



Seguridad en la base de datos ¿ Como nos protegen los estándares?

Frano Capeta Mondoñedo
Country Manager I-SEC Perú.

Securing Business

www.i-sec.org

COPYRIGHT 2000 - 2006 / I-SEC INFORMATION SECURITY S.A.



BIENVENIDO A I-SEC INFORMATION SECURITY INC.



Presencia de



en el Mundo

Securing Business

www.i-sec.org

COPYRIGHT 2000 - 2006 / I-SEC INFORMATION SECURITY S.A.



DIFERENCIALES I-SEC

- ① Somos Líderes en **SERVICIOS PROFESIONALES** en Seguridad de la Información en Latinoamérica.
- ① Trayectoria de 15 años desarrollando proyectos de Seguridad de la Información en Argentina y Latinoamérica.
- ① Desarrollamos Diagnósticos basados en Normas Internacionales, como la Norma ISO 17799 Seguridad de la Información (ahora 27001), Cobit, ITIL, entre otras.
- ① Nuestro Plantel de Profesionales cuenta con las Certificaciones más Prestigiosas.
- ① Nuestra Independencia Comercial es Garantía de Éxito

www.i-sec.org

COPYRIGHT 2000 - 2006 / I-SEC INFORMATION SECURITY S.A.



Nuestros Servicios



Consulting

Audit & Consulting Services:

- ① Profesionales Certificados
- ① Soluciones concretas, efectivas y sostenibles en el tiempo
- ① Independencia Comercial



Legal

I-SEC Legal & Forensic

- ① Asesoramiento Legal
- ① Esclarecimiento de ilícitos Informáticos



Education

Education Center

- ① Seminarios Internacionales
- ① Instructores Certificados
- ① Asesoramiento y Coaching permanente



InfoSecurity

InfoSecurity

- ① El Mega Evento de Seguridad de la Información
- ① 20 Ediciones realizadas en Latinoamérica

www.i-sec.org

COPYRIGHT 2000 - 2006 / I-SEC INFORMATION SECURITY S.A.

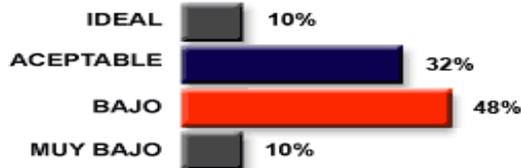


¿Por qué estamos en esta reunión?

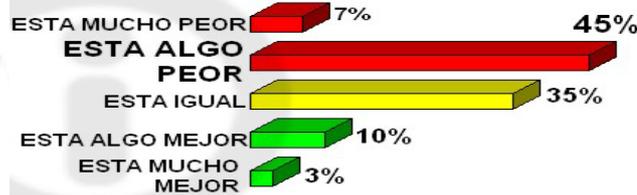


Seguridad el eslabón mas débil

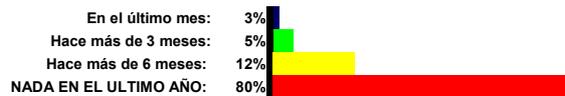
¿En qué nivel de seguridad cree Usted que se encuentra su organización?:



Si tuviera que evaluar TODAS las acciones de seguridad que IMPLEMENTÓ en el 2006 y lo comparara con todos los nuevos riesgos y amenazas que surgieron, ¿ud considera que SU ORGANIZACIÓN esta mejor que el año anterior?



¿Cuándo fue la última vez que sus Directores y Gerentes han recibido Presentaciones de Concientización de Seguridad?



Algunos hechos

Hackers de Perú y Chile en disputa informática

Las diferencias entre peruanos y chilenos llegaron al ciberespacio. Mientras las autoridades del Ministerio Interior de Chile trataban de reparar la página web de la Oficina Nacional de Emergencia, hackeada por un peruano, los funcionarios del Poder Judicial peruano descubrieron que su sitio en Internet había sido presa de hackers chilenos. Presunto hacker peruano conversó en exclusiva con Elcomercio.pe.

De la edición impresa

- ▶ Restricción de agua en Lima es inminente por ausencia de lluvias
- ▶ Ninguna galería de Mesa Redonda tiene certificado de seguridad
- ▶ Aprueban envío de 5 cuadernos de extradiación
- ▶ Empezan a publicar resúmenes del TLC

Este año aumentarán los ataques cibernéticos

De acuerdo con un estudio de IBM sobre las amenazas potenciales a la seguridad en el 2006, se prevé una evolución o transformación fundamental en el delito cibernético, que cubre desde brotes a nivel mundial hasta ataques más pequeños y sigilosos con fines de extorsión y dirigidos a organizaciones específicas.

De la edición impresa

- ▶ Sobre consumo y calidad de vida
- ▶ Los niños aprenderán a ser responsables al tener un vehículo
- ▶ Notas breves

www.i-sec.org

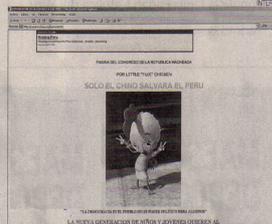
COPYRIGHT 2000 - 2006 / I-SEC INFORMATION SECURITY S.A.

NADIE ESTÁ A BUEN RECAUDO

Piratas informáticos intervinieron página del Legislativo en Internet

“Solo el Chino salvará al Perú”, decía el sitio electrónico asaltado por 'Fujichicken'

Los cibernautas que ingresaron ayer a la página Internet del Congreso de la República (www.congreso.gob.pe) se llevaron una sorpresa al ver que esta fue intervenida por un supuesto 'cracker' fujimorista, quien no encontró mejor manera de hacer propaganda a favor del ex presidente que dañando dicho sitio. El término 'cracker' se utiliza



SORPRESA. Esto vieron ayer quienes visitaron la página del Congreso.

para referirse al experto en informática que de mala fe ataca una web o un sistema.

“Solo el chino salvará al Perú. Abajo los abusos del Congreso con jugosos sueldos”, escribió el pirata, quien se identificó como 'Fujichicken'.

Poco antes de las siete de la noche, la página fue reparada.

Para intervenir se envenenó el sistema de dominio del nombre de la web del Congreso, 'redireccionándola' hacia una distinta. Así, al momento de ingresar a la página, aparece otra.

Es la segunda vez en menos de un mes que una página electrónica del Estado es alterada. En diciembre pasó lo mismo con el sitio del Poder Judicial.

(Más información en www.elcomercio.pe)

Un 60% de las redes WiFi carecen de cualquier tipo de protección

18/03/2006 - 18:46
NOTICIOSDOT, IBLNEWS

Las pruebas de "wardriving" (exploración de las redes inalámbricas al alcance en un recorrido concreto) llevadas a cabo a nivel internacional arrojan resultados preocupantes: casi un 60% de las redes carecen de protección alguna



Algunos datos

NEGOCIOS

Una nueva fiebre “enferma” a las empresas de todo el mundo: la seguridad de la información

La gestión de las políticas de seguridad de la información obsesiona a miles de empresas de todo el mundo. Ahora, ya no se conforman con controlar los datos circulantes; también quieren ahorrar millones.

www.i-sec.org

COPYRIGHT 2000 - 2006 / I-SEC INFORMATION SECURITY S.A.



Algunas premisas

- No existe la “verdad absoluta” en Seguridad Informática.
- No es posible eliminar todos los riesgos.
- La Dirección está convencida de que la Seguridad Informática no hace al negocio de la compañía.
- Cada vez los riesgos y el impacto en los negocios son mayores.

Algunas realidades

En mi compañía ya tenemos seguridad porque ...

- ... implementamos un firewall.
- ... contratamos una persona para el área.
- ... en la última auditoría de sistemas no me sacaron observaciones importantes.
- ... ya escribí las políticas.
- ... hice un penetration testing y ya arreglamos todo.

Algunas cifras

En general todos coinciden en:

El **80%** de los incidentes/fraudes/ataques son efectuados por personal interno

Fuentes:

The Computer Security Institute

Cooperative Association for Internet Data Analysis (CAIDA)

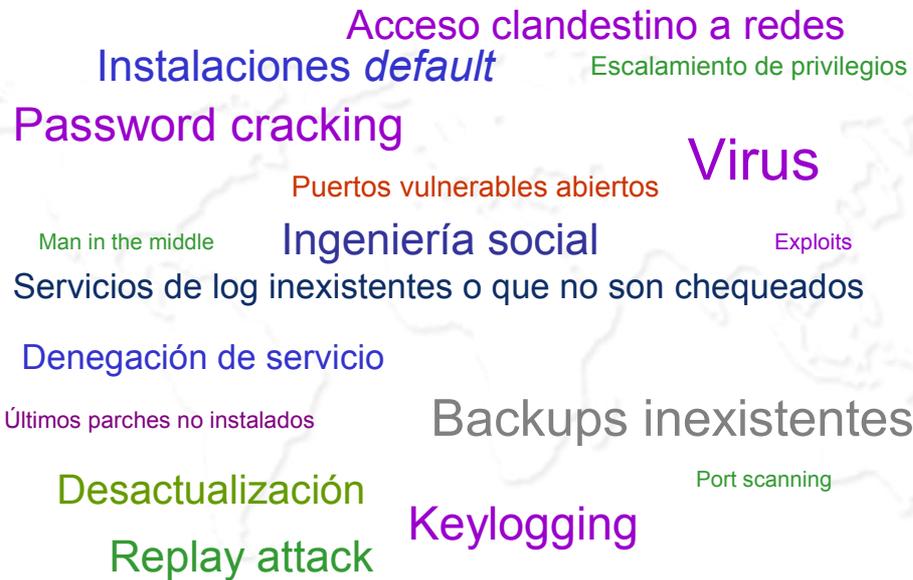
CERT

SANS

Qué Información proteger

- en formato electrónico / magnético / óptico
- en formato impreso
- en el conocimiento de las personas

Principales riesgos y su impacto en el negocio



Principales riesgos y el impacto en los negocios

En estos tipos de problemas es difícil:

- Darse cuenta que pasan, hasta que pasan.
- Poder cuantificarlos económicamente, por ejemplo ¿cuánto le cuesta a la compañía 4 horas sin sistemas?
- Poder vincular directamente sus efectos sobre los resultados de la compañía.

Principales riesgos y el impacto en los negocios

Se puede estar preparado para que ocurran lo menos posible:

- sin grandes inversiones en software
- sin mucha estructura de personal

Tan solo:

- ordenando la Gestión de Seguridad
- parametrizando la seguridad propia de los sistemas
- utilizando herramientas licenciadas

Si igual voy a hacer algo, porque no lo hago teniendo en cuenta las Normas Internacionales aplicables

Normas y Metodologías aplicables

- Objetivos de Control en Tecnologías de Información: **COBIT**
- British Standards Institute: **BS**
- International Standards Organization: **Normas ISO**
- Departamento de Defensa de USA: **Orange Book** / Common Criteria
- Sarbanes Oxley Act, Basilea II, HIPAA Act, **Leyes NACIONALES**
- OSSTMM, ISM3, **ISO 17799:2005, ISO 27001**

ISO17799-1 – Seguridad de la Información.
NORMALIZACION (Mejores Prácticas)

ISO 27001 – CERTIFICACION de Seguridad de la
Información

Norma ISO17799 (versión 2005)

1. Política de Seguridad
2. Organización de Seguridad
3. Administración de Activos
4. Seguridad de los Recursos Humanos
5. Seguridad Física y Ambiental
6. Gestión de Comunicaciones y Operaciones
7. Sistema de Control de Accesos
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
9. Administración de Incidentes de Seguridad de la Información
10. Plan de Continuidad del Negocio
11. Cumplimiento

Dominio 6: GESTION DE OPERACIONES Y COMUNICACIONES**6.1 Procedimientos y responsabilidades operativas**

Objetivo:

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.

Separación de funciones

Se debe considerar la separación de la gestión o ejecución de ciertas tareas o áreas de responsabilidad.

Siempre que sea difícil llevar a cabo la separación, se deben tener en cuenta otros controles:

- monitoreo de las actividades,
- pistas de auditoría y
- supervisión gerencial.

Dominio 7: SISTEMA DE CONTROL DE ACCESOS**Requerimientos de negocio para el control de accesos**

Objetivo: Controlar el acceso de información.

Política de control de accesos

Administración de accesos de usuarios

Administración de privilegios

Revisión de derechos de acceso de usuario

Limitación del horario de conexión

Dominio 8: Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

Objetivo: Asegurar que la seguridad este imbuida dentro de los sistemas de información

Protección de los datos de prueba del sistema

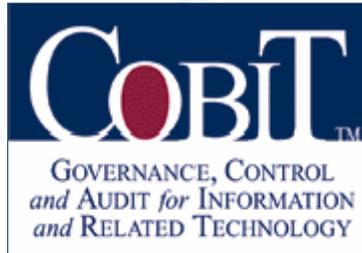
Control de acceso a las aplicaciones y a la información

Restricción de acceso a la información

Fuga de información

Pero no solo el Estándar ISO nos puede ayudar

¿Qué significa COBIT?



- **COBIT** es un acrónimo formado por las siglas derivadas de
 - **C**ontrol
 - **O**bjectives
 - for **I**nformation
 - and related **T**echnology

COBIT ... sus antecedentes

- **COBIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnología de Información (TI). – COBIT es la herramienta innovadora para el gobierno de TI.**

Recursos de Tecnología de Información



PROCESOS

Funciones de negocio y actividades que utilizan la tecnología de información



DATOS

Los objetos de datos en su sentido más amplio, es decir: externos internos, estructurados y no estructurados, gráficos, sonido, etc.



APLICACIONES

La suma de programas de aplicación, funciones de procesamiento y procedimientos manuales



TECNOLOGIA

Hardware, sistemas operativos, manejo de bases de datos, trabajo en redes, multimedia, telecomunicaciones y telefonía.



INSTALACIONES

Ambientes que albergan y soportan los sistemas y procesos informáticos



PERSONAL

Habilidades, conocimientos y productividad del personal para planificar, organizar, adquirir, entregar y dar soporte y monitorear servicios y sistemas de información.

www.i-sec.org

COPYRIGHT 2000 - 2006 / I-SEC INFORMATION SECURITY S.A.



Requerimientos de información para el Negocio

Requerimientos de Calidad

Calidad.
Costo.
Oportunidad.

Requerimientos Financieros (COSO)

Efectividad y eficiencia operacional.
Confiability de los reportes financieros.
Cumplimiento de leyes y regulaciones.

Requerimientos de Seguridad

Confidencialidad.
Integridad.
Disponibilidad.



www.i-sec.org

COPYRIGHT 2000 - 2006 / I-SEC INFORMATION SECURITY S.A.



I-SEC Information Security Inc.

COBIT Marco Referencial – Procesos de TI

Planeación y Organización

Adquisición e Implementación

Servicios y Soporte

Seguimiento

Definición del nivel de servicio
 Administración del servicio de terceros
 Administración de la capacidad y el desempeño
 Asegurar el servicio continuo

DS5 Garantizar la seguridad del sistema

Identificación y asignación de costos
 Capacitación de usuarios
 Soporte a los clientes de TI
 Administración de la configuración
 Administración de problemas e incidentes
 Administración de datos
 Administración de Instalaciones
 Administración de Operaciones

www.i-sec.org
COPYRIGHT 2000 - 2006 / I-SEC INFORMATION SECURITY S.A.

I-SEC Information Security Inc.

DS5 Garantizar la seguridad de los sistemas.

Que satisface los Requerimientos de Negocio: El Control Sobre el Proceso de TI.

Salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida.

Es habilitado por:

Controles de acceso lógico.

Considerando:

- *Autorización, autenticación y control de acceso*
- *Identificación de usuarios y perfiles de autorización*
- *Prevención y detección de virus*
- *Administración centralizada de la seguridad*
- *Entrenamiento de usuarios*
- *Pruebas y reportes de intrusión*

www.i-sec.org
COPYRIGHT 2000 - 2006 / I-SEC INFORMATION SECURITY S.A.

Ventajas del modelo Cobit

- **Compatibilidad entre los parámetros de evaluación de Auditoría y los objetivos de control de Cobit**
- **Flexibilidad en la parametrización de Cobit con respecto a los dominios y objetivos de control a evaluar en cada cliente**
- **Herramienta de documentación de hallazgos y recomendaciones**
- **Provee un marco único reconocido a nivel mundial de las “mejores prácticas” de control y seguridad de TI**
- **Consolida y armoniza estándares originados en diferentes países desarrollados.**
- **Concientiza a la comunidad sobre importancia del control y la auditoría de TI.**

En Conclusión:

Beneficios a tomar en cuenta

- Consolidación de la seguridad como tema estratégico.
- Planeamiento y manejo de la seguridad más efectivos.
- Mayor seguridad en el ambiente informático.
- Mejor reacción a incidentes de seguridad.
- Minimización de los riesgos inherentes a la seguridad de la información.
- Cuantificación de los posibles daños por ataques a la seguridad de la información.
- Orden en el trabajo bajo un marco normativo que evita la duplicación de tareas y facilita el intercambio de información.
- Concientización global sobre la importancia de la seguridad de la información.
- Aumento de la confianza de terceros.
- Mayor control de la información proporcionada a terceros.



**Seguridad en la base de datos
¿Como nos protegen los estándares?**

Gracias

**Frano Capeta Mondoñedo, Country Manager I-SEC Perú.
frano.capeta@i-sec.org**