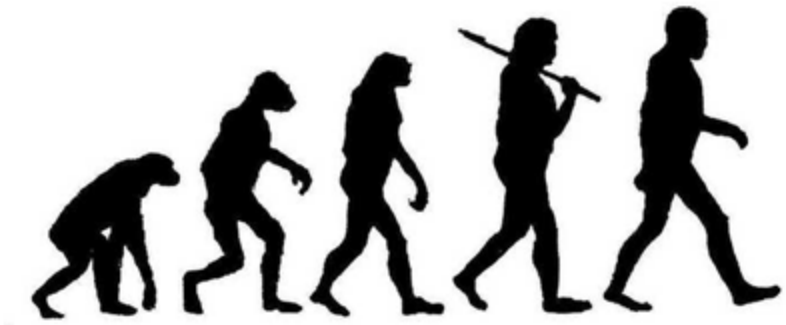
ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:
Una nueva década para avanzar

La RE-Evolución de la Seguridad



Felipe Silgado

CISSP, CISM, CRISC

Gerente TRS/ITE Advisory - PwC

15 de Junio de 2011

A la memoria de José de Jesús Lozano Gutiérrez

OBJETIVOS

- ✓Mostrar como ha evolucionado la seguridad
- ✓Presentar los drivers que llevarán a la evolución de la seguridad
- ✓Identificar los posibles escenarios hacia donde evolucionará la seguridad

Todos los derechos reservados

AGENDA

- ✓El pasado de la seguridad
- ✓Los nuevos *drivers* y la evolución
- ✓Reflexión final

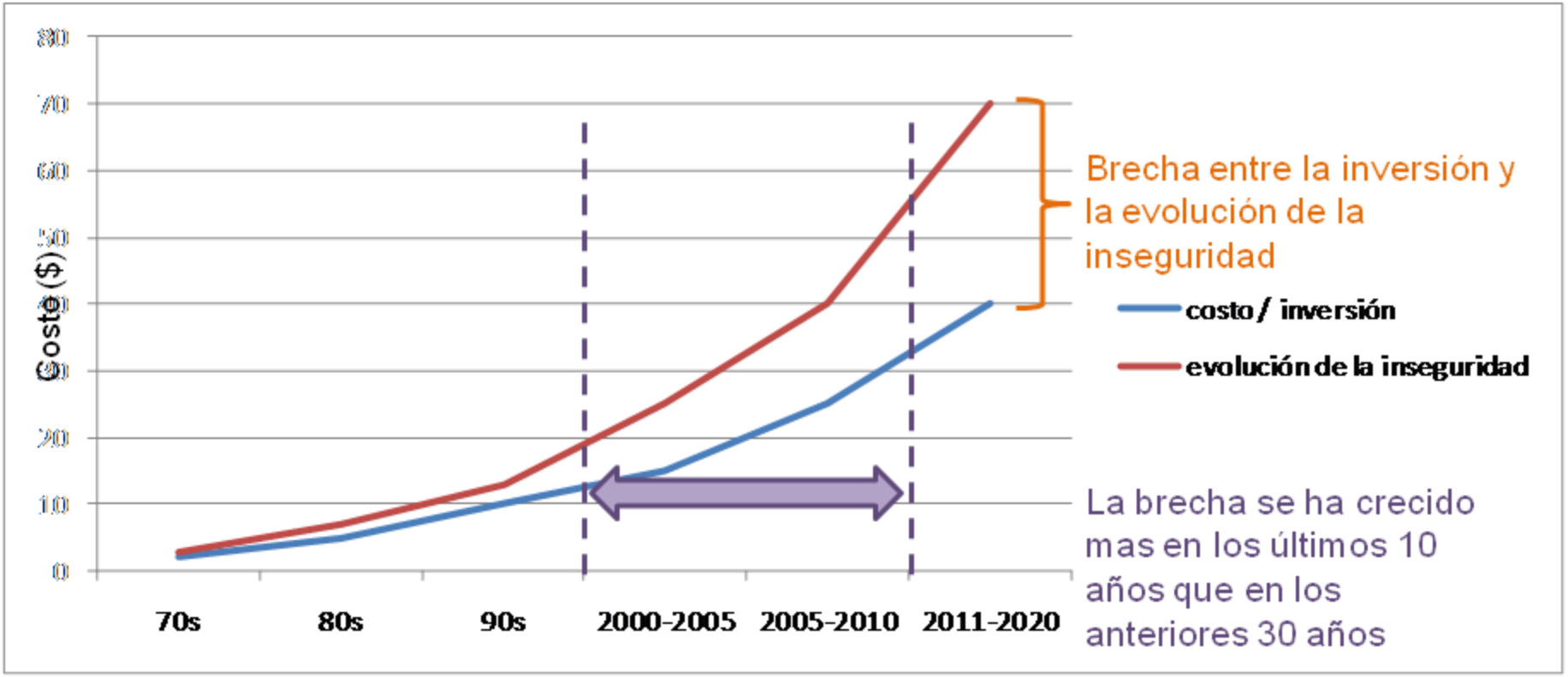
Todos los derechos reservados

AGENDA

- ✓El pasado de la seguridad
- ✓Los nuevos *drivers* y la evolución
- ✓Reflexión final

Todos los derechos reservados

EL PASADO DE LA SEGURIDAD



Fuente: Análisis de PwC

Todos los derechos reservados

EL PASADO DE LA SEGURIDAD

Causas del crecimiento de la brecha:

- ✓Evolución de la tecnología
- ✓Economía mundial
- ✓Falta de control interno
- ✓Inversiones realizadas sin basarse en el riesgo
- ✓El hacking como un negocio y una forma de respuesta socio-política o de protesta
- ✓Falta de sensibilización a los usuarios

Todos los derechos reservados

EL PASADO DE LA SEGURIDAD

70s

2020

Todos los derechos reservados

AGENDA

- ✓El pasado de la seguridad
- ✓Los nuevos *drivers* y la evolución
- ✓Reflexión final

Todos los derechos reservados

DRIVERS DE LA EVOLUCION

Drivers 2007 a 2010:

	2007	2008	2009	2010	Three-year % change*
Economic conditions	n/a	n/a	39%	49%	n/a
Business continuity/disaster recovery	68%	57%	41%	40%	-41%
Company reputation	44%	39%	32%	35%	-20%
Internal policy compliance	51%	46%	38%	34%	-33%
Regulatory compliance	54%	44%	37%	33%	-39%

Fuente: PwC Global State of Information Security 2011

Todos los derechos reservados

DRIVERS DE LA EVOLUCION

Los nuevos drivers:

- ✓Economía mundial
- ✓Cambio climático
- ✓Regulación
- ✓Guerras
- ✓Redes sociales y comunicaciones

Todos los derechos reservados

DRIVERS DE LA EVOLUCION

Los nuevos drivers:

- ✓Economía mundial
- ✓Cambio climático
- ✓Regulación
- ✓Guerras
- ✓Redes sociales y comu

PPP 2009 Rank	Country	GDP at PPP (constant 2009 US$bn)	PPP 2050 Rank	Country	Projected GDP at PPP (constant 2009 US$bn)
1	US	14256	1	China	59475
2	China	8888	2	India	43180
3	Japan	4138	3	US	37876
4	India	3752	4	Brazil	9762
5	Germany	2984	5	Japan	7664
6	Russia	2687	6	Russia	7559
7	UK	2257	7	Mexico	6682
8	France	2172	8	Indonesia	6205
9	Brazil	2020	9	Germany	5707
10	Italy	1922	10	UK	5628

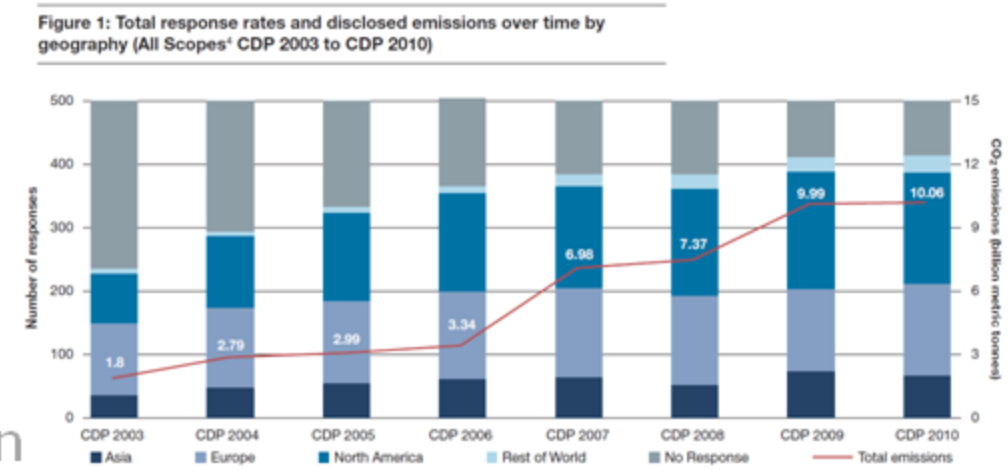
Fuente: The World in 2050 - PwC

Todos los derechos reservados

DRIVERS DE LA EVOLUCION

Los nuevos drivers:

- ✓Economía mundial
- ✓Cambio climático
- ✓Regulación
- ✓Guerras
- ✓Redes sociales y comun



Fuente: Carbon Disclosure Project 2010 Global 500 Report - PwC

Todos los derechos reservados

DRIVERS DE LA EVOLUCION

Los nuevos drivers:

- ✓Economía mundial
- ✓Cambio climático
- ✓Regulación
- ✓Guerras
- ✓Redes sociales y comu

- ✓Habeas Data (multas 03/2010 a 03/2011 > $1.900M)
- ✓Proyecto de ley estatutaria número 184 de 2010 (multas hasta 2000 SMLV)
- ✓Ley Lleras (derechos de autor)
- ✓SFC CE 052 (seguridad)
- ✓SFC CE 038 (control interno)
- ✓SFC CE 047 (riesgo operativo)
- ✓SOX / Basilea II

Todos los derechos reservados

DRIVERS DE LA EVOLUCION

Los nuevos drivers:

- ✓Economía mundial
- ✓Cambio climático
- ✓Regulación
- ✓Guerras
- ✓Redes sociales y comu

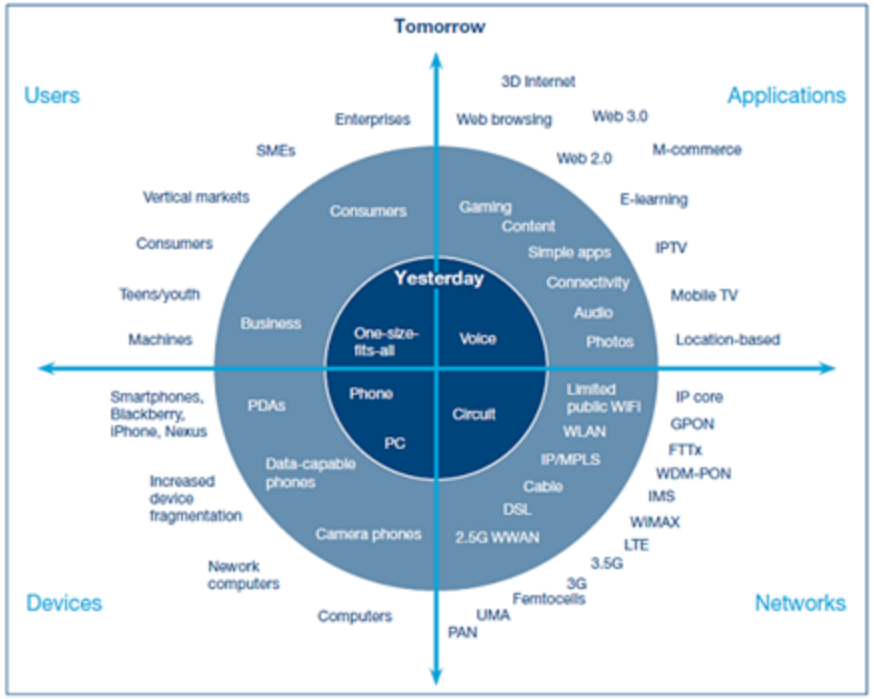
- ✓Iraq
- ✓Libia
- ✓Estados Unidos
- ✓Colombia

Todos los derechos reservados

DRIVERS DE LA EVOLUCION

Los nuevos drivers:

- ✓Economía mundial
- ✓Cambio climático
- ✓Regulación
- ✓Guerras
- ✓Redes sociales y comunicac



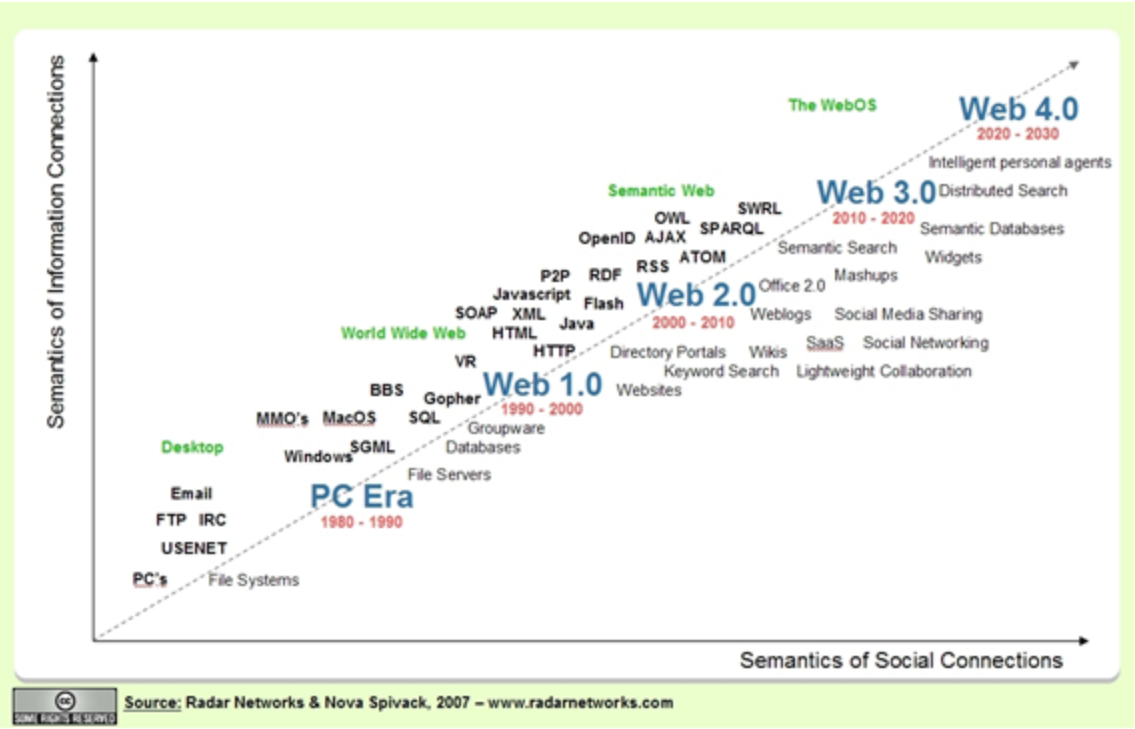
Fuente: Communications review Vol. 15 No. 2 - PwC

Todos los derechos reservados

DRIVERS DE LA EVOLUCION

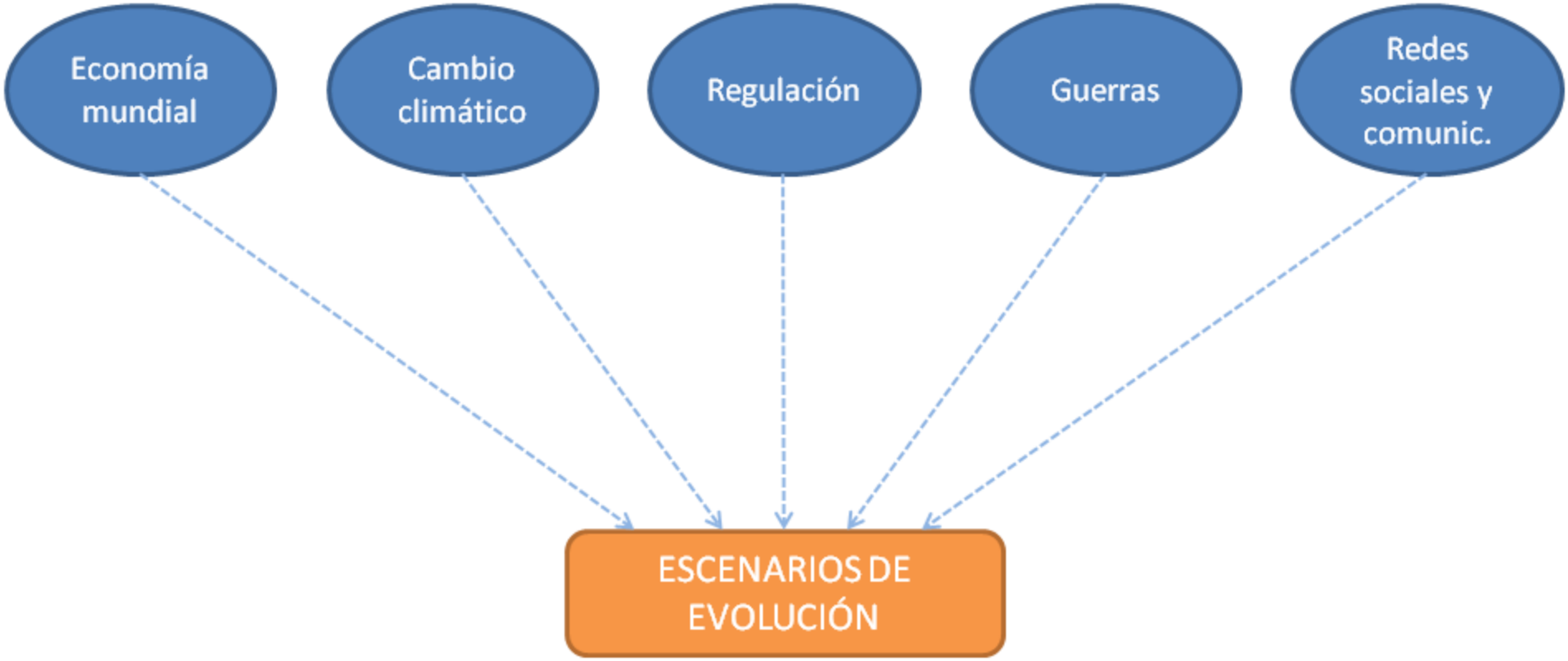
Los nuevos drivers:

- ✓Economía mundial
- ✓Cambio climático
- ✓Regulación
- ✓Guerras
- ✓Redes sociales y co



Todos los derechos reservados

DRIVERS DE LA EVOLUCION



Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

Green Security

- Tendencia mundial para mitigar el cambio climático.
- Cambiar la forma de operación de algunos controles de seguridad. Ejemplos:
  - ✓Firewalls/IPSs
  - ✓Sistemas de autenticación
  - ✓Formatos en papel con firmas autorizadas
- Cuánto CO_2 emiten los controles de seguridad?
- Un solo servidor emite 2 toneladas de CO_2 al año*.

*Fuente: http://www.moveneutral.com/calculations

Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

Green Security

•Pasos para la implementación de una estrategia verde:

Valorar
- Estado actual
- Centralización
- Convergencia
- Uso de papel

Diseñar (Re)
- Procesos
- Políticas
- Controles

Implementar
- Cambios en procesos de seguridad
- Sensibilización

Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

Green Security

- Cambio en la forma de operación de la seguridad

Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

Cloud Security

- Tendencia mundial sobre la migración de servicios informáticos a la nube. Ejemplo correo electrónico, herramientas de colaboración, repositorio de información, etc.
- Áreas clave de seguridad:
  - ✓Control de Acceso
  - ✓Continuidad del negocio
  - ✓Cumplimiento, regulación y privacidad
  - ✓Protección de los datos
  - ✓Eventos, Incidentes e investigación forense
  - ✓Control de cambios (update, parches, fixes, hardening…)

Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

Cloud Security

Figure 1: Do you currently use cloud services such as software as a service, platform as a service, or infrastructure as a service?

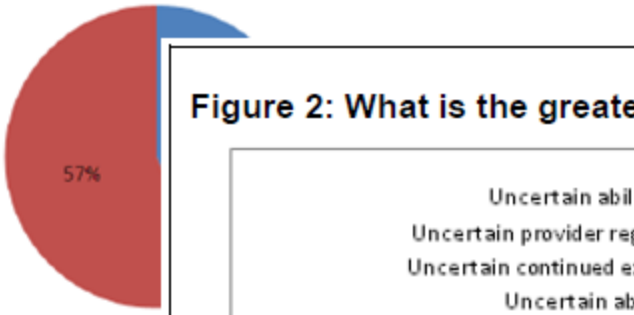
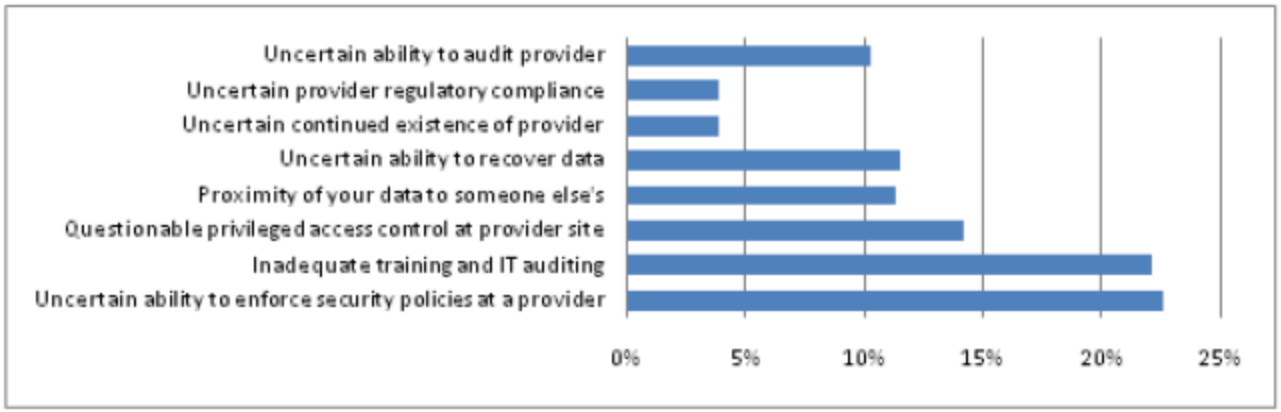


Figure 2: What is the greatest security risk to your cloud computing strategy?



Fuente: PwC Global State of Information Security 2010.

Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

Cloud Security

✓Control de Acceso: Se debe tener especial cuidado con aplicaciones legacy y con aplicaciones hechas en casa. Igualmente validar el manejo de roles y perfiles.

✓Continuidad del negocio: Se deben validar los servicios que ofrece el proveedor para garantizar la continuidad del servicio.

✓Cumplimiento, regulación y privacidad: Se debe asegurar que el proveedor cumpla con las regulaciones y tenga algún esquema de auditoria externa que garantice el cumplimiento y privacidad de los datos (SAS 70, ISO 27001…)

Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

Cloud Security

✓Protección de los datos: Se debe validar los controles que garanticen la confidencialidad, integridad y disponibilidad, e igualmente controles que garanticen independencia entre la información de la compañía y de otras compañías.

✓Eventos, Incidentes e investigación forense: Es necesario asegurar que el proveedor tenga un esquema de atención de incidentes y que puedan realizarse investigaciones forenses (por parte de la compañía o por un tercero independiente).

Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

Cloud Security

✓Control de cambios: Es necesario asegurar que el proveedor tenga un esquema de cambios, que garantice que cuando realice un cambio a otro cliente no afecte mi compañía, que los cambios puedan ser trazables y se realicen actualizaciones de parches y fixes de seguridad.

Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

Cloud Security

✓Evaluación del riesgo de migrar un servicio a la nube

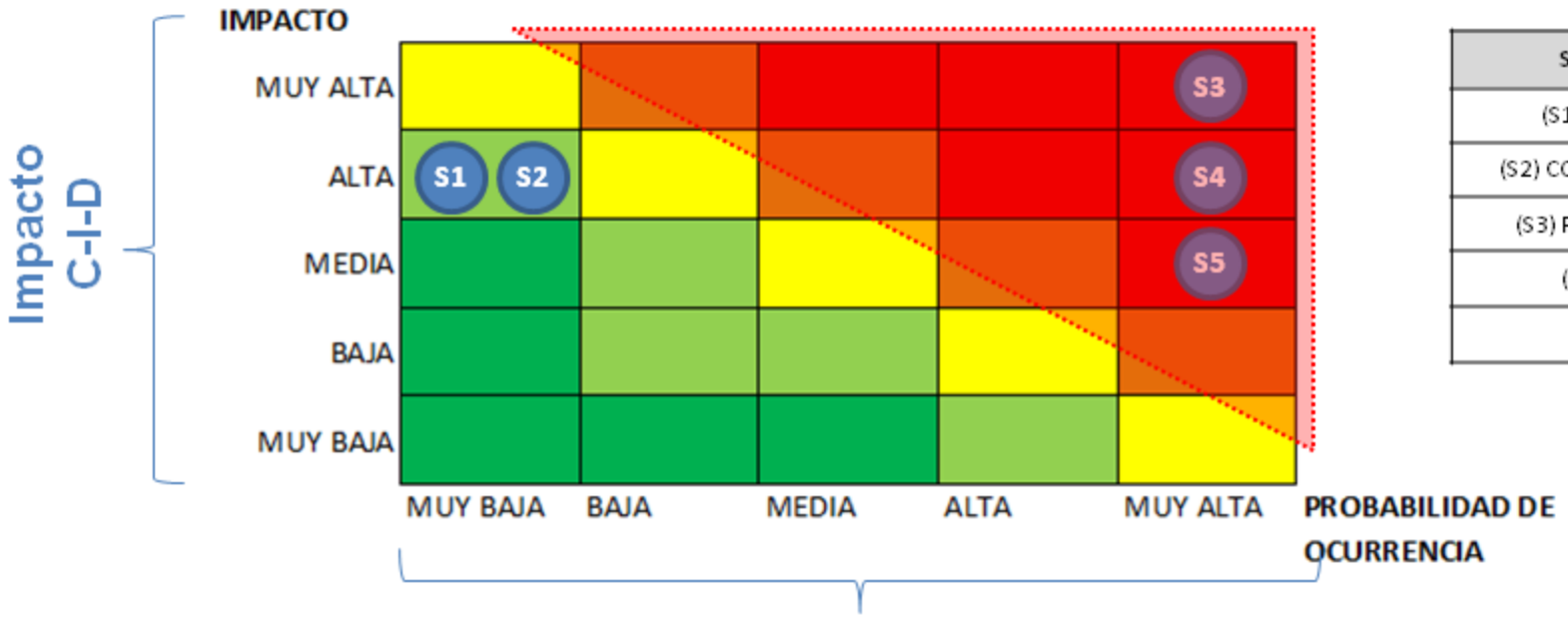
SERVICIO	CRITERIO						PROBABILIDAD DE OCURRENCIA
	CONTROL ACCESO	CONTINUIDAD NEGOCIO	CUMPLIMIENTO	PROTECCIÓN DE DATOS	INCIDENTES E INVESTIGACIÓN FORENSE	CONTROL DE CAMBIOS	
(S1) CORREO	✓	✓	✓	✓	✓	✓	MUY BAJO
(S2) COLABORACIÓN	✓	✓	✓	✓	✓	✓	MUY BAJO
(S3) REPOSITORIO	✓	✗	✓	✗	✗	✓	MUY ALTO
(S4) CRM	✓	✓	✗	✓	✗	✓	ALTO
(S5) ERP	✓	✓	✓	✓	✗	✓	MEDIO

Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

Cloud Security

✓Evaluación del riesgo de migrar un servicio a la nube



SERVICIO
(S1) CORREO
(S2) COLABORACIÓN
(S3) REPOSITORIO
(S4) CRM
(S5) ERP

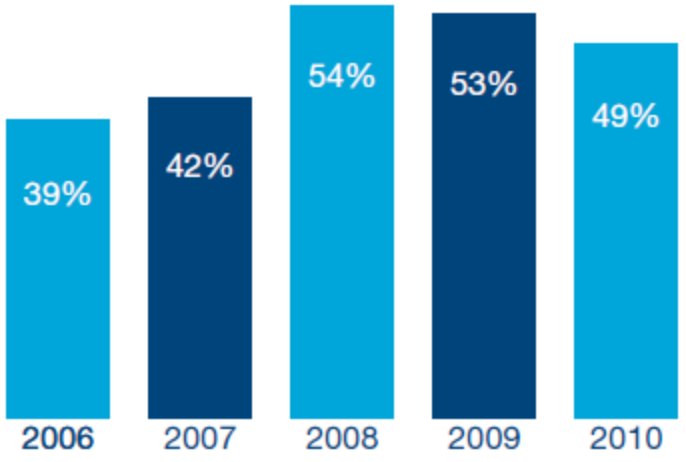
Controles de seguridad faltantes en el servicio del proveedor

Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

Sensibilización

•Las actividades de sensibilización se fortalecerán e incrementarán.



En 5 años todas las grandes y medianas empresas a nivel mundial deberán tener un programa de sensibilización implementado, y las pequeñas empresas empezarán también a tenerlo.

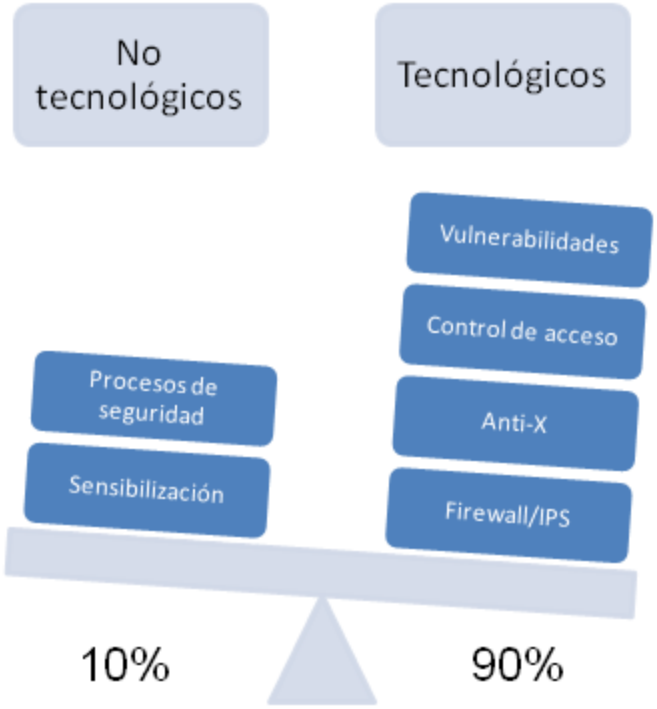
Fuente: PwC Global State of Information Security 2011

Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

Sensibilización

Presupuesto de inversión en controles de seguridad:



A pesar de que la alta gerencia sabe que el eslabón más débil en las organizaciones son las personas, no se invierte lo suficiente en sensibilización.

Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

Sensibilización

Temas de sensibilización:

Amenazas de nueva generación de dispositivos móviles

Amenazas del Teletrabajo

Amenazas de servicios Web 2.0, 3.0, 4.0…

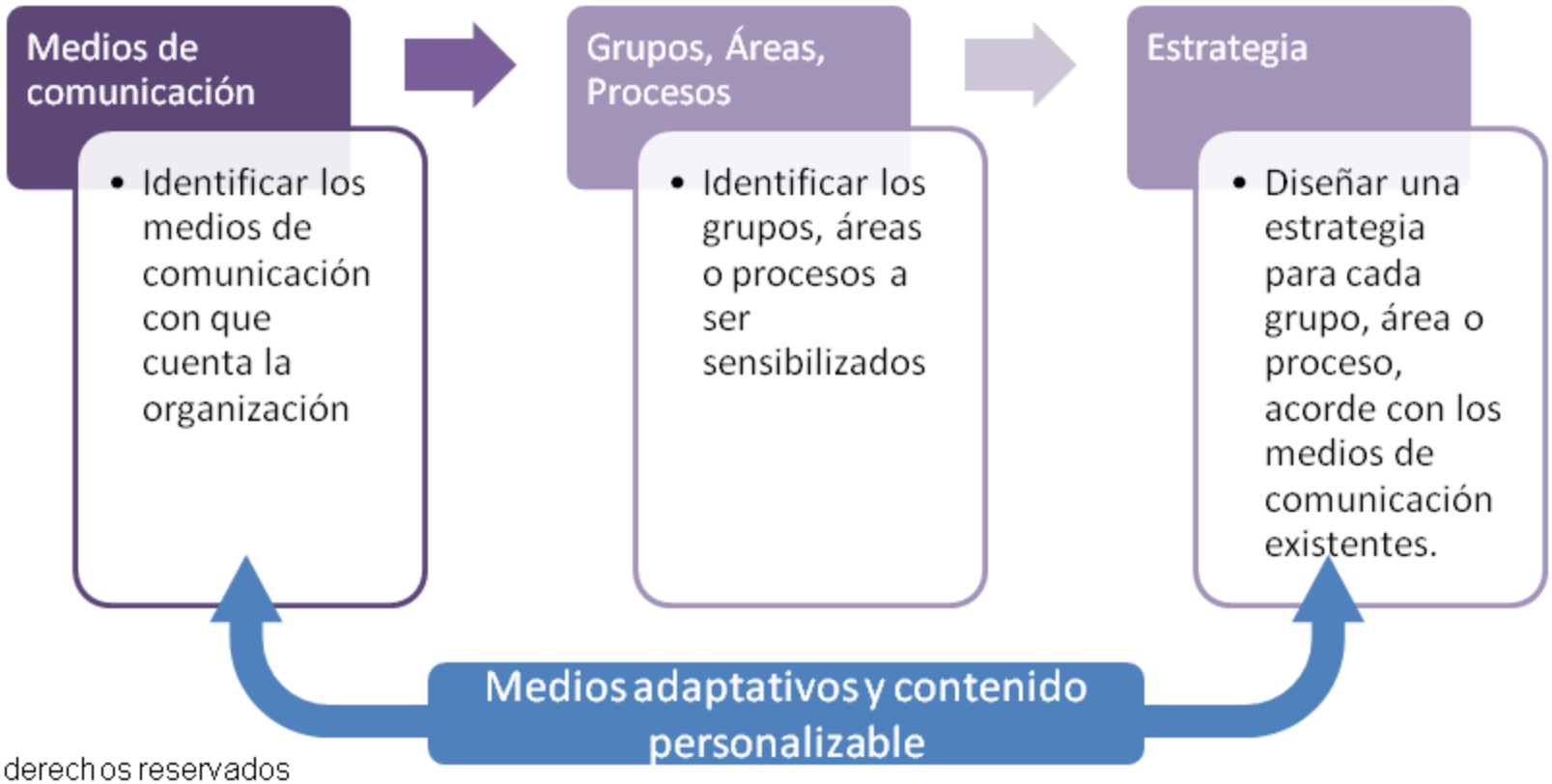
Amenazas de los servicios Cloud

Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

Sensibilización

Las estrategias de sensibilización deben mejorarse.



Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

Sensibilización

Cómo lograr que las personas adopten la seguridad de la información como práctica de su día a día?

- ✓ Cláusulas en el contrato
- ✓ Reglamento interno de trabajo
- ✓ Código de buen gobierno
- X Medición del Desempeño

Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

M-Commerce Security

El M-Commerce (Comercio a través de dispositivos móviles), ha venido creciendo los últimos años significativamente, con el aumento de competidores en tecnologías de dispositivos móviles y con las nuevas capacidades de estos dispositivos.

Algunos servicios de M-Commerce son: Pagos de servicios, compras en línea, entretenimiento, manejo de bancos, mercadeo y propaganda.

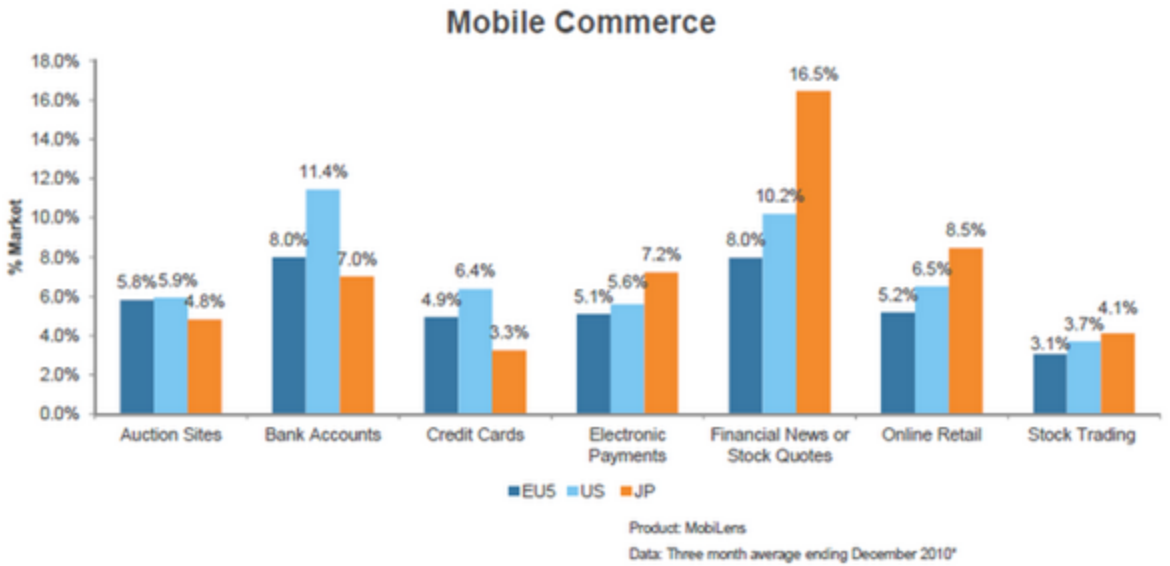
Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

M-Commerce Security

Mobile Phone Becoming a Transaction Medium

- In December 2010, 9.7 million Japanese mobile owners used mobile wallet to make a purchase



Fuente: The top 10 Countries For Mobile Commerce, Online Marketing Trends

Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

M-Commerce Security

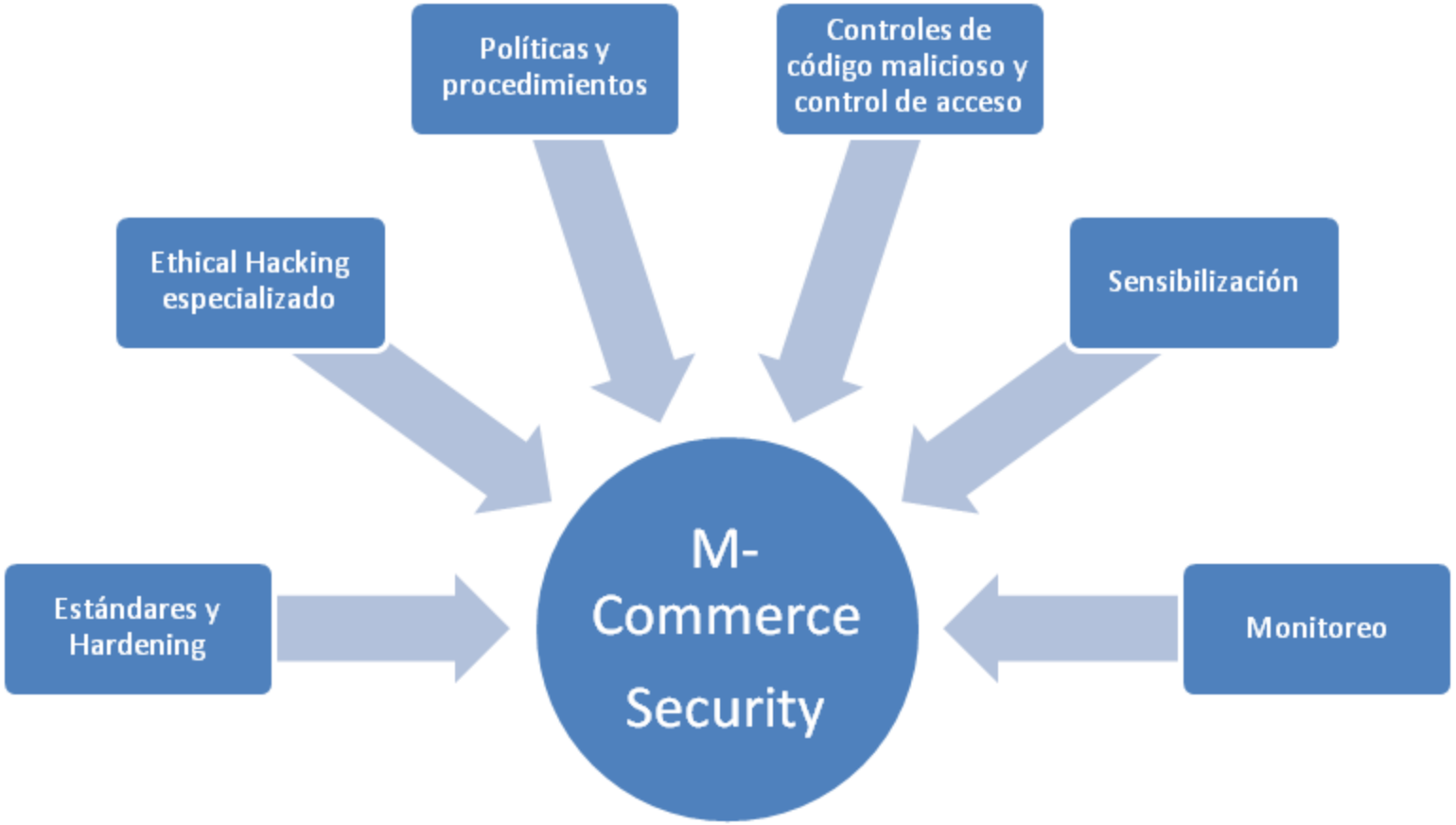
Amenazas

1. Pérdida o Robo
2. Código malicioso
3. Falta de hardening
4. Debilidades en los protocolos y/o en su implementación
5. Trazabilidad y auditoría
6. Esquemas de autenticación fuerte
7. Spoofing de la red o el sitio (phishing)
8. Protección de los datos almacenados en el dispositivo

Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

M-Commerce Security



Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

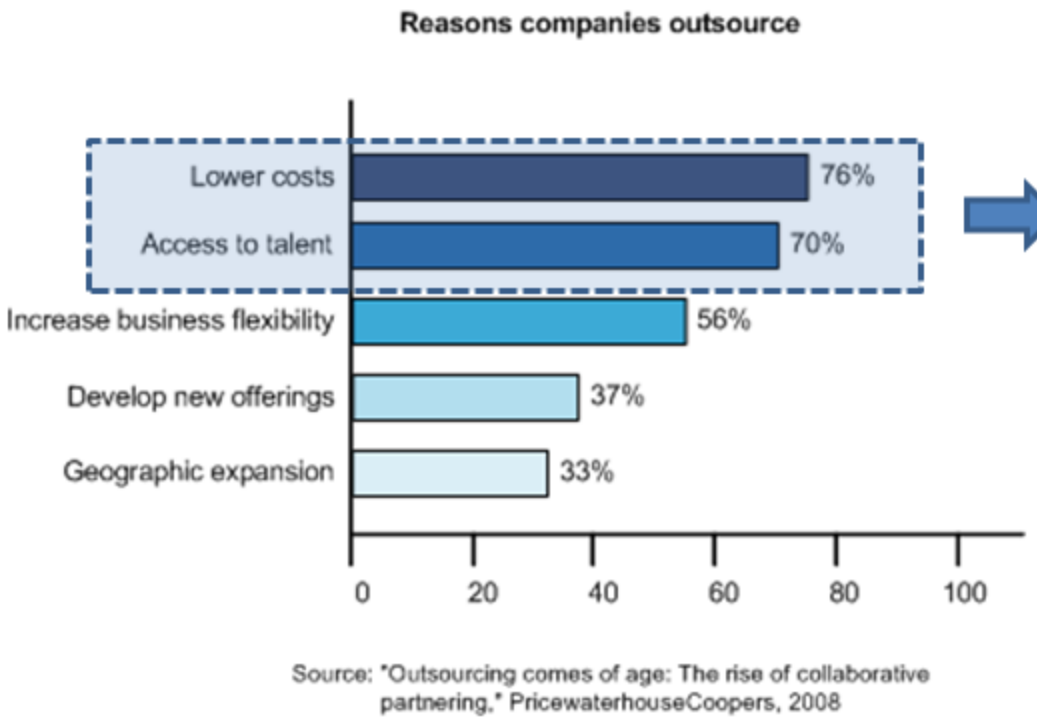
TERCERIZACIÓN DE LA OPERACIÓN

La tercerización de la seguridad o parte de las actividades se ha convertido en una realidad. Hemos visto como las organizaciones hoy han tercerizado servicios tales como: Ethical hacking, aseguramiento de infraestructura, monitoreo de incidentes, administración de infraestructura, no como un proyecto puntual sino como una actividad recurrente.

Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

TERCERIZACIÓN DE LA OPERACIÓN



Source: "Outsourcing comes of age: The rise of collaborative partnering," PricewaterhouseCoopers, 2008

Estas dos razones son las que hoy están impulsando la tercerización de la seguridad.

Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

TERCERIZACIÓN DE LA OPERACIÓN

Los Procesos críticos de seguridad que pueden ser tercerizados:

- ✓**Gestión de Vulnerabilidades** (Ethical Hacking)
- ✓**Gestión de Incidentes** (Monitoreo desde SOC)
- ✓**Gestión de Activos de Información** (levantamiento y mantenimiento de los activos de información y la clasificación de la información)
- ✓**Gestión de Riesgos** (Definición y actualización de las matrices de riesgos y los planes de tratamiento)
- ✓**Gestión de acciones correctivas y preventivas** (generadas a partir de la gestión de incidentes y vulnerabilidades)
- ✓**Gestión de la Continuidad del Negocio** (crear y actualizar el BCP).
- ✓**Gestión de Sensibilización** (crear, ejecutar y mantener la estrategia de sensibilización)
- ✓**Administración de dispositivos de seguridad**
- ✓**Auditorias al SGSI**

Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

TERCERIZACIÓN DE LA OPERACIÓN

Recomendaciones al tercerizar la seguridad:

✓Es importante tener en cuenta que los procesos de administración de dispositivos, auditoría al SGSI y Gestión de vulnerabilidades y de incidentes, no deberían tercerizarse con la misma empresa, ya que habría un problema de independencia.

✓Es necesario identificar claramente de donde a donde va el servicio tercerizado, para que no queden por fuera del alcance aspectos relevantes en la gestión de la seguridad.

Todos los derechos reservados

EVOLUCIÓN DE LA SEGURIDAD

TERCERIZACIÓN DE LA OPERACIÓN

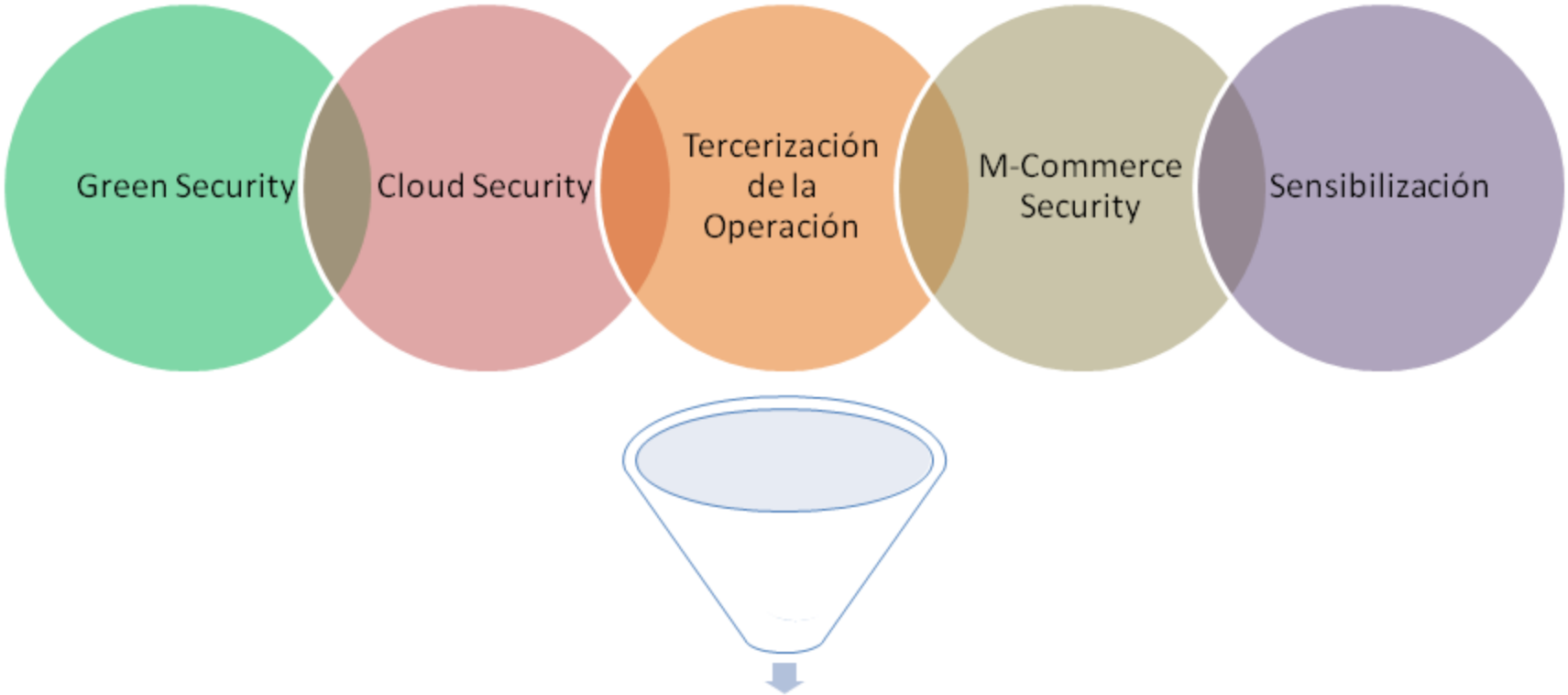
Recomendaciones al tercerizar la seguridad:

✓Es necesario revisar bien el gobierno de seguridad de la organización cuando se tercericen procesos, para identificar y establecer claramente cuales son sus responsabilidades y funciones.

✓Es necesario asegurar por contrato el cumplimiento de las políticas de seguridad de la organización y la regulaciones aplicables (p.e. CE-052)

Todos los derechos reservados

LA RE-EVOLUCION DE LA SEGURIDAD



Nueva planeación estratégica de seguridad

Todos los derechos reservados

AGENDA

- ✓El pasado de la seguridad
- ✓Los nuevos *drivers* y la evolución
- ✓Reflexión final

Todos los derechos reservados

REFLEXIÓN FINAL

Si hoy iniciara la seguridad de la información porque los primeros incidentes de seguridad se empezaran a percibir hoy…

iniciaríamos a llenarnos de controles tecnológicos de seguridad…

o iniciaríamos a sensibilizar a las personas?

qué sería mas efectivo y eficiente?

Todos los derechos reservados

REFERENCIAS

✓PwC, Global State of Information Security 2011
✓PwC, Global State of Information Security 2010
✓PwC, The World in 2050
✓PwC, Carbon Disclosure Project 2010 Global 500 Report
✓PwC, Communications review Vol. 15 No. 2
✓PwC, Outsourcing comes of age: The rise of collaborative partnering 2008
✓Radar Networks & Nova Spivack, 2007 Semantics of Social Connections
✓http://www.moveneutral.com/calculations
✓http://en.wikipedia.org/wiki/Mobile_commerce
✓http://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance
✓http://web.mit.edu/Saltzer/www/publications/protection/Basic.html
✓The top 10 Countries For Mobile Commerce, Online Marketing Trends

Todos los derechos reservados

PREGUNTAS O COMENTARIOS ?

Todos los derechos reservados

ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:
Una nueva década para avanzar

La RE-Evolución de la Seguridad

Felipe Silgado
CISSP, CISM, CRISC
Gerente TRS/ITE Advisory – PwC
felipe.silgado@co.pwc.com
http://www.pwc.com/co/es/seguridad-de-la-informacion/index.jhtml

A la memoria de José de Jesús Lozano Gutiérrez

Todos los derechos reservados