Datos Personales en el Ciclo de Vida de Desarrollo Seguro

Pablo Romanos

pabloromanos@green40.com

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

Data Protection Laws Around the World

- **Leyes de protección adecuadas y completas**
- **Esfuerzos pendientes por implementar leyes**
- **Sin Ley**

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.

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

- 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.

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:

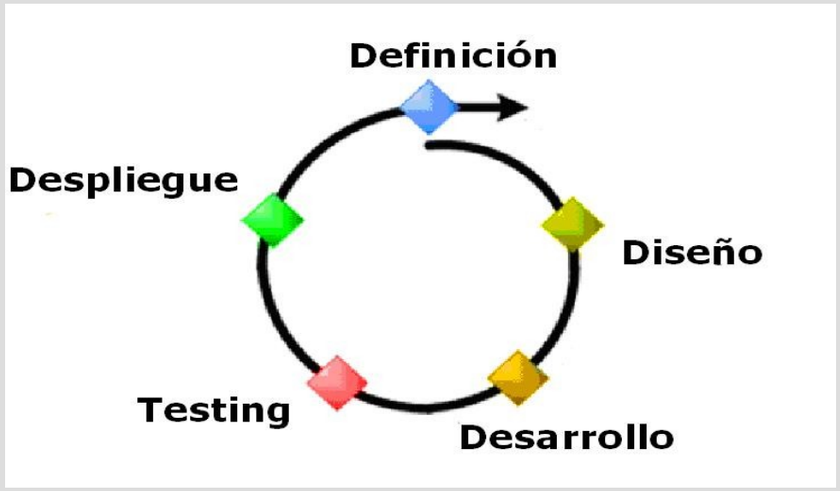
- evitar su adulteración, pérdida, consulta o tratamiento no autorizado.
- detectar desviaciones, intencionales o no, de información.

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).

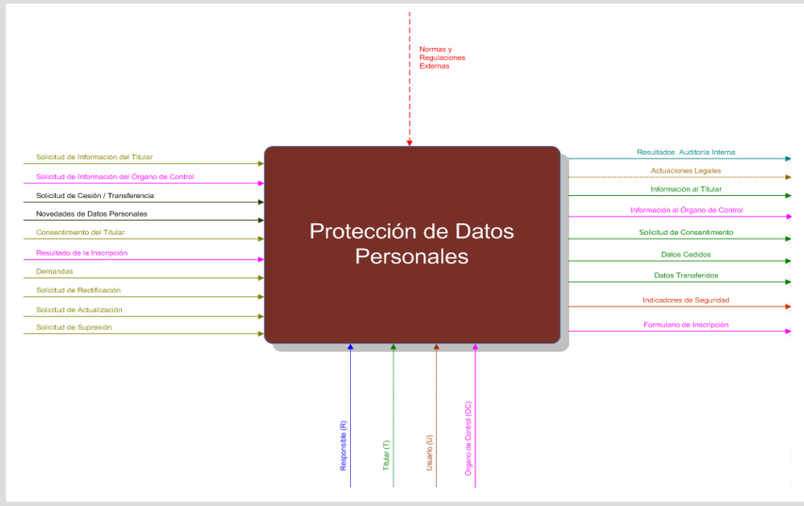
Para cada uno de los niveles se aplican medidas de seguridad según:

- 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

Donde Contemplamos los Datos Personales?



I - Ciclo de Vida de Desarrollo



II - Procesos de la Organización

III - RRHH de la Organización

1 - Seguridad en el Ciclo de Vida de la Aplicación

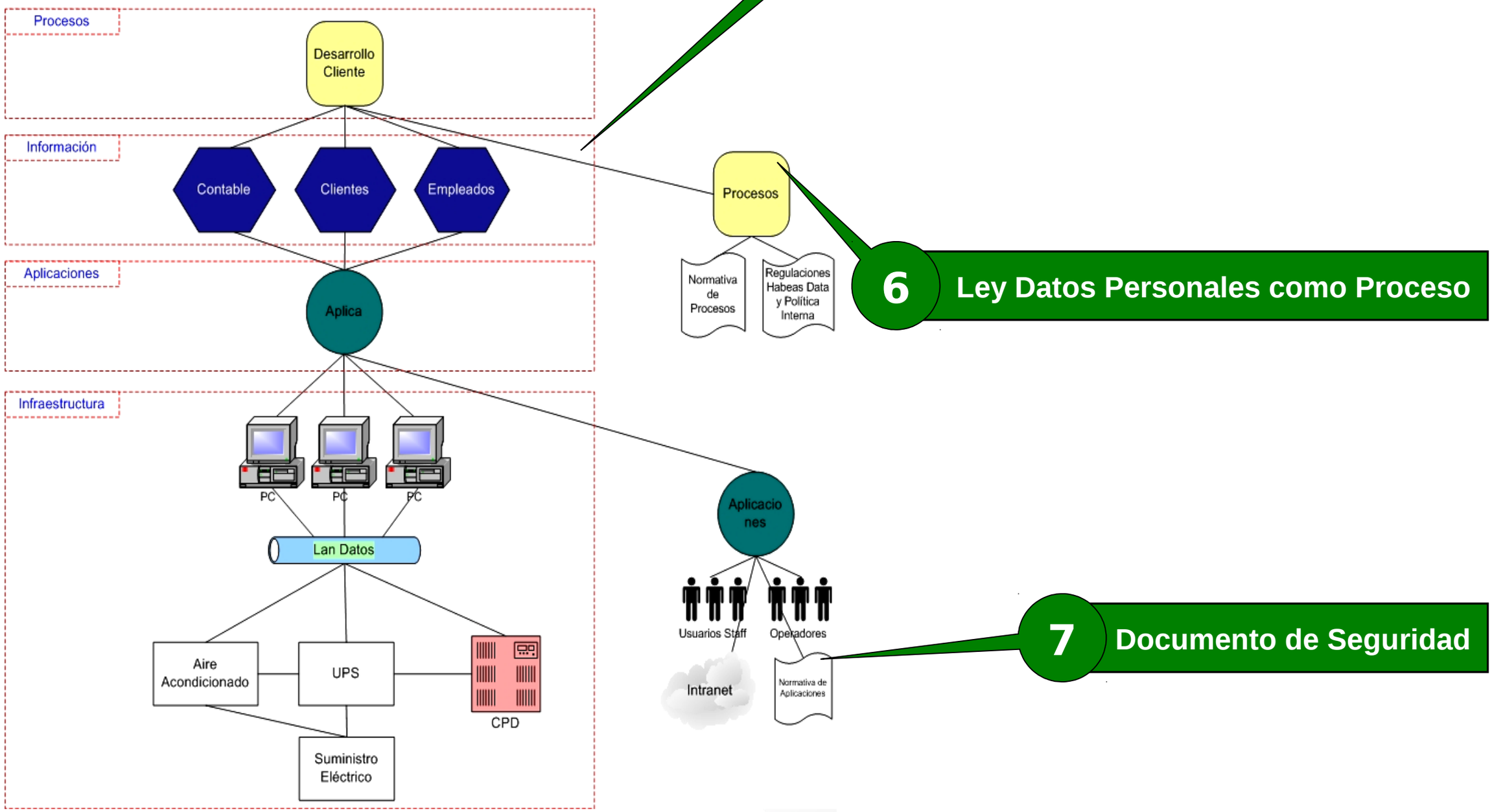
Dónde contemplamos los Datos Personales?

Dónde contemplamos los Datos Personales?

5 Declaración del Banco de Datos en DNPDP

6 Ley Datos Personales como Proceso

7 Documento de Seguridad



Dónde contemplamos los Datos Personales?

8 Procedimientos de Respuesta

9 Marco Normativo de Seguridad

10 Formación Continua

Novedades en Materia de Protección de Datos (I)

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