo que refiere a capacidades de inteligencia de amenazas, contando con procesos básicos de monitoreo de seguridad.

Para poder responder rápidamente y estar preparadas ante los nuevos escenarios y ciber ataques, las organizaciones requieren basar sus capacidades no sólo en lo que sucede puertas adentro, sino que deben entender el contexto de amenazas que afecta a organizaciones en general y de su industria en particular, adquiriendo información de inteligencia que sea relevante.

Casi 7 de cada 10 organizaciones han **implementado un programa de concientización** en ciber seguridad.

D

Se percibe la importancia de capacitar y concientizar a sus colaboradores sobre ciber riesgos y su impacto para la organización.

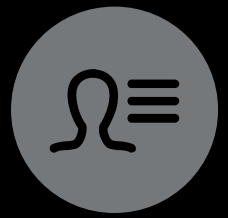
Gran parte del tiempo del ejecutivo de ciber riesgos y seguridad de la información se debe dedicar comunicar a sus pares, a la Alta Gerencia y a los Accionistas sobre esta problemática y así lograr adecuada visibilidad y apoyo en la ejecución de los programas a todos los niveles de la organización.

Principales tendencias identificadas

Evolución de la Gestión de ciber riesgos y seguridad de la información

D

La función de **Gestión de ciber riesgos y seguridad de la información** está evolucionando hacia un nuevo paradigma que incluye cuatro componentes centrales y estratégicos:



Gobierno

Establece la visión y estrategia, roles y responsabilidades, de la función de gestión de ciber riesgos y seguridad de la información, considerando las necesidades del negocio, leyes, regulaciones y recursos humanos y tecnológicos

Seguro

Se enfoca en la protección de la información y la tecnología que soportan los procesos clave del negocio, implementando controles adecuados al riesgo y a la amenazas propias de la organización.

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.

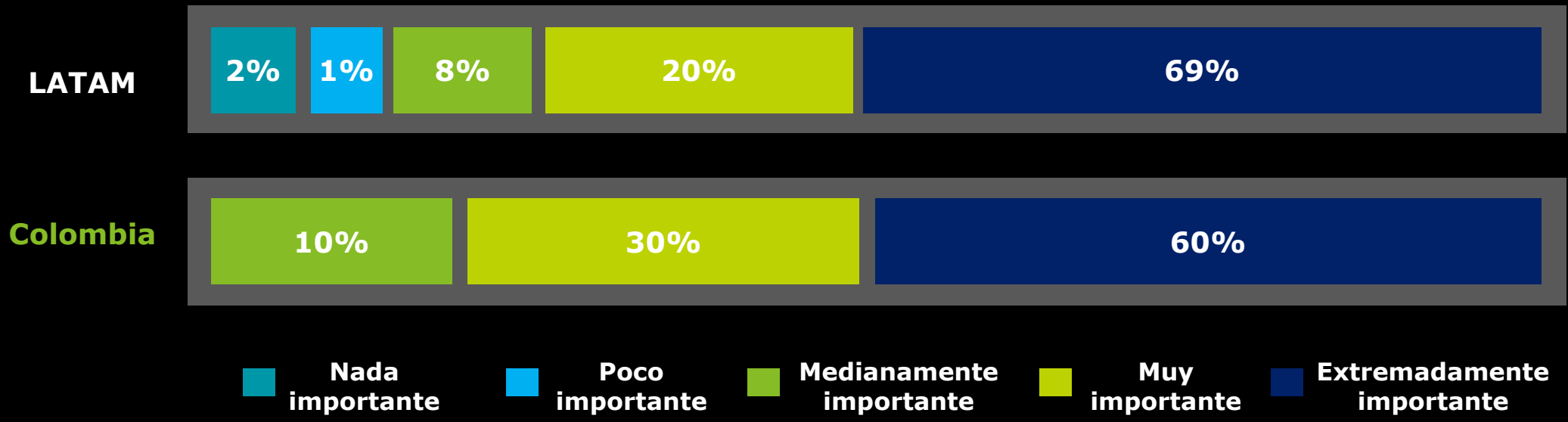
Resiliente

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

Gobierno
Estrategia y Marco de Gestión

Importancia de la Ciber Seguridad para las Organizaciones

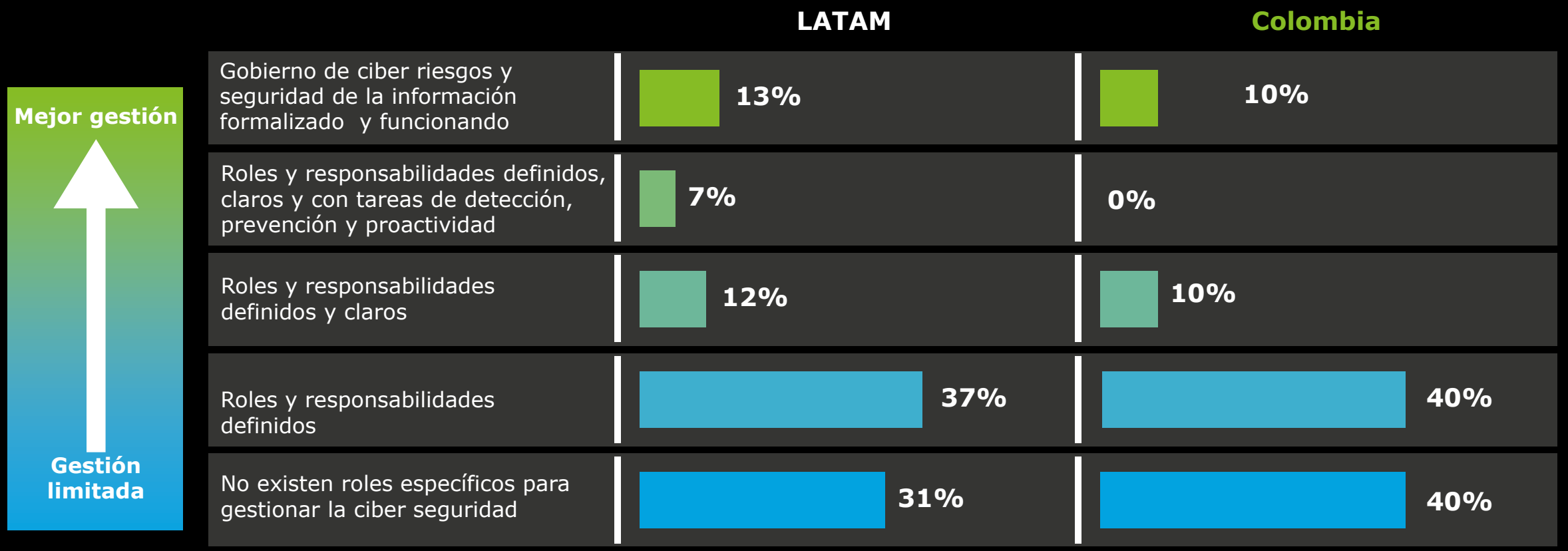


D

Para las organizaciones de AL&C, la ciber seguridad es un componente muy importante de su modelo de gobierno y gestión.

Sin embargo, pueden existir inconsistencias entre la manifestación de dicha importancia versus los presupuestos asignados y/o el nivel de madurez de sus prácticas de gestión de ciber seguridad.

Gobierno de Ciber Seguridad, Definición de Roles y Responsabilidades



D

Una mejor y más especializada función de ciber seguridad habilitará a las organizaciones para tomar decisiones más efectivas, con visión de futuro y con capacidades para facilitar el desarrollo de negocios digitales de forma segura.

La formalización de una estructura de gobierno de ciber seguridad es un paso inicial clave para fortalecer las capacidades y madurez de la organización en esta área de gestión.

Presupuesto Asignado a Ciber Seguridad

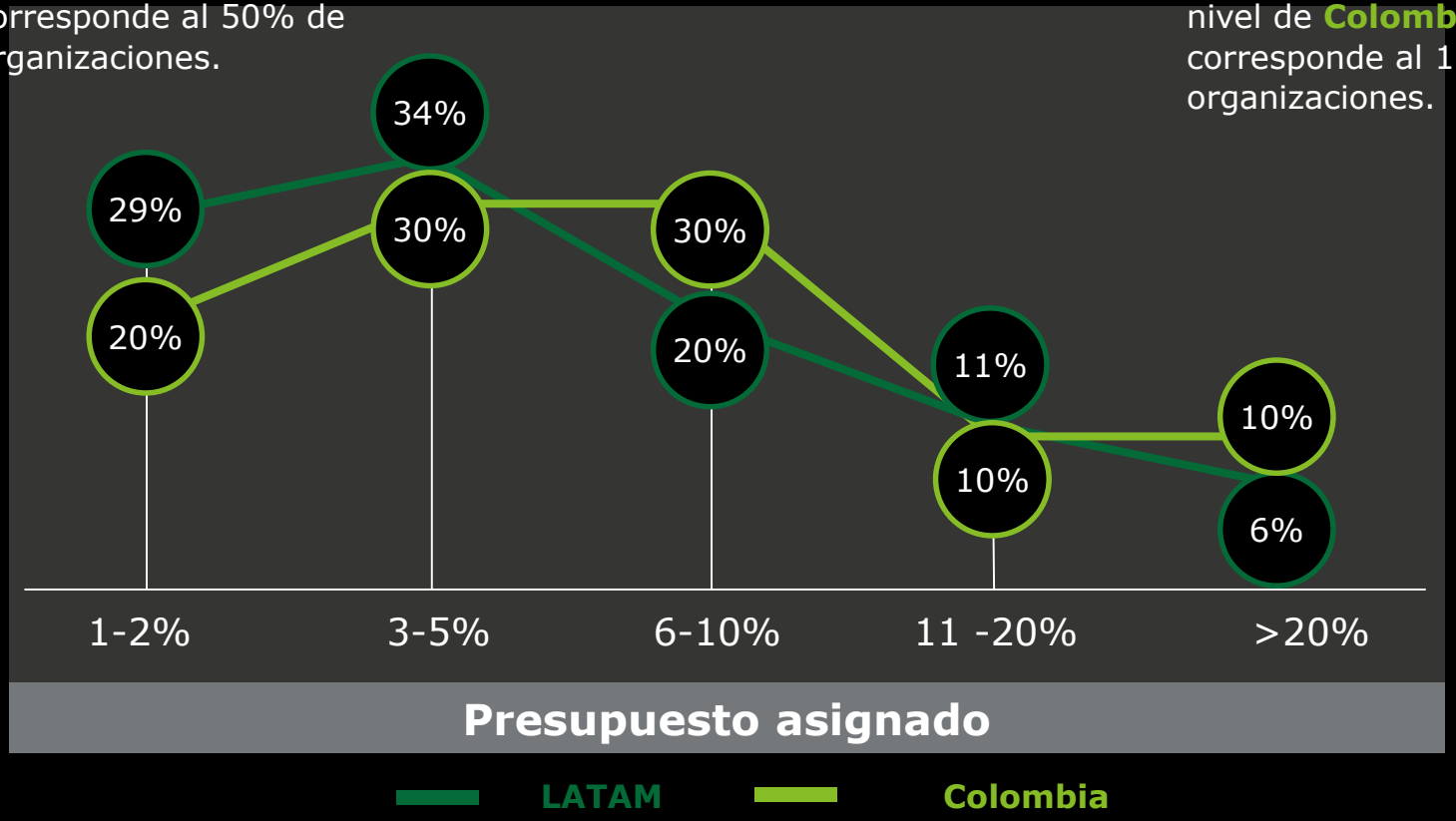
D

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

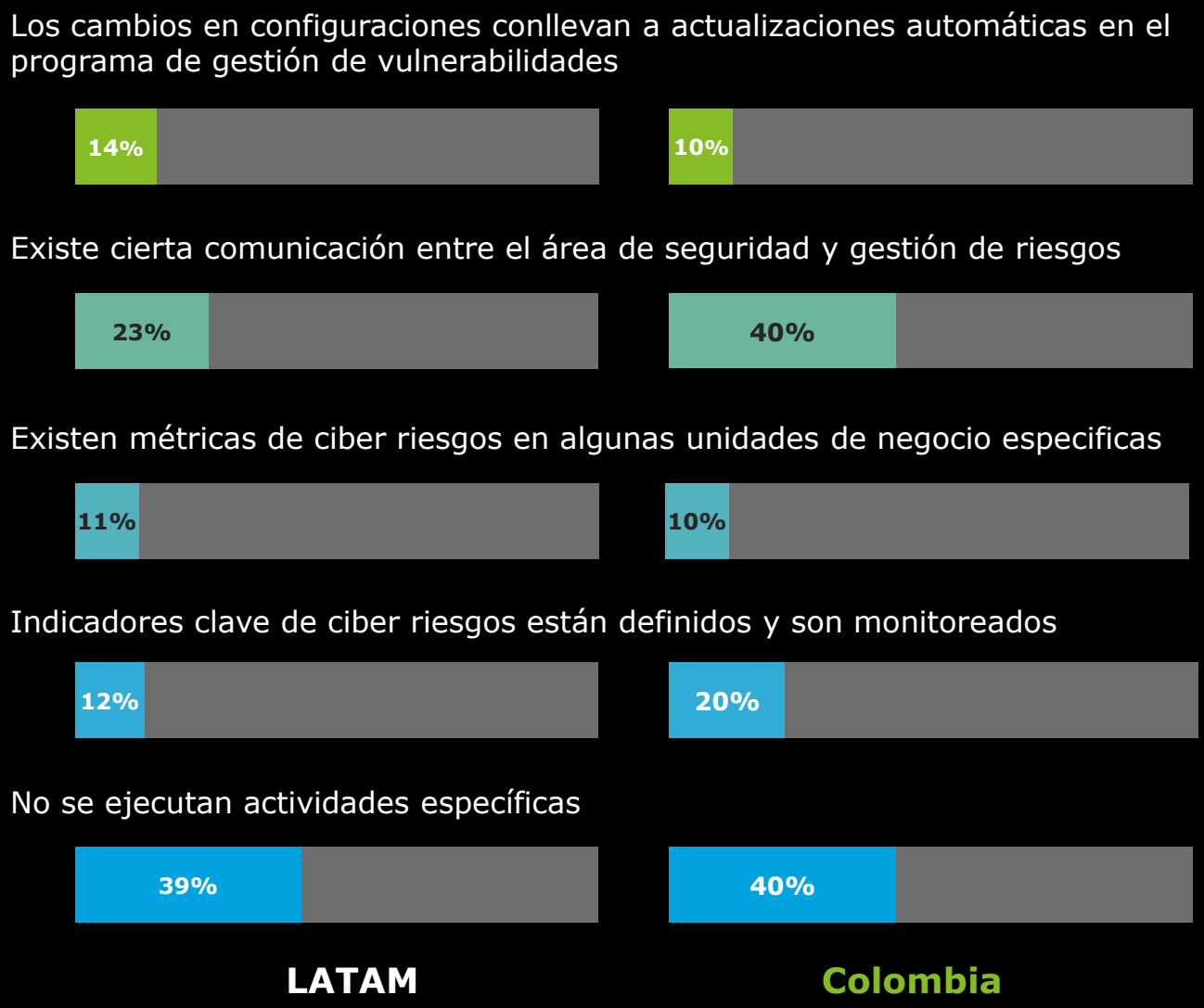
El presupuesto debe estar en línea con el apetito de riesgo de la organización.

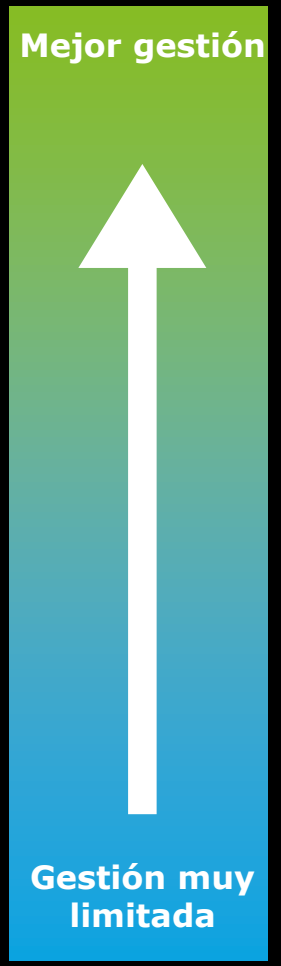
A nivel **LATAM**, el 63% de las organizaciones asigna Ciber Seguridad entre un 1% y 5% del presupuesto que asigna a TI; mientras que a nivel de **Colombia** corresponde al 50% de organizaciones.

A nivel **LATAM**, sólo un 17% de las organizaciones asigna un equivalente al 11% o mas de su presupuesto de TI a Ciber Seguridad; mientras que a nivel de **Colombia** corresponde al 10% de organizaciones.



Gestión de Ciber Seguridad Integrada con Otros Procesos Clave



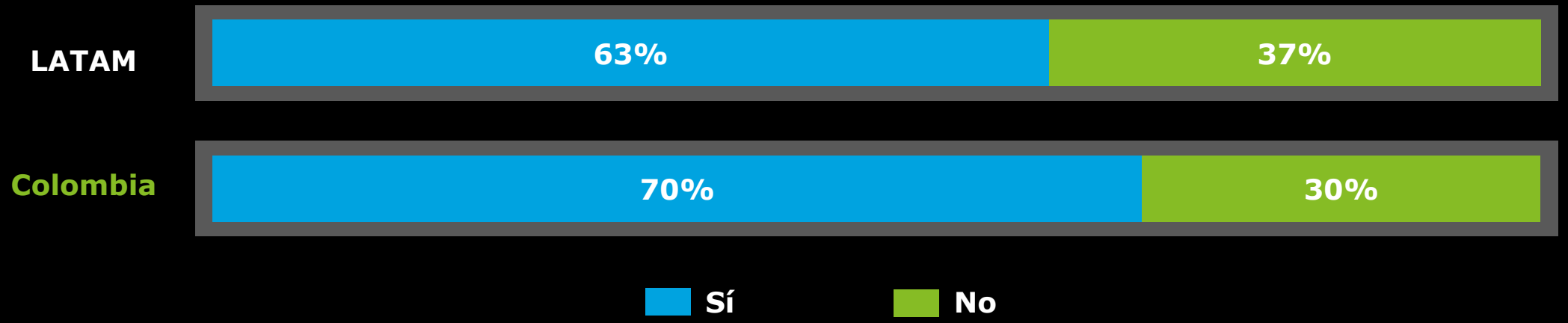


D

Las Organizaciones en AL&C se encuentran en un proceso de integración de sus operaciones de ciber seguridad con otros procesos de gestión.

Es importante desarrollar y monitorear indicadores de ciber riesgos, a fin de tener un adecuado entendimiento del nivel de exposición y madurez de la organización en sus prácticas de ciber seguridad.

Utilización de Servicios Gestionados y Tercerización como Estrategia para Complementar Capacidades Ciber



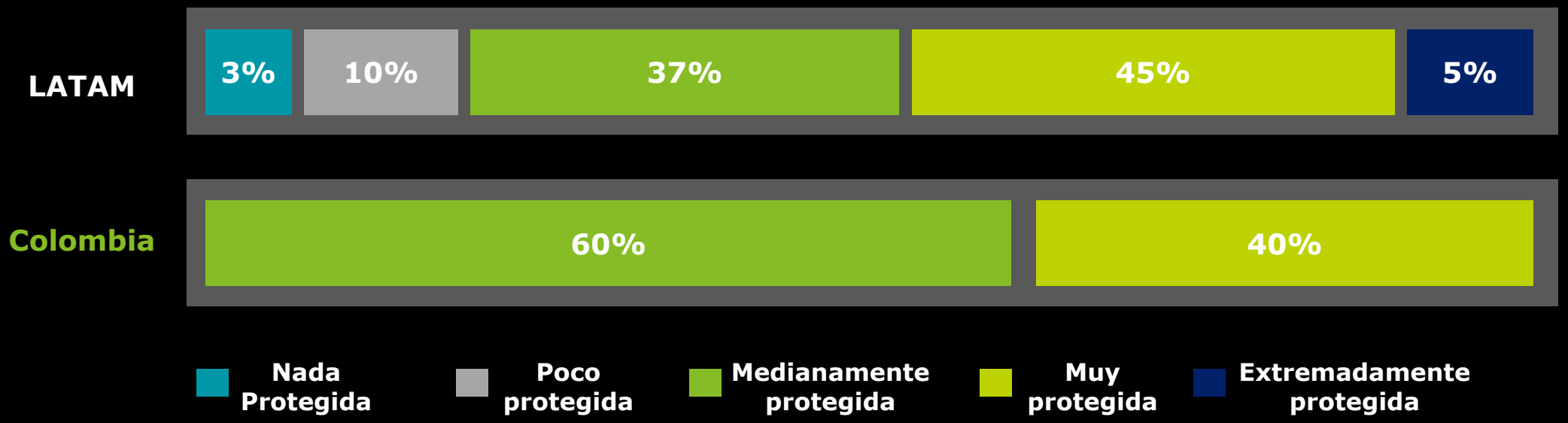
D

Las dificultades que enfrentan las organizaciones de AL&C en relación a disponibilidad de recursos humanos calificados en cantidad y calidad, sumado a la complejidad de la gestión ha empujado a un gran número de organizaciones a tercerizar procesos de ciber seguridad.

Definir una estrategia de uso de proveedores expertos para soportar la gestión de ciber es un aspecto clave del modelo de gobierno de ciber seguridad en el contexto actual.

Seguro
Protección de la información

Nivel de Protección Ciber de las Organizaciones

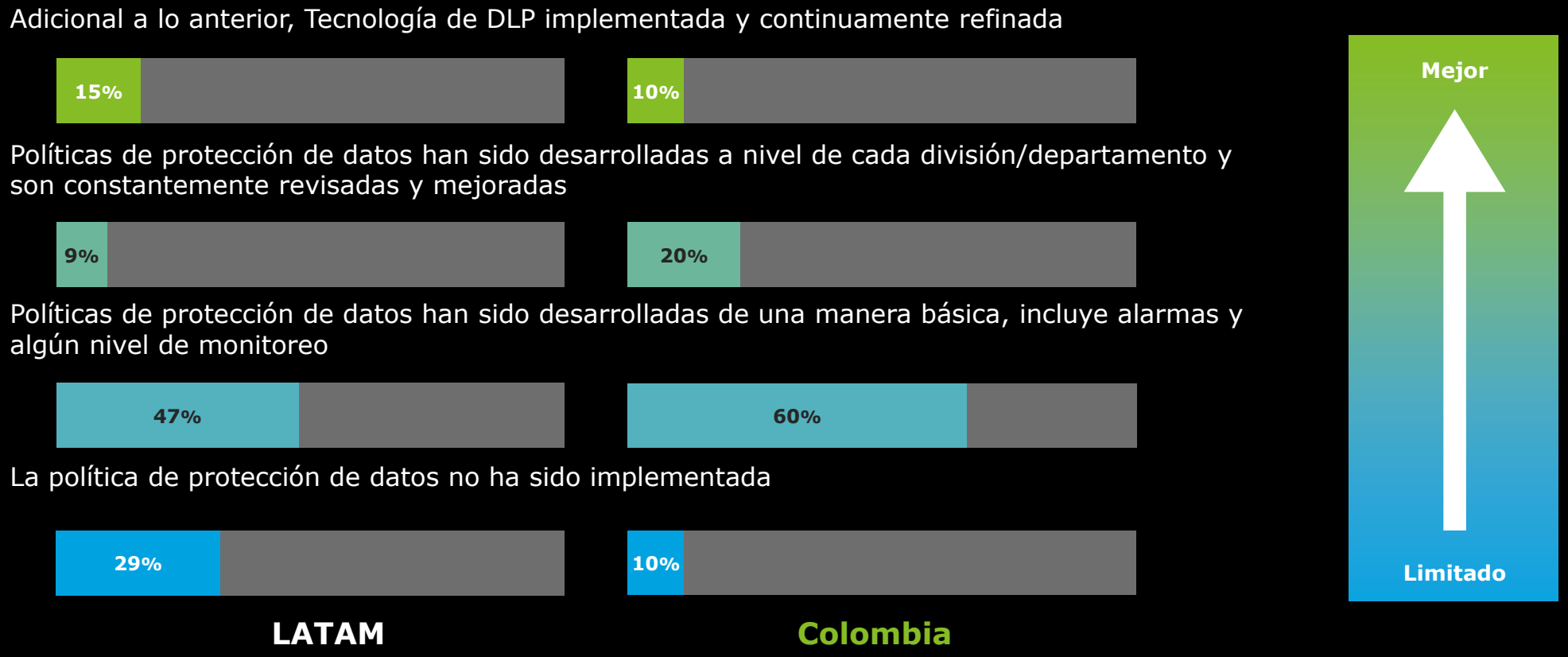


D

La mitad de las organizaciones se sienten muy protegidas respecto a los ciber riesgos; sin embargo, la madurez de ciertas prácticas claves en la gestión de ciber riesgos como monitoreo, respuesta ante incidentes y ciber inteligencia, pueden indicar un grado de optimismo mayor al que dichas capacidades ameritarían.

Las organizaciones deben considerar que la digitalización de sus negocios y el incremento de la sofisticación de los ataques requieren el desarrollo de nuevas capacidades.

Actividades Realizadas por las Organizaciones para Prevenir el Robo de su Información

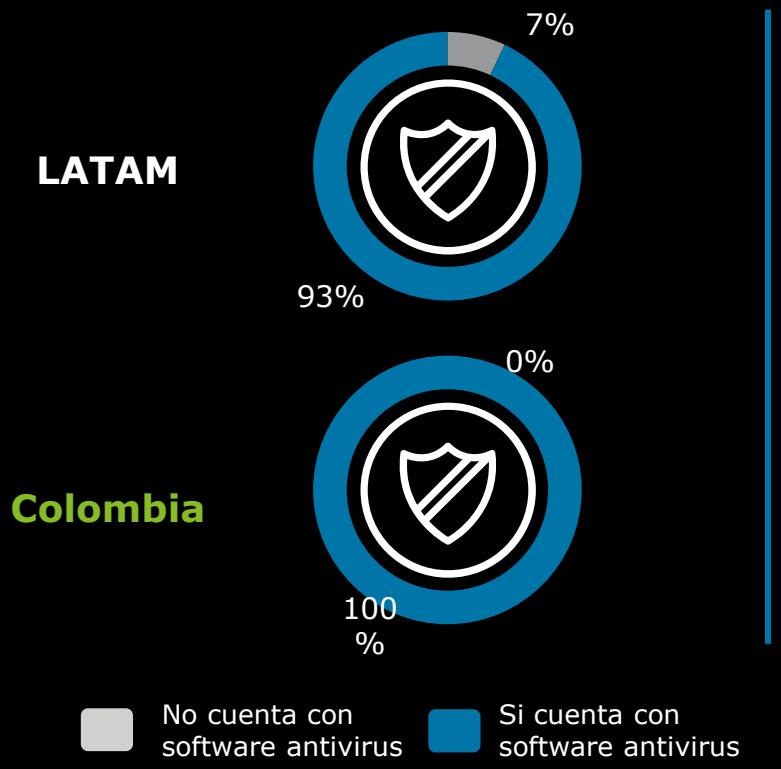


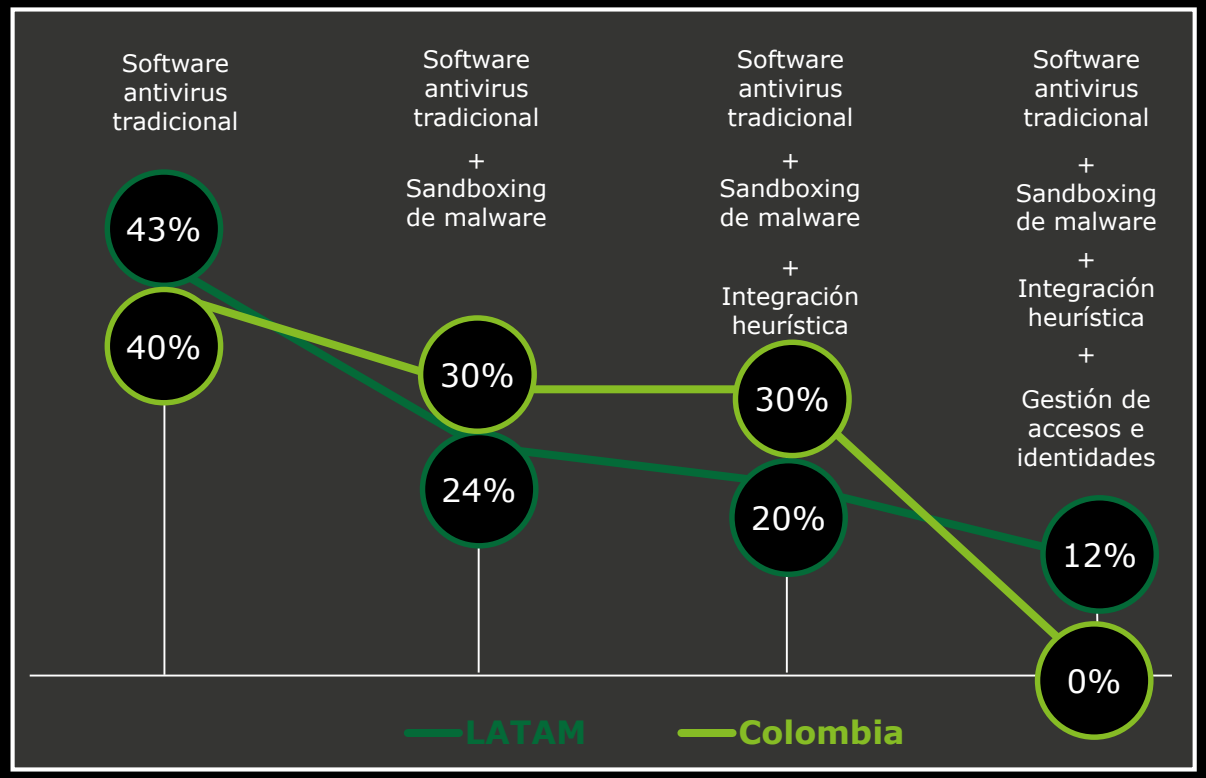
D

La información es considerada hoy uno de los activos más relevantes para las organizaciones.

A nivel general, las organizaciones en AL&C se encuentran en un estado medio de protección de su información, surgiendo la necesidad de focalizar e invertir en tecnologías que soporten las políticas definidas.

Capacidades Tecnológicas de Detección y Protección ante Amenazas de Malware / Código Malicioso



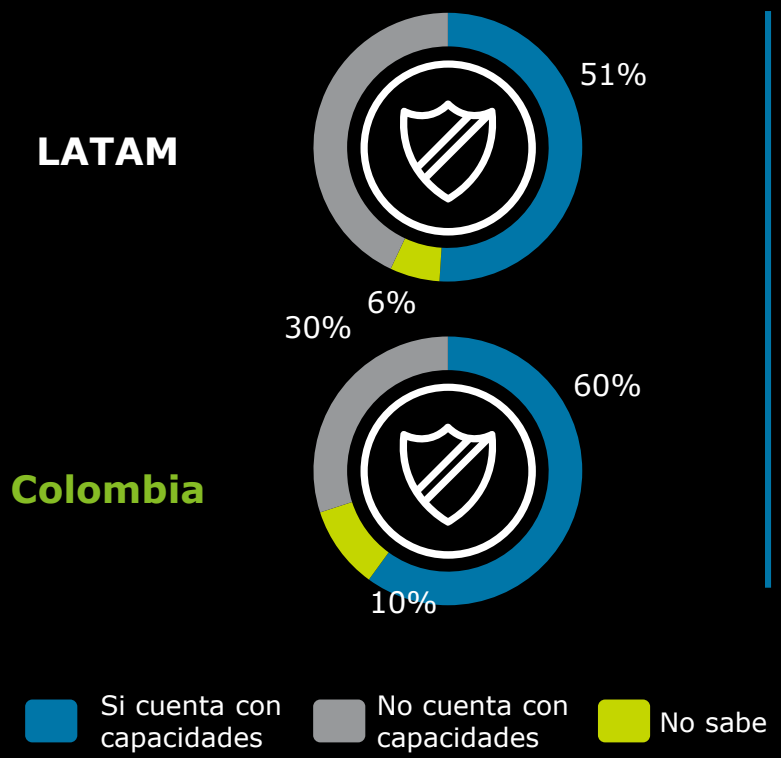


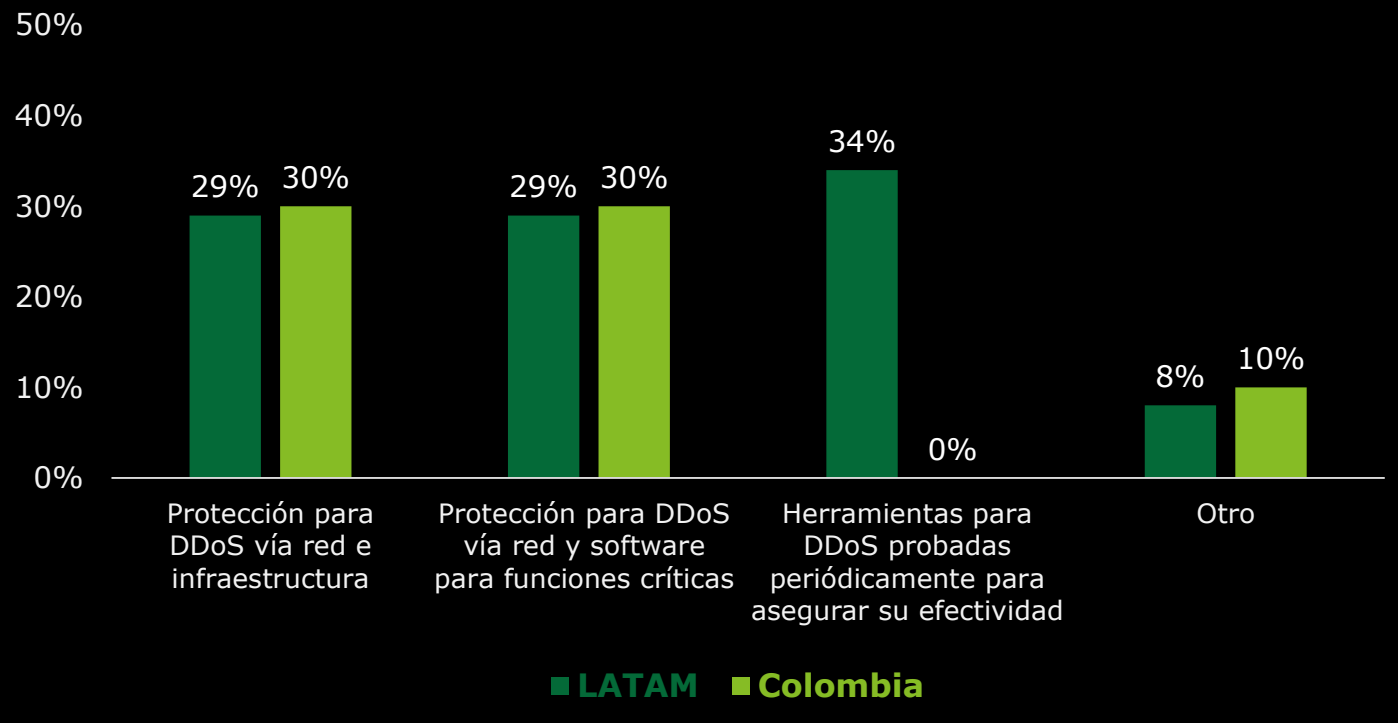
D

En el contexto de ciber amenazas actual, las organizaciones deben contar con diferentes tecnologías destinadas a proteger su información y sus sistemas contra amenazas del tipo malware o código malicioso.

Si bien en AL&C se observa el uso de tecnologías adicionales al tradicional anti-virus, aún existen oportunidades de mejora en esta área de protección crítica.

Protección Contra Ataques de Denegación de Servicio

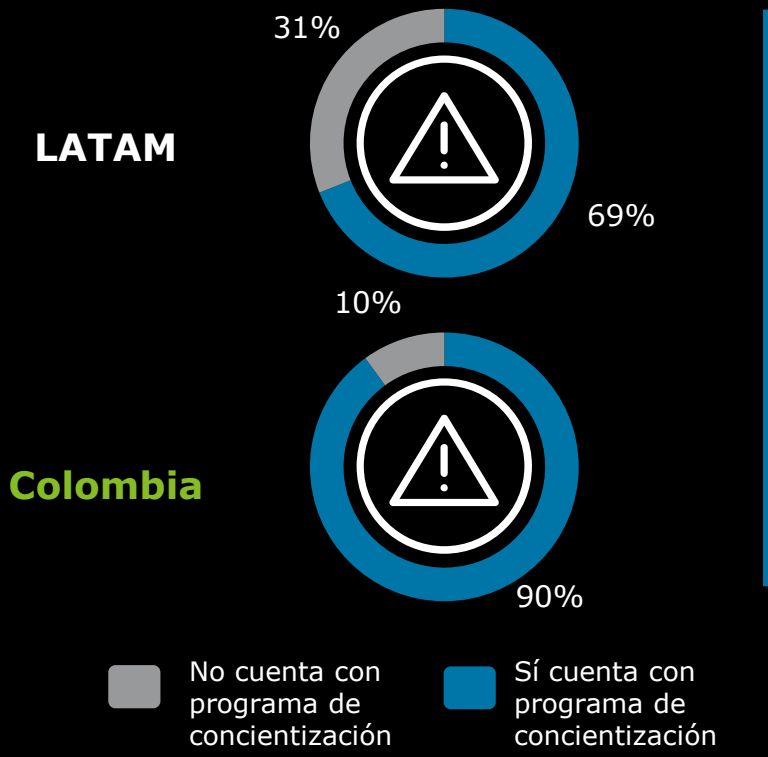


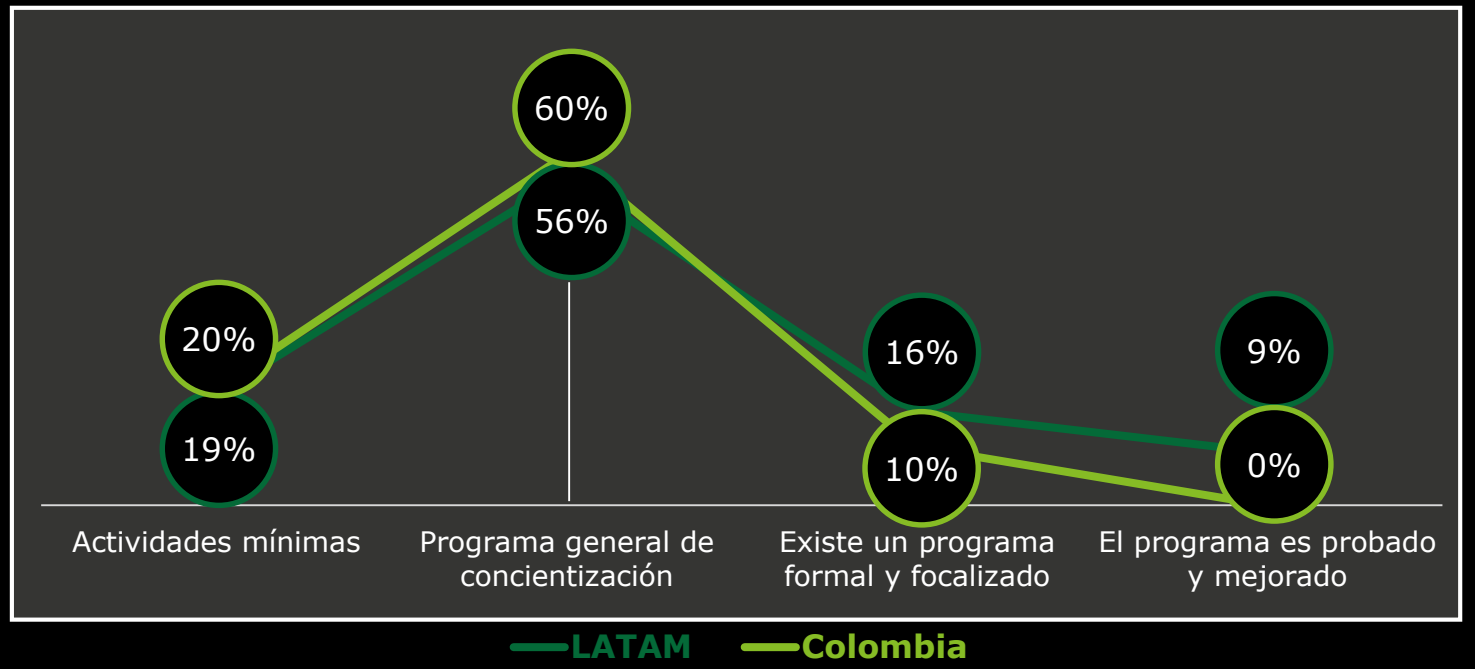


D

La importancia de los ataques de negación de servicio siguen incrementándose en las operaciones de las empresas, ocasionando fuertes impactos. Las empresas deben continuar trabajando en la optimización y actualización de herramientas para la protección de DDoS que les permita disminuir los riesgos en estos ataques.

Programa de Concientización sobre Ciber Amenazas





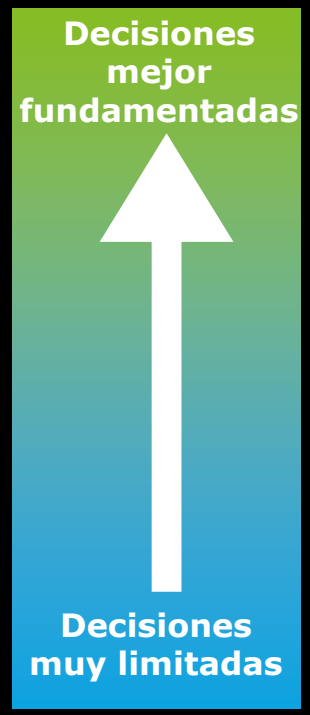
D

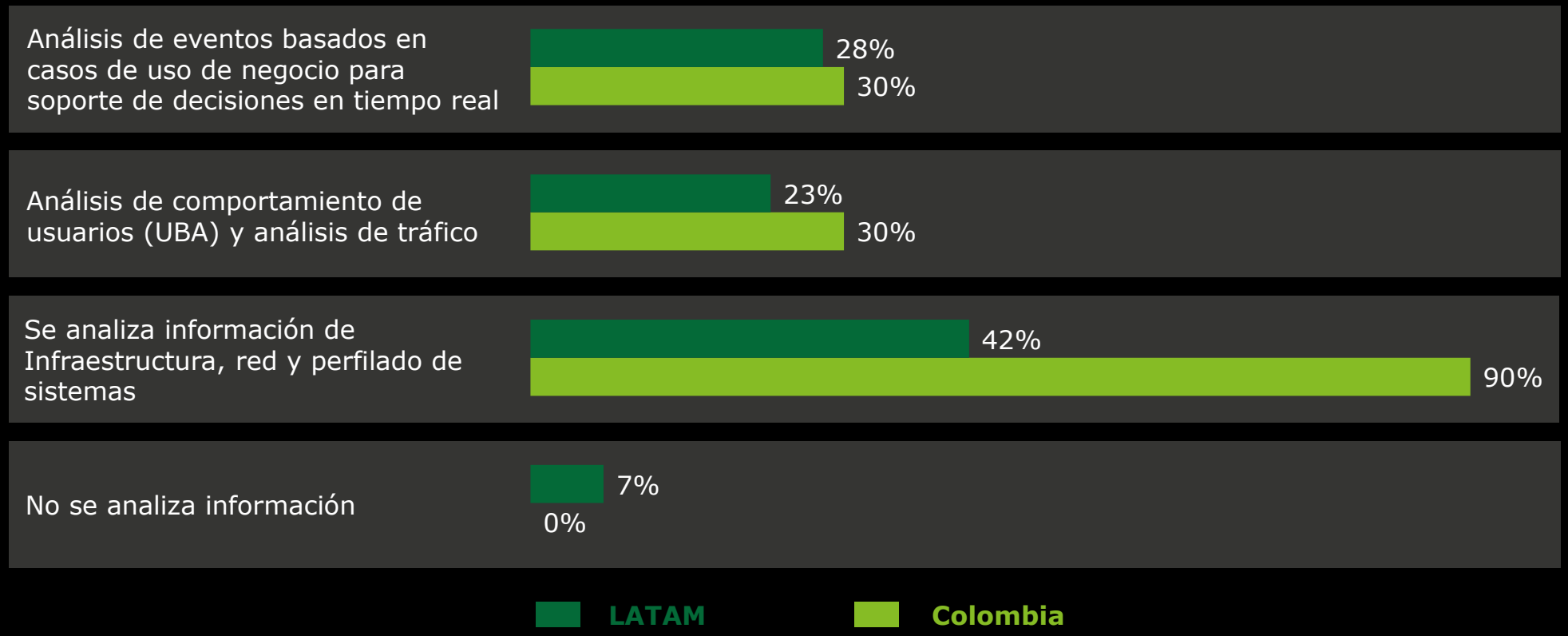
El factor humano sigue siendo un factor de vital importancia para la seguridad de la información. Su importancia radica en que resulta una alternativa de entrada a las organizaciones y mediante la cual muchos controles tecnológicos pueden ser burlados.

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

Vigilante
Monitoreo Proactivo de Amenazas y Eventos

Análisis de Información de Eventos y Amenazas de Ciber Seguridad

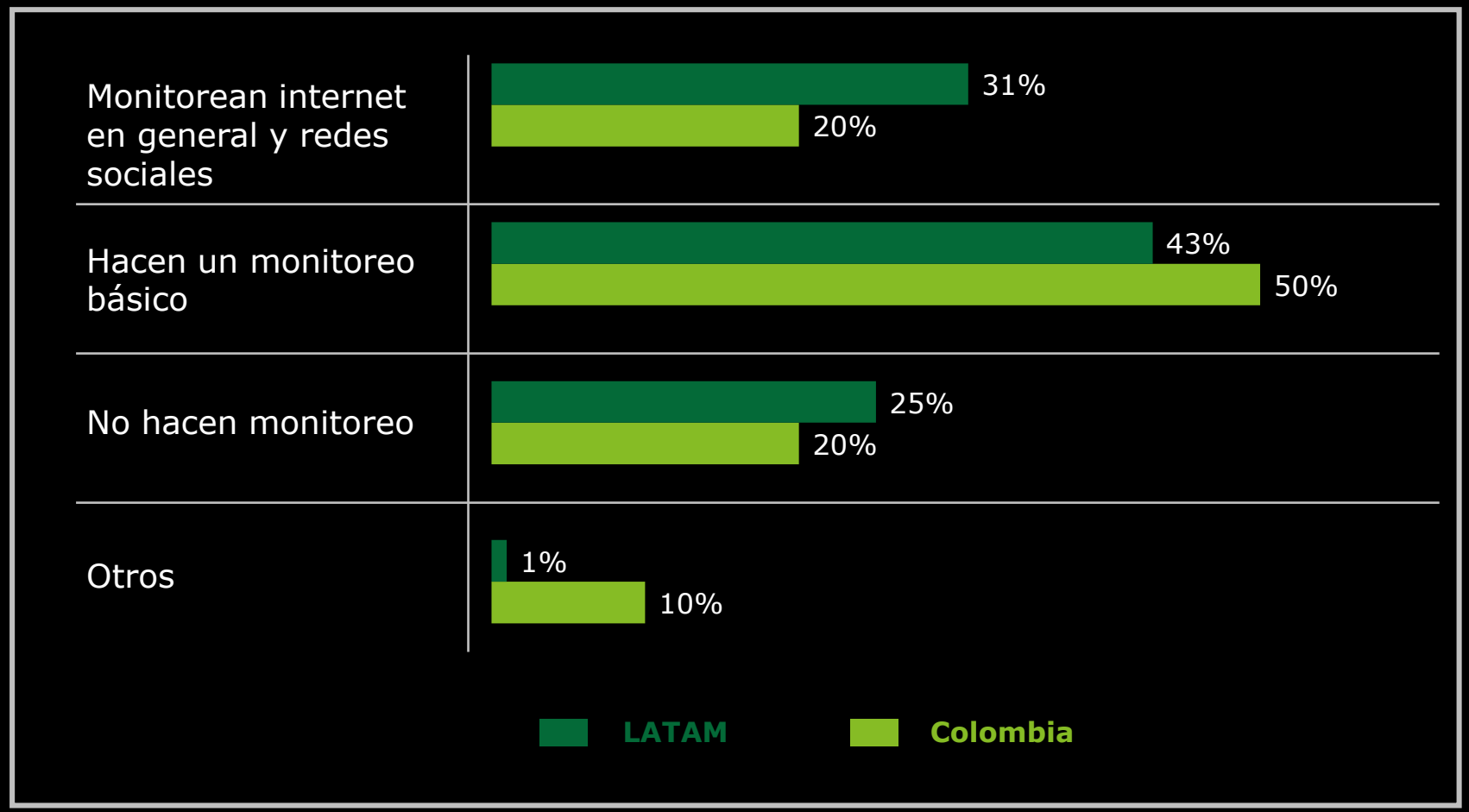




D

Las organizaciones en AL&C deben optimizar su proceso para recopilar registros, analizar tendencias y anomalías y utilizar los resultados para tomar decisiones mejor sustentadas.

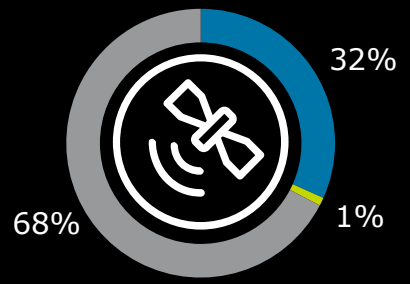
Monitoreo de Información Disponible en Internet

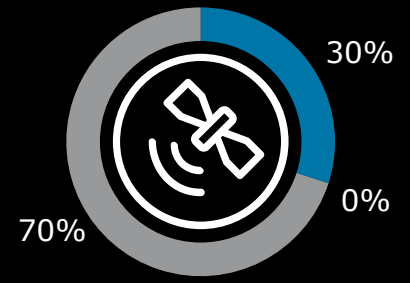


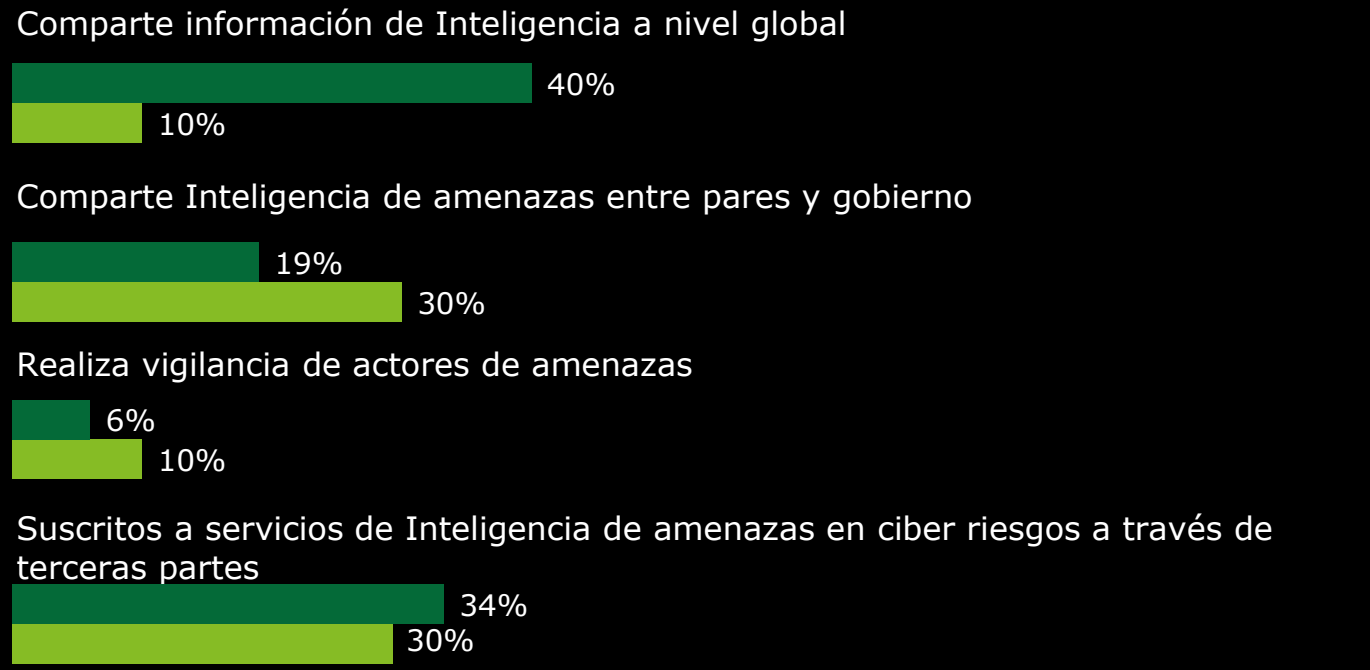
D

La proliferación de información en Internet y la capacidad de impactar la reputación de la marca y la organización requiere que se monitoreen las fuentes públicas de información de forma practica, para descubrir información sensible y para tomar acciones lo más rápido posible

Inteligencia de Amenazas







No recopila ni comparte información | No está seguro | Si recopila y comparte información

LATAM | Colombia

D

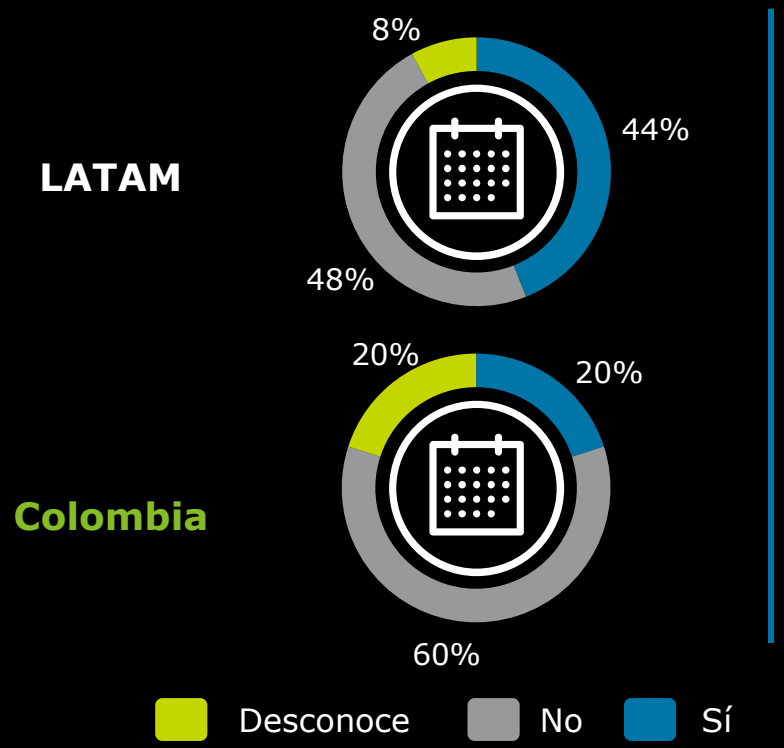
En un ambiente de constante cambio tecnológico y donde el modelo de operación es usualmente 24/7, contar con información actualizada de la situación de amenazas y riesgos de ciber seguridad resulta una competencia clave a desarrollar por las organizaciones.

En AL&C aún hay mucho trabajo por recorrer para recolectar, almacenar y compartir información para un análisis de inteligencia de las amenazas que active procesos interno de preparación y respuesta.

Resiliente
Respuesta Rápida y Efectiva

Incidentes de Ciber Seguridad Sufridos por las Organizaciones

Tuvieron ciberataques en los últimos 24 meses



Cantidad de ciber ataques experimentados en los últimos 24 meses

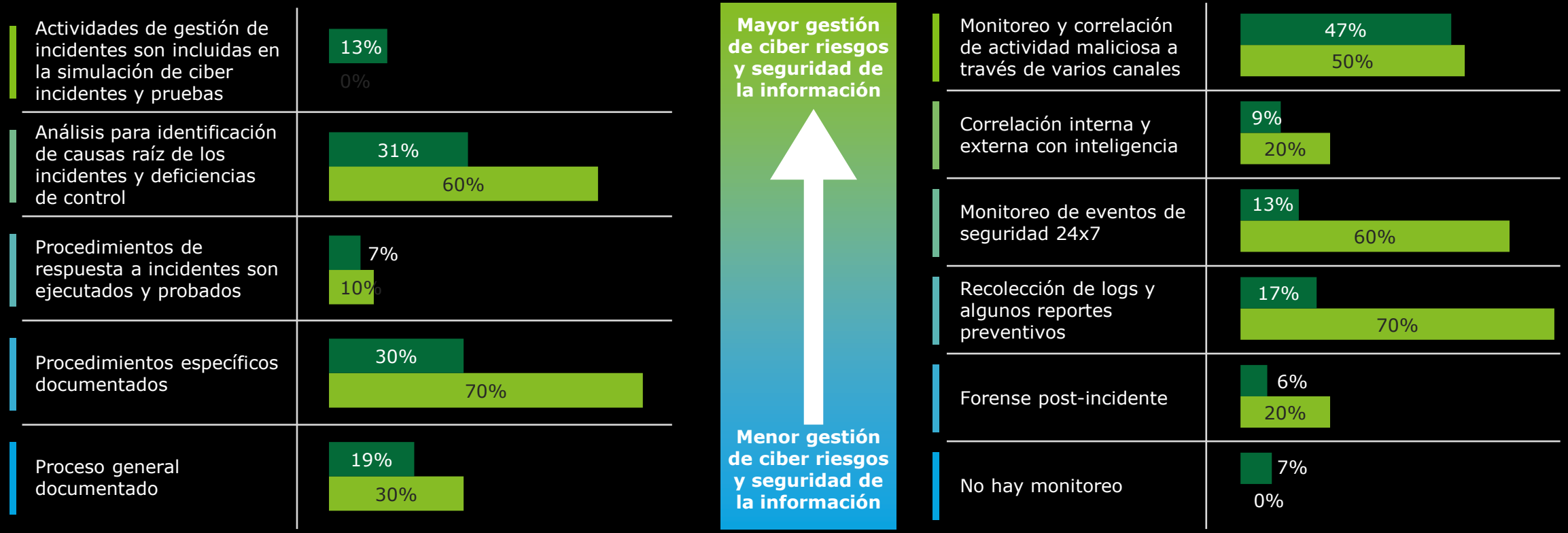
	LATAM	Colombia
1	21%	10%
2	21%	10%
3+	48%	0%
Desconoce	9%	0%

D

Las Organizaciones de AL&C deben considerar como altamente probable sufrir uno o varios incidentes de ciber seguridad al año.

Consistente con tendencias globales reportadas, muchas de las organizaciones no tienen claridad sobre la cantidad de incidentes sufridos o del impacto.

Gestión de Ciber Incidentes

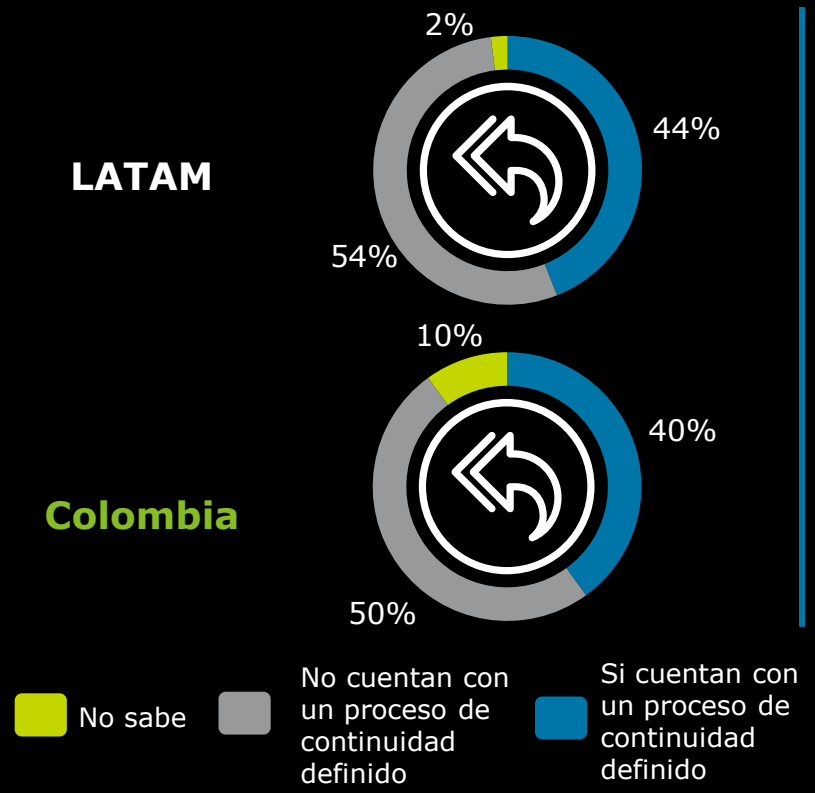


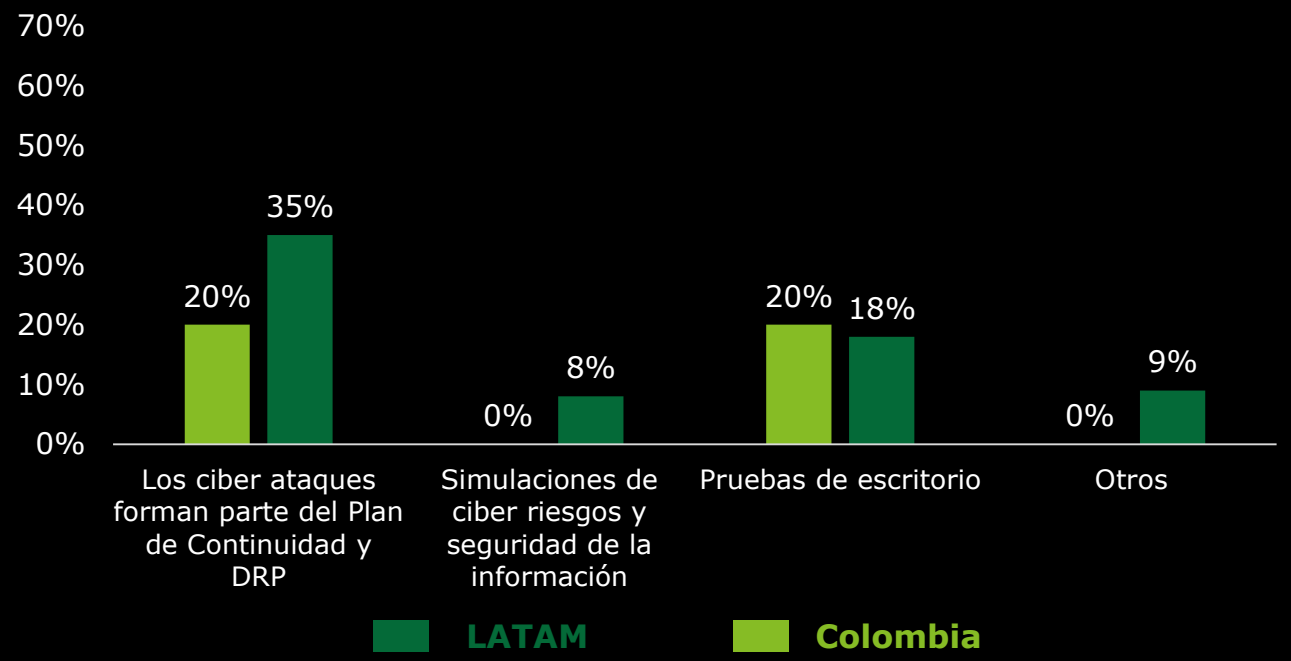
D

Estar preparado para prevenir y atender incidentes de ciber seguridad debe ser un objetivo estratégico.

Contar con un proceso robusto, documentado y probado es todavía un desafío para las organizaciones en AL&C.

Escenario Ciber como Parte del Programa de Continuidad de Negocios





D

Más de la mitad de las organizaciones en AL&C no han incorporado el escenario ciber dentro de sus programas de continuidad de negocio, y sólo un 3% de las organizaciones realiza algún tipo de simulación de un incidente ciber para validar su nivel de preparación y respuesta.

Consideraciones Finales

Consideraciones finales

1

La ***evolución de los modelos de negocio, la transformación digital y el contexto de amenazas*** está empujando a las organizaciones en AL&C a poner mayor atención en su gestión de ciber seguridad y a dedicar más recursos

2

Sin embargo, prácticas como el ***monitoreo de eventos, la inteligencia de amenazas y el desarrollo de procesos de detección y respuesta ante incidentes ciber*** aún presentan un nivel de madurez bajo en comparación a lo que las propias organizaciones manifiestan como requerido.

3

Dado el nivel de ocurrencia de incidentes reportado por las propias organizaciones, es fundamental que se redoblen los esfuerzos en mejorar las capacidades de respuesta, ***incorporando el escenario de evento ciber dentro de los programas de continuidad y gestión de crisis organizacional***.

4

Es importante que las organizaciones verifiquen la efectividad de sus ***capacidades de protección, monitoreo y respuesta***, a fin de no solo mejorarlo, sino de asegurar que funcionarán adecuadamente cuando se requieran.

Acerca de Deloitte

Acerca 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 **América Latina y Caribe contamos con más de 600 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

Wilmar Castellanos
Partner
Colombia Cyber Risk Leader
wcastellanos@deloitte.com

Samuel Ardila
Cyber Risk Senior Manager
slardila@deloitte.com

Andrés González
Cyber Risk Manager
agonzalezr@deloitte.com

Carolina Rubio
Cyber Risk Manager
crubio@deloitte.com

Oscar Cardoso
Cyber Risk Manager
oscardoso@deloitte.com

Yoli González
Cyber Risk Manager
ypgonzalez@deloitte.com

Luisa Díaz
Cyber Risk Manager
lfdiaz@deloitte.com

Deloitte.