Datos Personales en el Ciclo de Vida de Desarrollo Seguro

Pablo Romanos

Green40

Organización OWASP UdeMM

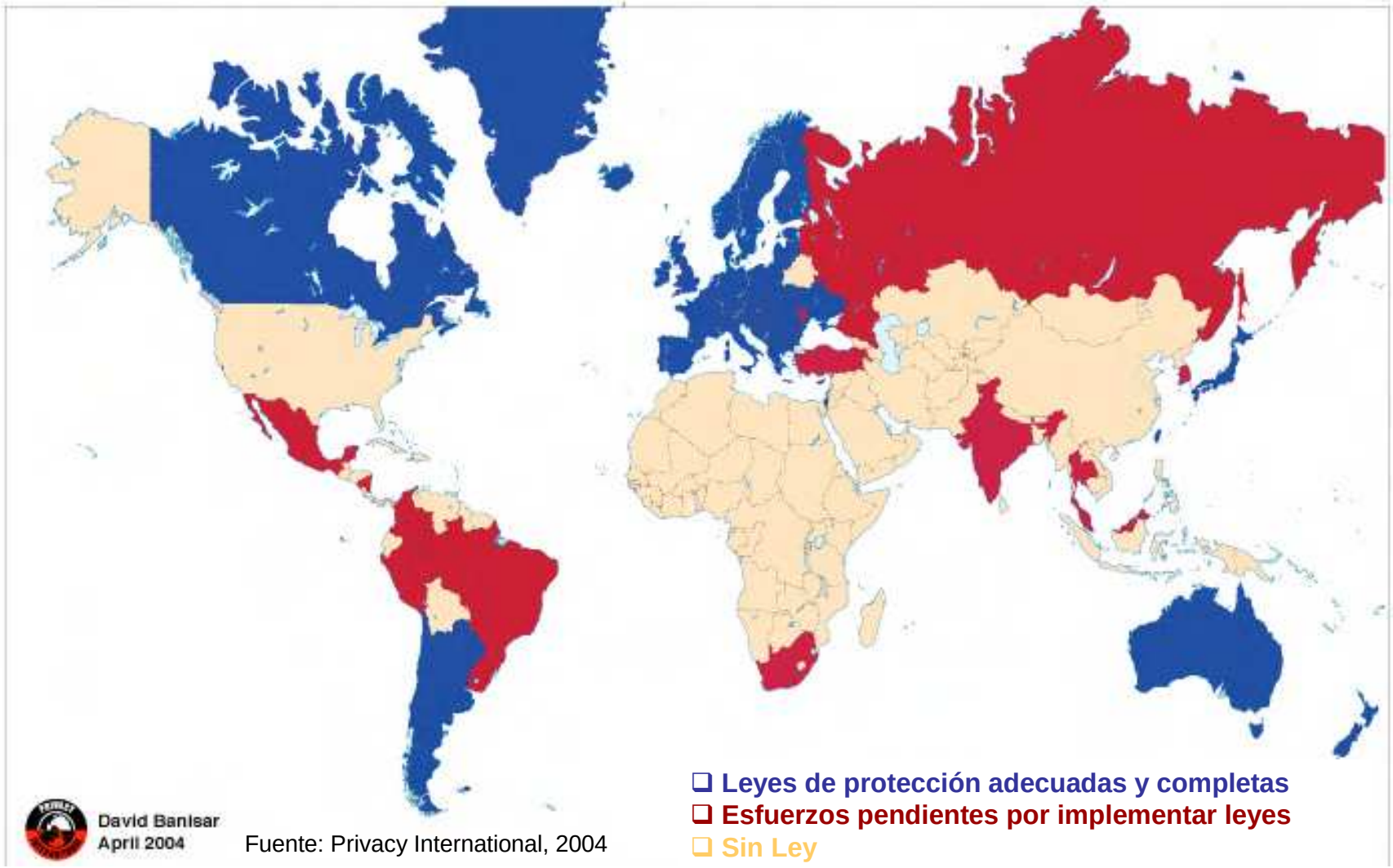
pabloromanos@green40.com

De que hablamos cuando hablamos de Protección de Datos Personales?

Proteger de forma integral los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados, destinados a dar informes.

autodeterminación informativa
como derecho humano

Leyes de Protección de Datos en el Mundo



Fuente: Privacy International, 2004

Ley 25326 - Definiciones

- Datos Personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.
- Datos Sensibles: Raza / etnia, política, convicciones, religión, filosofía / moral, sindical, salud, sexual, datos relacionados con violencia de género.
- Archivo o banco de datos: Conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento.
- Responsable de archivo o banco de datos: Persona física o de existencia ideal, pública o privada, que es encargado de un archivo o banco de datos.
- Titular de los datos: Toda persona física o persona de existencia ideal, cuyos datos sean objeto del tratamiento (dueño de los datos).
- Usuario de datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, en archivos o a través de conexión con los mismos.

Ley 25326 - Derechos de los Titulares

- Consulta gratuita del banco, registro o base de datos personales.
- Acceso a los datos.
- Rectificación, actualización o supresión gratuitas - excepto casos indicados por ley.
- Datos sobre antecedentes penales o contravencionales solo pueden ser usados por la entidades públicas competentes.
- Establecimientos sanitarios y profesionales de la salud, pueden usar datos sobre salud física o mental respetando el secreto profesional.
- Organizaciones políticas, sindicales y religiosas pueden tener registros de sus integrantes o afiliados.
- Derecho a no suministrar datos sensibles. Excepción en caso de:
  - Interés general autorizado por ley
  - Uso estadístico / científico, con datos disociados

Ley 25326 - Obligaciones de los Usuarios (Tratamiento)

- Registrar el archivo.
- Obtener el consentimiento del titular
- Informar al titular expresamente:
  - Finalidad, destinatarios, existencia del archivo, responsable del archivo y su domicilio, derecho del titular de acceso, rectificación y supresión.
- Seguridad de los datos.
- Actualización de datos cuando corresponda.
- No almacenar datos sensibles salvo excepciones expresas por ley.
- Destruir los datos cuando ya no sirvan para su finalidad.
- Obtener autorización del titular para ceder datos.

Disposición 11/06
Medidas de Tratamiento

El Usuario o Responsable del Archivo de datos debe adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de los datos personales con el objeto de:

- ❑ evitar su adulteración, pérdida, consulta o tratamiento no autorizado.
- ❑ detectar desviaciones, intencionales o no, de información.

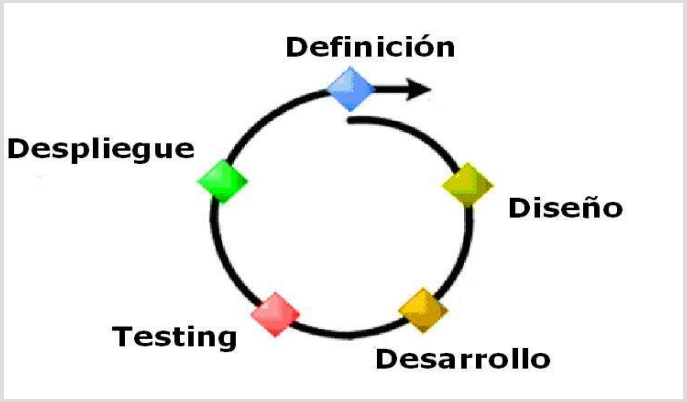
Se establecen tres niveles de seguridad: Básico, Medio y Crítico, conforme la naturaleza de la información tratada, pautas aplicables también a los archivos no informatizados (registro manual).

Para cada uno de los niveles se aplican medidas de seguridad según:

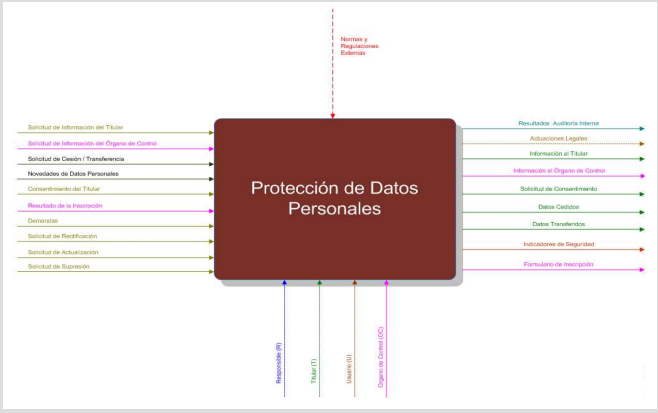
- ❑ la confidencialidad e integridad de la información contenida en el banco de datos respectivo;
- ❑ la naturaleza de los datos y la correcta administración de los riesgos a que están expuestos,
- ❑ el impacto que tendría en las personas la falta de integridad o confiabilidad debidas.

Dónde Contemplamos los Datos Personales?

The OWASP Foundation
http://www.owasp.org



I - Ciclo de Vida de Desarrollo



II - Procesos de la Organización

III - RRHH de la Organización

I - Seguridad en el Ciclo de Vida de la Aplicación

Dónde contemplamos los Datos Personales?

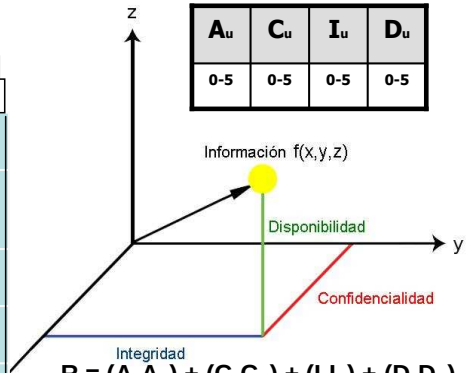
1 - Clasificación y Requisitos de Tratamiento

The OWASP Foundation
http://www.owasp.org

Clasificación de la Información (ACID)

AUDITABILIDAD
DISPONIBILIDAD
INTEGRIDAD
CONFIDENCIALIDAD

SECRETA	Su difusión afecta directamente al "core- business"
CONFIDENCIAL	Información de alta sensibilidad por impacto financiero, potencial de fraude, o requisitos legales
RESTRINGIDA	Información accesible por ciertas áreas, pero no toda la compañía
USO INTERNO	Información accesible por todos los miembros de la Organización
PUBLICA	Sin restricciones en su difusión



A_u	C_u	I_u	D_u
0-5	0-5	0-5	0-5

$$R = (A-A_u) + (C-C_u) + (I-I_u) + (D-D_u)$$

Clasificación de los Datos Personales

Básico: datos elementales de la persona

Nombre y apellido, documento de identidad, domicilio y teléfono, fecha de nacimiento, identificación tributaria o previsional, ocupación.

Medio: datos que debe guardar secreto por expresa disposición legal

Remuneración, estado civil, patrimonio, e-mail, datos bancarios.

Crítico: datos definidos como datos sensibles

Origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical, información de salud, información de la vida sexual, datos relac. c/ violencia de género.

CRÍTICO	**>4**
MEDIO	**3:4**
BAJO	**0:2**

Tratamiento

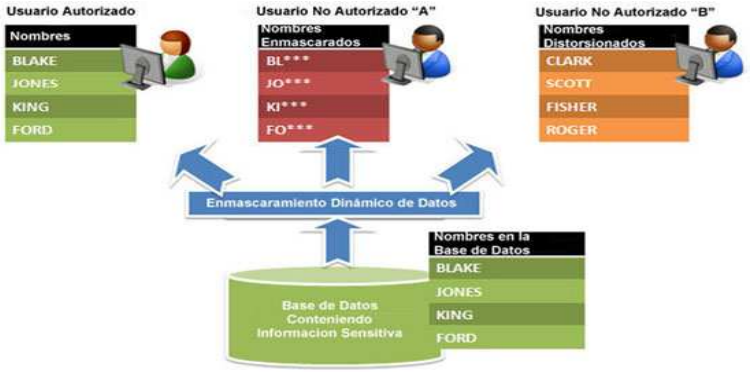
equivalencia directa entre ISO 27002 y Disp.11/06

TEXTO_PREG	TEXTO_METRICA	N1	Equivalencia	V.TARGET_ISO	V.TARGET_4609
Disponer de un Documento de Seguridad de Datos Personales	1.0.0_Existencia del documento de seguridad	Nivel BASICO	(M) 15.01.04.00 Protección de datos e información de carácter personal	Cumplimiento de Leyes y Regulaciones	Gestión de Seguridad de la Información
El Documento de Seguridad debe especificar los procedimientos y las medidas de seguridad a observar sobre los archivos, registros, bases y bancos que contengan datos de carácter personal.	1.0.1_Alcance del documento de seguridad	Nivel BASICO	(M) 15.01.04.01 Legislación vigente	Cumplimiento de Leyes y Regulaciones	Gestión de Seguridad de la Información
El Documento de Seguridad deberá mantenerse en todo momento actualizado y ser revisado cuando se produzcan cambios en el sistema de información.	1.0.2_Mantenimiento del documento de seguridad	Nivel BASICO	(M) 05.01.02.01 Actualización de la PS	Política de Seguridad	Gestión de Seguridad de la Información
El Documento de Seguridad deberá contener funciones y obligaciones del personal.	1.1.0_Funciones y obligaciones del doc de seg.	Nivel BASICO	(M) 06.01.03.00 Responsabilidades sobre la SI	Normativa de Organización de la Seguridad	Gestión de Seguridad de la Información
El Documento de Seguridad deberá contener la descripción de los archivos con datos de carácter personal y los sistemas de información que los tratan.	1.2.0_Descripción de archivos y sistemas en el doc de seg.	Nivel BASICO	(M) 06.01.03.06 Definición de activos y procesos de seguridad	Normativa de Organización de la Seguridad	Gestión de Seguridad de la Información
El Documento de Seguridad deberá contener la descripción de las rutinas de control de datos de los programas de ingreso de datos y las acciones a seguir ante los errores detectados a efectos de su corrección. Todos los programas de ingreso de datos, cualquiera sea su modo de procesamiento (batch, interactivo, etc.), deben incluir en su diseño, rutinas de control, que minimicen la posibilidad de incorporar al sistema de información, datos ilógicos, incorrectos o faltantes.	1.3.0_Control de errores en el doc de seg.	Nivel BASICO	(M) 12.02.02.00 Validaciones en las aplicaciones	Gestión de Desarrollo	Gestión de Seguridad de la Información
El Documento de Seguridad deberá contener registros de incidentes de seguridad.	1.4.0_Registro de incidentes en el doc de seg.	Nivel BASICO	(M) 07.02.02.09 Procedimiento de registro para cada nivel	Normativa de Tratamiento de la Información	Control de Cambios
El Documento de Seguridad deberá contemplar la notificación, gestión y respuesta ante los incidentes de seguridad.	1.4.1_Comunicación de incidentes en el doc de seg.	Nivel BASICO	(M) 13.01.01.03 Informe de incidencias de seguridad	Gestión de Operaciones	Estrategia de IT
El Documento de Seguridad deberá contener los procedimientos para efectuar las copias de respaldo y de recuperación de datos.	1.5.0_Procedimientos de backup en el doc de seg	Nivel BASICO	(M) 10.05.01.09 Procedimiento de restauración	Normativa de Tratamiento de la Información	Gestión de Seguridad de la Información
El Documento de Seguridad deberá contener la relación actualizada entre Sistemas de Información y usuarios de datos con autorización para su uso.	1.6.0_Relación sistema-usuario en el doc de seg.	Nivel BASICO	(M) 11.02.01.07 Registro de los accesos de cada usuario	Gestión de Accesos	Normativa de Tratamiento de la Información
El Documento de Seguridad deberá contener los procedimientos de identificación y autenticación de los usuarios de datos autorizados para utilizar determinados sistemas de información.	1.7.0_Procedimientos de acreditación en el doc de seg.	Nivel BASICO	(M) 11.02.01.08 Procedimiento de actualización del registro de usuarios	Normativa de Control de Accesos	Plan de Contingencia
En el caso en que el mecanismo de autenticación utilice contraseña, la misma será asignada por el responsable de seguridad de acuerdo a un procedimiento que garantice su confidencialidad.	1.7.1_Procedimiento de confidencialidad del mecanismo de autentic.	Nivel BASICO	(M) 11.02.03.01 Compromiso para secreto de contraseñas de usuario	Gestión de Accesos	Cumplimiento de Leyes y Regulaciones
El procedimiento de confidencialidad deberá prever el cambio periódico de las contraseñas (lapso máximo de vigencia) las que deberán estar almacenadas en forma ininteligible.	1.7.2_Cambio periódico de contraseñas en Procedimiento de confidencialidad	Nivel BASICO	(M) 11.02.03.03 Contraseña temporal	Gestión de Accesos	Gestión de Seguridad de la Información
El Documento de Seguridad deberá contener el control de accesos de usuarios a datos y recursos necesarios para la realización de sus tareas para lo cual deben estar autorizados.	1.8.0_Control de accesos en el doc de seg.	Nivel BASICO	(M) 11.01.01.00 Política de Control de Accesos	Normativa de Control de Accesos	Normativa de Organización de la Seguridad
El Documento de Seguridad deberá contener las medidas de prevención adoptadas a efectos de impedir amenazas de software malicioso (virus, troyanos, etc.) que puedan afectar archivos con datos de carácter personal.	1.9.0_Adopción de medidas de prevención de software malicioso	Nivel BASICO	(M) 10.04.01.00 Controles de detección de código malicioso	Gestión de Operaciones	Normativa de Organización de la Seguridad
Instalar y actualizar, con la periodicidad pertinente, software de detección y reparación de virus, ejecutándolo rutinariamente.	1.9.1_Instalación y actualización de software antivirus	Nivel BASICO	(M) 10.04.01.06 Software de detección y corrección de código malicioso	Gestión de Operaciones	Normativa de Organización de la Seguridad

2 y 3 – Enmascaramiento y Requisitos con Terceros

Enmascaramiento de los Datos

- Estático o Dinámico.
- Pueden ser usados pero no interpretados (información ininteligible).
- Conservan la estructura y las características de la información original.
- Desarrolladores y Testers pueden emplear datos realistas preservando la confidencialidad.



Requisitos en Relaciones con Terceros

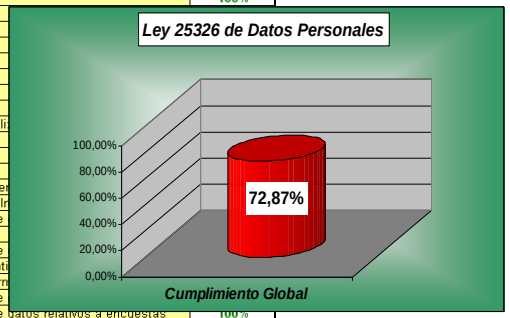
- en contratos con subcontratistas (ej: subcontratista que presta servicio a dos empresas rivales).
- garantías de confidencialidad.
- derecho de acceder y auditar.
- de acceso a datos reales.
  - **procedimiento de acceso temporal a datos reales.**
- en contratos de cesión y subcesiones de datos.

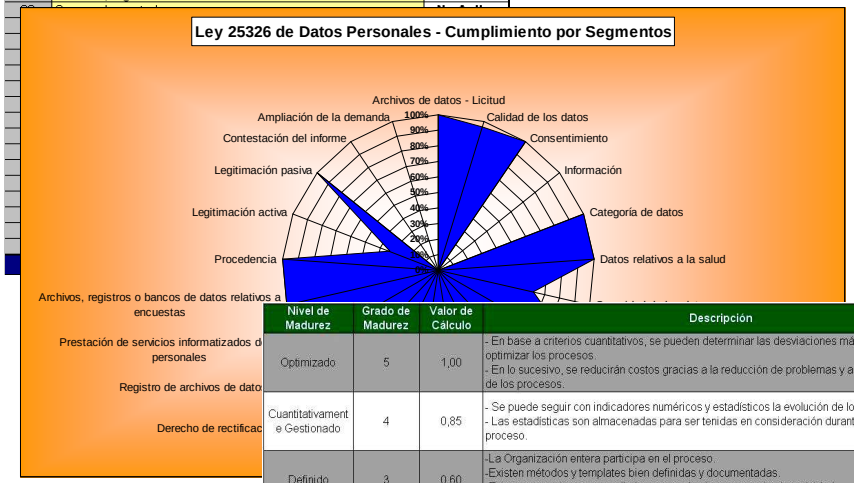
4 – Tablero de Control y Seguimiento

Cumplimiento Ley Protección de Datos Personales

Ley 25326

Artic.	Ley de Protección de Datos Personales	Cumplim.
3	Archivos de datos - Licitud	100%
4	Calidad de los datos	96%
5	Consentimiento	100%
6	Información	0%
7	Categoría de datos	100%
8	Datos relativos a la salud	100%
9	Seguridad de los datos	
10	Deber de confidencialidad	
11	Cesión	
12	Transferencia internacional	
13	Derecho de información	
14	Derecho de acceso	
15	Contenido de la información	
16	Derecho de rectificación, actuali	
17	Excepciones	
18	Comisiones legislativas	
19	Gratuidad	
20	Impugnación de valoraciones pe	
21	Registro de archivos de datos. In	
22	Archivos, registros o bancos de	
23	Supuestos especiales	
24	Archivos, registros o bancos de	
25	Prestación de servicios informati	
26	Prestación de servicios de inform	
27	Archivos, registros o bancos de	
28	Archivos, registros o bancos de datos relativos a encuestas	100%





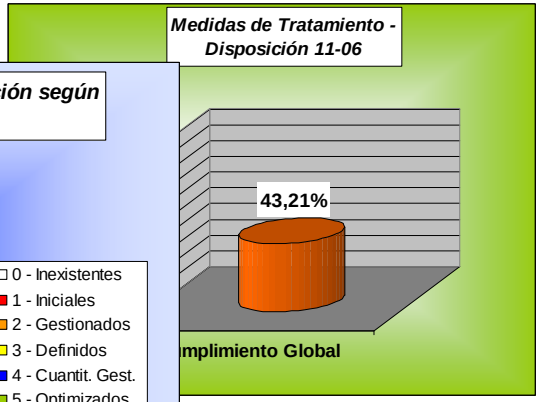
Nivel de Madurez	Grado de Madurez	Valor de Cálculo	Descripción	Clave	Aspectos
Optimizado	5	1,00	- En base a criterios cuantitativos, se pueden determinar las desviaciones más comunes y optimizar los procesos. - En lo sucesivo, se reducirán costos gracias a la reducción de problemas y a la continua revisión de los procesos.	Mejora Continua	Formalización
Cuantitativamente Gestionado	4	0,85	- Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. - Las estadísticas son almacenadas para ser tenidas en consideración durante la optimización del proceso.	Indicadores	
Definido	3	0,60	-La Organización entera participa en el proceso. -Existen métodos y templates bien definidas y documentadas. -Existen normativas y procedimientos aprobados que regulan la actividad. -Los correspondientes actores han sido formados.	Procedimientos	
Gestionado	2	0,15	-Se normalizan las buenas prácticas en base a la experiencia y el método. -Están definidos los productos a realizar, y los hitos para su revisión. -Las definiciones no aplican a nivel corporativo, ni existe normalización.	Buenas Prácticas	Implantación
Inicial	1	0,05	-Estado donde el éxito de las actividades se basa, la mayoría de las veces, en el esfuerzo personal. -Los procedimientos son inexistentes o localizados en áreas específicas.	Esfuerzo Personal	
Inexistente	0	0,00	-No se realiza ningún aspecto de la actividad.	Sin Acciones	
N/A	0	0,00	No Aplica	N/A	

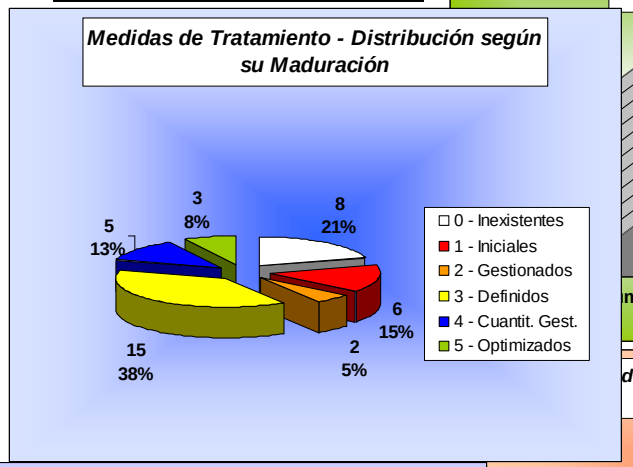
Cumplimiento de las Medidas de Tratamiento

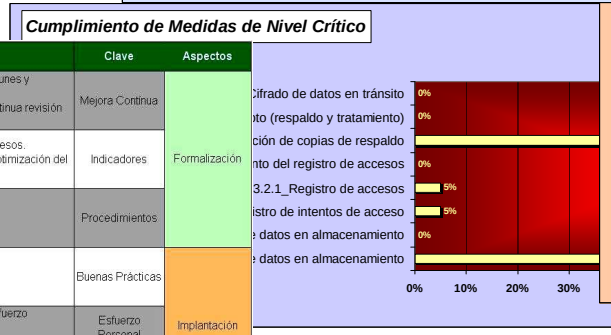
Disposición 11/06

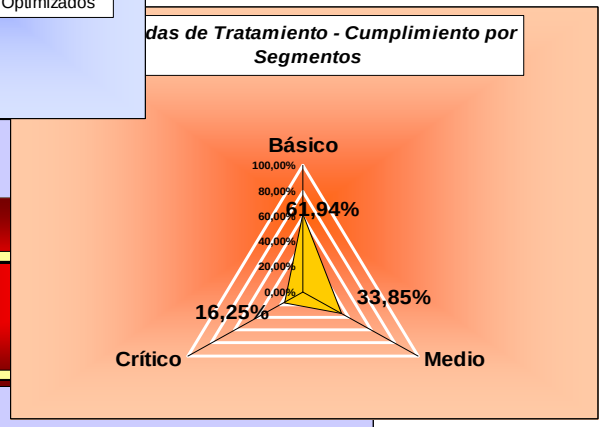
	Total	Básico	Medio	Crítico
0 - Inexistentes	11	3	4	4
1 - Iniciales	6	3	1	2
2 - Gestionados	3	2	1	0
3 - Definidos	16	7	7	2
4 - Cuantit. Gest.	3	3	0	0
5 - Optimizados	0	0	0	0

	% Cump.	Maduración
Básico	61,94%	3 - Definido
Medio	33,85%	2 - Gestionado
Crítico	16,25%	2 - Gestionado
Total	43,21%	2 - Gestionado

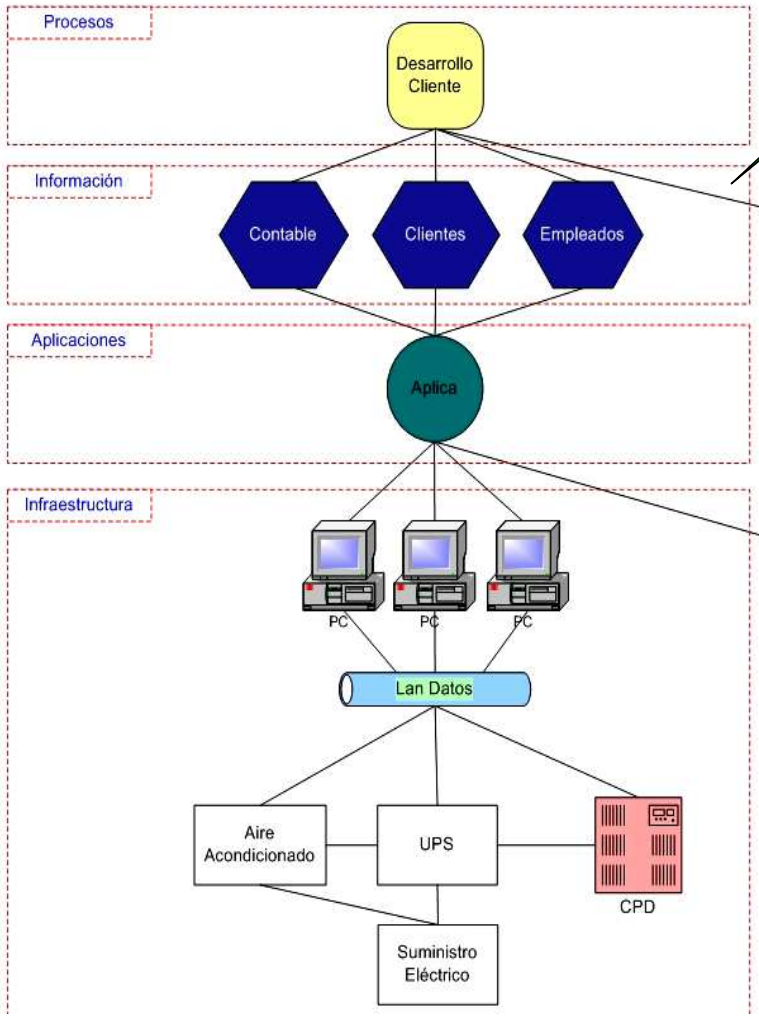








Dónde contemplamos los Datos Personales?

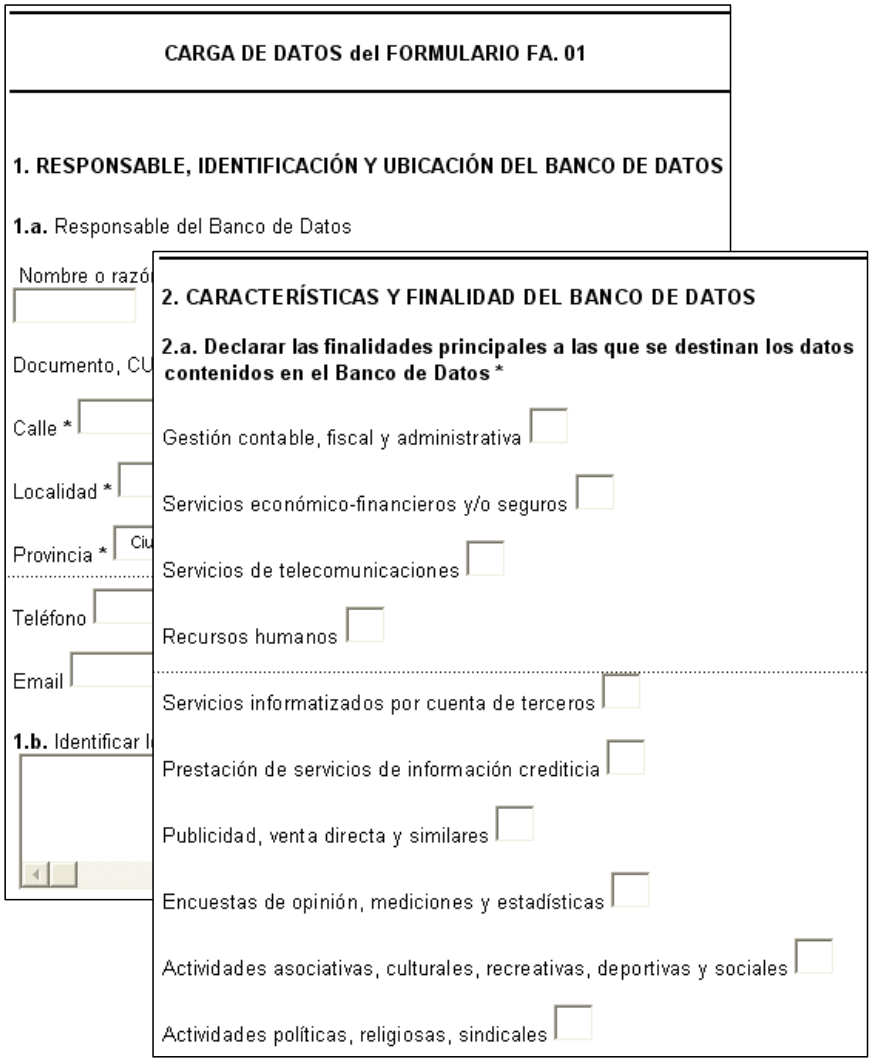


5 Declaración del Banco de Datos en DNPDP

6 Ley Datos Personales como Proceso

7 Documento de Seguridad

5 – Declaración del Banco de Datos en la DNPDP



CARGA DE DATOS del FORMULARIO FA. 01

1. RESPONSABLE, IDENTIFICACIÓN Y UBICACIÓN DEL BANCO DE DATOS

1.a. Responsable del Banco de Datos

Nombre o razó

Documento, CU

Calle *

Localidad *

Provincia *

Teléfono

Email

1.b. Identificar l

2. CARACTERÍSTICAS Y FINALIDAD DEL BANCO DE DATOS

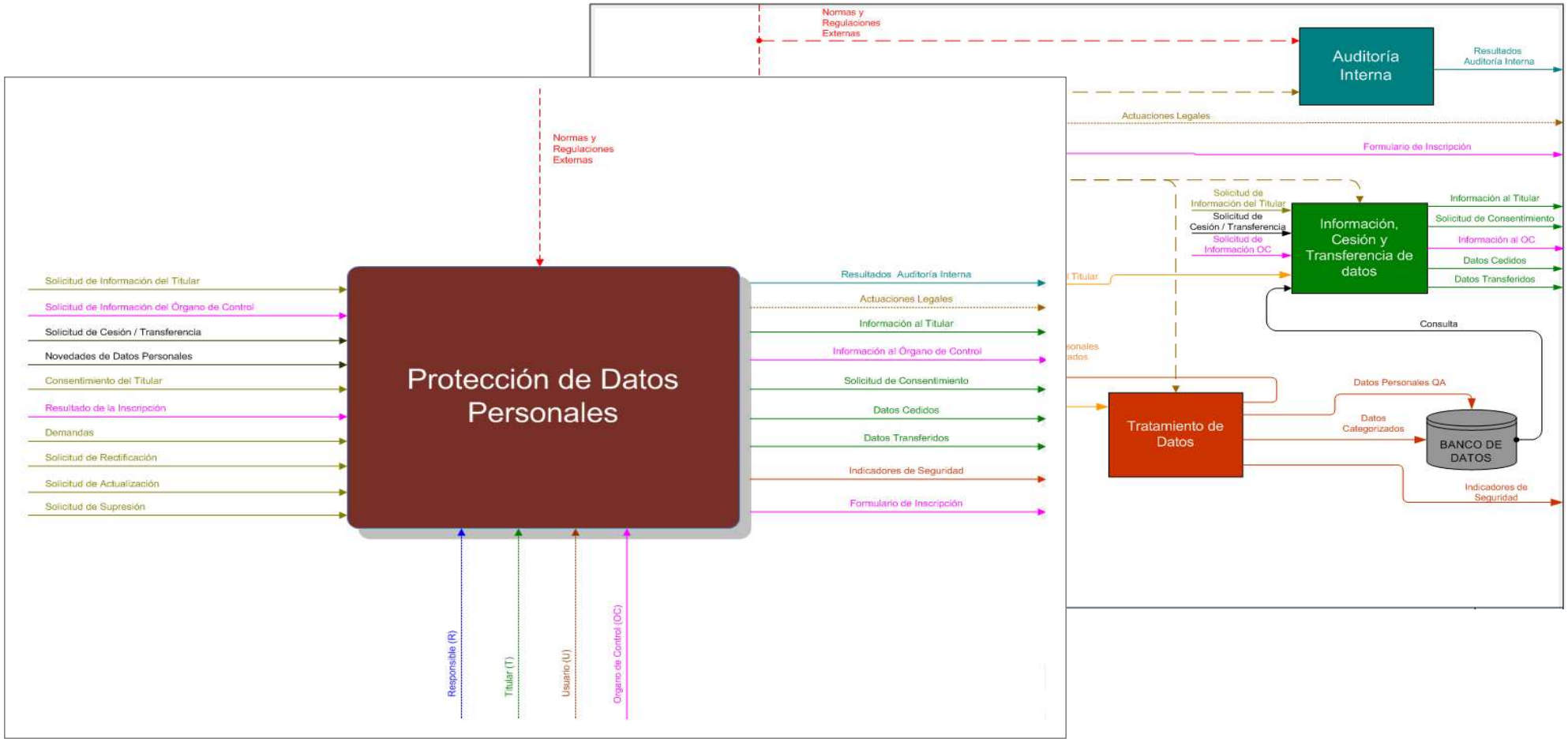
2.a. Declarar las finalidades principales a las que se destinan los datos contenidos en el Banco de Datos *

- Gestión contable, fiscal y administrativa
- Servicios económico-financieros y/o seguros
- Servicios de telecomunicaciones
- Recursos humanos
- Servicios informatizados por cuenta de terceros
- Prestación de servicios de información crediticia
- Publicidad, venta directa y similares
- Encuestas de opinión, mediciones y estadísticas
- Actividades asociativas, culturales, recreativas, deportivas y sociales
- Actividades políticas, religiosas, sindicales

El Registro contiene:

1. Nombre y domicilio del Responsable de la base de datos;
2. Ubicación física de la base de datos;
3. Características y finalidad de la base de datos;
4. Naturaleza de los datos personales contenidos en cada archivo;
5. Forma de recolección y actualización de datos;
6. Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos;
7. Modo de interrelacionar la información registrada;
8. Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información;
9. Tiempo de conservación de los datos;
10. Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.

6 – Ley de Datos Personales como Proceso



Definición	LDAP*	SAP	AS400
Caracteres mínimos de contraseñas	6	6	6
Dígitos requeridos en contraseñas	1	1	1
Mayúscula requerida en contraseñas	1	1	No viable**
Historial de contraseñas	5	5	5
Máximo log-in fallidos	3	3 x 2	3
Acciones a tomar	Bloqueo cuenta por siempre	Bloqueo cuenta por siempre	Bloqueo cuenta por siempre
Caducidad de contraseña	90 días	90 días	90 días
Bloqueo pantalla por inactividad	5 min.	600 seg.	No viable***

* En implementación.
** AS400 no es "case sensitive"
*** No es posible implementar este control ya que provoca la cancelación de procesos.

5.2 Medidas de seguridad para Datos Personales de Nivel Medio

5.2.1. Identificación del Responsable (u órgano específico) de Seguridad

A continuación se describen los órganos/responsables de seguridad:

Comité de Seguridad de la Información

- Mantenerse informado sobre el estado de cumplimiento de la legislación vigente en materia de Protección de Datos Personales.
- Facilitar los recursos para las acciones necesarias para gestionar dicho cumplimiento.

Jefe de Seguridad de la Información

- Gestionar las acciones necesarias para dar cumplimiento a la normativa en materia de Protección de Datos Personales, entre otras:
  - Asistir a la organización en el registro de las bases de datos personales, y el mantenimiento de dicho registro actualizado
  - Definir las medidas de seguridad a ser aplicadas en las bases de datos personales
  - Controlar la correcta implementación y mantenimiento de dichas medidas de seguridad

Anexo H - Inventario de soportes

El responsable de seguridad deberá tener un inventario actualizado de los soportes que contienen datos de carácter personal del archivo.
A continuación se propone un modelo de inventario:

Página nº _____

Archivo: NOMBRE DE ARCHIVO					
ALTAS		BAJAS			
Etiqueta/Tipo de soporte	Fecha	Reutilización	Destrucción	MÉTODO	Fecha
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /

Dónde contemplamos los Datos Personales?

8 Procedimientos de Respuesta

9 Marco Normativo de Seguridad

10 Formación Continua

8 – Procedimientos de Respuesta al Afectado

Derecho	Plazo	Artículo
Acceso	10 días corridos	Art.14
Rectificación, Actualización, Supresión.	5 días hábiles	Art. 16

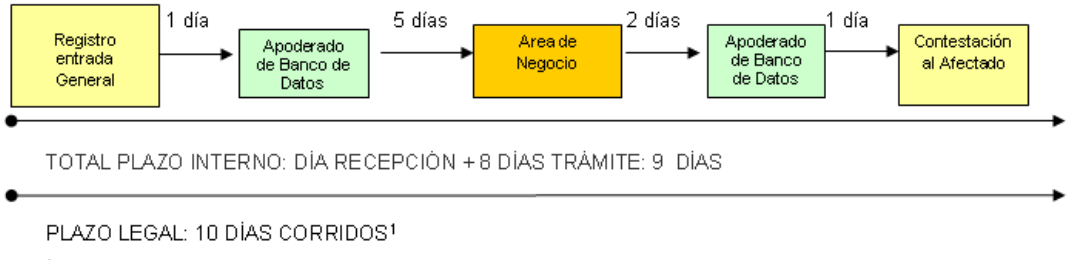
FORMULARIO PARA EL EJERCICIO DEL DERECHO DE ACCESO
Petición de información sobre los datos personales incluidos en un Archivo, registro, base o banco de datos[1].

DATOS DEL RESPONSABLE DEL BANCO DE DATOS O DEL TRATAMIENTO DE DATOS
Nombre:
Dirección:
Localidad: Provincia:

DATOS DEL SOLICITANTE
D./Dª. ....., con dc
..... nº..... piso ..... de
..... Provincia de .....
teléfono ....., con D.N.I ....., del que acc
del presente escrito manifiesta su deseo de ejercer su derecho de
el artículo 14 de la Ley Nº 25.326, y los artículos 14 y 15 de la F
25.326 aprobada por Decreto Nº 1558/01.

SOLICITA.-
1.- Que me facilite gratuitamente el acceso a los datos existent
bases o registros en el plazo máximo de diez (10) días a contar
solicitud, entendiendo que si transcurre este plazo sin contestació
denegada. En este caso se podrá interponer el reclamo ante la Dire
de Datos Personales y quedará expedita la vía para ejercer la accic
personales, en virtud de lo dispuesto por el artículo 14 de la Ley N
su Decreto Reglamentario Nº 1558/01.

Procedimiento Interno para Solicitud de Acceso



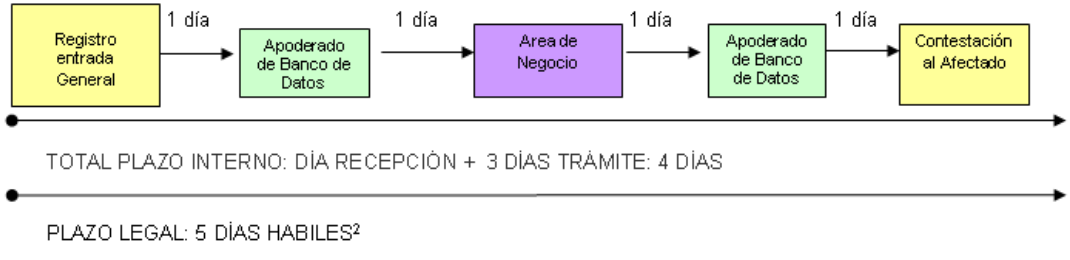
FORMULARIO PARA LA RECTIFICACIÓN, ACTUALIZACIÓN O SUPRESIÓN DE DATOS PERSONALES INCLUIDOS EN BANCOS DE DATOS (1)

DATOS DEL RESPONSABLE DEL BANCO DE DATOS
Nombre:
Domicilio:
C.P. Localidad:
Provincia:
Mail:

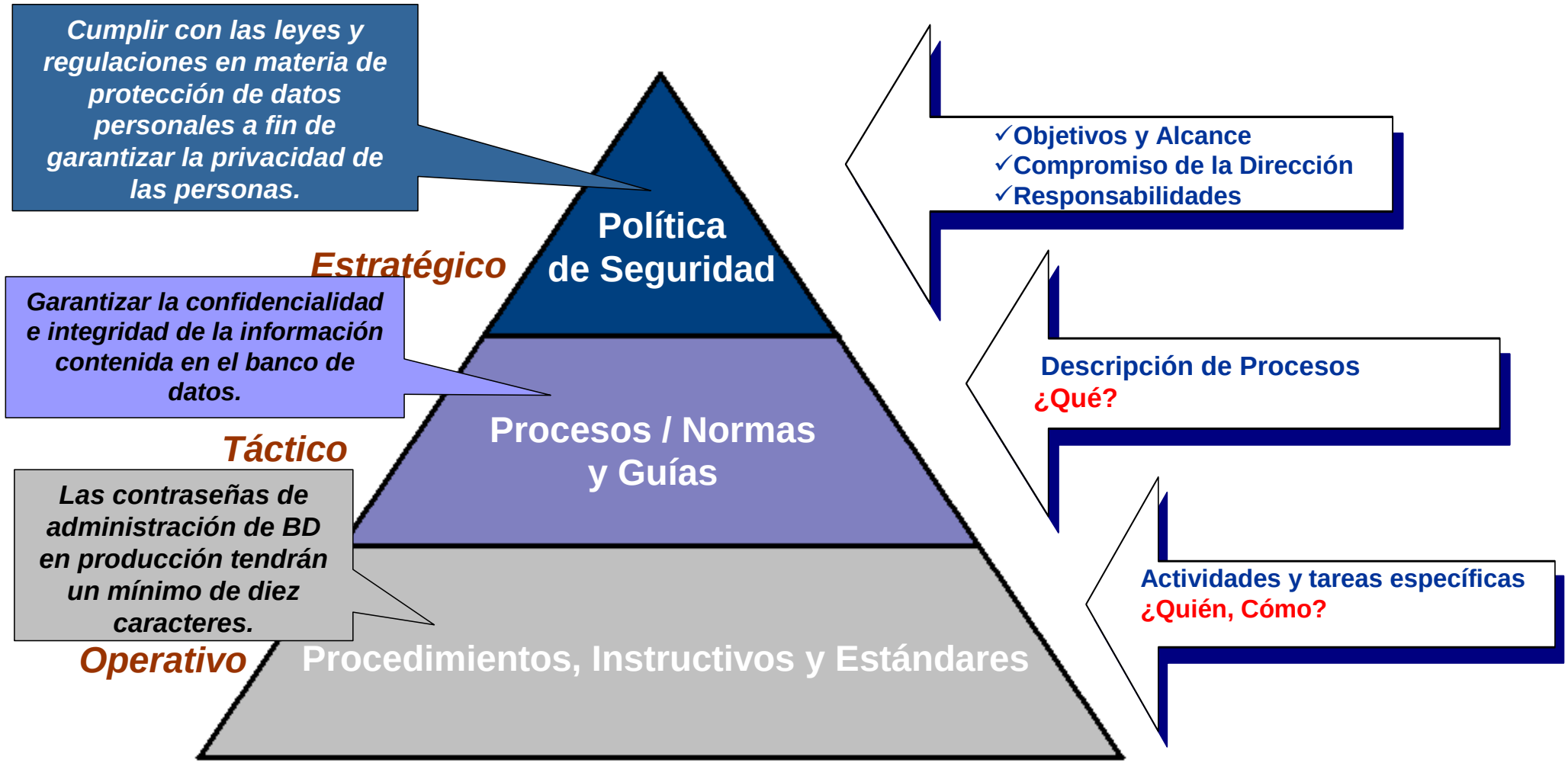
DATOS DEL SOLICITANTE (TITULAR DE LOS DATOS PERS
D./Dª. .....
..... Nº .....
Localidad ..... Provincia de ..
C.P. ....., teléfono ....., con D.N.I .....
fotocopia, por medio del presente escrito manifiesta su de
rectificación / actualización / supresión, de conformidad
25.326, y el artículo 16 de su Decreto Reglamentario Nº 1558/0

SOLICITO:
1. Que en el plazo de cinco (5) días hábiles desde la recepci
gratuitamente a la **rectificación/actualización/supresi**
persona que se encuentren en su base de dato
rectificarse/actualizarse/suprimirse se enumeran en
acompañan los documentos que acreditan su veracidad.
2. Que me comuniquen por escrito a la dirección arriba indicada, la **rectificación/actualización/supresión** de los datos una vez realizada.
3. Que para el caso que el responsable del banco de datos considere que la **rectificación/actualización/supresión** no procede, lo comunique en forma motivada, por escrito y dentro del plazo de cinco (5) días.

Procedimiento Interno para Solicitud de Rectif, Actual, Sup.



9 – Marco Normativo de Seguridad



10 – Formación Continua

Etapas del Plan

Etapa I	Etapa II	Etapa III	Etapa IV	Etapa V	Etapa VI	Etapa VII
Contexto Sponsorship	Diagnóstico	Definiciones Diseño	Desarrollo Creación de Materiales	Implementación	Evaluación y Aprendizaje	Sustentabilidad
• Identificar la estrategia empresarial • Determinar el alcance • Lograr apoyo, acordar responsabilidades y construir • Promulgar el Plan como parte de la mejora continua	• Identificación de audiencias • Identificación de la cultura organizacional • Fast assessment inicial (indicadores iniciales sobre las prácticas de los usuarios)	• Acordar lo que se entregará al cliente (SLA) • Diseñar el enfoque y planificar • Establecer parámetros de seguimiento	• Creación de la solución: contenido, estructura, formato y fuente de los mensajes • Selección y combinación de medios • Autotesting de calidad de la solución	• Guía de escenarios de implementación • Preparación logística • Aplicar herramientas de comunicación • Analizar y ajustar el plan (desviaciones)	• Fast assesment final (indicadores finales sobre las prácticas de los usuarios) • Análisis de los cambios producidos • Recomend. para la gestión	• Mantenimiento: acciones periódicas para reforzar lo aprendido • Actualización de objetivos por cambios del entorno

¿Quién es Responsable de la Seguridad de la Información?

Tres años de prisión para un joven que se hizo pasar en Facebook por el príncipe de Marruecos

Un joven ingeniero marroquí que se hizo pasar en el sitio de internet Facebook por el príncipe Mulay Rashid, el hermano pequeño del rey Mohammed VI de Marruecos, fue condenado a tres años de prisión y a pagar una multa de 10.000 dirhams (cerca de 900 euros). El fiscal había reclamado "un castigo ejemplar por [Ver nota ...]

Publicado por: Dr. Santiago Profumo el Thursday 10 April 2008
Posted in derecho internacional, estafa, facebook, internet, robo de identidad | No Comments »

lanacion.com

Habrían robado los datos de 12 millones de personas

La justicia federal busca determinar si la Anses filtró registros a una empresa pri

infobae.com

El "robo del siglo" en Internet

Votá ☆☆☆☆☆ Resultado ☆☆☆☆☆ 0 voto Recomendar Tamaño del texto

Si bien no se conoce la cantidad de afectados en tres países ni el monto que robaron los piratas, expertos en seguridad informática dijeron que el robo de información correspondiente a **códigos PIN** y bandas magnéticas de **tarjetas de débito** es el "peor de la historia" y que esto es recién "la punta del témpano"

Un gran número de clientes del banco Citibank sufren en carne propia lo que los expertos en seguridad informática llaman el "peor robo de la historia".

HSBC recibe multa por pérdida de datos personales

Sancionan con más de 3 millones de euros a tres filiales del banco HSBC, por la pérdida de datos confidenciales de 180 mil clientes

Comenta la nota

EFE
EL UNIVERSAL
LONDRES, ING MIÉRCOLES 22 DE JULIO DE 2009
07:50 La Autoridad británica de Servicios Financieros (FSA) ha multado con más de 3 millones de libras (3.47 millones de euros) a tres filiales del banco HSBC por la pérdida de datos confidenciales de clientes, informa hoy la BBC.

Nuevo Reglamento de Protección de Datos de la Unión Europea

- Incorporación del Derecho al olvido (cancelación automática de los datos).
- Incorporación del Derecho a la portabilidad de datos (transferencia de un soporte a otro).
- Posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición de manera telemática.
- Posibilidad de cobrar una tasa frente a solicitudes de derecho de acceso reiteradas o excesivas.
- Obligación de realizar una evaluación de impacto de la protección de datos, previo de efectuar operaciones de tratamiento arriesgadas.
- Realización de análisis de riesgos, evolucionando el actual modelo de reactivo a preventivo.
- Deber de establecer el período de conservación de los datos.

Novedades en Materia de Protección de Datos (II)

- Las empresas con más de 250 empleados o las Administraciones públicas tendrán que tener la figura del Data Protection Officer.
- Obligación de notificar la violación de datos, con el fin de concientizar a los responsables del tratamiento a aplicar medidas de seguridad más estrictas.
- Posibilidad de certificación para los productos y servicios que cumplen con las normas de protección de la intimidad.
- Mayor exigencia de cooperación entre las Autoridades de Control a nivel internacional.
- Creación de "ventanilla única" en las Autoridades de Control. Derecho a presentar un reclamo ante la autoridad de control de cualquier estado miembro.
- El Consejo Europeo de Protección de Datos tendría un procedimiento reforzado para imponer actuaciones a las Autoridades de Protección de Datos nacionales.
- Posibilidad de denunciar o demandar por parte de organismos, organizaciones o asociaciones, en nombre del interesado (Legitimación activa).
- La no obligatoriedad de declarar ficheros.

Muchas Gracias

Pablo Romanos
pabloromanos@green40.com