Madurez de la Seguridad en Organizaciones de Latino América

Vicente Gozalbo Moragrega
World Wide Security Tiger Team
Tef: +573182210281
vgozalbo@co.ibm.com

Boston MA, USA
21 de Octubre de 2014

Agenda

- Presentación (5’)
- Introducción al ESMW - Enterprise Security Maturity Workshop (15’)
- Análisis de los Datos correspondientes a LatinoAmerica (30’)
- Preguntas y Respuestas (10’)

Presentación

Vicente Gozalbo - Presentación

- World Wide Security Tiger Team Senior Sales Consultant

- Ingeniería de Telecomunicaciones, UPV, España
- Master en Redes de ordenadores y Comunicaciones avanzadas, UPV España (1999)
- Executive MBA (Escuela Europea de Negocios, 2005)
- Diplomado Comercio exterior (EADA – China, 2006)

- + 20 años de experiencia en IT,
- 14 Años de experiencia en Seguridad IT
  - IBM (6 + 7 años),
  - RSA Security – Spain & Portugal Country Manager (2 años),
  - Selesta BP, Integrador (4 años)

- Experiencia Laboral en +25 paises, cientos de empresas.
- Miembro del Subcomité 27 de normalización de Tecnologías de Seguridad (Aenor - ISO, España)
- Foco en Banca, Gobierno y Telecomunicaciones

- Decenas de referencias en LA y Europa, Grupo AVAL, ScotiaBank, Santander, Davivineda, BBVA, Telefonica, Ecopetrol, Tenaris, Banco de España, Banco Pichincha, YPF….

Introducción al taller de madurez de seguridad corporativa

¿Por donde Empiezo ?

IBM Center for Applied Insights

A new standard for security leaders

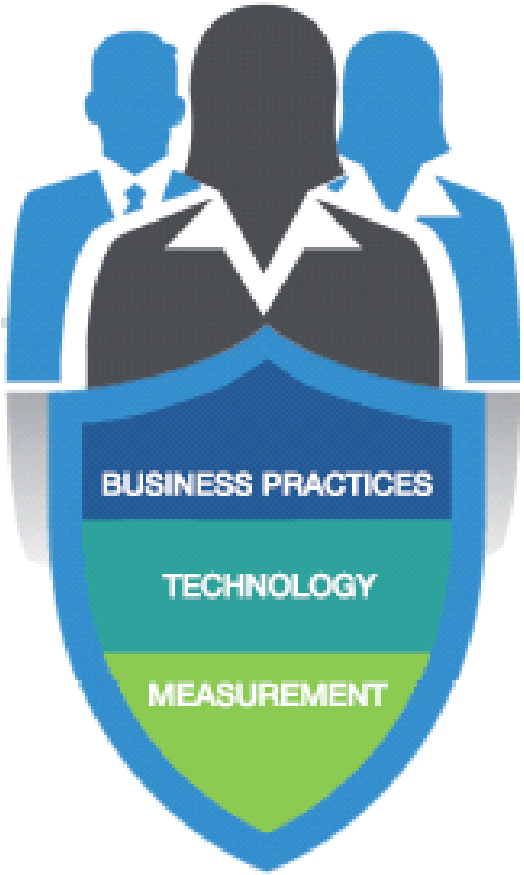
Insights from the 2013 IBM Chief Information Security Officer Assessment

IBM Center for Applied Insights

Finding a strategic voice

Insights from the 2012 IBM Chief Information Security Officer Assessment

Aquellos profesionales que tienen la combinación adecuada de practices de seguridad y que acometen los retos actuales están evolucinoando hacia un Nuevo estándar de lider de seguridad.



- **Formalice su rol como CISO**
- **Establezca una estrategia de seguridad**
- **Desarrolle relaciones de negocio efectivas**
- **Construya Confianza**
- **Invierta en tecnología avanzada cuando ésta sea necesaria para el negocio.**
- **Refuerce su seguridad en el entrono móvil**
- **Comparta información**
- **Haga foco en el impacto económico del riesgo.**
- **Preste atención a las preocupaciones sobre riesgo reputacional y satisfacción del cliente.**
- **Traduzca e integre métricas.**

"Strategic vision… Global consistency… Lots of communication… speak business value, understand risk… minimize the impact… be on the bleeding edge…"

Características del Worksop de Madurez de Seguridad de IBM (ESMW)

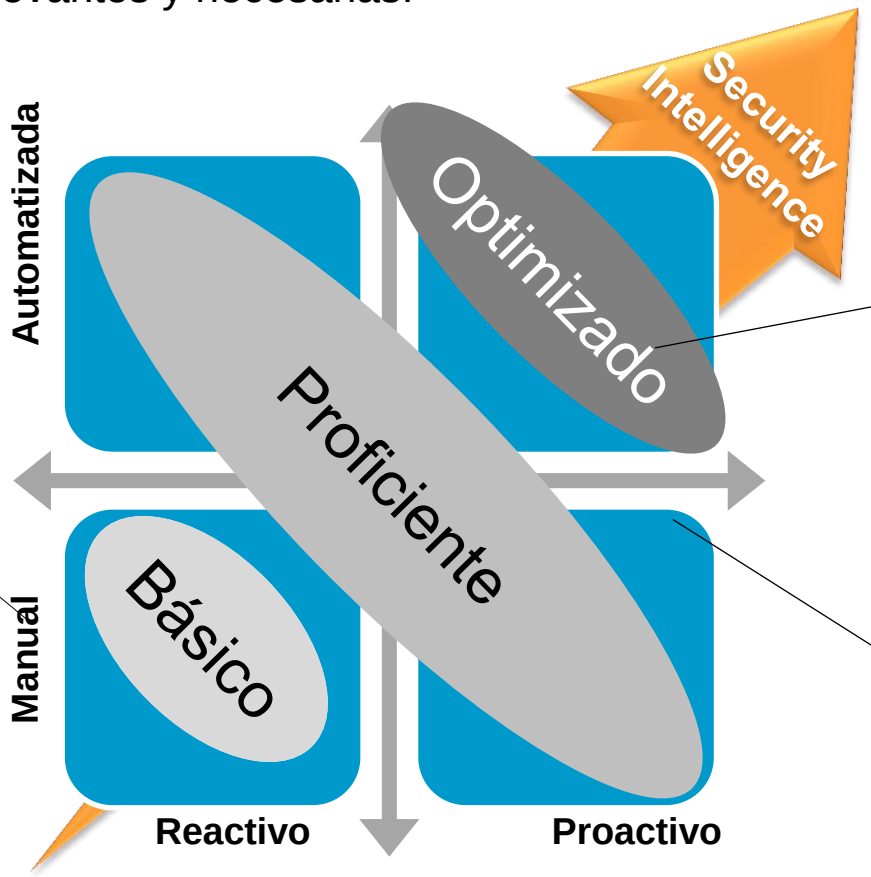
- Objetivos
  - **Revisar** de la madurez (1-5) de 35 Controles de Seguridad en 5 ámbitos:
    - Seguridad en Infraestructuras
    - Seguridad en Aplicaciones
    - Seguridad de los Datos
    - Seguridad de las Identidades
    - GRC e inteligencia de Seguridad
  - **Hallar** el estado de la **seguridad actual** de la organización
  - **Establecer** el estado de la madurez de la **seguridad objetivo** en base al negocio
  - **Diseñar** una **estrategia corporativa** y acciones tácticas para alcanzarlo

- Duración: en 3- 4 semanas se realizan:
  - 5 Teleconferencias con entrevistas
  - 1 Taller de duración de un día completo
  - 1 Presentación ejecutiva de resultados
  - 25 Horas de Dedicación en total

Enterprise Security Maturity Workshop

Esta valoración de alto nivel evalua la posición de seguridad en cinco áreas **Analítica de la Seguridad y GRC, Personas, Datos, Aplicaciones, Infraestructura**

Luego, se recomendarán evaluaciones / análisis contextuales de continuación en las dimensiones que son relevantes y necesarias.

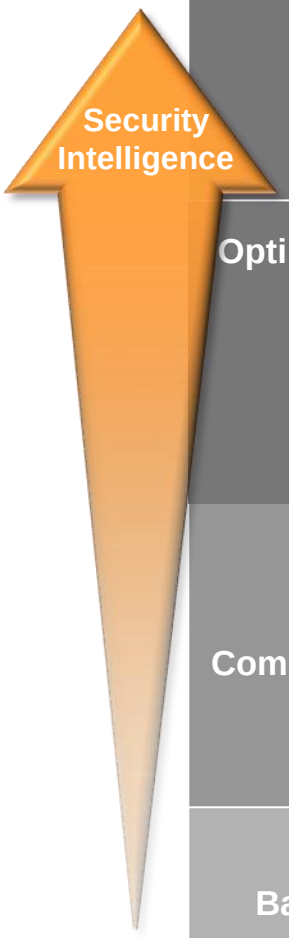


Básico
Las organizaciones emplean ***protección de perímetro***, que regula la generación de repostes manuales de acceso y *feeds*

Optimizado
Las organizaciones usan analítica de seguridad ***predictiva y automatizada*** para impulsar hacia una ***inteligencia de seguridad***

Proficiente
La seguridad está dividida en el ***tejido de IT*** y **operaciones de *negocio***

El concepto de “Security Intelligence” permite avanzar controles hacia una seguridad optimizada



	Security Intelligence: Gestión de Eventos e Información de Seguridad (SIEM) Correlación Avanzada y análisis profundo Investigación de las amenazas externas.			
Optimizada	Análisis de Roles Gobernanza de la identidad Control de usuarios privilegiados	Análisis de los flujos de datos Gobernanza de la información	Aplicaciones Seguras por reingenieria de procesos Detección del Fraude	Monitoreo de red avanzado Forénsica y minería de datos de seguridad Sistemas Críticos Seguros
Competente	Aprovisionamiento de usuarios Gestión de Accesos Autenticación Robusta	Monitoreo de Accesos DLP Prevención de pérdida de datos	Cortafuegos de aplicación Escaneo en código fuente	Seguridad en entoros virtualizados Gestión de Activos Gestión de la seguridad en la red y en el endpoint.
Basica	Directorio Centralizado	Cifrado Control de Accesos	Escaneo de vulnerabilidad en Aplicacaciones	Seguridad Perimetral Anti-virus
	Personas	**Datos**	**Aplicaciones**	Infraestructuras

Los Controles de Seguridad

Governance, Risk, Compliance	
1	Information Security Policy
2	Enterprise Security Architecture
3	Governance Structure
4	Threat Risk Assessment
5	Information Asset Profile
6	Security Risk Management
7	Regulatory Compliance
8	Awareness Training
9	Incident Response and Management
10	CERT

Gestión de Identidad	
11	Background Screening
12	Identity Establishment
13	Single Sign-on
14	Authentication Services
15	Access Control Services
16	User Provisioning
17	Other Entity Provisioning
18	Identity Credential Management
19	Privileged & Shared Identity Management

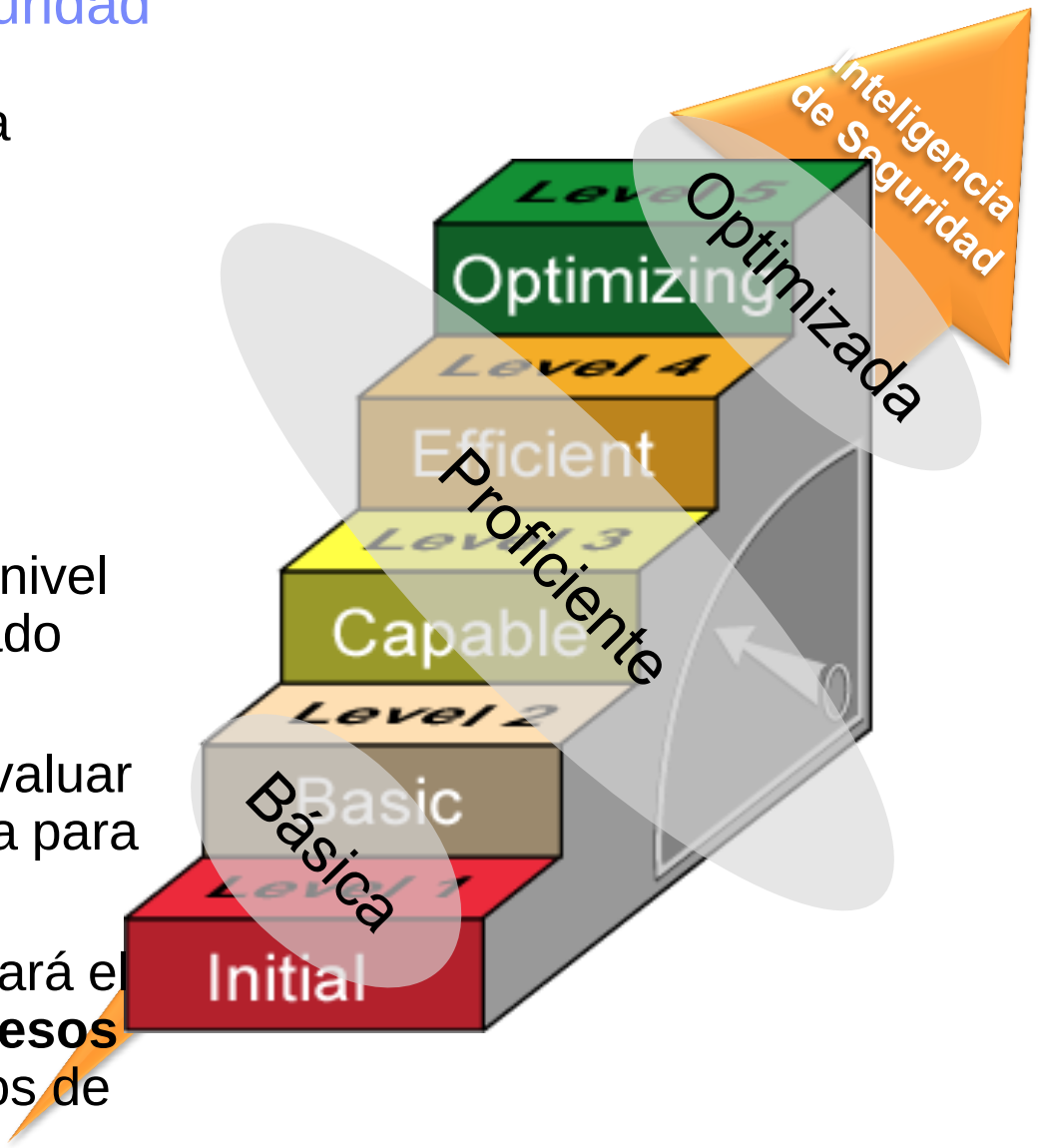
Datos	
20	Fraud Detection
21	Data Transaction Security
22	Database Configuration
23	Master Data Control
24	Key Management
25	Data Lifecycle Management
26	Security in Business Continuity Planning

Aplicaciones	
27	Security in SDLC Process
28	Secure Coding Practices
29	Operational Application Support Environment
30	Design Patterns

Infraestructuras	
31	Remote Access Infrastructure
32	Intrusion Defence
33	Network Security Infrastructure
34	Standard Operating Environment
35	Patch Management
36	Vulnerability Scanning and Assessment
37	Event Correlation
38	Asset Management

El modelo de Madurez de Seguridad de IBM proporciona la base para medir la posición de seguridad

- Los controles se describen a través de un modelo de capacidades
- El modelo de capacidades proporciona 5 niveles para identificar una posición de seguridad para cada control
- Cada control se mide por el nivel de riesgo de negocio aceptado asociado con cada nivel
- La valoración se usa para evaluar su posición actual y deseada para cada control.
- La valoración también evaluará el balance de **Personas, Procesos** y **Tecnología** en los dominios de seguridad



IBM Security Maturity Model – Ejemplo: Política de Seguridad

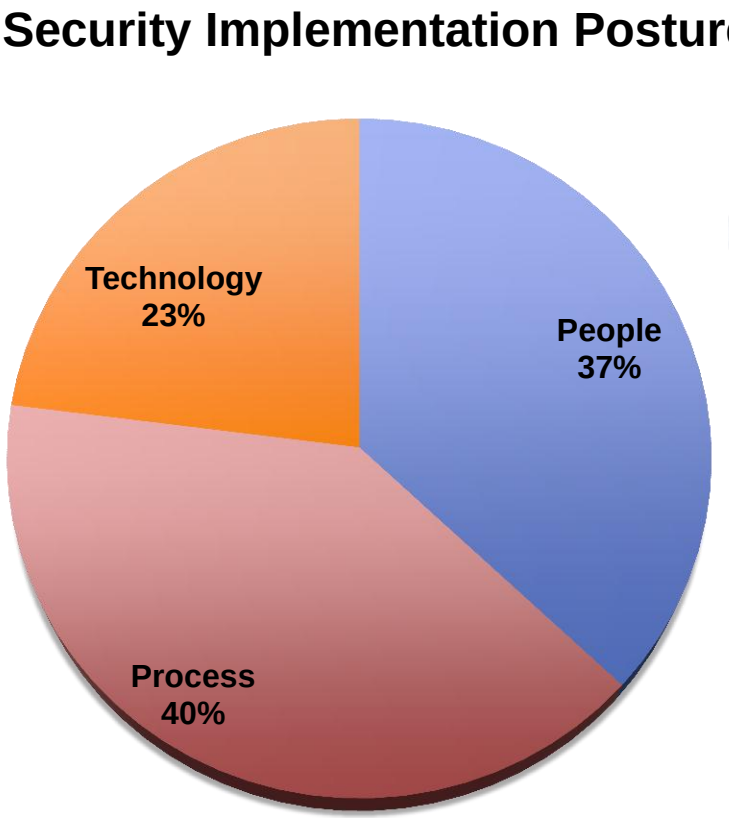
IBM Security Capability Model	
Nivel	**Descripción**
1 – Inicial	Los procesos, políticas y sistemas de seguridad se caracterizan como ad hoc, incluso de forma caótica, y puede variar de una unidad de negocio a otra unidad de negocio. Se definen pocos procesos y el éxito depende del esfuerzo individual y los actos heroicos. Los procesos pueden ejecutarse manualmente o a través de sistemas rudimentarios o anticuados. Los procesos y sistemas se visualizan como fuertes inhibidores a nuevos negocios y a la adopción de nuevos modelos de tecnología.
2 - Básico	Los procesos y políticas de seguridad básicos se establecen al punto de que se puede intentar repetir los mismos pasos. Los procesos se pueden ejecutar manualmente pero típicamente se ejecutan usando algún nivel de automatización básica. Existe un nivel básico de uniformidad empresarial en las unidades de negocio. Los procesos y sistemas se visualizan como inhibidores moderados a nuevos negocios y a la adopción de nuevos modelos de tecnología.
3 - Capaz	Los procesos y políticas de seguridad se documentan, estandarizan e integran en un proceso y política estándar en toda la empresa. Todas las unidades de negocio utilizan versiones aprobadas, adaptadas del proceso, políticas y sistemas de tecnología estándar de la organización. Todas las unidades de negocio comprenden y se adhieren consistentemente a las políticas empresariales. Los procesos y sistemas se visualizan como al menos neutrales a nuevos negocios y a la adopción de nuevos modelos de tecnología.
4 - Eficiente	Las medidas detalladas del cumplimiento y efectividad de políticas personalizadas se reúnen en toda la empresa. Tanto los procesos como los sistemas se comprenden y controlan cuantitativamente. Los procesos y sistemas se visualizan como activadores (*enablers*) de nuevos negocios y a la adopción de nuevos modelos de tecnología.
5 - Optimizar	El mejoramiento continuo de procesos de seguridad es activado a través de la retroalimentación cuantitativa del proceso y los sistemas, y desde el pilotaje de ideas y tecnologías innovadoras. Los procesos y sistemas de seguridad se visualizan como fuertes activadores de nuevos negocios y a la adopción de nuevos modelos de tecnología.

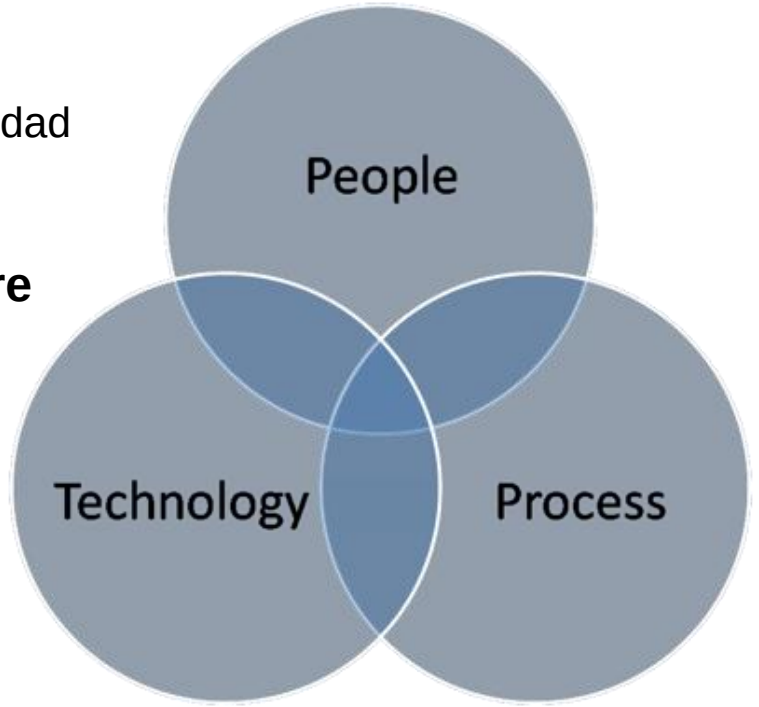
Workshop Questionnaire

No	Security Capability	Maturity Level / Measurements					Comments and Observations
		Current Level	People	Proccess	Technology	Target Level	
GRC							
1	Information Security Policy	Level 3	20%	60%	20%	Level 4	Needs further Awareness training
2	Enterprise Security Architecture	Level 2	40%	60%	0%	Level 5	Modeling tools would be beneficial to the proccess
3	Governance Structure	Level 3	40%	50%	10%	Level 3	
4	Threat Risk Assessment	Level 2	50%	50%	0%	Level 4	
5	Information Asset Profile	Level 1	20%	30%	50%	Level 5	

Security Implementation Insight – Balance de Personas, Procesos, Tecnología

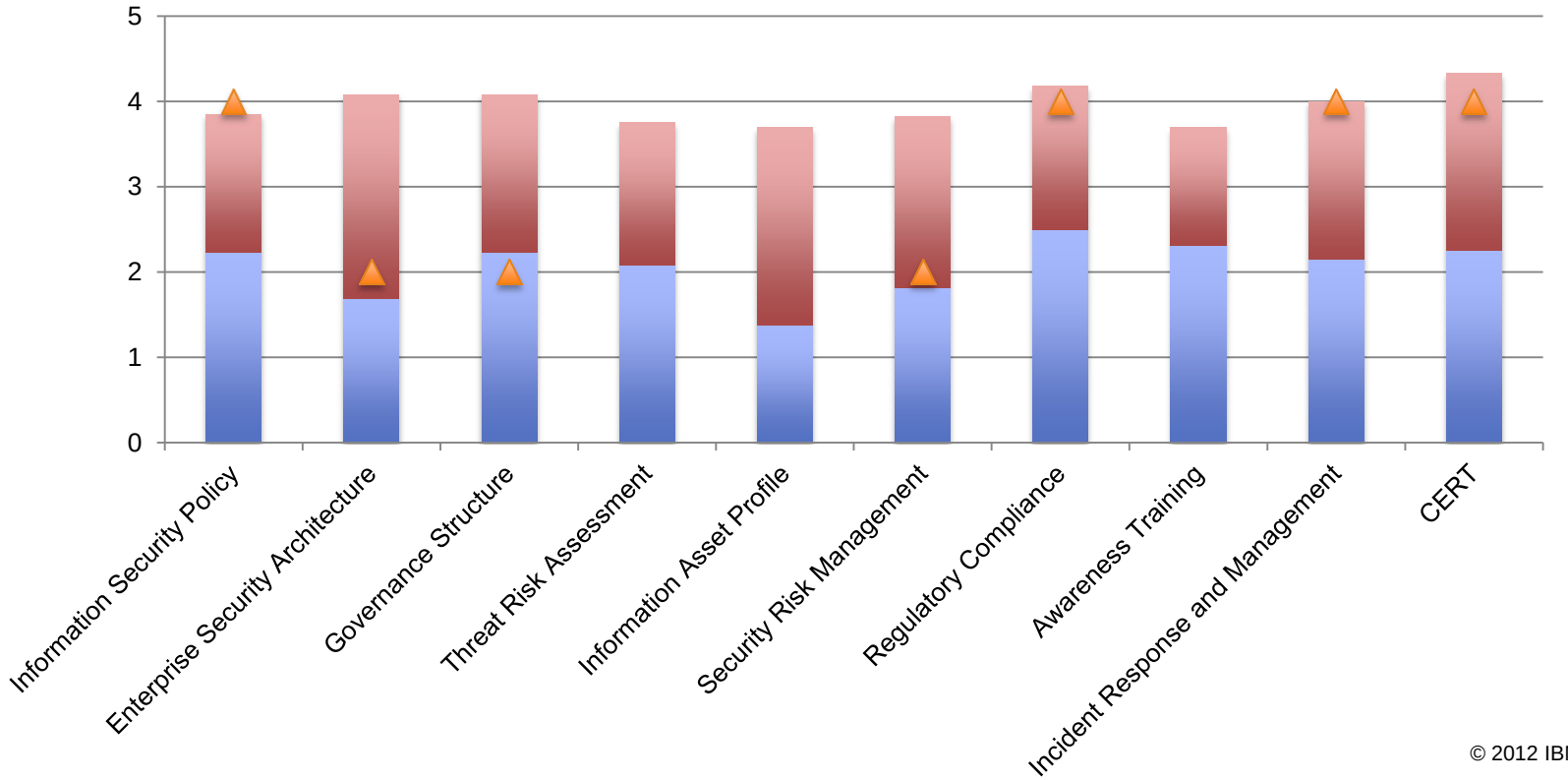
- Cómo se implementan los controles de seguridad en su organización hoy





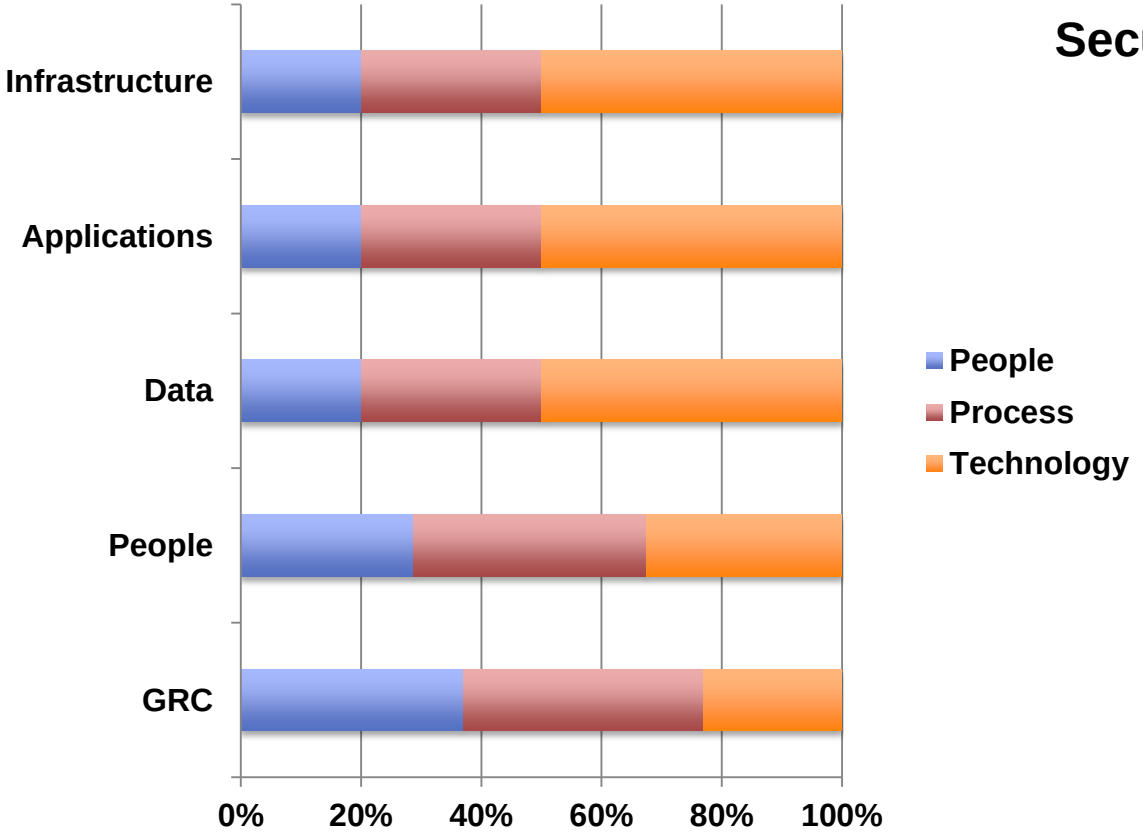
Resultados Ejemplo del Taller (GRC Domain)

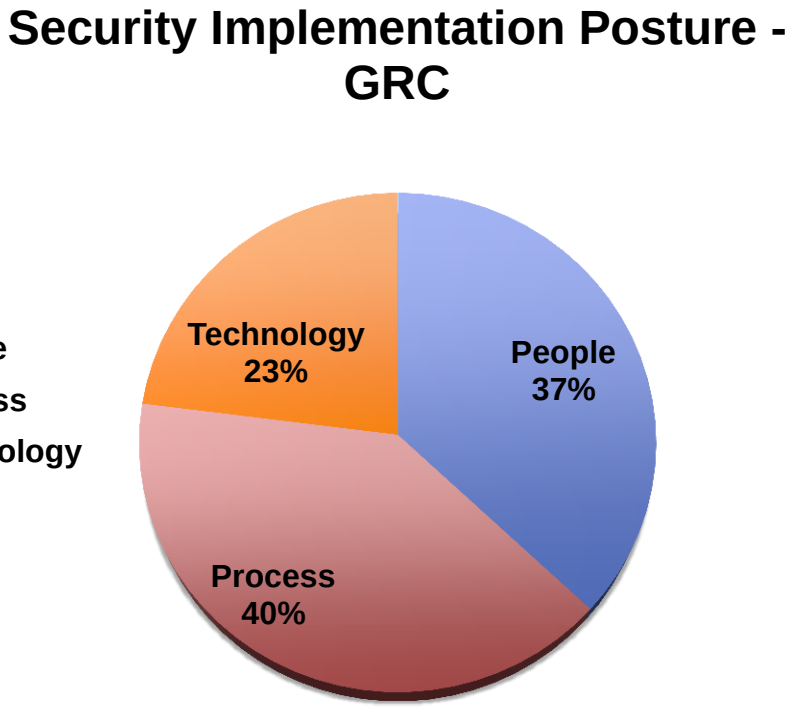
- Los resultados contienen una comparación gráfica de los niveles de madurez actual (Azul) y objetivo (rojo) y la posición de la industria, donde esté disponible (triangulo)
- Cada sección tiene un cuadro similar que proporciona una comparación para todos los controles de seguridad



Resultados Ejemplo del Taller – Resumen

- Este es un resumen de un taller de madurez hipotético que muestra la mezcla actual de Personas, Procesos y Tecnología que se utiliza para implementar la seguridad en la organización.



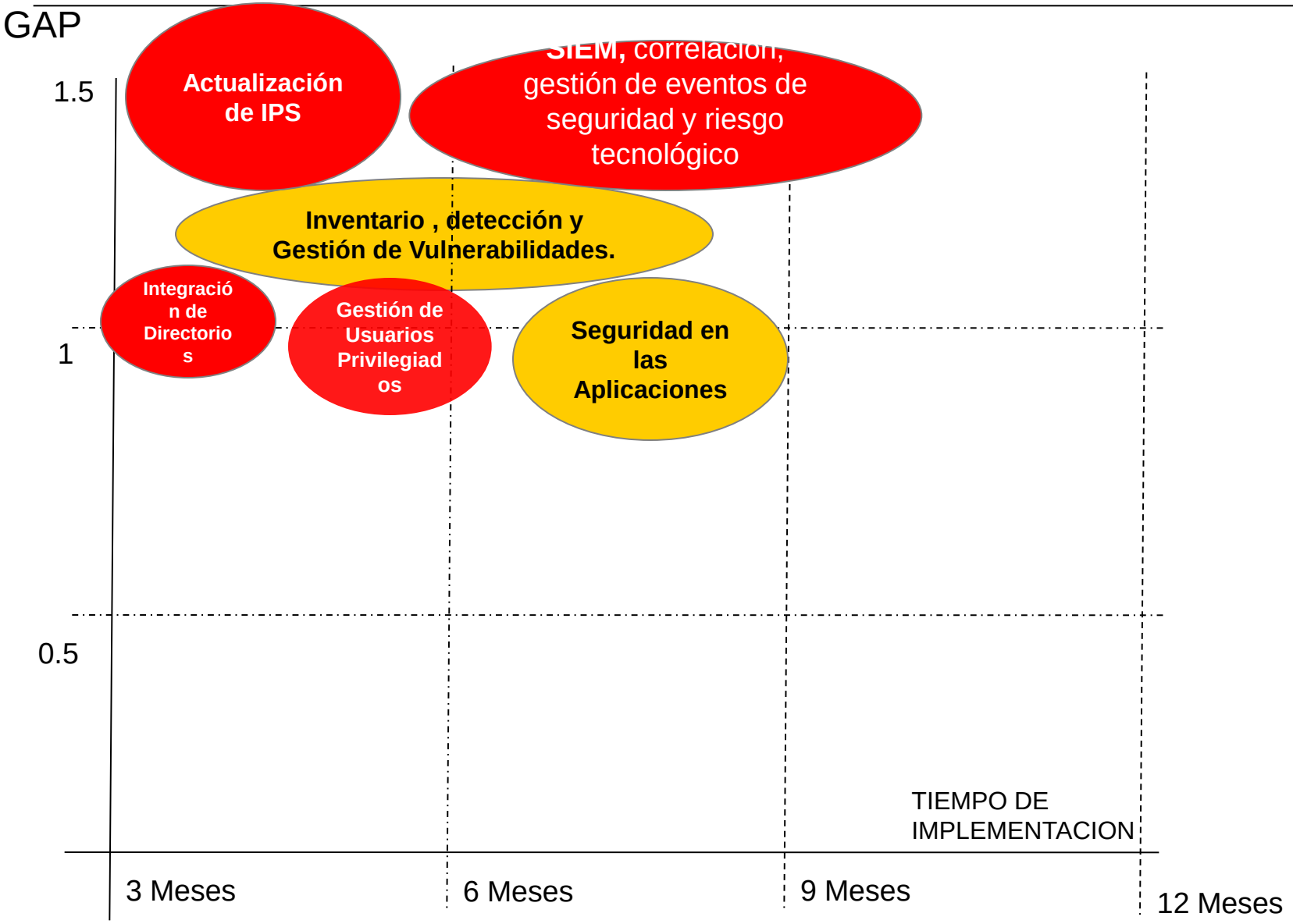


Visión táctica

Controles con más GAP

Domain	Control	Current Maturity	Gap	Target Maturity
Infrastructure	Intrusion Defence and Protection	2.5	1.5	4
People	Identity Establishment	4	1	5
Application	Application Inventory	2	1	3
People	Persons Identity Lifecycle Management	2.5	1	3.5
People	System and Service Account Lifecycle Mgmt	2	1	3
GRC	Regulatory Compliance	3	1	4
Data	Fraud Prevention & Detection	2	1	3
People	Remote Access To Corporate Data and Apps	2	1	3
People	Privileged & Shared Identity Management	2	1	3
Data	Data Classification & Database Configuration	2	0.5	2.5
Infrastructure	Asset Management	2	0.5	2.5
Infrastructure	Vulnerability Scanning & Assessment	2.5	0.5	3
Data	Data Transaction Security	2	0.5	2.5
Application	Secure Design & Threat Modelling	2.5	0.5	3
GRC	Information Security Policy	2.5	0.5	3
Data	Data Lifecycle Management	2	0.5	2.5
Infrastructure	Patch Management	2.5	0.5	3
Application	Secure Coding Practices	3	0.5	3.5
GRC	Security Risk Management	2.5	0.5	3
GRC	Incident Response & Management	2	0.5	2.5
GRC	Security in Business Continuity Planning	2	0.5	2.5
Infrastructure	Network Security Infrastructure	2	0.5	2.5
People	Authentication Services & SSO	2	0.5	2.5
Application	Application Security Assessment & Testing	2.5	0.5	3
GRC	Security Culture & Awareness Training	2	0.5	2.5
Application	Vulnerability Remediation & Risk Mitigation	3	0.5	3.5
GRC	Enterprise Security Architecture	2	0.5	2.5
Infrastructure	Event Correlation	2	0	2
GRC	Governance Structure	3	0	3
Infrastructure	Standard Operating Environment	2.5	0	2.5
GRC	Information Asset Profile	2	0	2
GRC	Threat Risk Assessment	3.5	0	3.5
Data	Encryption & Key Management	2	0	2
People	Authorization Services	2.5	0	2.5

Visión estratégica - Roadmap



Madurez de los controles de Seguridad en Latino América

Ejecución del ESMW

- Realizado en más de 80 clientes seleccionados en todo el mundo de todos los sectores
- En Latinoamérica se ha ejecutado en más de 15 clientes de 9 países. (Mexico, Guatemala, Costa Rica, Panamá, Colombia, Peru, Ecuador, Venezuela, Chile)
- Sectores principales son Banca y Finanzas y grandes grupos industriales.
- Entrevistados más de 200 especialistas de 15 organizaciones públicas y privadas.
- Se presentan los resultados de los 5 controles con más madurez, y los 5 controles con menos madurez

Estadísticas Comparativas

5 Mejores controles - Media

Domain	Control	Current Maturity	Gap	Target Maturity
GRC	Regulatory Compliance	4	1	5.00
People	Identity Credential Management	3.1	1.3	4.40
GRC	Security Culture & Awareness Training	3	1.5	4.50
GRC	Information Security Policy	2.75	1.09	3.84
Application	Application Security Assessment & Testing	2.74	1.37	4.11

Barings Bank (de 1762 a 1995) fue la compañía bancaria comercial más antigua de Londres hasta su colapso en 1995 después de que uno de los empleados, Nick Leeson, perdiera 827 millones de libras, aproximadamente 1200 millones de dólares en 1995, fundamentalmente especulando en contratos de futuros.

Índice [ocultar]

1 Historia
2 Acontecimientos que llevaron al colapso del Banco Barings
3 Véase también
4 Otras lecturas
5 Enlaces externos

Barings Bank

Industria	Servicios financieros
Fundación	1762
Fundador(es)	Sir Francis Baring
Desaparición	26 de febrero de 1995
Sede	Londres, Reino Unido

Cronología

Barings Bank	ING Group

Nick Leeson

- Pasó de auditor de operaciones a operador en bolsa y mantuvo sus accesos (**SoD**)
- Aprovechó la falta de seguridad en los accesos a las aplicaciones para ocultar operaciones fallidas en bolsa.
- Hundió el Banco **en un dia**, que fue rescatado (comprado) por 1 Libra por el ING Group
- Pasó 6 años en la cárcel.
- Hoy es consultor de Seguridad y da conferencias.
- Reclama **mejores regulaciones** y recomienda **cumplimiento**

Las famosas, carne de 'hacker'

- Se filtran fotos íntimas de un centenar de artistas robadas de iCloud
- Jennifer Lawrence admite ser víctima del ataque informático mientras otras artistas lo niegan

ROSA JIMÉNEZ CANO | San Francisco | 1 SEP 2014 - 20:06 CEST 56

Archivado en: Jennifer Lawrence Actrices Hollywood Cine americano Apple
Filtración documentos Industria cine Gente Cine Empresas Economía Medios comunicación

La actriz Jennifer Lawrence / CORDON

1.465 229 13 56

Enviar Imprimir Guardar

Estrellas del cine y musas de la canción se han quedado al desnudo tras un fallo de seguridad en iCloud, el almacenamiento en la nube de Apple. En las imágenes aparecen desde la oscarizada Jennifer Lawrence a Rihanna, pasando por Avril Lavigne, Amber Heard, Gabrielle Union, Hayden Panettiere y Hope Solo. Y la lista continúa: Hilary Duff, Jenny McCarthy, Kaley Cuoco, Kate Upton, Kate Bosworth, Keke Palmer y Kim Kardashian también podrían estar entre las afectadas, aunque no se han pronunciado al respecto. Lawrence, que aparece posando en biquini, en ropa interior e incluso desnuda, ha sido la primera en anunciar que adoptará medidas legales. Lo ha hecho a través de su representante en un comunicado a la web TMZ.

investigación en BlackHat, la conferencia de *hackers* más importante, celebrada en Las Vegas en agosto, apunta a un fallo de seguridad de Apple: "*Find My iPhone* (la web para localizar y bloquear un teléfono perdido) ha podido ser la causa de tan desgraciado accidente, ya que supuestamente, y a través de este servicio, era posible realizar ataques de fuerza bruta, una vieja técnica que utiliza un posible usuario con una lista de posibles credenciales contra usuarios conocidos. El atacante tan solo necesitaría el correo de las víctimas y un buen archivo de contraseñas a utilizar. Si la víctima tuviese una contraseña débil, el siguiente paso sería entrar en iCloud, y descargarse el material deseado".

Garrido explica que el servicio ya se ha arreglado, pero el agujero potencial llevaba varios días expuesto en GitHub, un almacén de *software* compartido. La empresa de la manzana, por ahora, no se ha pronunciado.

Como suele ser habitual, los expertos subrayan la importancia de no colgar contenido íntimo en Internet, cambiar las claves de acceso con frecuencia e intentar que en cada servicio sea diferente. Ángel Prado, del equipo de seguridad de Salesforce, considera que se podría haber evitado usando un "segundo factor de identidad", un servicio cada vez más extendido que solo permite acceder al correo o servicios personales tras introducir la contraseña y un código que se envía al teléfono móvil en forma de SMS. "No es infalible, pero refuerza", insiste.

La pena para este tipo de delitos en EE UU pueden llegar a los 10 años de cárcel, como sucedió en 2012, cuando se accedió sin permiso a los ordenadores de Scarlett Johansson y Mila Kunis, entre otras actrices, y se difundieron las fotos sin su consentimiento. En España el delito no tiene una tipificación clara. Según fuentes de la Guardia Civil se podrían considerar delitos desde revelación de secretos, que se podría aplicar a quienes las difundan aunque no las hayan robado, a robo con fuerza, "por insistir hasta hacerse con las claves".

Estadísticas Comparativas

5 Peores controles - Media

Domain	Control	Current Maturity	Gap	Target Maturity
People	System and Service Account Lifecycle Mgmt	1.8	2	3.80
Infrastructure	Event Correlation	1.8	2.4	4.20
Infrastructure	Asset Management	1.76	2.72	4.48
People	Privileged & Shared Identity Management	1.75	2.65	4.40
GRC	Information Asset Profile	1.5	1.75	3.25

Dos detenidos por atacar el sistema central informático de Tous

Foto: ALFONSO HERRANZ

Los arrestados cambiaban precios de productos de tiendas de España, México y Estados Unidos

BARCELONA, 17 Mar. (EUROPA PRESS) -

Los Mossos d'Esquadra de la Unidad Central de Delitos Informáticos detuvieron este lunes a dos hombres como presuntos autores de un delito de daños informáticos de alcance internacional contra una empresa catalana, ha informado este sábado la policía catalana en un comunicado.

La investigación empezó a finales del 2011 cuando una conocida empresa catalana dedicada al diseño y comercialización de joyas, Tous, según han explicado a Europa Press fuentes conocedoras, advirtió a la policía de que su sistema central informático estaba siendo atacado.

Los detenidos son Juan Carlos S.B., de 41 años, y Juan S.L., de 46, ambos españoles, que presuntamente estaban realizado los ataques desde ordenadores a nombre de una empresa que se había encargado hasta el 2010 de la gestión informática de Tous.

Como consecuencia de estas "intrusiones", se estaba produciendo la paralización del sistema comercial y las consecuentes pérdidas millonarias, según la policía, y que afectaban sobre todo a los precios de los productos, lo que repercutía en la información relativa a precios, stock y material almacenado.

Jérôme Kerviel

Jérôme Kerviel es el hombre que protagonizó el mayor fraude de la historia en enero de 2008 cuando causó la pérdida de 4900 millones de euros debido a actividades fraudulentas. Kerviel, de nacionalidad francesa nació el 11 de enero de 1977 y fue administrador de operaciones financieras, graduado en la Universidad de Lyon. Trabajaba en la *Société Générale* en París, uno de los bancos más prestigiosos de Francia (el segundo en importancia) y uno de los más grandes de Europa, y en donde protagoniza el desajuste financiero más grande de la historia que hizo temblar los mercados en todos los continentes.

Usó **sus privilegios como administrador de sistemas** para eliminar controles de inversion.

Apostaba con deuda soberana Alemana. Tras invertir 50 mil millones de euros en una unica operación, generó un agujero de **4.900 millones de Euros**

Societé Genrale tuvo que ser rescatada por el estado Francés

Alegó **que la gerencia del Banco era conocedora de estas operaciones** y los alentaba, y que él era un mero ejecutor y que **no ganó ni un céntimo** por esas operaciones.

Jerome Kerviel fue juzgado y sentenciado a una **multa de 5000 millones** de euros y 8 años de prisión.

El bróker Jerome Kerviel que dejó un agujero de 5.000 millones sale de la cárcel

- El operador de Bolsa ha pasado tres meses en prisión antes de pasar a libertad condicional

AGENCIAS | **París** | 8 SEP 2014 - 10:34 CEST 57

Archivado en: Jérôme Kerviel Bolsa Mercados financieros Finanzas

Enviar vídeo

Su abogado aseguró que "**ya no hay caso Kerviel, sino un caso Société Générale**" e indicó que ha presentado denuncias por **falsificación de declaraciones de su cliente**, pero también por **estafa**, al considerar que **el banco alteró documentos para evitar su propia responsabilidad**.

Conclusiones

- Se realizan **antes** los controles de **obligado cumplimiento** para el negocio y aquellos que son más fáciles de implementar **manualmente** y no necesitan tecnologías e inversión

- **Se dejan para después aquellos** que necesitan más tecnología (inversión), pero que al madurarlos representarían un **habilitador para el negocio.**

- Las compañías necesitan de sus CIO/CISO/CSO **liderazgo** para priorizar aquello que es importante para el negocio

- *"The Main thing is keeping the Main Thing the Main Thing"*

ibm.com/security