ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

XVI Jornada Internacional de Seguridad Informática

VIII **Encuesta Latinoamericana de Seguridad de la Información**

Nuevos horizontes para América Latina

Jeimy J. Cano M., Ph.D, CFE

Gabriela María Saucedo Meza, MDOH

ORGANIZACION DE LOS ESTADOS AMERICANOS

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

.co

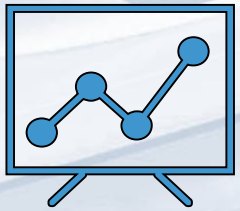
POLITECNICO INTERNACIONAL

Junio 2016

AGENDA

DOCUMENTOS REFERENTES REVISADOS

ANÁLISIS Y TENDENCIAS IDENTIFICADAS



CONCLUSIONES

ANÁLISIS CONSOLIDADOS

Demografía

Presupuestos

Incidentes

Evidencia digital

Riesgos: estándares, incidencias

Obstáculos

Capital intelectual

Para la academia

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

XVI Jornada Internacional de Seguridad Informática

SECTORES PARTICIPANTES

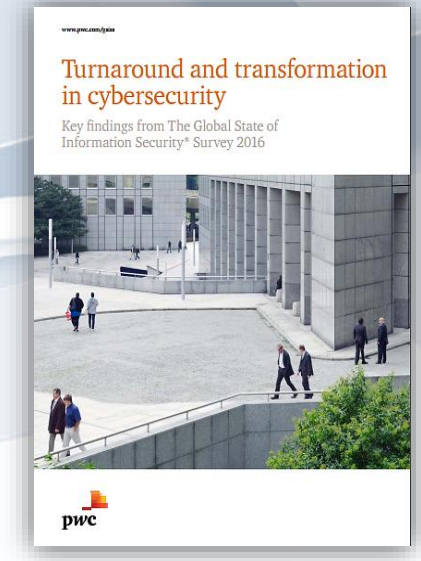
Servicios Financieros y Banca	14,0%	46
Construcción / Ingeniería	1,0%	2
Telecomunicaciones	10,0%	31
Sector de Energía e Hidrocarburos	2,0%	6
Salud	2,0%	7
Alimentos	0,0%	0
Educación	9,0%	30
Gobierno / Sector público	33,0%	108
Manufactura	2,0%	7
Consultoría Especializada	14,0%	47
Fuerzas Armadas	4,0%	14
Retail / Consumo masivo	0.3%	1
Otra (Por favor especifique)	9,0%	29

DEMOGRAFÍA

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

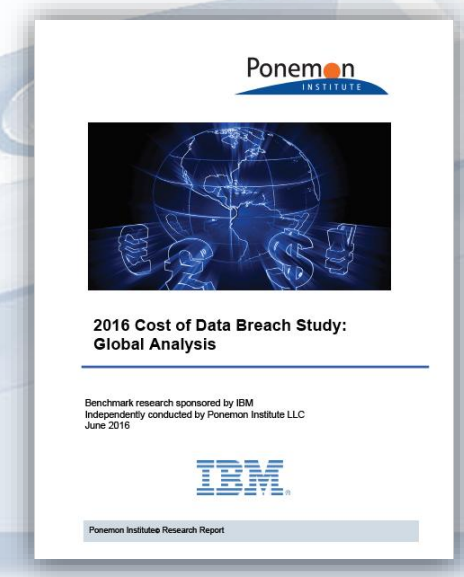
XVI Jornada Internacional de Seguridad Informática

http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf



file:///C:/Users/vicerrectoria/Downloads/pwc-global-state-of-information-security-survey-20%20(1).pdf

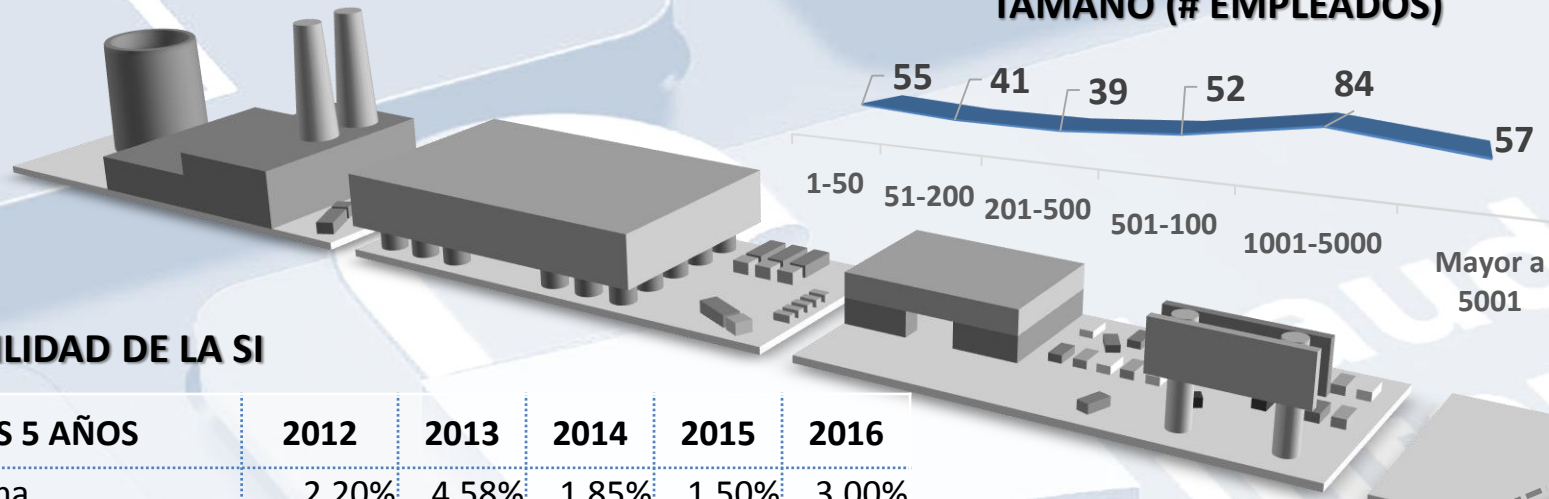
file:///C:/Users/vicerrectoria/Downloads/gx-ers-assessing-cyber-risk.pdf



https://www-01.ibm.com/marketing/iwm/dre/signup?source=mrs-form-1995&S_PKG=ov49542

DOCUMENTOS REFERENTES REVISADOS

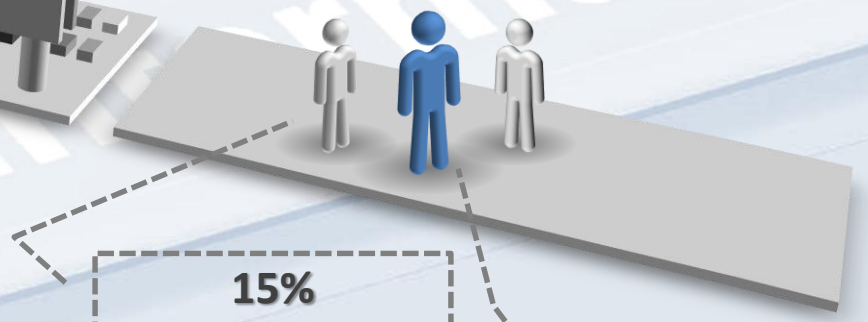
TAMAÑO (# EMPLEADOS)



RESPONSABILIDAD DE LA SI

ÚLTIMOS 5 AÑOS	2012	2013	2014	2015	2016
Auditoría interna	2,20%	4,58%	1,85%	1.50%	3.00%
Director de SI/S de I	23,61%	25,83%	26,94%	34.70%	**43.00%**
Director Departamento de Sistemas/Tecnología	36,67%	33,75%	35,42%	13.70%	16.00%
Gerente Ejecutivo	3,61%	2,50%	2,21%	3.40%	3.00%
Gerente de Finanzas	0,28%	0,42%		0.40%	0.00%
Gerente de Operaciones	3,89%	0,83%	3,69%	3.40%	2.00%
Gerente de Riesgos					5.00%
Gerente de Planeación					2.00%
No especificado	14,72%	17,50%	15,87%	14.90%	14.00%
Tercerizado	-	0,83%	1,11%	0.80%	1.00%
Otros cargos	15,00%	13,75%	12,92%	14.90%	14.90%

CARGO PARTICIPANTES



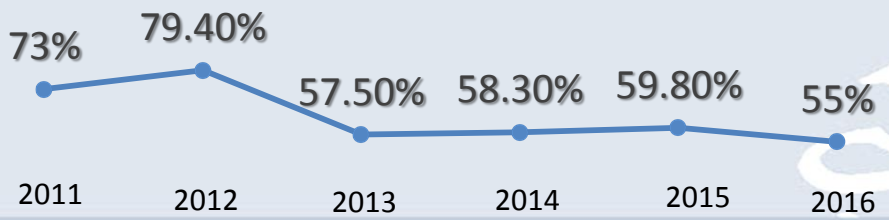
15%
Director/Jefe de Sistemas/Tecnología

19%
Otros cargos: consultores, docentes, abogados, fraud managers

DEMOGRAFÍA

	% DE DISTRIBUCIÓN DEL PRESUPUESTO 2016					
SECTOR	Entre el 0 y el 2%	Entre el 3 y el 5%	Entre el 6 y el 8%	Entre el 9 y el 11%	Más del 11%	% TOTAL INVERSIÓN
Construcción / Ingeniería	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Consultoría Especializada	4.26%	8.51%	6.38%	0.00%	4.26%	23.40%
Educación	13.33%	3.33%	0.00%	3.33%	3.33%	23.33%
Fuerzas Armadas	14.29%	21.43%	0.00%	0.00%	14.29%	50.00%
Gobierno / Sector público	8.33%	4.63%	4.63%	5.56%	4.63%	27.78%
Manufactura	14.29%	14.29%	0.00%	0.00%	0.00%	28.57%
Otra (Por favor especifique)	13.79%	6.90%	0.00%	6.90%	3.45%	31.03%
Retail / Consumo masivo	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Salud	14.29%	14.29%	0.00%	0.00%	0.00%	28.57%
Sector de Energía e Hidrocarburos	33.33%	33.33%	0.00%	0.00%	0.00%	66.67%
Servicios Financieros y Banca	15.22%	15.22%	4.35%	2.17%	0.00%	36.96%
Telecomunicaciones	16.13%	12.90%	3.23%	3.23%	3.23%	38.71%

EMPRESAS CON PRESPUESTO ASIGNADO PARA LA SI



PRESUPUESTOS

TIPOS INCIDENTES DETECTADOS (985 incidencias)

Manipulación de aplicaciones de software	4.0%	43
Instalación de software no autorizado	**12.0%**	122
Accesos no autorizados al web	8.0%	78
Fraude electrónico	3.0%	29
Virus/Caballos de Troya	**13.0%**	129
Robo de datos	3.0%	30
Monitoreo no autorizado del tráfico	2.0%	20
Negación del servicio (DOS/DDOS)	6.0%	56
Pérdida de integridad de la información	3.0%	28
Pérdida/Fuga de información crítica	3.0%	27
Suplantación de identidad	3.0%	26
Acciones de ingeniería social	4.0%	42
Phishing	**11.0%**	107
Pharming	1.0%	7
Espionaje	1.0%	10
Ramsonware	5.0%	50
Ataque de aplicaciones Web (XSS, SQL Injection, Directory Transversal, etc)	5.0%	48
Robo de elementos críticos de hardware (notebooks, discos, etc.)	4.0%	36
Incidentes relacionados con la privacidad de los datos personales (publicación de información personal, solicitudes de eliminación de datos personales, etc.)	3.0%	32
Ciber-Ataques (APT o ataques dirigidos, denegación de servicios masiva)	4.0%	37
Ninguno	1.0%	13
Otra (Por favor especifique)	1.0%	15

XVI Jornada Internacional de Seguridad Informática

SECTORES ATACADOS ENTRE 1 Y 7 VECES POR TAMAÑO DE ORGANIZACIÓN

SE RECIBE NOTIFICACIÓN DE:

- Empleados **28%**
- Análisis de registros de auditoría/sistema de archivos/registros Firewall **23%**

91% DENUNCIA INCIDENTES

SE NOTIFICA A:

- Directivos **40%**
- Equipo de atención de incidentes (CSIRT) **23%**

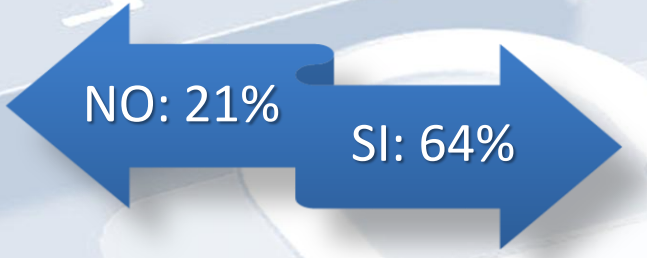
CONDICIONES PARA DENUNCIAR:

Con canales de comunicación privados y seguros	**31.0%**
Con garantías de no revelación de información a terceros	24.0%
Con protocolos estrictos de aseguramiento y control de la información	24.0%
Con rendición de cuentas por parte de la entidad que los recibe	11.0%
Con una auditoria de un tercero independiente que vele por los intereses de quien informa	9.0%

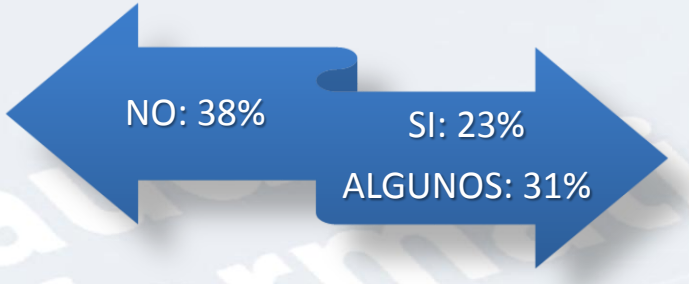
MOTIVO DE NO DENUNCIA:

- Publicación de noticias desfavorables en los medios/pérdida de imagen **25%**

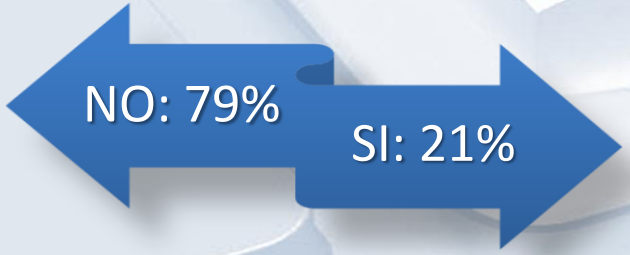
Consciencia de la evidencia digital



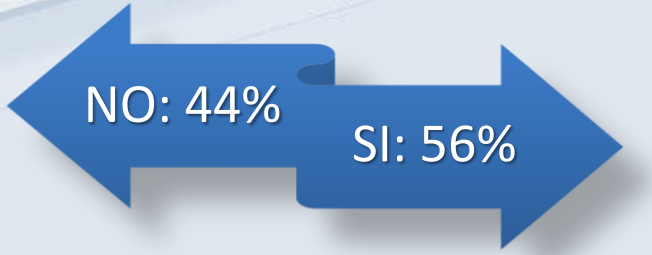
Procedimiento aprobado e implementado (administración de evidencia digital)



Estrategia de e-discovery o descubrimiento electrónico para litigios o reclamaciones legales



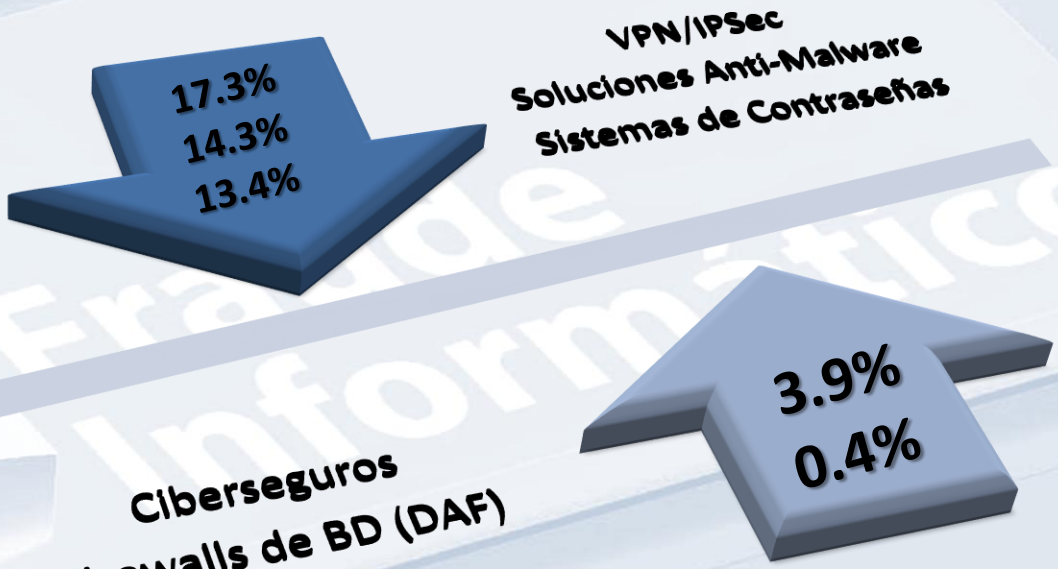
Contactos con autoridades nacionales e internacionales



EVIDENCIA DIGITAL

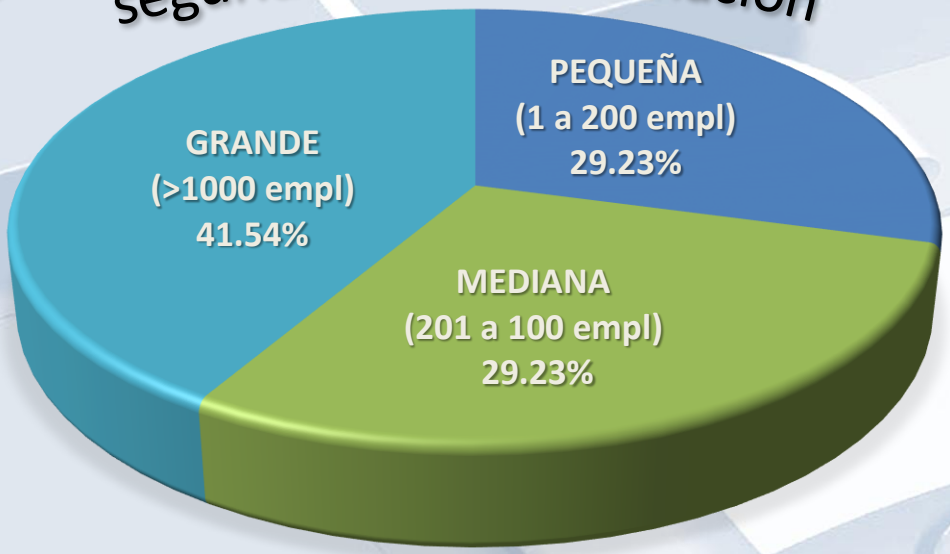
Sistemas de Contraseñas	58.2%	191
Soluciones Anti-Malware	55.5%	182
Firewalls tradicionales (Hardware/Software)	51.8%	170
VPN/IPSec	50.3%	165
Biométricos (huella digital, iris, etc.)	33.2%	109
Cifrado de datos	37.2%	122
Firmas digitales/certificados digitales	33.2%	109
Proxies/Proxies inversos	33.2%	109
Firewalls de nueva generación	32.0%	105
Web Application Firewalls (WAF)	28.4%	93
Sistemas de detección y/o prevención de intrusos IDS/IPS tradicionales	29.3%	96
IDS/IPS de nueva generación	22.3%	73
Smart Cards	16.2%	53
Soluciones de monitoreo de redes sociales	18.9%	62
Firewalls de Bases de Datos (DAF)	15.5%	51
SIEM (Security Information Event Management)	18.9%	62
Servicio de SOC	12.8%	42
Herramientas Anti –DDoD	11.0%	36
Servicios de inteligencia de amenazas	9.5%	31
ADS (Anomaly detection systems)	4.6%	15
Tercerización de la seguridad informática	6.7%	22
Herramientas de validación de cumplimiento con regulaciones internacionales	6.7%	22
Ciber seguros	7.0%	23
Otro (Por favor especifique)	0.9%	3

MECANISMOS PROTECCIÓN (6 en promedio x empr.)



RIESGOS

Empresas que realizan evaluaciones de seguridad de la información



47% DESARROLLAN PROCESO DE EVALUACIÓN DE RIESGOS

87% CUENTAN CON METODOLOGÍAS DE GESTIÓN RIESGOS

ISO 31000	23.0%
ISO 27005	22.0%
GRC (Governance, Risk & Compliance)	13.0%
Magerit	12.0%
ERM(Enterprise Risk Managment)	11.0%
Otra	7.0%
SARO	6.0%
AS/NZ 4360	3.0%
Octave	3.0%

SECTOR con mayor # eval.	PEQUEÑA	MEDIANA	GRANDE	GLOBAL
Consultoría Especializada	**12.31%**	1.92%	1.54%	15.77%
Gobierno / Sector público	5.38%	**11.92%**	**15.00%**	**32.31%**
Servicios Financieros y Banca	2.69%	4.23%	7.69%	14.62%

ESTÁNDAR		REGULACIÓN	
ISO 27001 30%	**ITIL** 15%	**ENTES DE SUPERVISIÓN** 51%	**NINGUNA** 33%

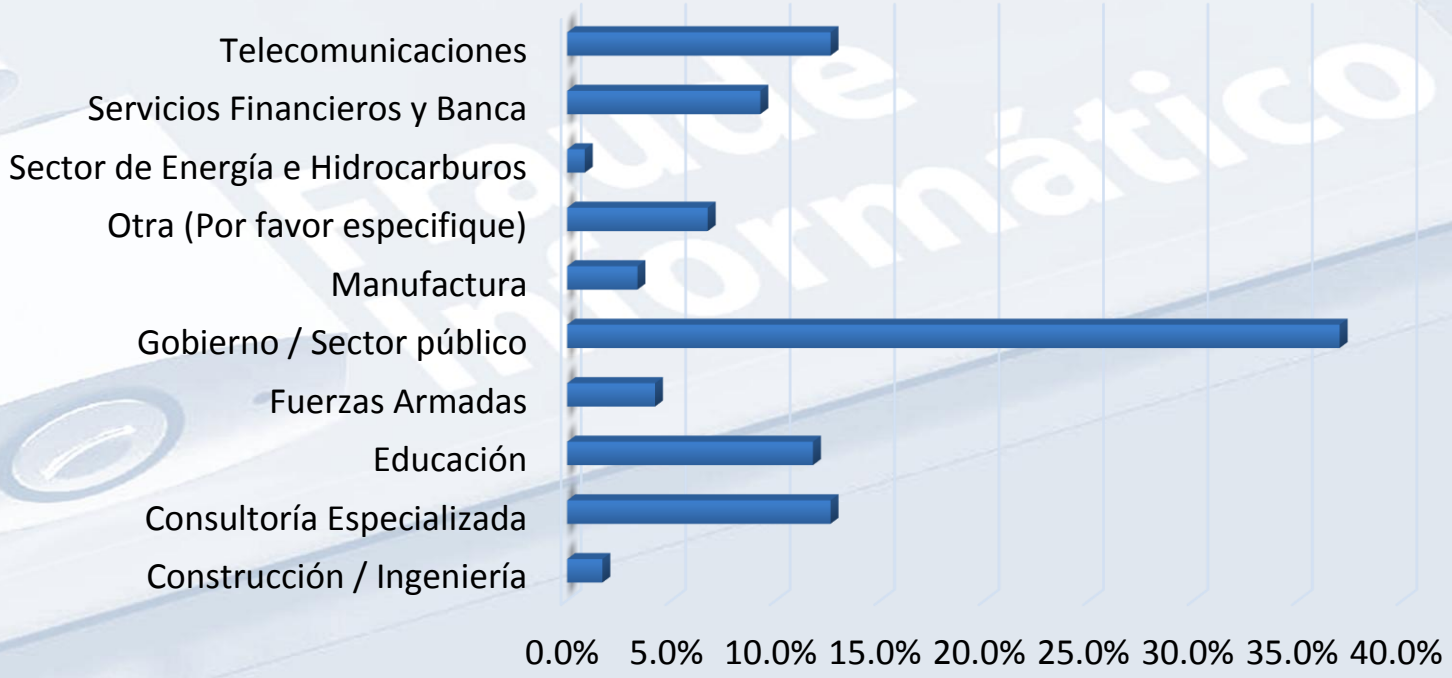
RIESGOS

EMPRESAS SIN METODOLOGÍAS PARA GESTIÓN RIESGOS Y SUS MOTIVOS

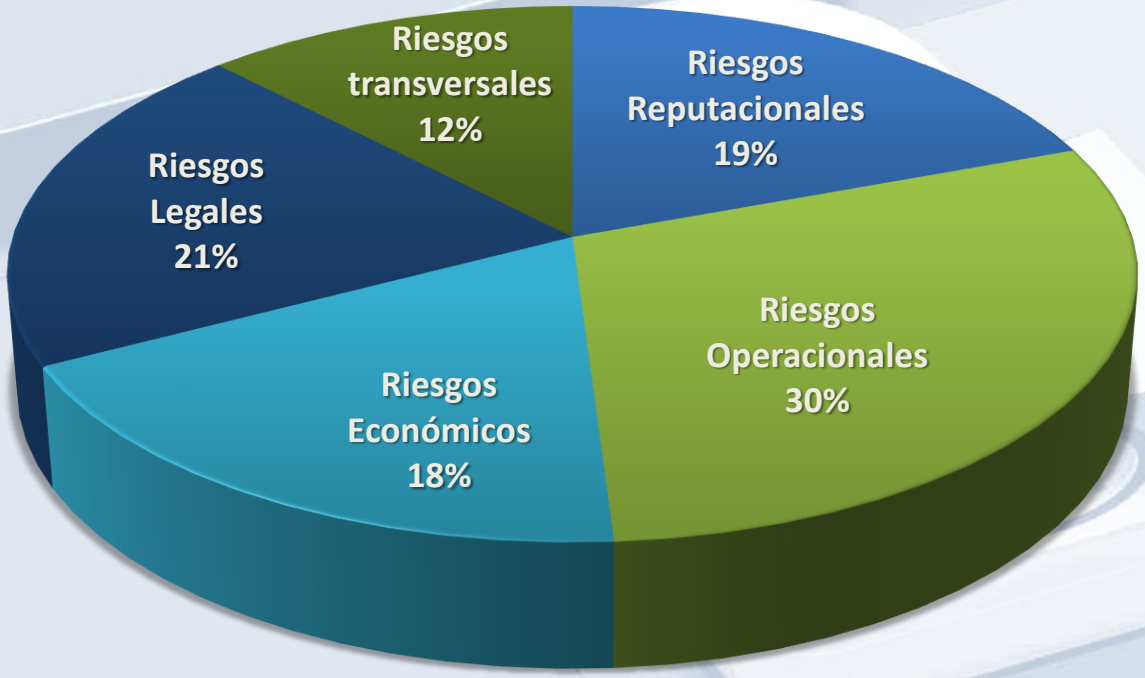
53%

Se realiza dentro del proceso de gestión de riesgo empresarial de la organización	31.0%
No se tiene un proceso formal de gestión de riesgos ni corporativo, ni de información	**29.0%**
Desconocimiento del tema	16.0%
Falta de presupuesto	13.0%
No se tiene asociados riesgos con el tratamiento de la información	4.0%
Otros	7.0%

SECTORES QUE NO DESARROLLAN PROCESOS DE EVALUACIÓN DE RIESGOS DE S.I.



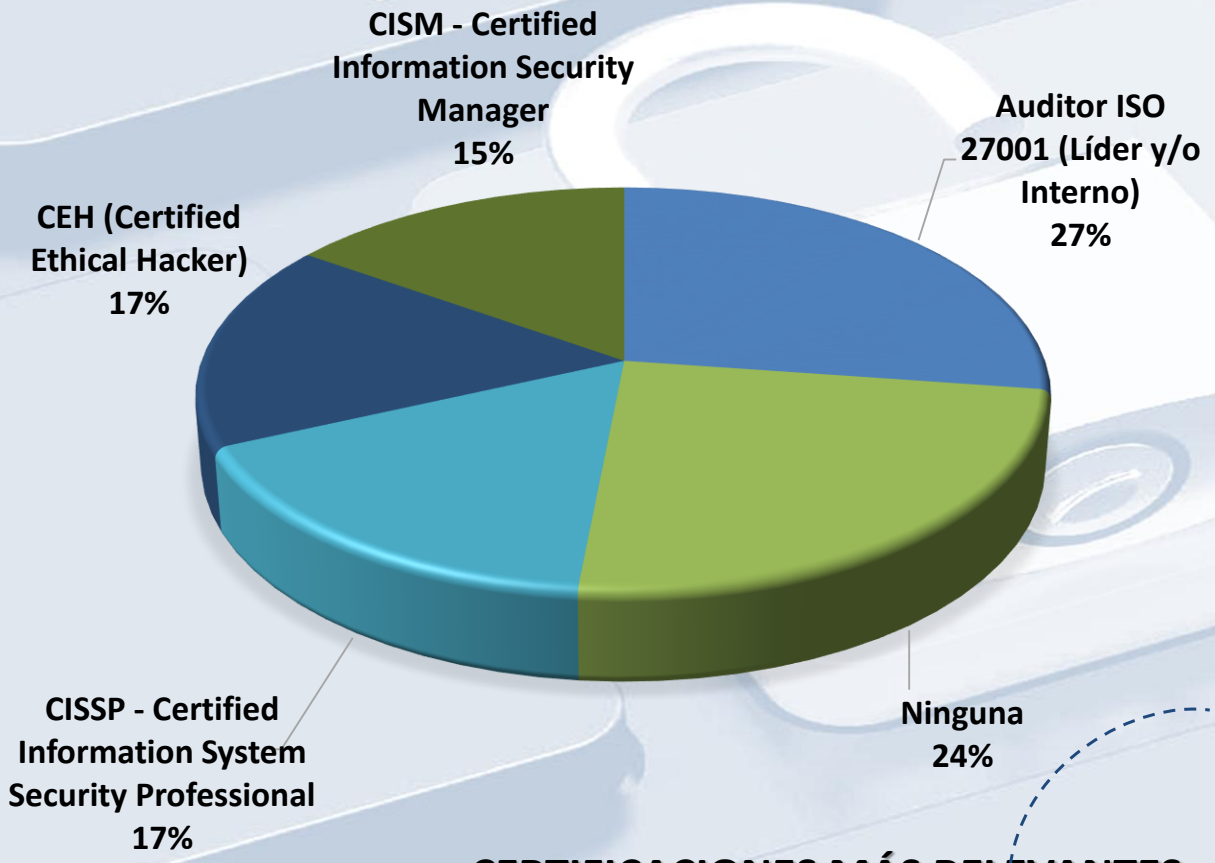
ASOCIACIÓN DEL RIESGO DE S.I. EN LAS ORGANIZACIONES



OBSTÁCULOS PARA LOGRAR LA SEGURIDAD DE LA INFORMACIÓN	2015	2016
Ausencia o falta de una cultura en seguridad de la información		38.7%
Falta de apoyo directivo	41.6%	32.3%
Poco entendimiento de la seguridad de la información	33.5%	32.0%
Falta de colaboración entre áreas/departamentos	45.7%	30.5%
Falta de formación técnica	24.9%	25.6%
Poca visibilidad del tema a nivel ejecutivo	35.7%	25.3%
Inexistencia de política de seguridad	24.9%	20.4%
Poco entendimiento de los flujos de la información en la organización	22.6%	20.1%
Falta de tiempo	31.2%	19.8%
Complejidad tecnológica	24.0%	19.5%
Escasa formación en gestión segura de la información		19.5%
Habilidades gerenciales de los CISO’s	15.8%	13.1%

OBSTÁCULOS

CERTIFICACIONES DEL PERSONAL QUE LABORA EN EMPRESAS PARTICIPANTES



NÚMERO DE COLABORADORES DEDICADOS A LA SI

TAMAÑO DE LA EMPRESA	1 a 5	11 a 15	6 a 10	Más de 15	Ninguna
1-50	10.0%	0.9%	0.4%	0.4%	7.0%
51-200	7.4%	0.0%	0.0%	0.4%	3.1%
201-500	7.4%	0.4%	0.9%	0.4%	2.2%
501-1000	9.2%	2.2%	1.3%	0.9%	3.9%
1001-5000	15.3%	0.9%	2.2%	4.8%	1.3%
> 5001	4.8%	2.2%	4.8%	6.1%	0.4%
Total general	**54.1%**	6.6%	9.6%	13.1%	16.6%

CERTIFICACIONES MÁS RELEVANTES

CISSP – Certified Information System Security Professional	15.0%
CISM – Certified Information Security Manager	13.0%
Auditor ISO 27001 (Líder y/o Interno)	12.0%
CRISC- Certified in Risk and Information System Control	10.0%
CEH (Certified Ethical Hacker)	10.0%

EXPERIENCIA

61%

+ 2 AÑOS

CAPITAL INTELECTUAL

TEMAS CLAVES/RELEVANTES DEL RESPONSABLE DE LA SI

Amenazas persistentes avanzadas	11.0%	169
Ciber seguridad	11.0%	168
Seguridad y control en la computación en la nube	11.0%	168
Malware en dispositivos móviles	10.0%	160
Fuga de información sensible	10.0%	151
Fraude Informático	10.0%	153
Ataques a infraestructuras críticas	9.0%	134
Ciber espionaje	6.0%	101
Inteligencia de la Seguridad	6.0%	99
Internet de la cosas – IoT	5.0%	80
Ciber guerra	4.0%	62
Grandes datos y analítica	4.0%	70
Ciber armas	2.0%	33

BRECHAS IDENTIFICADAS (COMPETENCIAS NECESARIAS)

Capacidades técnicas y/o experiencia	18.0%	154
Habilidades gerenciales (liderazgo, comunicación, carisma, rendición de cuentas, proyecciones financieras)	16.0%	131
Habilidades para entender el negocio	15.0%	125
Habilidades para comunicar e interconectar negocios y necesidades en materia de seguridad de la información	15.0%	124
Formación académica y técnica	15.0%	123
Visión práctica de estrategias livianas, sencillas y efectivas para el aseguramiento de la información	14.0%	122
Capacidades prospectivas y de pronóstico	7.0%	60

PERCEPCIÓN SOBRE LA ACADEMIA EN TEMAS DE SI

	Están ofreciendo programas académicos de grado y/o posgrado…	La formación se limita a cursos cortos	No ofrecen programas académicos o cursos cortos en esta área	Se han dejado desplazar por certificaciones generales y de producto	El nivel de investigación en el área es escasa o insuficiente	Hacen poca difusión sobre éstos temas	Los profesores tienen poca formación académica en el tema	Hay poca motivación de los estudiantes para estudiar el tema	Existen limitados laboratorios e infraestructura para soportar los…	Hay pocas (o nulas) alianzas con proveedores de tecnología de…
Series1	14.0%	12.0%	6.0%	8.0%	13.0%	11.0%	9.0%	6.0%	9.0%	11.0%

PARA LA ACADEMIA

CONCLUSIONES

Se advierte una ***tendencia a la baja en la inversion en la S.I*** en las empresas de latinoamérica, donde el **33%** de las empresas invierten en promedio US$50.000 o menos.

Tendencia confirmada con el Informe Global de Seguridad de la Información de PwC 2016 – 29% en Latam.

El ***phishing, el malware y la instalación de software no autorizado*** establecen el **36%** de las amenazas más materializadas en la región.

Tendencias que están correlacionadas con el informe de Ernst & Young 2015 – 35% a nivel global.

Se advierte una ***tendencia de uso de autenticación de doble factor*** (contraseñas, biométricos, tokens), así como de ***firewall de Base de Datos*** y la adquisición de ***ciberseguros***.

Tendencia que se verifica en el Informe Global de Seguridad de la Información de PwC 2016 – 58% en Latam y el reporte de valoración del ciberriesgo de Deloitte 2016.

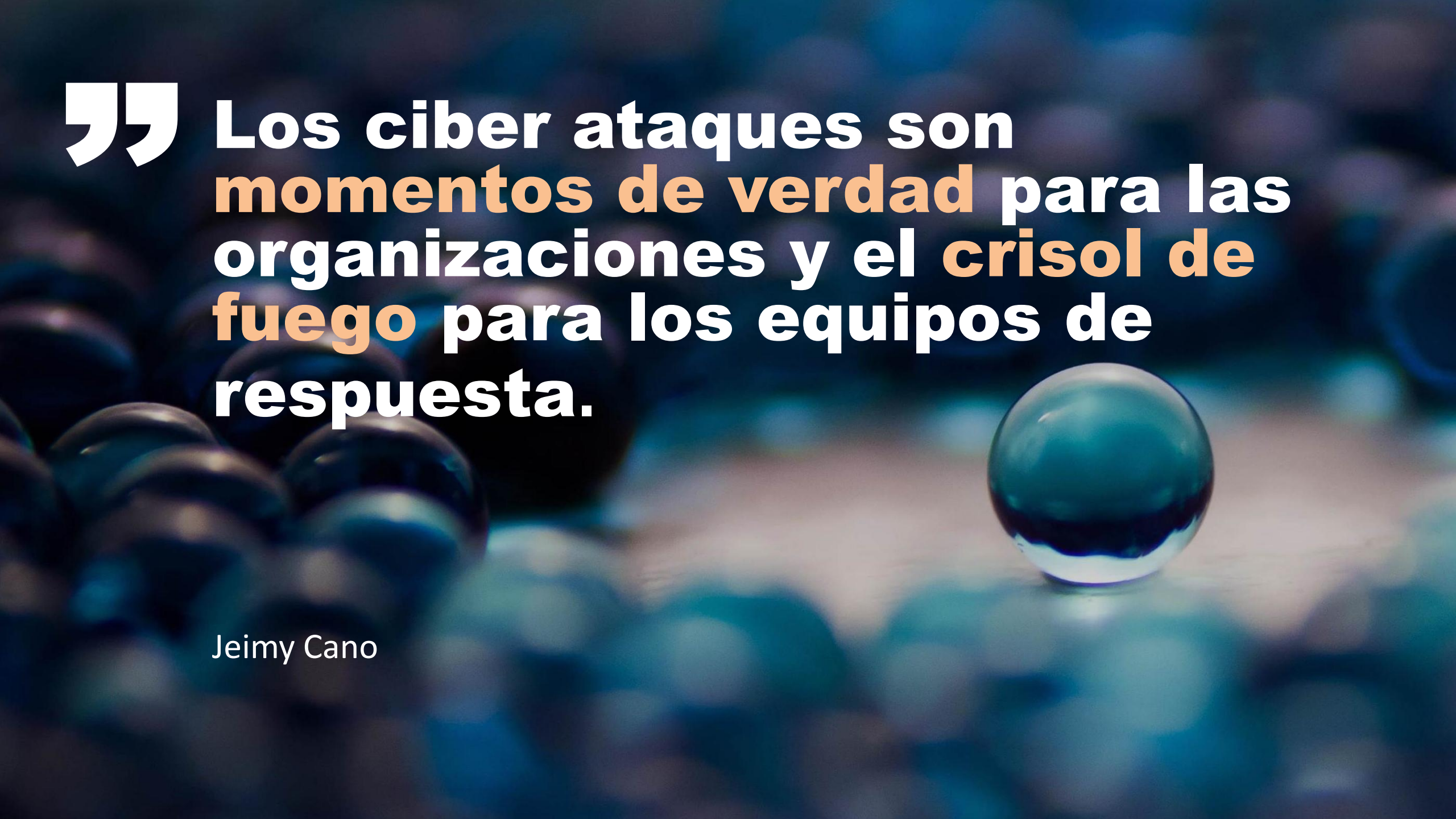
CONCLUSIONES

La empresas en latinoamérica exigen como mínimo ***dos (2) años de experiencia en S.I para contratar su personal*** en esta área. Adicionalmente privilegian que los seleccionados tengan certificaciones como ***la ISO 27001 (Auditor Interno y/o líder), CISSP o CEH***. Adicionalmente tienen en promedio ***5 personas dedicadas de tiempo complete a la S.I .***

Tres temas claves deben tener los ejecutivos de S.I: ***APT, Ciberseguridad y seguridad y control en la nube.***

Tres temas a mejorar en los *profesionales de S.I*: ***capacidades técnicas, habilidades gerenciales y entendimiento del negocio***.

Retos de la academia: ***aumentar nivel de I+D, docentes mejor formados y mayores alianzas con proveedores.***


Los ciber ataques son momentos de verdad para las organizaciones y el crisol de fuego para los equipos de respuesta.
Jeimy Cano

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

XVI Jornada Internacional de Seguridad Informática

VIII **Encuesta Latinoamericana de Seguridad de la Información**

Nuevos horizontes para América Latina

Jeimy J. Cano M., Ph.D, CFE

Gabriela María Saucedo Meza, MDOH

ORGANIZACION DE LOS ESTADOS AMERICANOS

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

.co

POLITECNICO INTERNACIONAL

Junio 2016