

Protección de Datos

ISACA

Montevideo, 18 de Setiembre 2009

Jornadas IUAI



Agenda

- Objeto de Protección
- Contexto y Limitaciones
- Principios Generales – Requerimientos
- El proceso de la Empresa
- Estrategia y Objetivos de Control (Cobit)
- Controles o Buenas Prácticas (ISO 27000)
- Conclusiones



Objeto de Protección

PROTECCIÓN DE DATOS PERSONALES

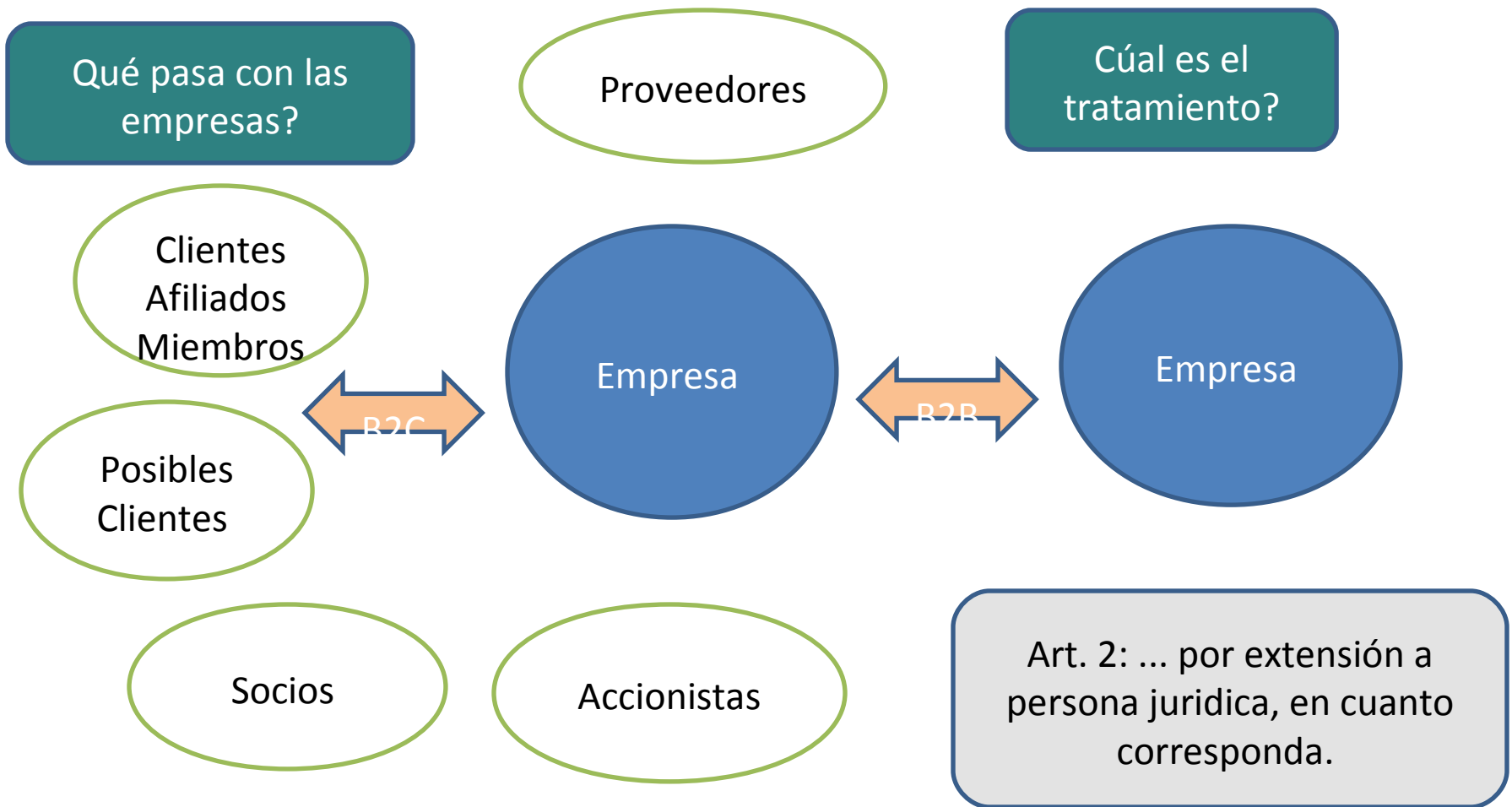
P
R
I
V
A
C
I
D
A
D



I
N
T
I
M
I
D
A
D

**Quando mueren los datos
personales?**

Contexto y Limitaciones



Principios Generales



- Legalidad: inscriptas y cumpliendo con la ley.
- Responsabilidad: responsable de la BD pasible de sanciones administrativas y acciones indemnizatorias.
- Veracidad: veraces, adecuados, ecuanimes y no excesivos .
- Finalidad: no podrán ser usados para finalidades distintas o incompatibles con las que motivaron su obtención.

Principios Generales



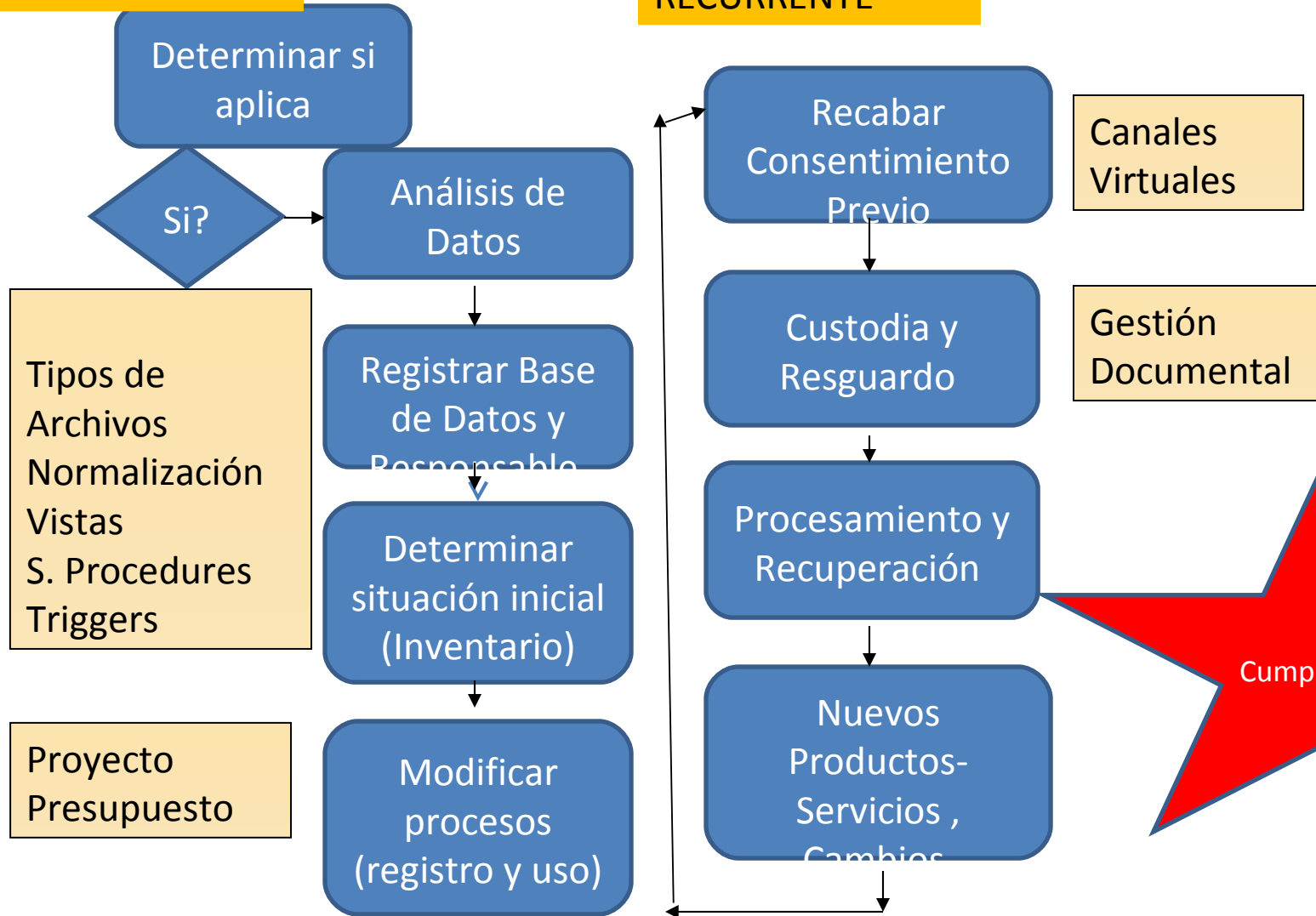
- Previo Consentimiento: libre, previo, expreso e informado.
- Seguridad de los Datos: el responsable o usuario, debe adoptar medidas para garantizar seguridad y confidencialidad.
- Reserva: uso de BD en forma reservada y exclusiva a operaciones habituales del giro o actividad del usuario estando prohibida toda difusión a terceros. Aclaración, definiciones!!.

El Proceso de la Empresa



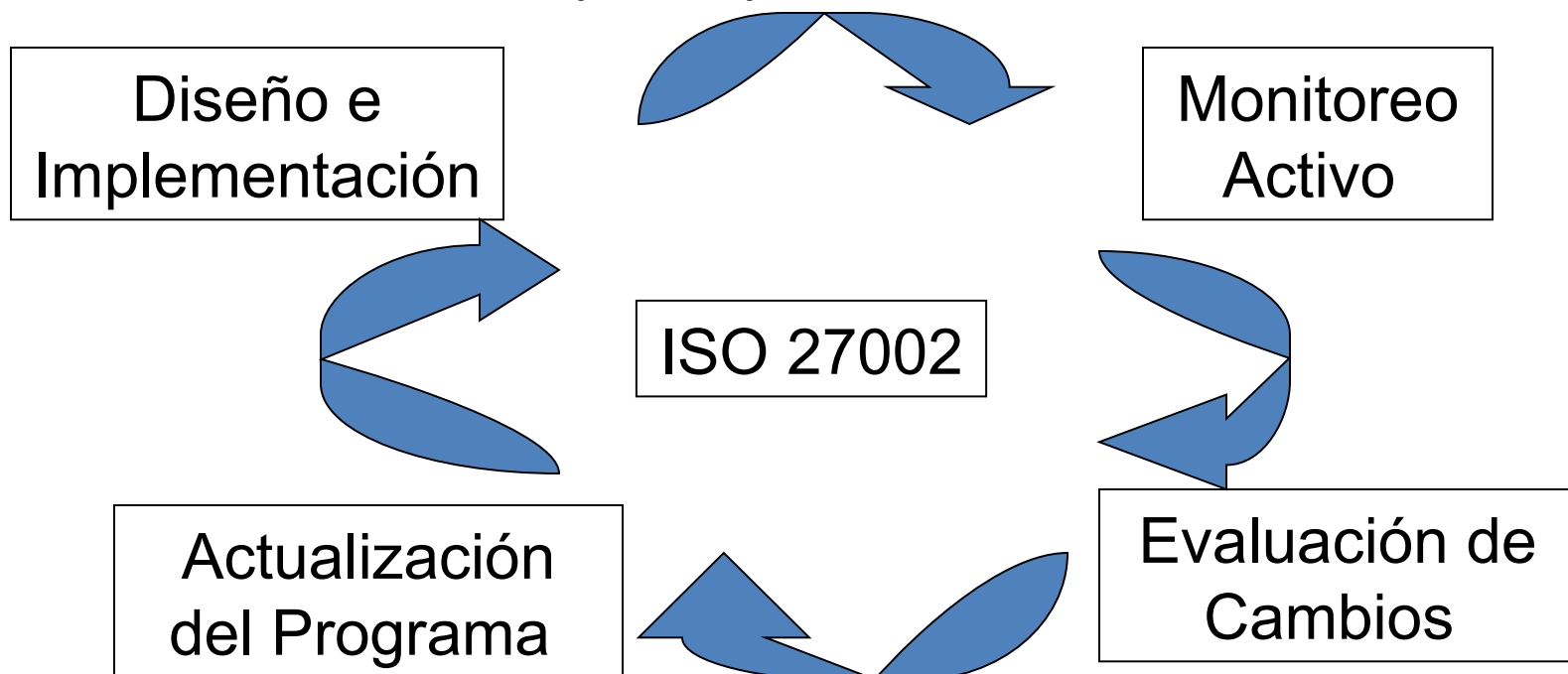
PRIMERA VEZ

RECURRENTE



Gestión de Seguridad

- Sistema de Gestión de Seguridad de la Información (SGSI)



Requerimientos

- Legalidad → registro y responsabilidades
- Responsabilidad → Accountability
- Veracidad → mínimos e íntegros
- Finalidad → uso permitido
- Previo Consentimiento → aprobación previa
- Seguridad de Datos → Confidencialidad, Integridad y Disponibilidad (CIA)
- Reserva → Confidencialidad, uso permitido

Requerimientos, Estrategia y Objetivos de Control

Requerimientos /Estados	Registrar	Recabar	Custodiar	Almacenar	Recuperar	Procesar	Transferir/Compartir	Descartar
Legalidad	Inventario y responsables							Plazo legal Vigencia
Veracidad		Integridad y Mínimo	Integridad y Disponibilidad	Consistencia e Integridad	CIA			
Finalidad		Abarcativo y Detallado, Integridad.			CIA y Uso Autorizado	Uso Autorizado	CIA y Uso Autorizado	
Previo Consentimiento		Canal Válido Volúmen Grado de Detalle						
Seguridad		Proceso Documentado, Evidenciable y Traceable.	CIA	CIA	CIA	CIA	CIA	Destrucción Segura
Reserva			Confidencialidad y Uso Autorizado	Confidencialidad y Capacidad	Confidencialidad y Uso Autorizado	Confidencialidad y Uso Autorizado	CIA y Uso Autorizado	Destrucción Segura
Responsabilidad	Cumplir requerimientos de la Ley. Concientización, entrenamiento, cláusulas de responsabilidad y uso autorizado.							

Requerimientos



- Derechos de los Titulares: cuando se recaben los datos (canal válido, volúmen, detalle)
 - Finalidad: abarcativa y detallada
 - Destinatarios: abarcativa y preventiva (outsourcing)
 - Existencia BD y responsable
 - Consecuencias de proporcionar los datos
 - Derechos de acceso, modificación, eliminación entre otros (usuarios, perfiles). Presentación
- Derechos de Acceso de los titulares: cada 6 meses y satisfecha en 5 días hábiles. Recuperación y presentación

Finalidad

- Empresa: XXX (Financiera)
- Fecha: XXX
- Cliente: XXX
- Finalidad: autorizo a la empresa XXX a utilizar mis datos personales para todo propósito relacionado a productos y servicios financieros. Firma: XXXX

Finalidad

- Identifique los propósitos para los cuales autoriza a utilizar su información:
 - Tarjetas de crédito y débito
 - Productos Bancarios tradicionales
 - Productos Bancarios de inversión
 - Fondos mutuos
 - Seguros
 - Compartir o vender mis datos
 - Tercerización de servicios

Buenas Prácticas Uso Autorizado



- Uso Autorizado
 - Concientización y training (8.2.2)
 - Controles de Procesos de Gestión de Seguridad
 - Políticas de Uso de Internet, correo, software, etc. (7.1.3 y 11.4.1)
 - Controles de Procesos de Negocio
 - Controles manuales
 - Herramientas de usuario final (Office)
 - Controles Automatizados (12)
 - Aplicaciones y Base de Datos
 - Controles basados en los datos (vistas, filtros)
 - Controles basados en el software (codificación)

Buenas Prácticas Integridad



- Integridad
 - Concientización y training (8.2.2)
 - Cláusulas de Ingreso, Política de Uso de Recursos (8.1y 8.2)
 - Contratos, Acuerdos de Niveles de Servicio (SLA) (6.2.3)
 - Soporte Físico
 - Control de Acceso (11)
 - Tarjetas de Identificación, espacio autorizado
 - Archiveros o muebles con llaves, autorización, faxes
 - Revisiones Espacio de Trabajo Seguro (9 y 11.3.3)
 - Soporte Magnético
 - Alguien que hace y otro que aprueba (maker/checker) (10.1.3, 12.2)
 - Hash, CRC (12.3)
 - Firma Digital, encriptación (12.3)

Buenas Prácticas Integridad



- Integridad
 - Soporte Magnético
 - Control de Acceso (11)
 - Sistema Operativo- Aplicaciones-Base de Datos
 - » Perfiles/roles mínimos y basados en necesidad de conocer
 - » Revisión de Perfiles
 - Herramientas de Oficina (Office)
 - Arquitectura y Configuración Segura de la Infraestructura (Firewalls, IDS, revisión de contenidos, filtros, antivirus)
 - Monitoreo y supervisión continua de la infraestructura (patcheo de vulnerabilidades, test de penetración, Hackeo Ético)
 - Bloqueo de puertos, ejecución de código
 - Segregación de funciones en desarrollo y administración de usuarios
 - Seguridad en el manejo de medios magnéticos (10.8)
 - Transferencia Segura (10.8 ,10.9, 12.3)
 - Protocolos (SSL), Correo Seguro (PGP), Wireless Seguro, Encriptación de Adjuntos
 - Servicios Tercerizados (outsourcing) (10.2)

Buenas Prácticas Confidencialidad



- **Confidencialidad**
 - Concientización y training (8.2.2)
 - Cláusulas de Ingreso, Política de Uso de Recursos (8.1 y 8.2)
 - Contratos, Acuerdos de Niveles de Servicio (SLA) (6.2.3)
 - Soporte Físico
 - Idem. Integridad
 - Etiquetado (labeling) (10.7.1, 10.8.3)
 - Soporte Magnético
 - Encriptación, escrambleado (12.3)
 - Uso de Datos de Producción (12.4.2)
 - Bloqueo de puertos (11.4.4)
 - Control de Acceso: idem Integridad
 - Seguridad en el manejo de medios magnéticos y equipos (9.2.4, 10.7)
 - Transferencia segura: idem. Integridad
 - Servicios Tercerizados (outsourcing) (10.2)

Buenas Prácticas Disponibilidad



- Disponibilidad
 - Concientización y training (8.2.2)
 - Cláusulas de Ingreso, Política de Uso de Recursos (8.1, 8.2)
 - Contratos, Acuerdos de Niveles de Servicio (SLA) (6.2.3)
 - Soporte Físico
 - Archiveros o muebles ignífugos con copias de llaves (9.2)
 - Personas autorizadas (titular y suplente) (9.1)
 - Registros vitales (10.5.1)
 - Soporte Magnético
 - Priorización adecuada de requerimientos de la ley considerando los plazos (Análisis de Impacto al Negocio) (14.1.2)
 - Plan de Manejo de Crisis (14.1.1)

Buenas Prácticas Disponibilidad



- Disponibilidad
 - Soporte Magnético
 - Plan de Recuperación de Desastres (14.1.3, 14.1.4)
 - Infraestructura contingente (sitio alternativo)
 - Comunicaciones redundantes
 - Recuperación de Aplicaciones de acuerdo a priorización
 - Política y resguardo de backups de datos
 - Comunicaciones a terceros sobre impactos de la interrupción
 - Pruebas periódicas del plan
 - Documentación, lecciones aprendidas
 - Servicios Tercerizados (outsourcing)
 - Descartar los datos (10.7.2, 12.5.4)
 - Depuración de datos (backups vigentes)
 - Destrucción Segura de datos (BD y medios)

Estamos preparados?

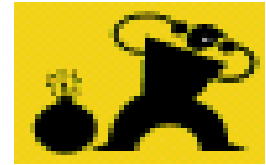
Finalmente no nos encontremos así

...



Conclusiones

- Que pasa cuando ocurran Incidentes de Seguridad que generen situaciones de no cumplimiento pero no “claramente” adjudicables al responsable?.



- Se recomienda contar con:
 - Seguridad Informática (familia ISO 27000)
 - Control Interno informático (Cobit)
 - Gestión integral de TI (Cobit, ITIL, CMMi)

Referencias

- Ley actual Protección de Datos Personales 18.331 (2008)
- Ley anterior Protección de Datos Comerciales 17.838 (2004)
- Ley Española 15/99, Real Decreto Español 994 (Medidas de protección para ficheros automatizados) y Reglamento de Seguridad
- Informe sobre Protección de Datos Personales
 - Por: Lic. Déborah C. Rivas Berastegui - IT Advisory - KPMG Uruguay.
Revisión Legal: Dra. Giovanna Lorenzi Lozano - Asesoramiento Tributario y Legal - KPMG Uruguay
- Cobit, ISO 27000
- Red de Agencias de Protección de Datos:
<http://uk.ask.com/>



Preguntas

“La conclusión es que sabemos muy poco y sin embargo es asombroso lo mucho que conocemos. Y más asombroso todavía que un conocimiento tan pequeño pueda dar tanto poder”

Bertrand Arthur William Russell