Cisco Security Index

Resumen Ejecutivo

Patrocinado por Cisco y realizado por la consultora Kaagan Research, el primer Latin American Security Index proporciona un punto de referencia para comprender cómo las empresas de la región evalúan la seguridad de su información clave, y cuáles son sus esfuerzos para establecer y mantener estándares que ayuden a conservar segura esa información.

El Cisco Security Index (CISI) ha sido creado con base en las respuestas a una encuesta realizada por la consultora Kaagan Research a más de 600 gerentes de sistemas de información de compañías pertenecientes a seis países Latinoamericanos.

El Index es una medida referente a cómo los especialistas en tecnologías de la información ven las políticas y prioridades corporativas críticas, las determinaciones para obtener asesoría sobre riesgos, prácticas de administración y acceso, entre otros aspectos claves de la IT.

CISI incorpora evaluaciones relacionadas con la familia de estándares ISMS, que comprenden estándares sobre Información de la Seguridad publicadas conjuntamente por la International Organization for Standardization (ISO) y la International Electrotechnical Commission (IEC). El índice refleja en gran parte el marco estructurado ISO 27001, que es el estándar con el cual deben certificarse los sistemas de administración de Seguridad de la Información de las organizaciones.

En función de determinar una puntuación para el Indice, fueron sopesadas e incorporadas 10 categorías al CISI, en concordancia con la determinación de prioridades de Cisco. La fuente de los datos utilizados por el CISI para determinar los puntajes generales del Index fueron las respuestas a preguntas que están comprendidas dentro de cada categoría.

El puntaje del Cisco Security Index – que puede ir desde el 0 como la calificación mínima y el 100 como la máxima - para el año 2007 en América Latina es de 64, lo que demuestra que aún cuando las empresas están haciendo un buen trabajo en cuanto a la implementación de políticas de seguridad de la información, aún hay mucho camino por recorrer y situaciones por mejorar.

A modo de resumen sumario, se puede decir que las preocupaciones más importantes para los gerentes de áreas IT en la región están relacionadas con la multitud de amenazas a la seguridad que pueden interrumpir la eficiencia y la productividad de las empresas.

Otro punto que surge del Index es que los ejecutivos admitieron tener algunas dudas en cuanto a cómo lograr tener un nivel de reportes óptimo de los problemas de seguridad, y también procedimientos de control de daños que sean verdaderamente efectivos.

Puntajes obtenidos durante el Cisco Security Index

Por país

País	Puntaje
México	66
Chile	64
Venezuela	64
Brasil	63
Argentina	62
Colombia	62
Total América Latina	64

Por tamaño de empresa

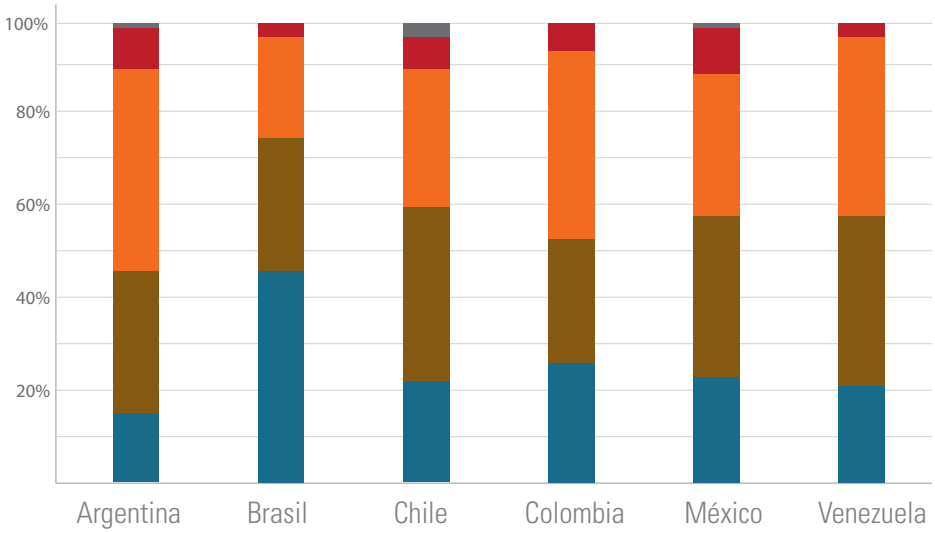
Tipo de Empresa	Puntaje
Menos de 300 empleados	63
De 300 a1.000 empleados	65
Más de 1.000 empleados	68

Puntos Positivos a Destacar

La seguridad de la información se ha convertido en un asunto de alta prioridad dentro de las gerencias de las organizaciones de América Latina.

¿Cuán prioritaria es la Seguridad de la Información para la alta gerencia de su compañía?

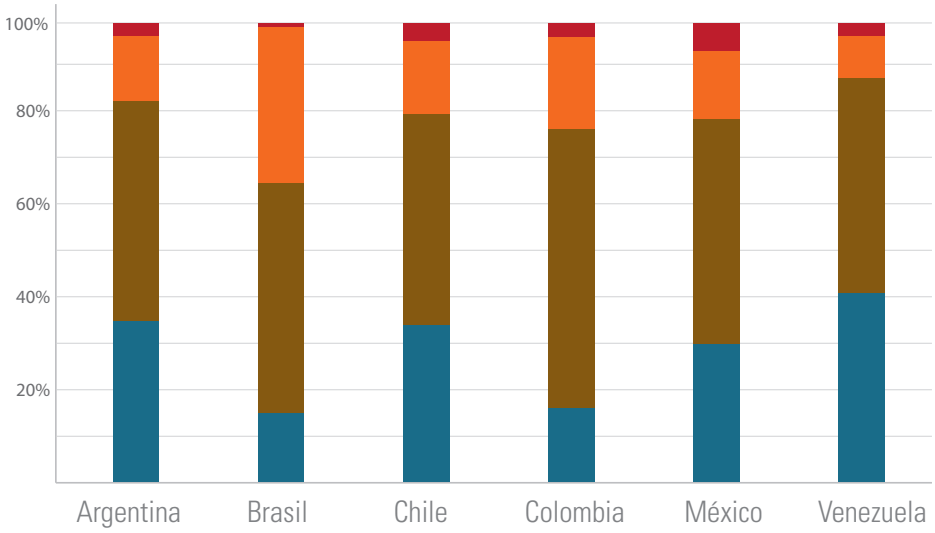
	Arg	Bra	Chi	Col	Mex	Vnz
No lo es	1%	0%	3%	0%	1%	0%
Baja	9%	3%	7%	6%	10%	3%
Moderada	44%	22%	30%	41%	31%	39%
Bastante Alta	31%	29%	38%	27%	35%	37%
Muy Alta	15%	46%	22%	26%	23%	21%



La gran mayoría de quienes respondieron a la encuesta confían en que sus organizaciones están bien protegidas, tanto en lo que se refiere a los problemas de seguridad internos como a los de origen externo.

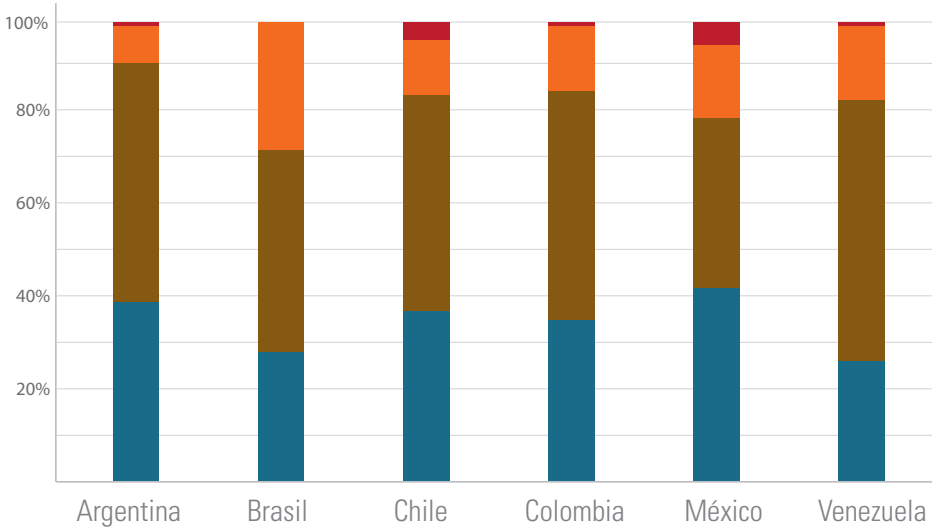
¿Cuánto confía usted en que su organización está protegida de amenazas internas a la Seguridad de la Información?

	Arg	Bra	Chi	Col	Mex	Vnz
Nada Seguro	3%	1%	4%	3%	6%	3%
No Muy Seguro	14%	34%	16%	20%	15%	9%
Algo Seguro	48%	50%	46%	61%	49%	47%
Muy Seguro	35%	15%	34%	16%	30%	41%



¿Cuánto confía usted en que su organización está bien protegida de las amenazas externas a la Seguridad de la Información?

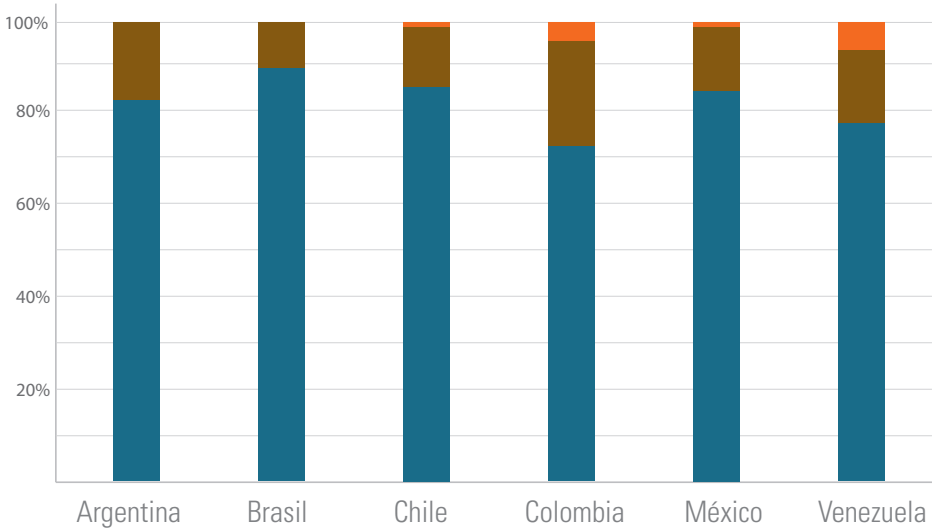
	Arg	Bra	Chi	Col	Mex	Vnz
Nada Seguro	1%	0%	4%	1%	5%	1%
No Muy Seguro	8%	28%	12%	14%	16%	16%
Algo Seguro	52%	44%	47%	50%	37%	57%
Muy Seguro	39%	28%	37%	35%	42%	26%



Los analistas hallaron que la mayoría de las compañías relevadas tienen establecidas prácticas estándares de políticas de seguridad.

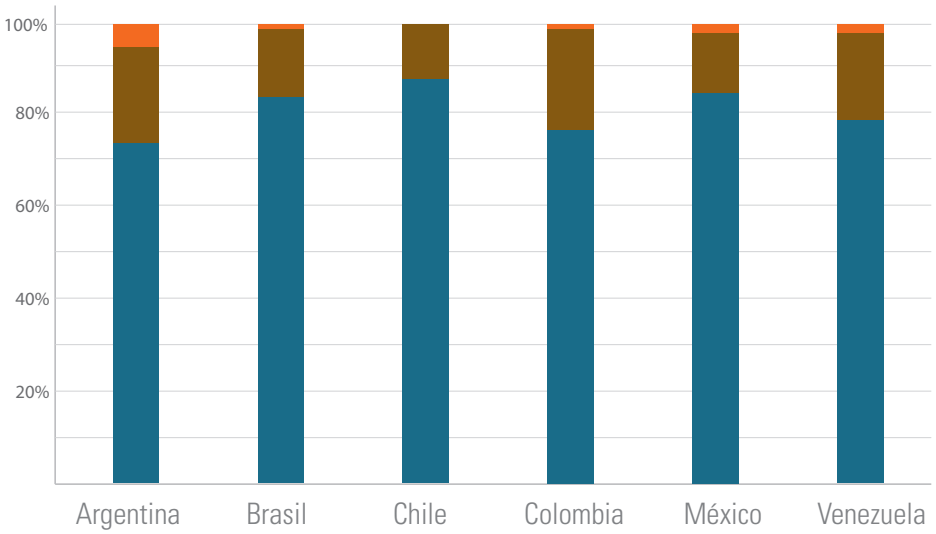
¿Su organización tiene instalados los requerimientos de seguridad necesarios para garantizar la continuidad del negocio a través de toda la organización?

	Arg	Bra	Chi	Col	Mex	Vnz
No es Seguro	0%	0%	1%	4%	1%	6%
No	17%	10%	13%	23%	14%	16%
Si	83%	90%	86%	73%	85%	75%



¿La política de continuidad del negocio dentro de su organización es sometida a revisión periódica, dentro de intervalos planificados?

	Arg	Bra	Chi	Col	Mex	Vnz
No Sabe	5%	1%	0%	1%	2%	2%
No	21%	15%	12%	22%	13%	19%
Si	74%	84%	88%	77%	85%	79%

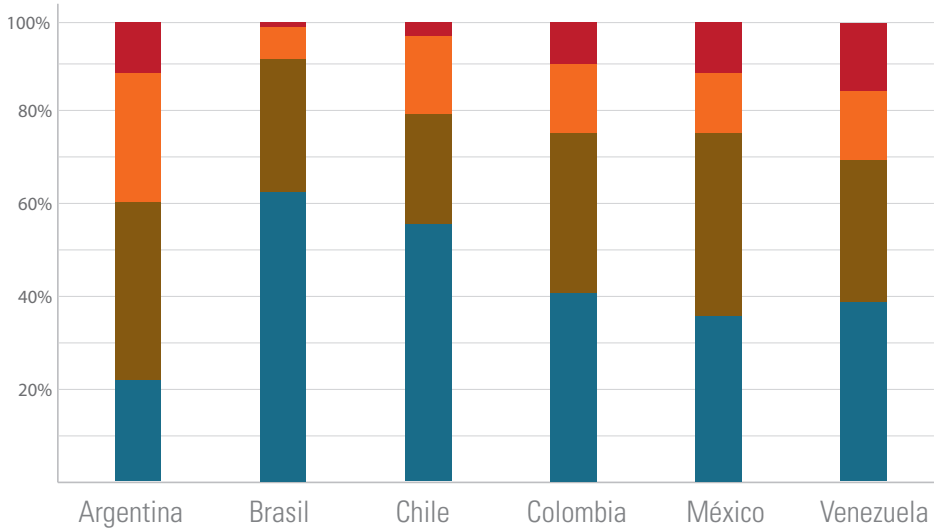


Lo que queda por mejorar

A pesar de que los ejecutivos encuestados indicaron tener altos niveles de confianza en cuanto a que sus compañías están bien protegidas contra las amenazas de seguridad provenientes del exterior, los gerentes IT también se mostraron preocupados por el riesgo que para la Seguridad de la Información pueden representar tanto los hackers como los ex empleados.

Niveles de preocupación en cuanto a las amenazas a la Seguridad de la Información en la empresa: hackers e intrusos

	Arg	Bra	Chi	Col	Mex	Vnz
Nada Preocupado	11%	1%	3%	9%	11%	15%
No Muy Preocupado	28%	7%	17%	15%	13%	15%
Algo Preocupado	39%	29%	24%	35%	40%	31%
Muy Preocupado	22%	63%	56%	41%	36%	39%



Aún cuando los gerentes de IT informaron tener instaladas aplicaciones para manejar el tema seguridad, por lo general no informan la existencia de problemas de seguridad a la administración a tiempo y cuando es necesario. Esto tiene efectos negativos para las compañías;

Los resultados obtenidos a través del sondeo muestran que las empresas más chicas tienden a tener menos y peores sistemas y aplicaciones de seguridad instalados, comparadas con las firmas grandes. Hay mucho trabajo por hacer dentro del segmento para concientizar a las Pequeñas y Medianas Empresas (PyMEs) acerca de la importancia que tiene el mantenimiento de la seguridad de su información y de sus datos más sensibles.

Metodología

Las entrevistas se llevaron a cabo entre el 23 de octubre y el 14 de diciembre de 2007, entre Jefes del área de Tecnologías de la Información, Jefes de Información de Seguridad, Directores de Administración de Sistemas de Información y Gerentes de Tecnologías de la Información.

Los principales sectores corporativos consultados fueron:

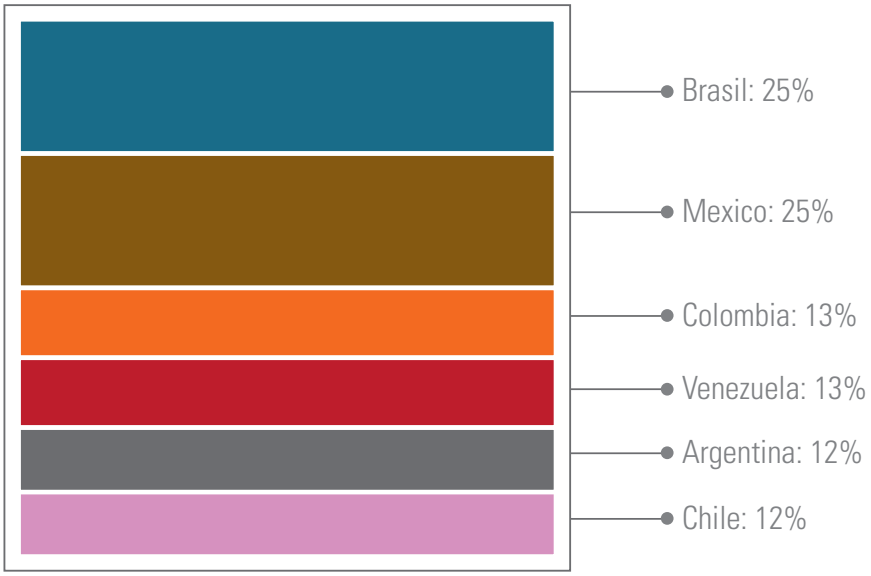
- Manufactura (40%)
- Servicios (10%)
- Finanzas/Seguros/Bienes raíces (10%)
- Comercios mayoristas (6%)
- Energía/Empresas de servicios públicos/ Petróleo (5%)
- Comercios al por menor (4%)
- Transporte (3%)
- Construcción (3%)
- Agricultura/ Pesca (3%)
- Cuidado de la salud (3%)

El puntaje del Index se ubica en el 0 (como la calificación mínima) y el 100 (como la máxima). Un puntuación perfecta de 100 representa los máximos niveles de implementación y compromiso con lo que podrían considerarse las mejores prácticas en lo que se refiere a políticas de Seguridad de la Información.

También representa las creencias de los gerentes de IT en cuanto a haber alcanzado las metas vinculadas con enfrentar los desafíos y las amenazas a la Seguridad de la Información.
Por el contrario, un puntaje de 0 refleja una falta total de adherencia a las prácticas de Seguridad de la Información generalmente aceptadas, y un reflejo de una posición totalmente alejada de la protección y la defensa contra las amenazas a la Seguridad de la Información en las organizaciones.

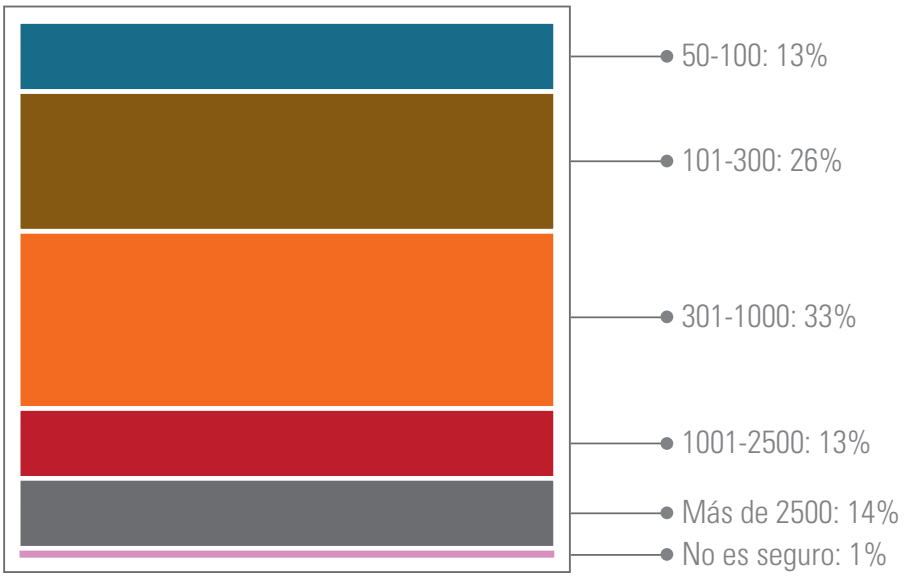
Los países en los cuales se realizó la encuesta fueron: Argentina, Brasil, Chile, Colombia, México y Venezuela.

Detalle por país



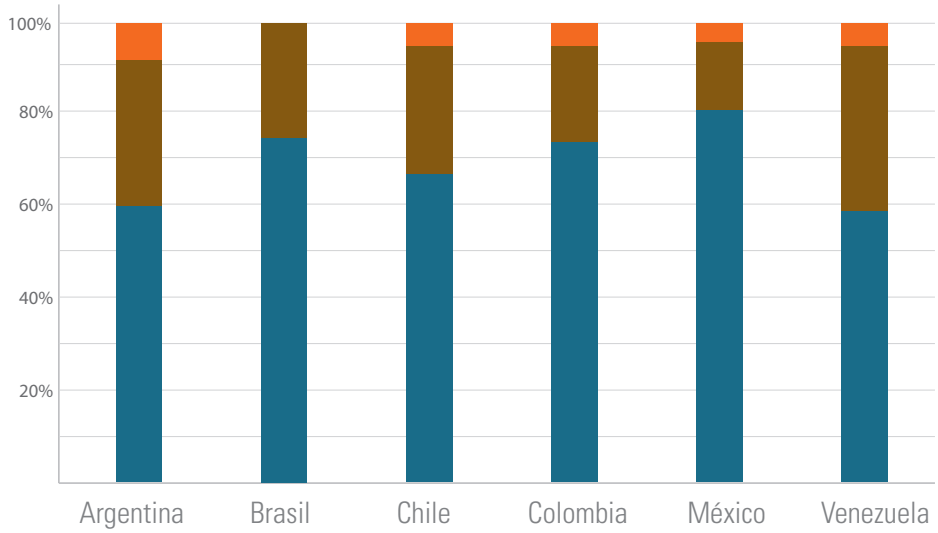
Un tercio de los especialistas en IT entrevistados trabajan en empresas compuestas por entre 301 y 1.000 empleados, y la mayor parte de los encuestados se desempeñan en compañías nacionales (con la Argentina y Venezuela captando el mayor porcentaje de firmas de origen extranjero).

Cantidad de Empleados en las Organizaciones Encuestadas



Origen de las empresas encuestadas

	Arg	Bra	Chi	Col	Mex	Vnz
Compañias "Indigenous"	8%	0%	5%	5%	4%	5%
Owned	32%	25%	28%	21%	15%	36%
Compañía Nacional	60%	75%	67%	74%	81%	59%



Los puntos de la investigación fueron:

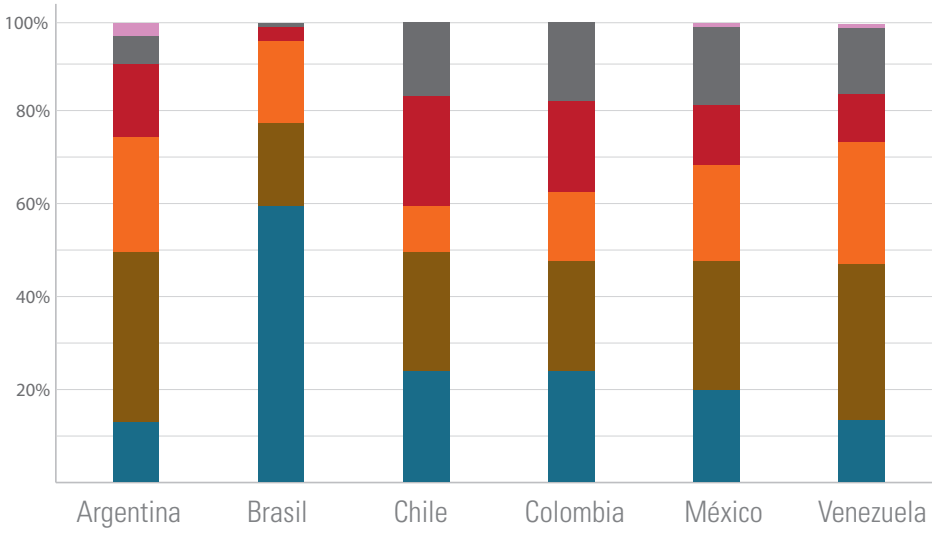
- Cambios en lo que respecta a los riesgos para la seguridad a través del tiempo;
- Políticas de seguridad corporativa;
- Evaluación y tratamiento del riesgo;
- Políticas de control de accesos;
- Gestión de la continuidad del negocio;
- Procedimientos de cumplimiento de políticas;
- Manejo de las comunicaciones y de las operaciones;
- Administración de los incidentes en Seguridad de la Información;
- Protocolos para la gestión de los activos;
- Adquisición, desarrollo y mantenimiento de los sistemas de información;
- Seguridad física y ambiental;
- Organización de la Seguridad de la Información;
- Integración de la Seguridad de la Información

Generalidades de la Situación

En los últimos 3 años, la mayoría de los gerentes de IT del Brasil (60%) han visto un "gran incremento" de los riesgos a la Seguridad de la Información en sus organizaciones; en otros países, los cambios han sido descriptos con menor dramatismo, con alrededor de la mitad de los encuestados afirmando que los riesgos se habían incrementado "un tanto" durante ese lapso de tiempo.

¿Cómo se modificaron los riesgos a la Seguridad de la Información en los últimos tres años?

	Arg	Bra	Chi	Col	Mex	Vnz
Otro /No Sabe	3%	0%	0%	0%	1%	1%
Gran Disminución	6%	1%	16%	17%	17%	14%
Disminución Moderada	16%	3%	24%	20%	13%	10%
Sin Modificaciones	25%	18%	10%	15%	21%	26%
Aumento Moderado	37%	18%	26%	24%	28%	33%
Gran Aumento	13%	60%	24%	24%	20%	16%

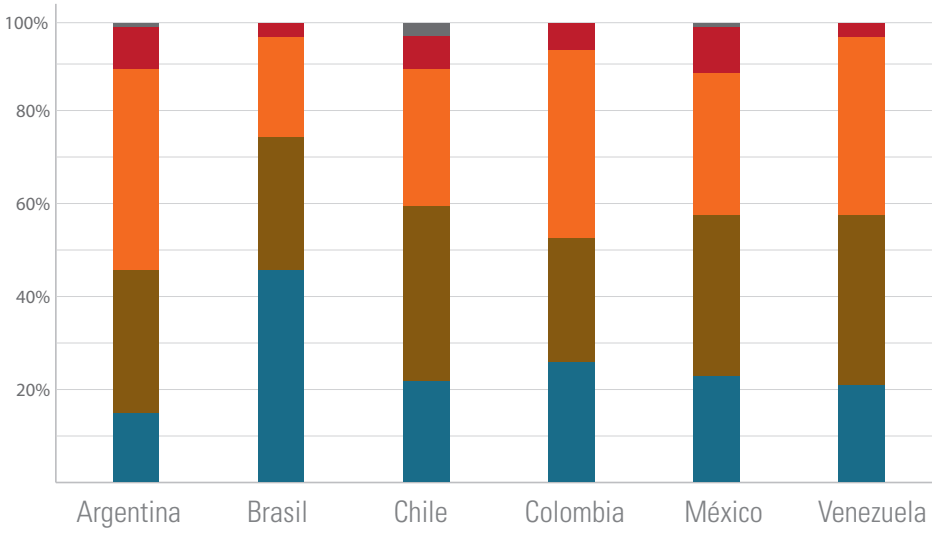


De acuerdo con los especialistas en IT, la alta gerencia de las corporaciones brasileñas es la que más se inclina a dar a la Seguridad de la Información una alta prioridad, contrariamente a lo que sucede en las altas administraciones de la Argentina, que le otorgan menos importancia.

En los casos en los que los riesgos a la Seguridad Informática fueron considerados como muy numerosos en los últimos años, la seguridad tendió a incrementar su importancia en cuanto a prioridades.

¿Cuán prioritaria es para su alta gerencia la Seguridad de la Información?

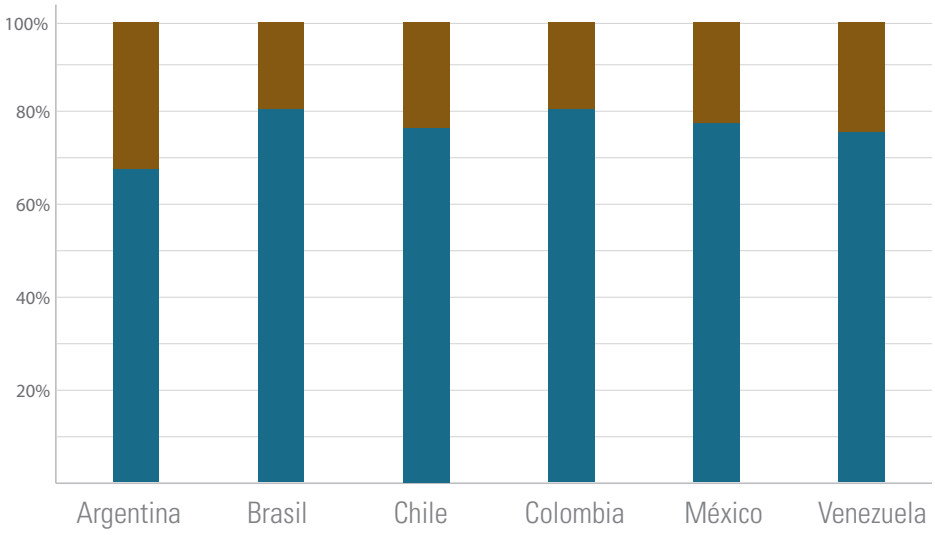
	Arg	Bra	Chi	Col	Mex	Vnz
No es	1%	0%	3%	0%	1%	0%
Baja	9%	3%	7%	6%	10%	3%
Moderada	44%	22%	30%	41%	31%	39%
Bastante Alta	31%	29%	38%	27%	35%	37%
Muy Alta	15%	46%	22%	26%	23%	21%



La existencia de una política de seguridad aprobada por una administración oficial es una práctica estándar en la mayoría de las empresas encuestadas, y cuanta más importancia le otorgan a la Seguridad de la Información los altos niveles directivos mayores posibilidades hay de que dichas políticas sean cumplidas en tiempo y forma.

¿Su compañía tiene una política de seguridad aprobada oficialmente?

	Arg	Bra	Chi	Col	Mex	Vnz
No	32%	19%	23%	19	22%	24%
Si	68%	81%	77%	81%	78%	16%



Los encuestados en Brasil (68%) y México (61%) son los que más se inclinan a trabajar en compañías en las cuales las Políticas de Seguridad son aprobadas a nivel del Consejo de Administración.

Dichas políticas son menos propensas a ser aprobadas a nivel de Consejo de Administración en Colombia, donde más de un tercio de los especialistas en IT describieron esta situación (35%).

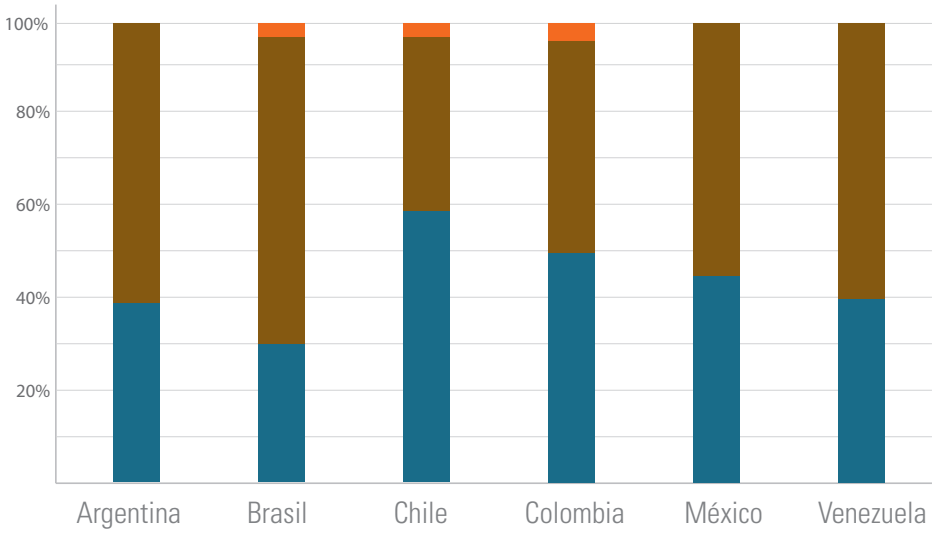
Cuando el área de gerencia da prioridad a la Seguridad de la Información, las empresas tienden en mayor medida a medir sus costos.

¿Cuán cercana es la relación de las políticas de Seguridad de la Información con el Consejo de Administración de su empresa?

La política de Seguridad de la Información está...	Arg	Bra	Chi	Col	Mex	Vnz
Aprobada a nivel del directorio	53%	68%	52%	38%	61%	56%
En proceso de ser aprobada por el directorio	6%	6%	7%	6%	11%	7%
Formalmente aprobada pero no a nivel del directorio	14%	23%	20%	18%	14%	18%
No aprobada a nivel del directorio	27%	2%	19%	35%	13%	19%
No sabe - no contesta	0%	1%	2%	3%	1%	0%

Las organizaciones chilenas lideran el terreno de la medición formal de los costos de seguridad en sus negocios (59%), seguidos por Colombia (50%). Como contrapartida, las empresas brasileñas son las que menos se inclinan por las métricas de costos (30%).

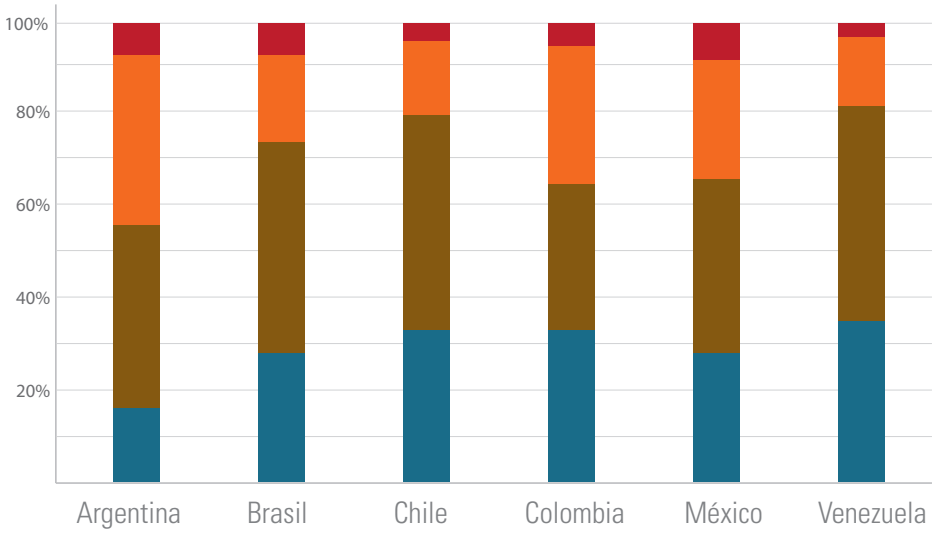
¿Su organización mide el costo total que le representa la Seguridad de la Información?



	Arg	Bra	Chi	Col	Mex	Vnz
No Sabe	0%	3%	3%	4%	0%	0%
No	61%	67%	38%	46%	55%	60%
Sí	39%	30%	59%	50%	45%	40%

La mayoría de los dirigentes de IT en todos los países consideran que el nivel de amenaza representado por los ataques de virus es serio, con Chile y Colombia como las naciones donde más preocupación se registra.

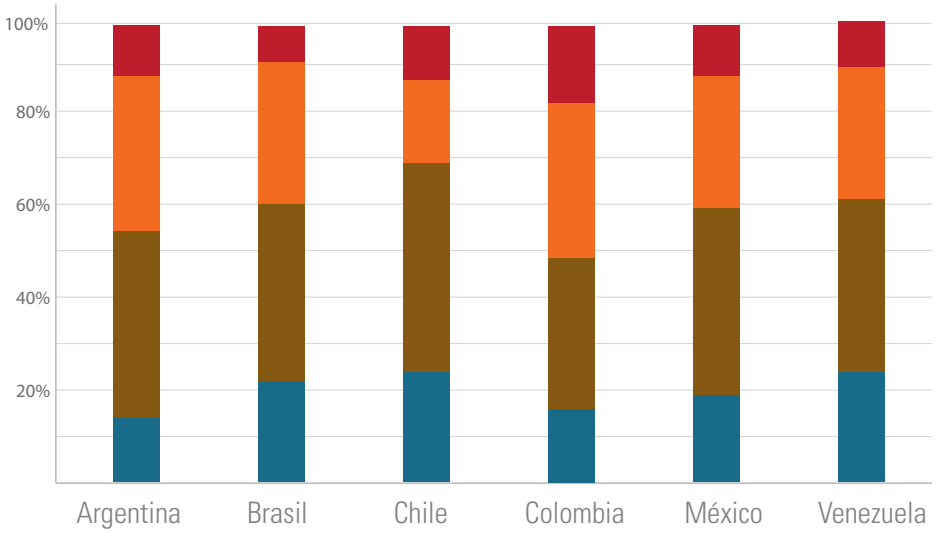
Nivel actual de amenazas: virus o gusanos



	Arg	Bra	Chi	Col	Mex	Vnz
No Sabe	7%	7%	4%	5%	8%	3%
Moderadamente Serio	37%	19%	16%	30%	26%	15%
Muy Serio	40%	46%	47%	32%	38%	47%
Extremadamente Serio	16%	28%	33%	33%	28%	35%

Los chilenos son, también, quienes más se preocupan por el peligro que representan el spyware y el malware.

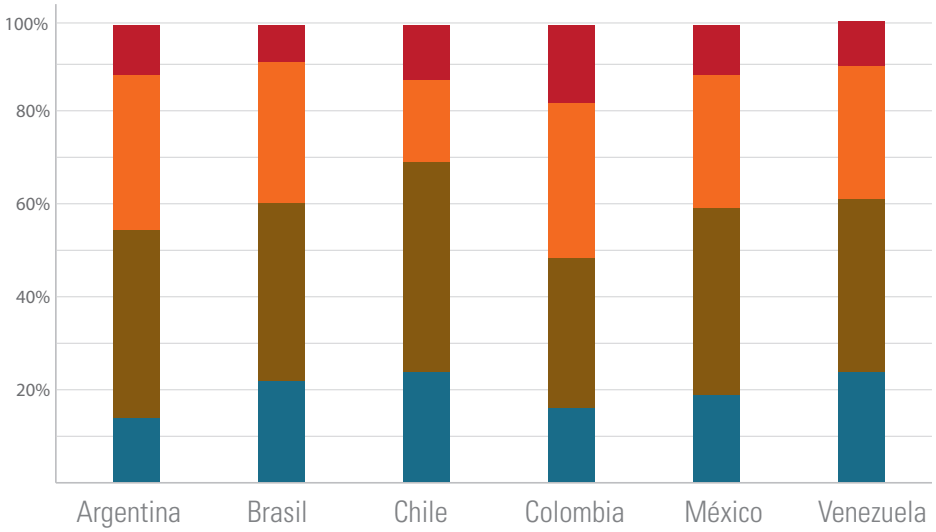
Nivel actual de amenazas: Spyware / malware



	Arg	Bra	Chi	Col	Mex	Vnz
Ninguno	11%	8%	12%	17%	11%	10%
Moderadamente Serio	34%	31%	18%	34%	29%	29%
Muy Serio	41%	39%	46%	33%	41%	38%
Extremadamente Serio	14%	22%	24%	16%	19%	24%

Por su parte, el riesgo del robo de datos de clientes es percibido con mayor fuerza en el Brasil (donde el 74% de los encuestados lo considera como “extremadamente“ o “muy severamente“ riesgoso), seguido por Chile (64%) y Venezuela (57%)

Nivel actual de amenazas: Robo de datos de clientes desde el exterior

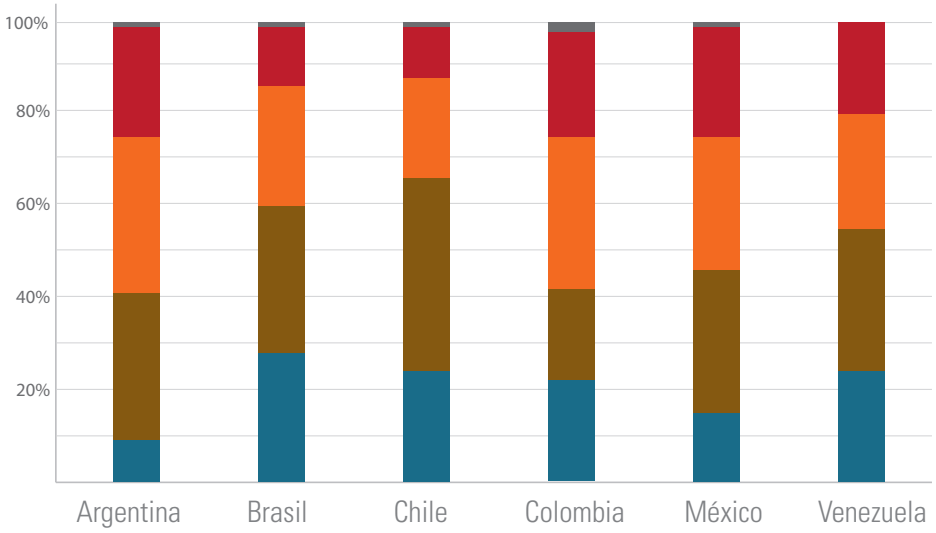


	Arg	Bra	Chi	Col	Mex	Vnz
Ninguno	20%	10%	11%	16%	19%	16%
Moderadamente Serio	25%	16%	25%	35%	27%	27%
Muy Serio	31%	40%	35%	28%	37%	33%
Extremadamente Serio	24%	34%	29%	21%	17%	24%

Dichos tres países también mostraron una tendencia a ver a considerar como amenazas serias a los botnets, al phishing, al pharming, a la violación de datos de empleados, a los ataques contra las redes y a la pérdida de datos móviles.

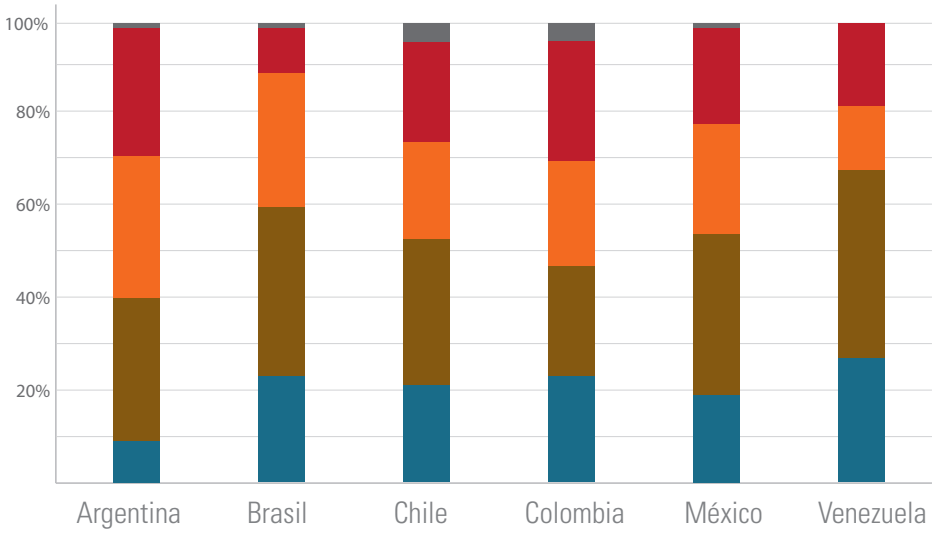
Nivel actual de amenazas: Botnets que toman un control remoto de los recursos de IT

	Arg	Bra	Chi	Col	Mex	Vnz
No Sabe	1%	1%	1%	2%	1%	0%
Ninguno	24%	13%	11%	23%	24%	20%
Moderadamente Serio	34%	26%	22%	33%	29%	25%
Muy Serio	32%	32%	42%	20%	31%	31%
Extremadamente Serio	9%	28%	24%	22%	15%	24%



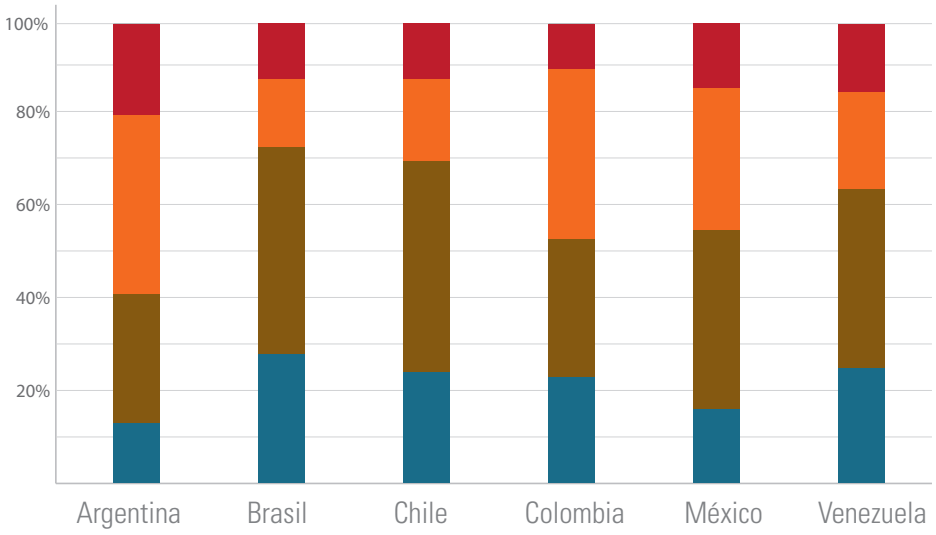
Nivel actual de amenazas: Phishing / Pharming

	Arg	Bra	Chi	Col	Mex	Vnz
No Sabe	1%	1%	4%	4%	1%	0%
Ninguno	28%	10%	22%	26%	21%	18%
Moderadamente Serio	31%	29%	21%	23%	24%	14%
Muy Serio	31%	37%	32%	24%	35%	41%
Extremadamente Serio	9%	23%	21%	23%	19%	27%



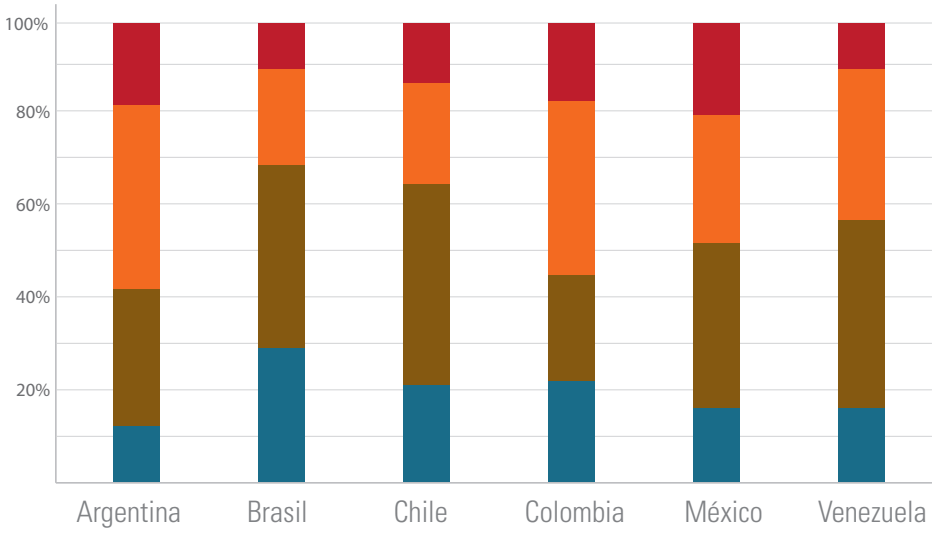
Nivel actual de amenazas: Acceso no autorizado de los empleados a archivos y/o datos

	Arg	Bra	Chi	Col	Mex	Vnz
Ninguno	20%	12%	12%	10%	14%	15%
Moderadamente Serio	39%	15%	18%	37%	31%	21%
Muy Serio	28%	45%	46%	30%	39%	39%
Extremadamente Serio	13%	28%	24%	23%	16%	25%



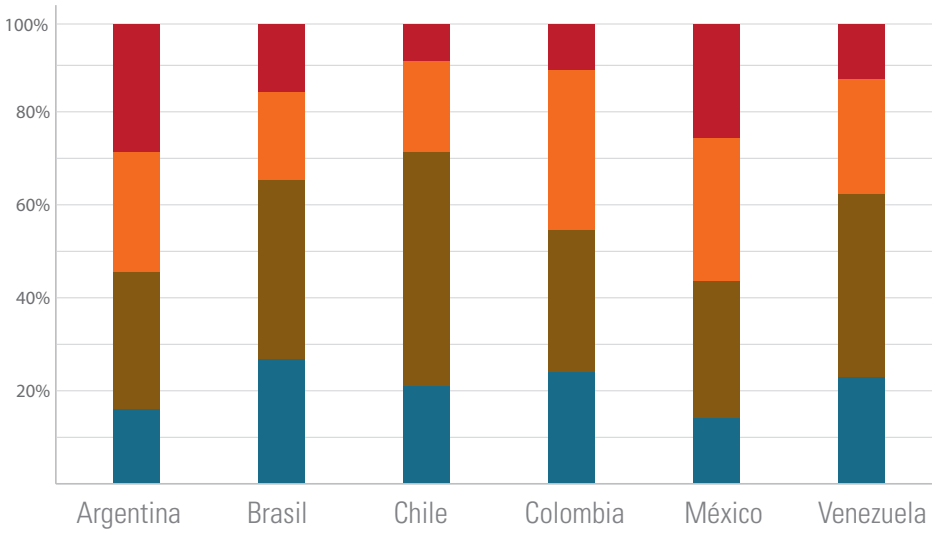
Nivel actual de amenazas: Ataques de denegación de servicio u otro tipo de ataques a las redes

	Arg	Bra	Chi	Col	Mex	Vnz
Ninguno	18%	10%	13%	17%	20%	10%
Moderadamente Serio	40%	21%	22%	38%	28%	33%
Muy Serio	30%	40%	44%	23%	36%	41%
Extremadamente Serio	12%	29%	21%	22%	16%	16%



Nivel Actual de Amenazas: Pérdida o robo de dispositivos móviles con contenido corporativo

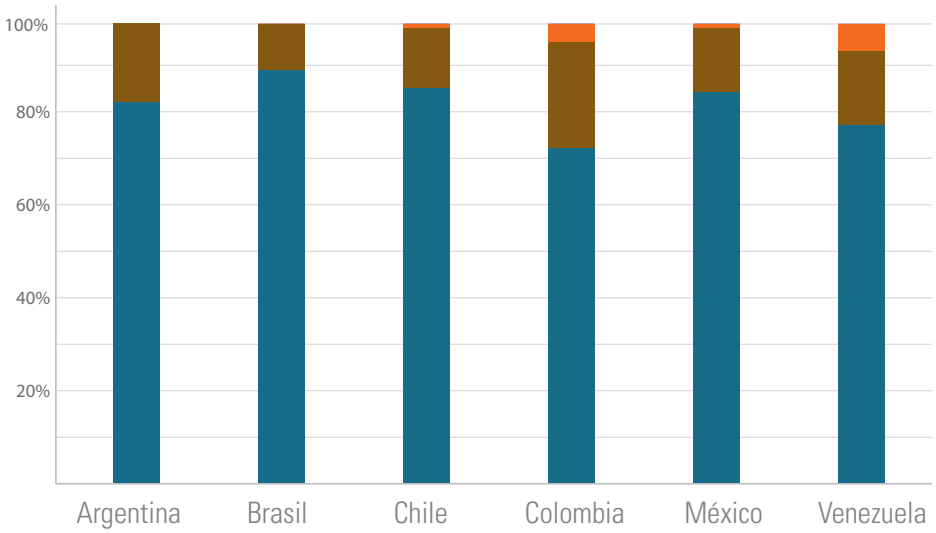
	Arg	Bra	Chi	Col	Mex	Vnz
Ninguno	28%	15%	8%	10%	25%	12%
Moderadamente Serio	26%	19%	20%	35%	31%	25%
Muy Serio	30%	39%	51%	31%	30%	40%
Extremadamente Serio	16%	27%	21%	24%	14%	23%



La gran mayoría de las empresas en todos los países encuestados tienen instalados requerimientos de Seguridad de la Información para mantener la continuidad del negocio, y dichas políticas son repasadas y revisadas a intervalos planificados y establecidos.

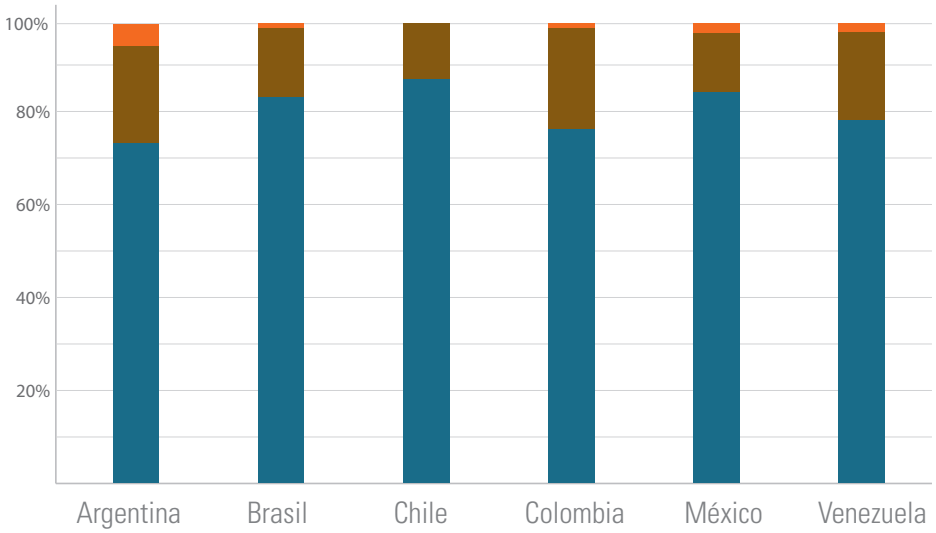
¿Su organización tiene instalado un proceso que cumpla los requerimientos de Seguridad de la Información necesarios para mantener en pie la continuidad del negocio?

	Arg	Bra	Chi	Col	Mex	Vnz
No Sabe	0%	0%	1%	4%	1%	6%
No	17%	10%	13%	23%	14%	16%
Sí	83%	90%	86%	73%	85%	78%



¿La política de administración de la continuidad de los negocios en su organización está sujeta a revisión a intervalos planificados?

	Arg	Bra	Chi	Col	Mex	Vnz
No Sabe	5%	1%	0%	1%	2%	2%
No	21%	15%	12%	22%	13%	19%
Si	74%	84%	88%	77%	85%	79%

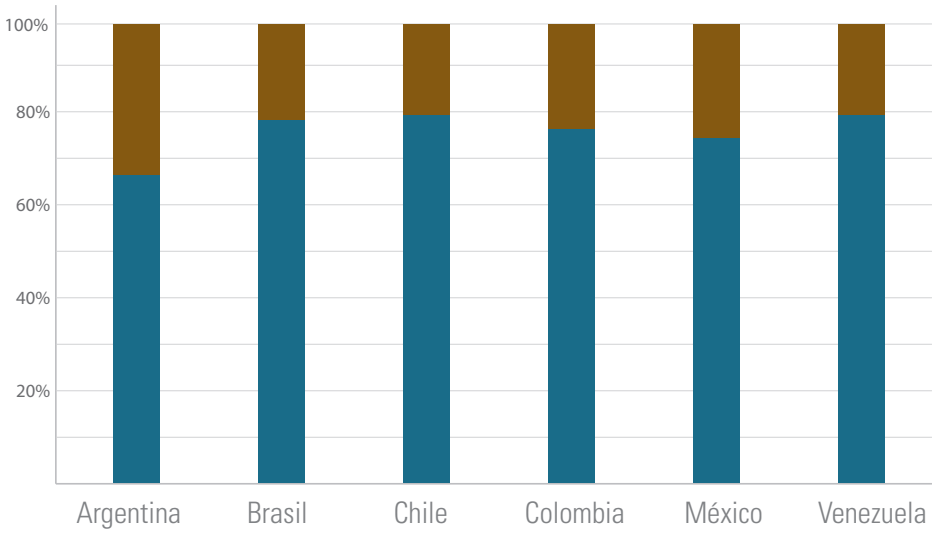


De país en país, los sondeados consideran que el software de control de acceso a las computadoras, las contraseñas múltiples, las passwords para múltiples aplicaciones y las claves no estáticas, están teniendo un uso más expandido.

La autenticación de usuarios por medio de la biometría no está siendo utilizada en la mayoría de las organizaciones, pero su mayor penetración se ve en compañías de Venezuela (43%) y México (40%).

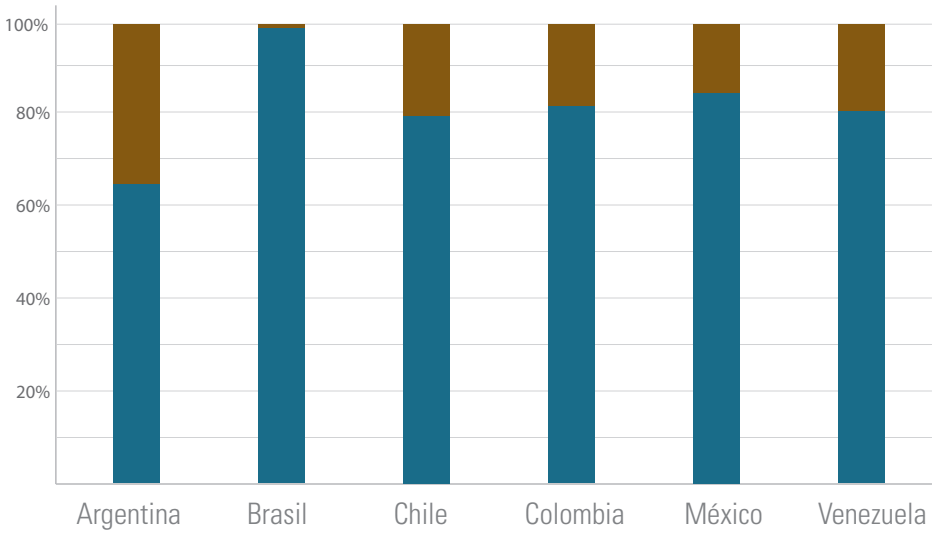
Herramientas actualmente utilizadas para proteger la seguridad de la Información: software de control de acceso a la PC

	Arg	Bra	Chi	Col	Mex	Vnz
No	33%	21%	20%	23%	25%	20%
Si	67%	79%	80%	77%	75%	80%



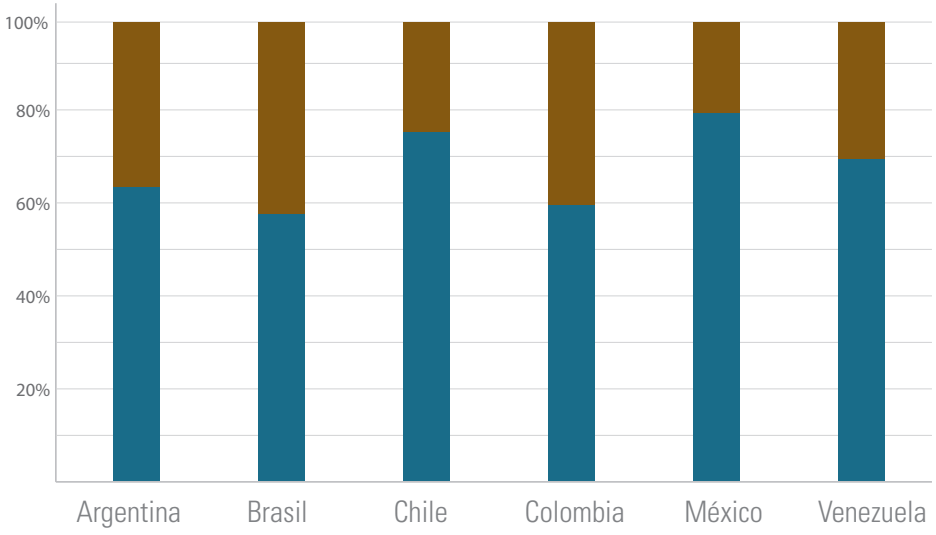
Herramientas actualmente utilizadas para proteger la Seguridad de la Información: Uso de múltiples passwords y claves

	Arg	Bra	Chi	Col	Mex	Vnz
No	35%	1%	20%	18%	15%	19
Si	65%	99%	80%	82%	85%	81%



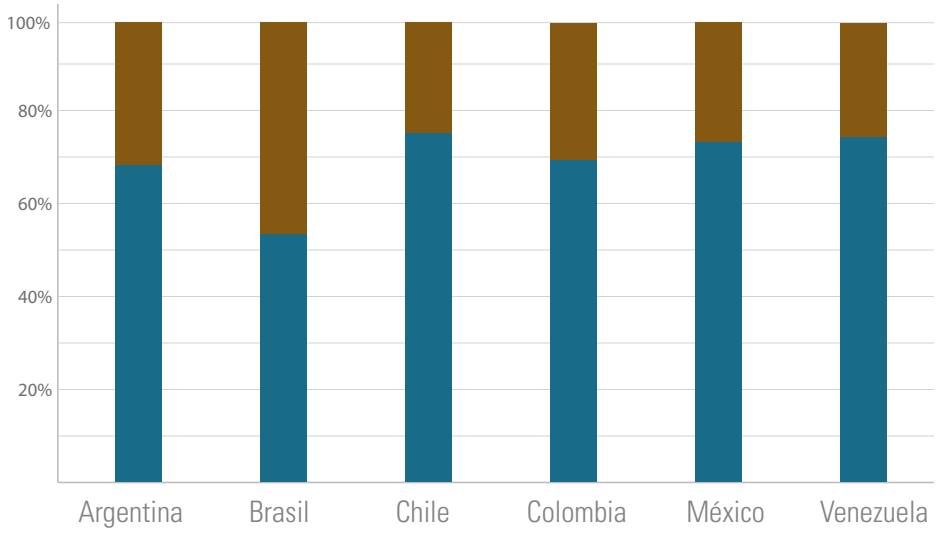
Herramientas actualmente utilizadas para proteger la Seguridad de la Información: Claves únicas o simplificadas para usar en múltiples aplicaciones

	Arg	Bra	Chi	Col	Mex	Vnz
No	36%	42%	24%	40%	20%	30%
Si	64%	58%	76%	60%	80%	70%



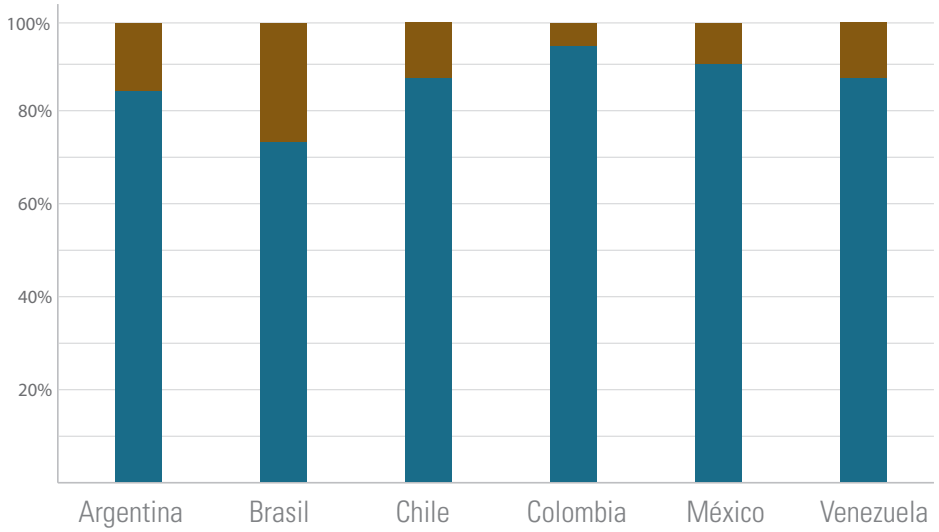
Herramientas actualmente utilizadas para proteger la Seguridad de la Información: Passwords de única vez / llaves de acceso / tarjetas inteligentes

	Arg	Bra	Chi	Col	Mex	Vnz
No	31%	46%	24%	30%	26%	25%
Si	69%	54%	76%	70%	74%	75%



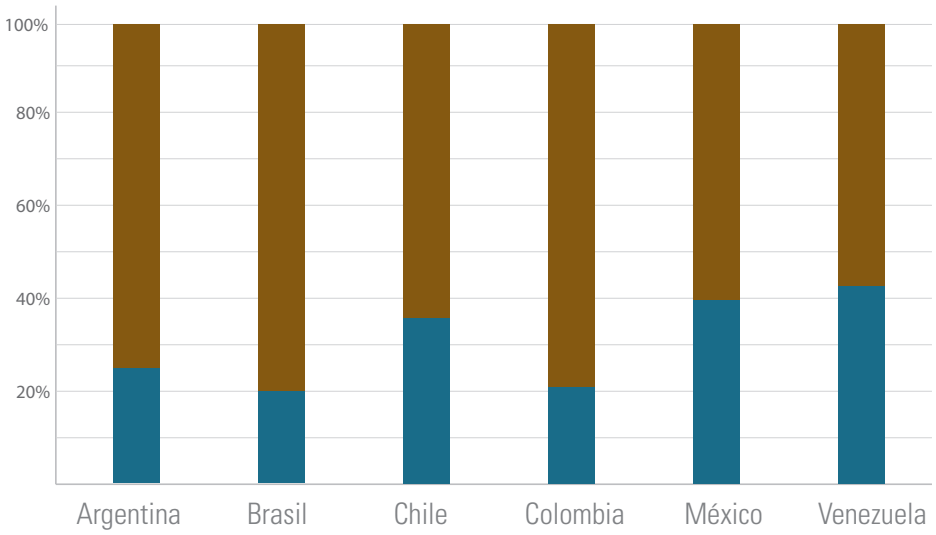
Herramientas actualmente utilizadas para proteger la Seguridad de la Información: Control de acceso basado en roles

	Arg	Bra	Chi	Col	Mex	Vnz
No	15%	26%	12%	5%	9%	12%
Si	85%	74%	88%	95%	91%	88%



Herramientas actualmente utilizadas para proteger la Seguridad de la Información: Autenticación de usuario a través de Biometría

	Arg	Bra	Chi	Col	Mex	Vnz
No	75%	80%	64%	79%	60%	57%
Si	25%	20%	36%	21%	40%	43%

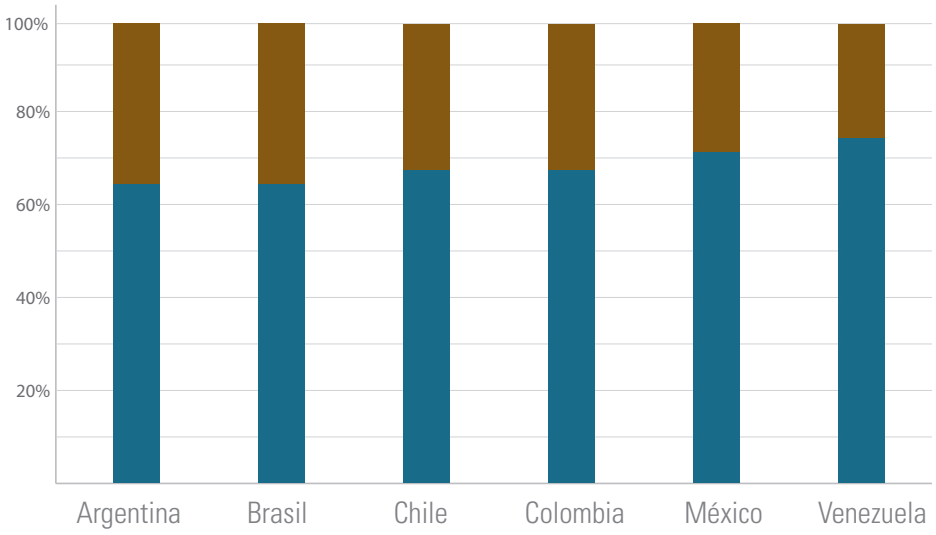


Los gerentes de IT de la Argentina (44%), Venezuela (43%) y México (40%) son los más propensos a asignarle una "A" a los actuales esfuerzos de sus organizaciones por recuperar información esencial en caso de fallas del sistema.

En la mayoría de las organizaciones consultadas en cada país hay (al menos en teoría), procedimientos para que los equipos de IT informen las posibles vulnerabilidades a la seguridad. Brasil está a la cabeza en cuanto a reportar más frecuentemente los problemas a la Seguridad de Información a la gerencia, mientras que México y Venezuela señalan ampliamente que dichos problemas son notificados "raramente" o "nunca".

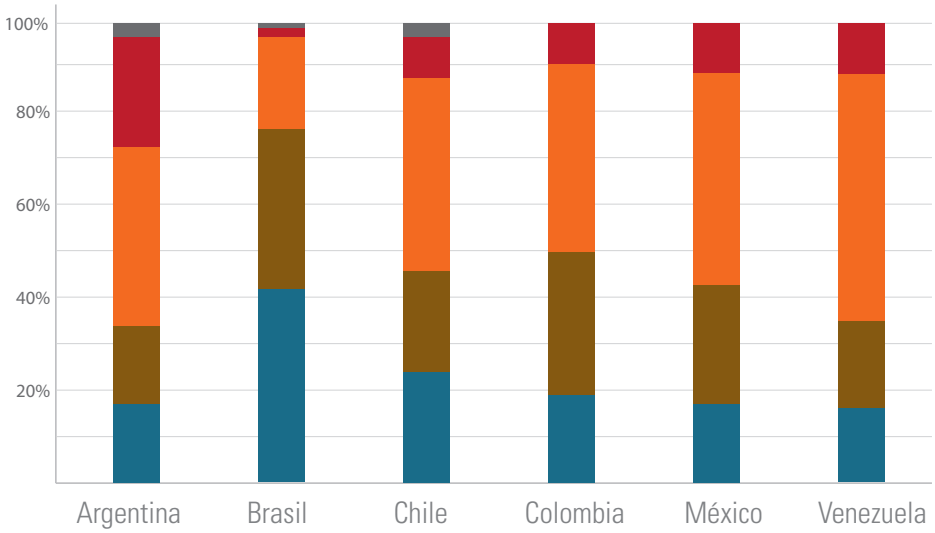
¿Poseen ustedes algún procedimiento para asegurar que todo el personal de sistemas de la información informe posibles falencias a la Seguridad de la Información?

	Arg	Bra	Chi	Col	Mex	Vnz
No	35%	35%	32%	32%	28%	25%
Si	65%	65%	68%	68%	72%	75%



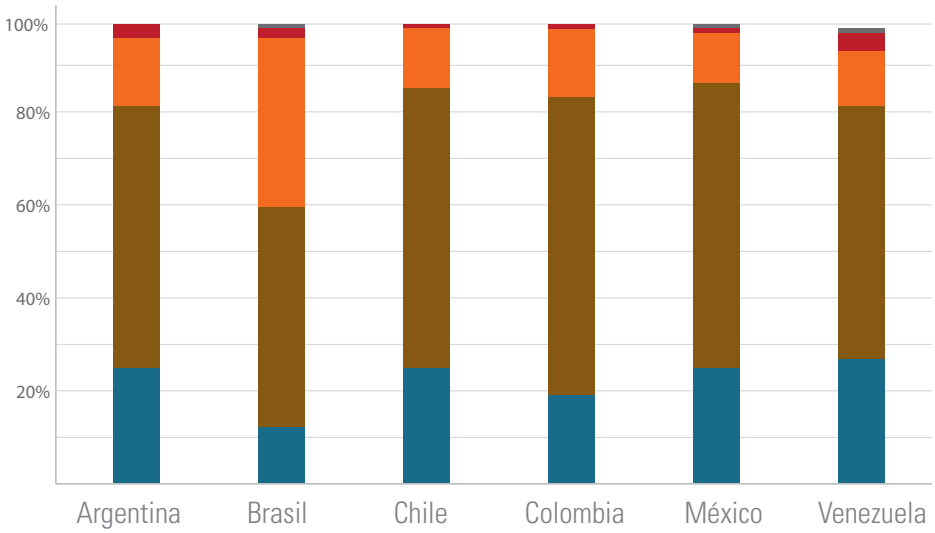
¿Cuán frecuentemente los problemas a la Seguridad de la Información son informados a la gerencia en el momento oportuno?

	Arg	Bra	Chi	Col	Mex	Vnz
No Sabe	3%	1%	3%	0%	0%	0%
Nunca	24%	2%	9%	9%	11%	11%
Rara Vez	39%	20%	42%	41%	46%	54%
A Veces	17%	35%	22%	31%	26%	19%
Siempre	17%	42%	24%	19%	17%	16%



¿Cómo calificaría usted la respuesta general de la organización y su capacidad de recuperación cuando se aplican esfuerzos de control de daños ante incidentes que afectan a la Seguridad de la Información?

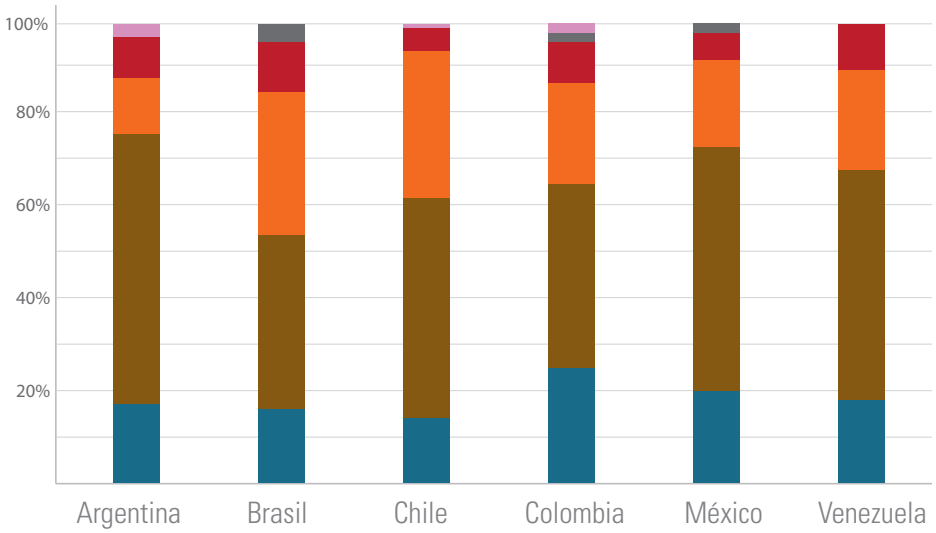
	Arg	Bra	Chi	Col	Mex	Vnz
No Sabe	3%	1%	0%	0%	1%	1%
Pobre	0%	2%	1%	1%	1%	4%
Justa	15%	37%	13%	15%	11%	13%
Bueno	57%	48%	61%	65%	62%	55%
Excelente	25%	12%	25%	19%	25%	27%



Los esfuerzos por documentar, mantener y hacer accesibles los procedimientos operativos ante riesgos han sido evaluados como “buenos” o “excelentes” por la mayoría de los encuestados en cada país. Los puntajes más negativos correspondieron a Brasil y a Chile.

Grados organizacionales: Tenemos procedimientos operativos documentados que están a disposición de todos los usuarios que los necesiten

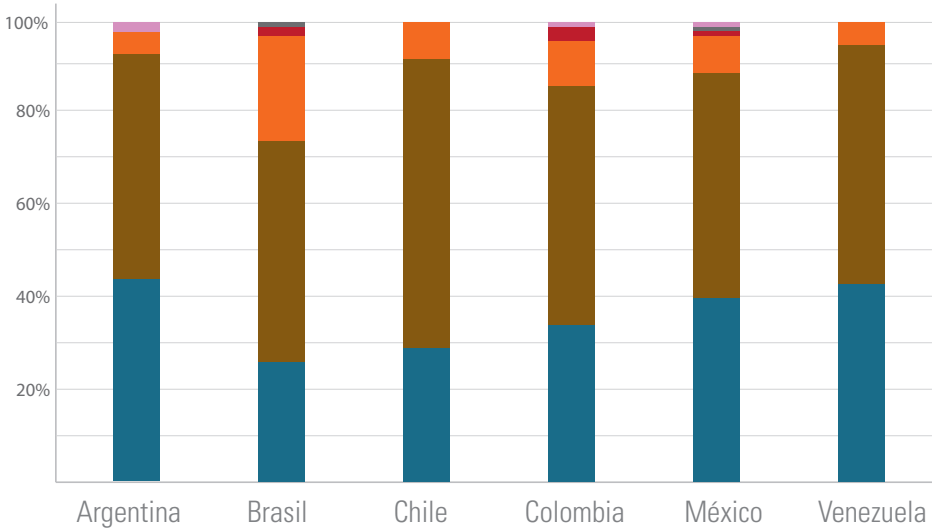
	Arg	Bra	Chi	Col	Mex	Vnz
No Sabe	3%	0%	1%	2%	0%	0%
F	0%	4%	0%	2%	2%	0%
D	9%	11%	5%	9%	6%	10%
C	12%	31%	32%	22%	19%	22%
B	59%	38%	48%	40%	53%	50%
A	17%	16%	14%	25%	20%	18%



Los gerentes de IT de la Argentina (44%), Venezuela (43%) y México (40%) son los que más se inclinan a asignarle una A a los esfuerzos de su organización para recuperar información esencial, en caso de fallas en el sistema.

Grados organizacionales: La información esencial y el software pueden ser recuperados luego de un desastre o de fallas en el sistema

	Arg	Bra	Chi	Col	Mex	Vnz
No Sabe	2%	0%	0%	1%	1%	0%
F	0%	1%	0%	0%	1%	0%
D	0%	2%	0%	3%	1%	0%
C	5%	23%	8%	10%	8%	5%
B	49%	48%	63%	52%	49%	52%
A	44%	26%	29%	34%	40%	43%

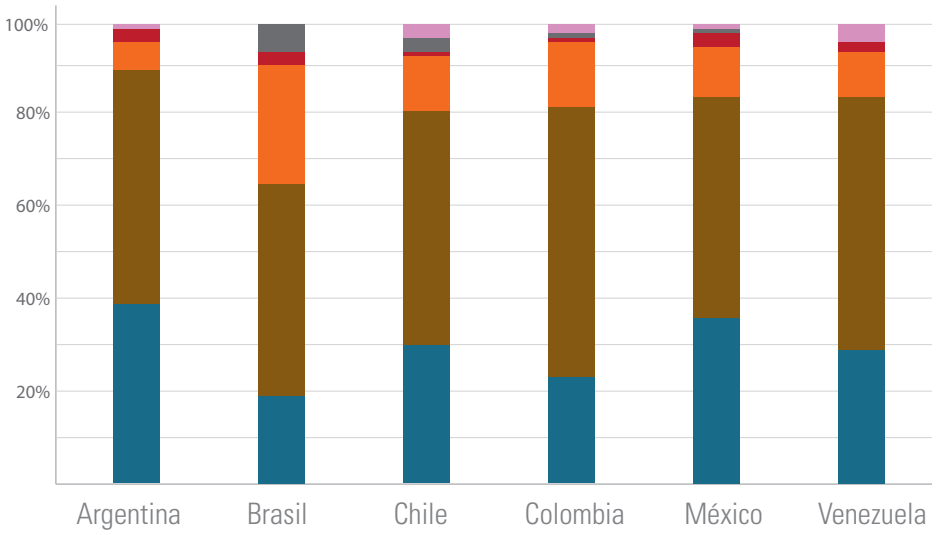


La gran mayoría de los encuestados en cada país le otorga altas calificaciones a la protección de la información del comercio electrónico, con los ejecutivos brasileños como los menos benévolos en ese sentido.

La integración de la seguridad física con la IT es más frecuente en las compañías chilenas (80%) y brasileñas (77%), y bastante menos común entre las organizaciones argentinas (59%)

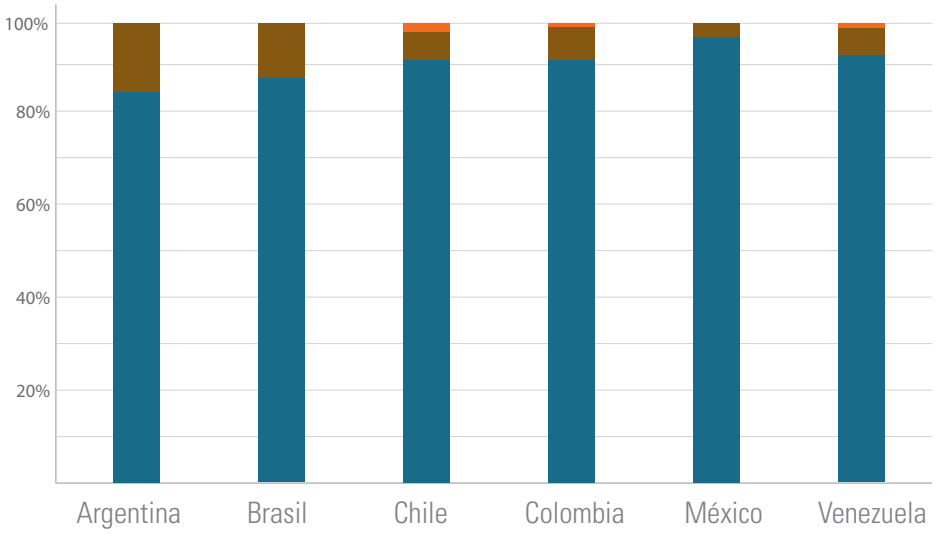
Grados organizacionales: Protección de la información procedente del comercio electrónico contra actividades fraudulentas y accesos o modificaciones no autorizados

	Arg	Bra	Chi	Col	Mex	Vnz
No Sabe	1%	0%	3%	2%	1%	4%
F	0%	6%	3%	1%	1%	0%
D	3%	3%	1%	1%	3%	2%
C	6%	26%	12%	14%	11%	10%
B	51%	46%	51%	59%	48%	55%
A	36%	19%	30%	23%	36%	29%



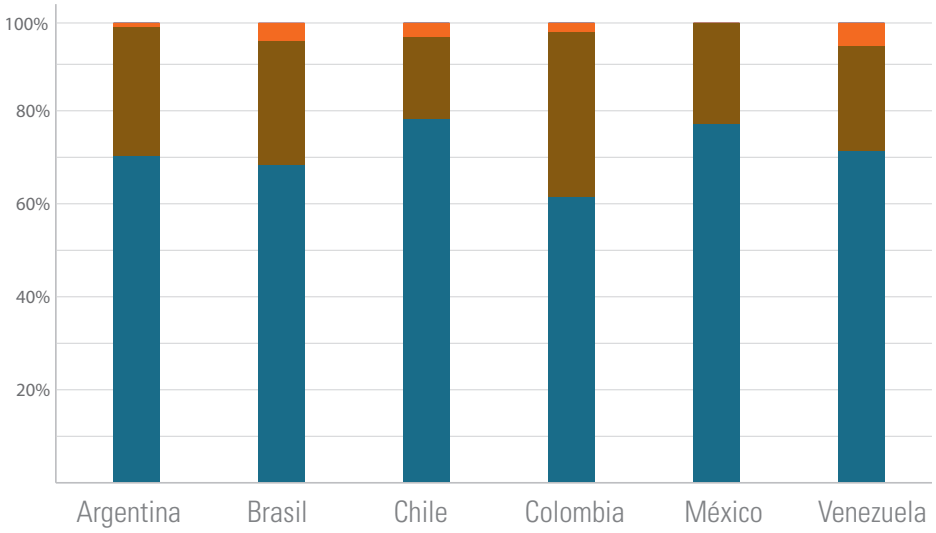
La identificación y el registro de los activos es una práctica estándar en casi todas las compañías, tales como el monitoreo y revisión de restricción de acceso a activos, y procedimientos de etiquetado de la información. Aún cuando los activos son clasificados en términos de valor, sensibilidad y importancia para la organización por la mayoría de las empresas en cada país, dicha práctica es menos común en Colombia, donde el 36% de los encuestados admitió que la rechaza.

Prácticas organizacionales de administración de activos: Todos los activos están identificados, y se mantiene un inventario o registro de los mismos



	Arg	Bra	Chi	Col	Mex	Vnz
No Sabe	0%	0%	2%	1%	0%	1%
No	15%	12%	6%	7%	3%	6%
Si	85%	88%	92%	92%	97%	93%

Prácticas organizacionales de administración de activos: Los activos son clasificados en términos de valor, sensibilidad e importancia para la organización



	Arg	Bra	Chi	Col	Mex	Vnz
No Sabe	1%	4%	3%	2%	0%	5%
No	28%	27%	18%	36%	22%	23%
Si	71%	69%	79%	62%	78%	72%

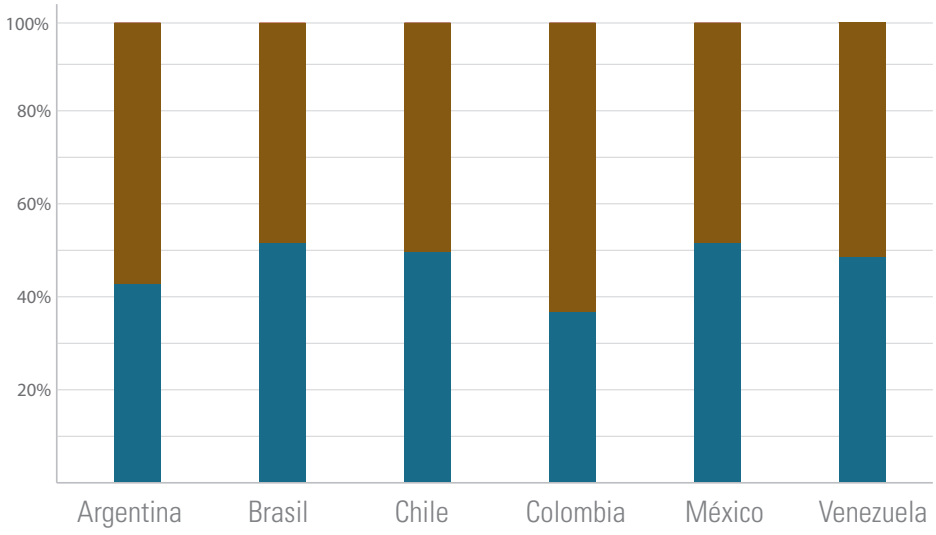
En promedio, menos de la mitad de las organización encuestadas cuentan hoy día con una política para el uso de controles criptográficos para la protección de la información. En ese sentido, Brasil y México, con el 52%, lideran la región.

Cuando la Seguridad de la Información es considerada como de alta prioridad por la alta gerencia, los controles criptográficos son mucho más comunes.

Cuando hay controles criptográficos en funcionamiento, los gerentes de IT califican, en su amplia mayoría, a dicha implementación como de altamente exitosa.

¿Su organización tiene una política acerca del uso de los controles criptográficos para la protección de la información?

	Arg	Bra	Chi	Col	Mex	Vnz
No	57%	48%	50%	63%	48%	51%
Si	43%	52%	50%	37%	52%	49%



Mediante la encuesta se ha podido observar en los diferentes países que los diversos ítems que conforman los controles físicos y ambientales han sido implementados por la mayoría de las organizaciones.

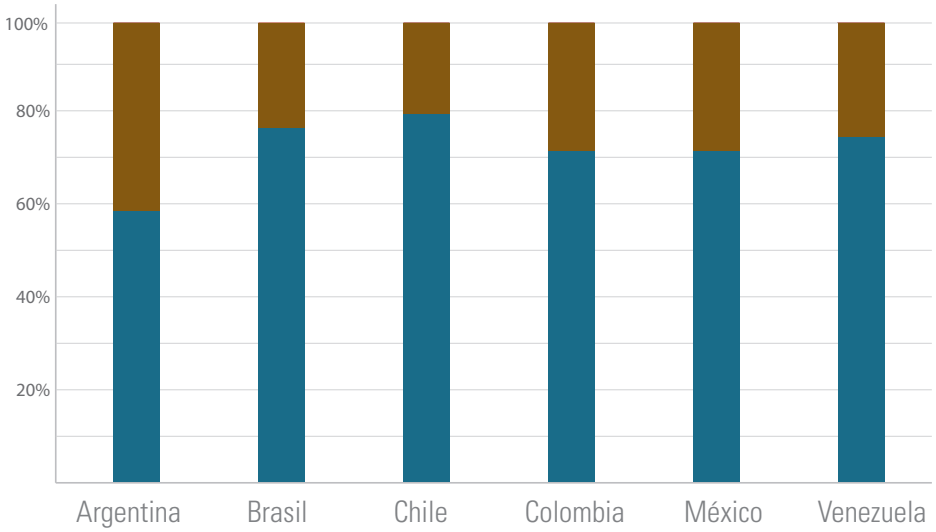
Cuando la amenaza potencial entra dentro de la seguridad física de borde, en los controles de entrada, la protección contra las riesgos ambientales o fallas en la provisión de energía, gran parte de las compañías tienen instaladas estrategias o políticas para asegurar sus activos críticos.

Servicios de procesamiento de la seguridad física de la información instalados en su organización

Acciones de Seguridad Física	Arg	Bra	Chi	Col	Mex	Vnz
Hemos implementado instalaciones de borde de seguridad física, tales como controles de entrada a puertas con tarjetas, paredes o áreas de recepción atendidas por personal	65%	65%	75%	74%	70%	78%
Controles de entrada accesibles sólo para personal autorizado dentro de diversas áreas de la organización	84%	86%	84%	72%	82%	79%
Las áreas con responsabilidad de procesamiento de la información tienen cabinas bajo llave o seguras	84%	72%	87%	84%	74%	84%
Se han instaurado políticas para proteger la información sensible de las amenazas ambientales tales como incendio, inundaciones o agitación civil	84%	72%	86%	84%	81%	78%
El equipamiento está protegido de las fallas energéticas y se instalaron fuentes de energía alternativas	88%	97%	87%	96%	88%	86%

La integración entre la seguridad física y la IT es más común en las empresas de Chile (80%) y del Brasil (77%), y menos frecuente entre las organizaciones argentinas (59%) Cuando la alta gerencia da prioridad a la Seguridad de la Información, dicha integración está más extendida como práctica.

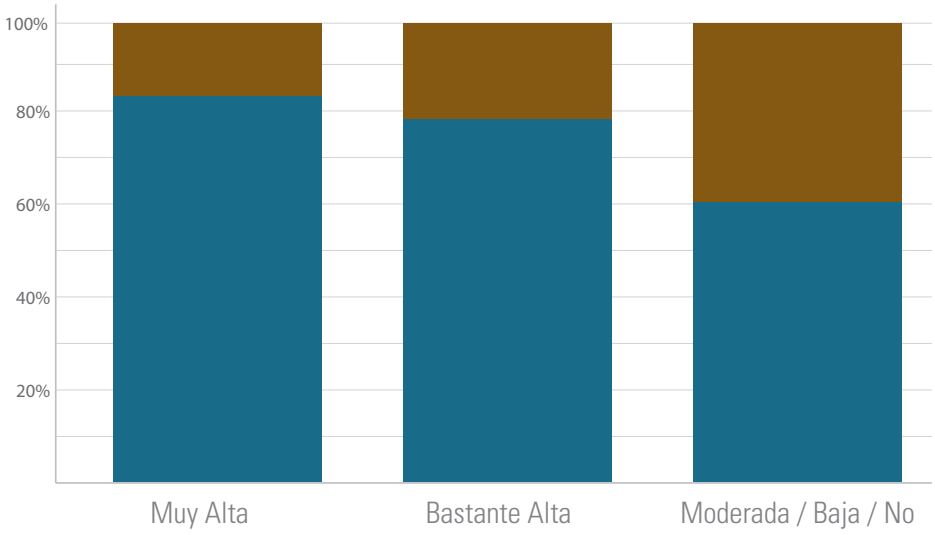
¿Está su compañía intentando integrar la seguridad física con el área de IT?



	Arg	Bra	Chi	Col	Mex	Vnz
No	41%	23%	20%	28%	28%	25%
Si	59%	77%	80%	72%	72%	75%

¿Está su compañía intentando integrar la seguridad física con el área de IT?

(Desde el punto de vista de la prioridad de la Seguridad de la Información para la alta gerencia)



	M. Alta	B. Alta	M/B/No
No	16%	21%	39%
Si	84%	79%	61%

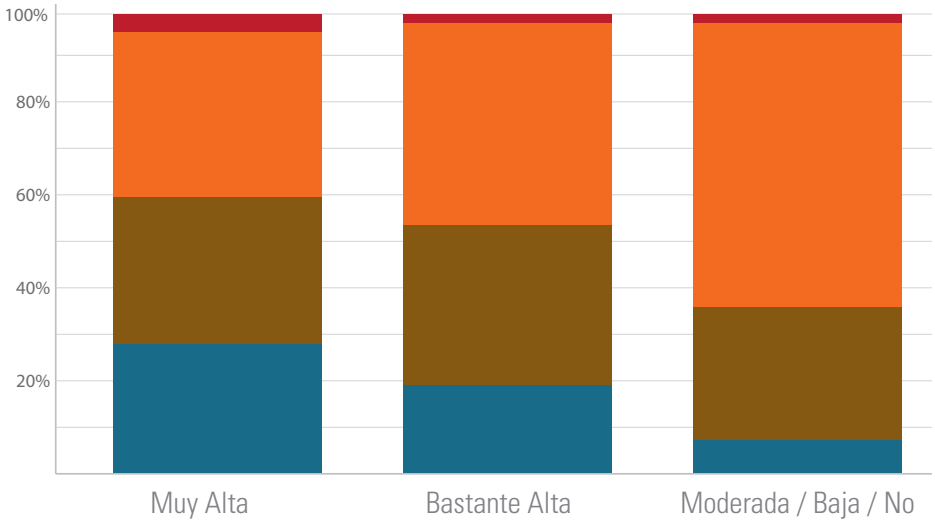
Las empresas de México entrenan a sus empleados en cuanto a políticas y procedimientos de seguridad con mayor frecuencia, con el 43% de las organizaciones del pais azteca brindando capacitación a sus trabajadores al menos dos veces al año.

Sin embargo, la encuesta revela que en todos los países la mayor parte de las respuestas informan como frecuencia mencionada más asiduamente la de “sobre bases irregulares”.

Cuando la Seguridad de la Información es una alta prioridad para la alta gerencia, el entrenamiento frecuente del personal de las empresas es más común.

¿Con cuánta frecuencia su organización entrena a sus empleados acerca de políticas y procedimientos relacionados con la Seguridad de la Información?

(Por prioridad de la Seguridad de la Información para la alta gerencia)



	M. Alta	B. Alta	M/B/No
No Sabe	4%	2%	2%
Irregularmente o Nunca	36%	44%	62%
Semestral o Anual	32%	35%	29%
Trimestral o Mas Frecuente	28%	19%	7%

El proyecto Cisco Security Index es el tercero de una serie de estudios patrocinados por Cisco y desarrollados por Kaagan Research and Associates, relacionados con la situación actual de la Seguridad de la Red en toda América Latina.

El primero de ellos se dio a conocer en octubre de 2003, bajo el título "Seguridad de la Red: Prioridad para Latinoamérica" (https://www.ciscoredaccionvirtual.com/redaccion/comunicados/ver_comunicados.asp?Id=709);

El segundo se hizo público en diciembre de 2005, junto con la empresa IBM: "Actitudes de los Gerentes IT de Latinoamérica respecto de la Seguridad de la Información - Amenazas a la seguridad incrementan en los países Latinoamericanos". Se encuentra en https://www.ciscoredaccionvirtual.com/redaccion/comunicados/comunicado.asp