Risk Optimization management inside IT governance

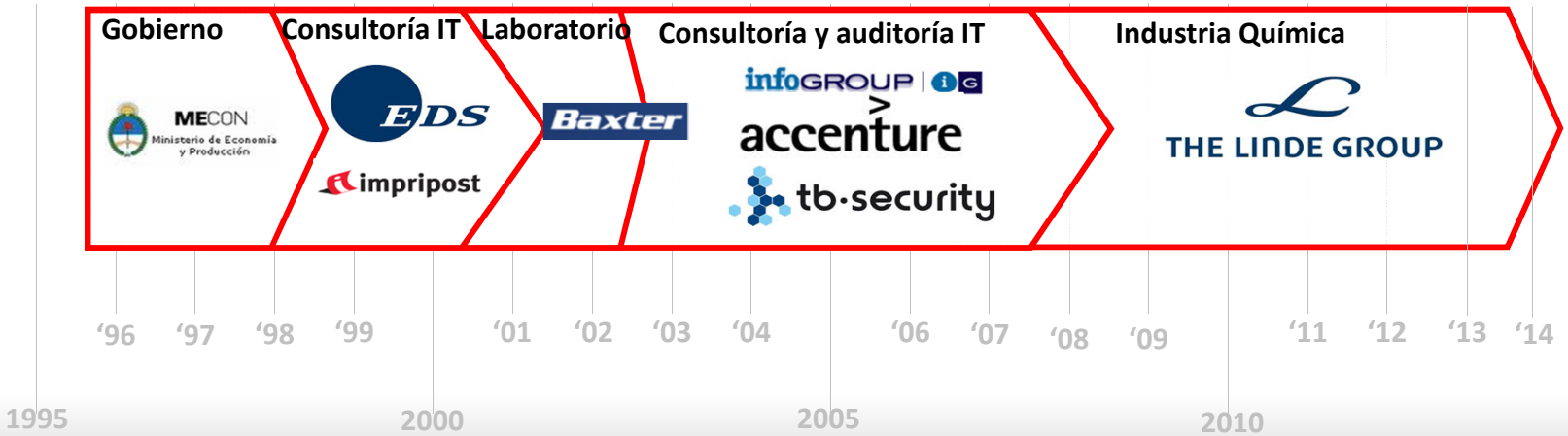
ISACA®
Trust in, and value from, information systems

THE LINDE GROUP

Bio y experiencia laboral

Ramiro Cid | ramiro@ramirocid.com | @ramirocid

- ✓ Spain & Portugal CISO & IT Manager en Linde
- ✓ Miembro del Linde European Regional Security Officers Team
- ✓ Miembro activo del Linde Global IT Security Committee
- ✓ Postgrado en Dirección de Empresas (IDEC-Universitat Pompeu Fabra),
- ✓ Licenciado en Sistemas de Información (Universidad de Buenos Aires)
- ✓ Certificaciones: CISM®, CGEIT®, ISO 27001:2013 LA , ISO 22301:2012 LA, ITIL® v.2 Foundation
- ✓ Profesional con más de 15 años de trayectoria en la industria de TI en diferentes sectores: Industria, Laboratorio, Banca, Gobierno, TI, etc., en diferentes empresas en España, Argentina y Andorra.



Agenda / Índice

1. Apetito al riesgo: 1er acercamiento	Slide 5
2. Preparación de las actividades de auditoría	Slide 6
3. Realización de la auditoría in situ	Slide 9
4. Preparación y distribución del informe de auditoría	Slide 11
5. Principales problemas encontrados respecto a la gestión de la Seguridad IT	Slide 13
6. Lecciones aprendidas	Slide 16

Cybersecurity Skills Crisis

Too Many Threats

62% INCREASE IN BREACHES **IN 2013**[1]

1 IN 5 ORGANIZATIONS HAVE **EXPERIENCED AN APT ATTACK**[4]

US $3 TRILLION TOTAL GLOBAL IMPACT OF **CYBERCRIME**[3]

8 MONTHS IS THE AVERAGE TIME **AN ADVANCED THREAT GOES UNNOTICED** ON VICTIM'S NETWORK[2]

2.5 BILLION **EXPOSED RECORDS** AS A RESULT OF A DATA BREACH IN THE PAST 5 YEARS[5]

Too Few Professionals

62% OF ORGANIZATIONS **HAVE NOT INCREASED SECURITY TRAINING IN 2014**[6]

1 OUT OF 3 SECURITY PROS ARE **NOT FAMILIAR WITH ADVANCED PERSISTENT THREATS**[7]

<2.4% **GRADUATING STUDENTS HOLD COMPUTER SCIENCE DEGREES**[8]

1 MILLION UNFILLED SECURITY JOBS WORLDWIDE[9]

83% **OF ENTERPRISES** CURRENTLY LACK THE RIGHT SKILLS AND HUMAN RESOURCES TO PROTECT THEIR IT ASSETS[10]

Enterprises are under siege from **a rising volume of cyberattacks.**

At the same time, the global demand for skilled professionals sharply outpaces supply. Unless this gap is closed, organizations will continue to face major risk. Comprehensive educational and networking resources are required to meet the needs of everyone from entry-level practitioners to seasoned professionals.

SOURCES: 1. *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **2.** *M-Trends 2013: Attack the Security Gap*, Mandiant, March 2013; **3.** *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **4.** *ISACA's 2014 APT Study*, ISACA, April 2014; **5.** *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **6.** *ISACA's 2014 APT Study*, ISACA, April 2013; **7.** *ISACA's 2014 APT Study*, ISACA, April 2014; **8.** *Code.org*, February 2014; **9.** *2014 Cisco Annual Security Report*; **10.** *Cybersecurity Skills Haves and Have Nots*, ESG, March 2014

CSX CYBERSECURITY NEXUS

ISACA® Trust in, and value from, information systems

Apetito al riesgo en una organización

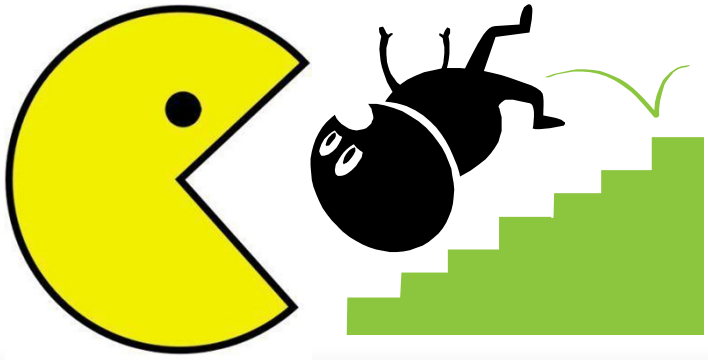
Madurez en la gestión del riesgo IT

Grado de madurez del "IT Governance"

+ Grado de alineamiento de IS con Negocio

+ Cultura organizacional

APETITO AL RIESGO



Preparación de las actividades de auditoría

Noviembre de 2013: Desarrollo de auditoría in situ interna a “un país de Europa”.

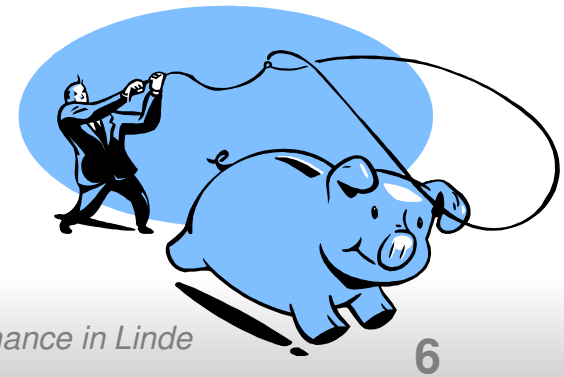
Previamente a la auditoría:

1) Se pidió al negocio que completara 2 plantillas para crear un BIA (Business Impact Analysis), 1ro: aplicaciones locales y 2do: aplicaciones globales.

En ambos casos se pidió:

Calcular impacto económico por pérdida de beneficio, productividad o incremento de costes operativos durante la duración de una contingencia (valor para cada aplicación), siendo el valor medido en un rango de:

- **Low:** hasta €10K
- **Medium:** desde €10K hasta €500K
- **High:** más de €500K



Preparación de las actividades de auditoría

Para cada uno de estos rangos, se pidió **calcular el valor del dinero perdido** teniendo en cuenta diferentes **períodos de tiempo** de duración de la contingencia, siendo los siguientes períodos:

- **8 horas**
- **1 día**
- **1 semana**
- **6 semanas**

Analizados los resultados se pudo ver que:

a) Varias aplicaciones de tipo **"low"** pasaban a **"medium"** luego de pasado una semana

b) Varias aplicaciones de tipo **"medium"** pasaban a **"high"** luego de pasado una semana

Preparación de las actividades de auditoría

2) Se envió el **Plan de Auditoría**: Descripción de las actividades.
Definición de los **objetivos**, **criterio** y **alcance**.

3) **Agenda de Auditoría:** Se **confirmaron las entrevistas con los "key users"** de varios departamentos (IS, Finanzas, Logística y Customer Service).

Un punto importante fue **fijar previamente los días/horas de las reuniones.** En estas se incluyó a personal de IS así como a varios departamentos del negocio.

4) Se **notificó al negocio la razón de la auditoría**, para que con su respaldo, el departamento de IS sepa la importancia de la misma.

Realización de la auditoría in situ

- ✓ Se realizaron entrevistas a IS y los departamentos de Comercial, Customer Services, Logística, Finanzas (conjuntamente en algunos casos con alguien de IS).
- ✓ Se efectuaron checklist con IS de grados de cumplimiento de la seguridad IT en distintos ámbitos (seguridad física, lógica, DRP, etc.)
- ✓ Se realizó una visita de revisión al Data Center.

Realización de la auditoría in situ

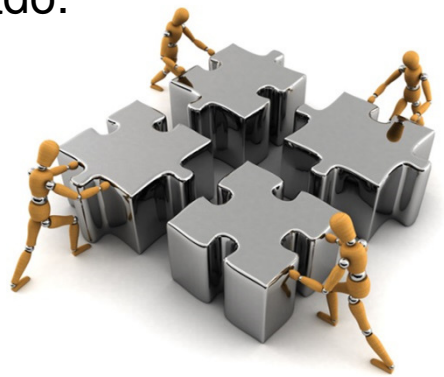
- ✓ Luego de finalizadas las entrevistas cada día los 3 auditores realizaron una reunión para comentar los principales hitos y GAPs encontrados en las entrevistas del día.
- ✓ Durante la auditoría se realizó la 1era versión del borrador del informe de auditoría.

Preparación y distribución del informe de auditoría

Una vez obtenidos los GAPs (no conformidades):

1) Se enviaron los resultados (borrador de informe de auditoría) al IS Manager del país auditado para solicitar su respuesta. El feedback recibido se tuvo en cuenta para el informe definitivo.

2) Una vez contrastadas las diferencias y hechas las correcciones, se envió los resultados al IS Manager para Europa y a los directores de las diferentes áreas del negocio del país analizado.

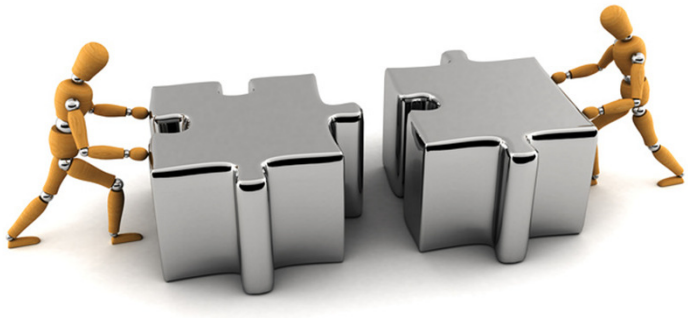


Preparación y distribución del informe de auditoría

Una vez obtenidos los GAPs (no conformidades):

3) Se convocó una teleconferencia para analizar los principales riesgos encontrados (centrándose de alto impacto y alta o media probabilidad).

4) Se desarrolló un calendario de acciones y responsables de la misma para poder llevar a cabo una mejora de la situación encontrada durante la auditoria.



Principales problemas encontrados respecto a la gestión de la Seguridad IT

Principales problemas encontrados para poder poner en práctica las mejoras:

1) **Escasez de recursos (personas) en el área de IS**. El departamento se queja de que el negocio no le proporciona el presupuesto necesario para poder realizar grandes mejoras en seguridad IT.

Con ello no se puede conseguir un grado de madurez en la gestión de la seguridad informática acorde a las necesidades del negocio.

Principales problemas encontrados respecto a la gestión de la Seguridad IT

Principales problemas encontrados para poder poner en práctica las mejoras:

2) **Falta de conocimiento por parte de IS de las necesidades del negocio.** Se detectaron 2 reclamos provenientes de casi todas las áreas del negocio:

a) IS no realiza **formación o comunicación a los empleados** respecto buenas prácticas en seguridad y uso de los sistemas de información y activos IT.

Problema difícil de sortear debido al limitado presupuesto de IS lo que dificulta realizar formaciones con empresas externas (por limitación del CAPEX) o internas con personal interno de IS (por limitación de recursos y saturación de carga de trabajo)

Principales problemas encontrados respecto a la gestión de la Seguridad IT

Principales problemas encontrados para poder poner en práctica las mejoras:

b) Finanzas había sufrido recientemente 2 ataques de **Ingeniería Social** donde por teléfono unas personas simularon ser personal del banco con el que trabaja la empresa y estuvieron cerca de lograr realizar una estafa.

Ambos ataques fueron evitados, sin embargo el departamento obró más por sentido común que por buenas prácticas en seguridad IT o procedimientos escritos a seguir ante este tipo de ataques.

Lecciones aprendidas

1) IS debe conocer más las necesidades del negocio en relación a la seguridad IT (preguntar, reunirse, encuestas, auditorías internas,…).

2) Poder gestionar seguridad IT de una manera efectiva el Departamento de IS requiere un mínimo de recursos (idealmente dedicados en forma exclusiva).

Lecciones aprendidas

3) La formación en seguridad IT a todo el staff de la organización es clave.

4) Las incidencias en seguridad IT son reales y se concretizan día trás día, hace falta concientizar más a la empresa para que entienda que los riesgos siempre existen y el impacto que puede ocasionar una incidencia puede ser mucho más cara que minimizar los riesgos a través de una gestión efectiva y eficiente de los mismos.

¿Dudas? ¿preguntas?

¡ Muchas gracias !

Ramiro Cid

CISM, CGEIT, ISO 27001 LA, ISO 22301 LA, ITIL

ramiro@ramirocid.com

http://ramirocid.com

@ramirocid

http://www.linkedin.com/in/ramirocid

http://es.slideshare.net/ramirocid

http://www.youtube.com/user/cidramiro