Sistemas de Información para la Gestión

Unidad 6:

IMPACTO ÉTICO, SOCIAL Y LEGAL EN LA GESTIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN

Unidad 6. IMPACTO ÉTICO, SOCIAL Y LEGAL EN LA GESTIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN

Contenidos:

Impacto ético, social y legal de las tecnologías de información: problemas éticos y sociales relacionados con las tecnologías de información. Políticas de Información y aseguramiento de la calidad de datos. Impactos legales en los Sistemas de Información. **Impacto ético, social y legal en la gestión de la infraestructura.** Políticas de TI. Normativas actuales y mejores prácticas en la utilización de tecnologías de internet.

Objetivos específicos:

- Entender que aspectos éticos, sociales y políticos generan los SI
- Conocer conceptos básicos de responsabilidad legal

Bibliografía Básica:

- Sistemas de información gerencial / Laudon, Kenneth C. (2012) Sistemas de información gerencial [texto impreso] / Laudon, Kenneth C.; Laudon, Jane P.. - 12a. ed.. - México : Pearson Educación, 2012. SBN 978-607-32-0949-6. Nota de contenido : Cap 4. Aspectos éticos y sociales en los sistemas de información)
- Normas del contexto legal en Argentina aplicables para cada tema especifico en los sistemas de Información

Plan de clase

- Introducción
- Derechos titulares
- Principios Generales
- Habeas Data
- Registro Documento Cuestionados
- Registro Nacional No Llame
- Facultades DNPDP
- Conclusiones

CONCEPTO

La protección integral de los datos personales garantiza el honor y la privacidad de la personas, como también el acceso a la información que sobre las mismas se registre

¿Qué son los datos personales?

Es información de cualquier tipo referida a personas físicas o de existencia ideal determinados o determinables

OBJETIVOS DE UN SISTEMA DE PDP :

- Asegurar un nivel adecuado al cumplimiento de las normas
- Ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos
- Ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas

ESCENARIO JURIDICO

- CONSTITUCION NACIONAL
- LEY Nº 25.326
- LEY N° 26.951
- DECRETO 1558/2001
- DISPOSICIONES DNPDP/RESOLUCIONES AAIP

Agencia de Acceso a la Información Pública
AAIP

La Agencia de Acceso a la Información Pública (Dirección Nacional de Protección de Datos Personales) es el órgano descentralizado del Ministerio de Justicia y Derechos Humanos de la Nación para el control de la Ley de Protección de Datos Personales

Ejerce las funciones encomendadas por la ley y su decreto reglamentario con plena independencia

SISTEMA DE PROTECCION DE DATOS PERSONALES

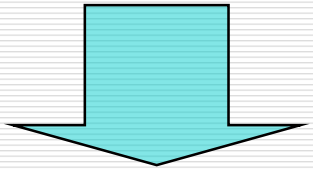
AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA

REGISTRO NACIONAL BASE DE DATOS

REGISTRO NACIONAL DOCUMENTOS CUESTIONADOS

REGISTRO NACIONAL NO LLAME

REGISTRO NACIONAL DE PDP



Registro obligatorio de bases de datos personales dispuesto por la Ley Nº 25.326 en la DNPDP

Personas humanas o de existencia ideal privadas y publicas que sean titulares de bases de datos personales o realicen tratamiento de información personal

CONCEPTOS DE LA LEY PDP

Conjunto organizado de datos personales objeto de procesamiento

Responsable BD

Titular de una BD

Base de Datos

Información de cualquier tipo referido a personas físicas y jurídicas

Datos Personales

Datos

Datos Sensibles

Datos personales que revelan origen racial, étnico, opinión política, convicciones religiosas, salud, vida sexual

Titular de Datos

Persona física o jurídica

Procesamiento

Recolección, conservación, ordenamiento, modificación, relaciones de BD

DEFINICIONES

Responsable de Archivo, registro, base o banco de datos: Titular del archivo

Datos Informatizados: Datos personales

Titular de los Datos: Humana o de existencia ideal cuyos datos sean objeto de tratamiento dentro de la Ley

Usuario de los datos: Usuario que efectúe tratamiento con los datos

Disociación de datos: No pueda asociarse a personas determinada o determinable

Bases de datos sujetas a inscripción

BD personales de organismos privados y privados, que excedan el uso exclusivamente personal y se destinen a dar informes deben inscribirse en la DNPDP.

¿Qué beneficios obtengo con la inscripción?

- Cumplir con la Ley N° 25.326. Presunción de licitud de la base de datos.
- Confianza con los clientes.
- Mayor competitividad.
- Buenas Prácticas. Código de Conducta Sectorial
- Evitar Sanciones
- Certificado de Inscripción

Principios Generales

1. Licitud (Inscripción BD)
2. Calidad de los datos
3. Consentimiento
4. Información
5. Categoría de datos
6. Datos relativos a la salud
7. Deber de Confidencialidad
8. Cesión
9. Transferencia Internacional
10. Seguridad de datos

PRINCIPIOS GENERALES

1. LICITUD DE DATOS

Bases de datos deben inscribirse conforme a ley 25.326

PRINCIPIOS GENERALES

2. CALIDAD d/ DATOS

Deben ser ciertos, adecuados, pertinentes, actualizados

Recolección no puede hacerse por medios desleales, fraudulentos

No pueden ser utilizados para otras finalidades a las previstas

Deben permitir derecho de acceso a su titular

Deben destruirse si dejan de ser necesarios

PRINCIPIOS GENERALES

3. CONSENTIMIENTO

Para que el tratamiento de datos sea LICITO debe mediar CONSENTIMIENTO por escrito del titular u otra modalidad equiparable.

Mecanismo validación de identidad eficaz.

PRINCIPIOS GENERALES

4. INFORMACION

Finalidad y destinatarios

Existencia de una base de datos, identidad domicilio de su responsable

Carácter obligatorio o facultativo de responder cuestionarios, en especial respecto a datos sensibles

Consecuencias de proporcionar datos, su negativa o inexactitud de los mismos
Posibilidad de ejercer derecho de acceso, rectificación y supresión de datos

PRINCIPIOS GENERALES

5. CATEGORIA DE DATOS

- Prohibido obligar a dar datos sensibles.
- Datos sensibles sólo se recolectan y tratan cuando medien razones de interés general. O finalidades estadísticas o científicas con datos disociados.
- Prohibido formar BD que revele datos sensibles. Excepto: organizaciones religiosas, políticas y sindicales.
- Antecedentes penales o contravencionales sólo tratados por autoridades públicas competentes.

PRINCIPIOS GENERALES

6. DATOS RELATIVOS A SALUD

Establecimientos vinculados a la salud pueden recolectar y tratar datos personales relativos a salud física y mental de pacientes que acudan o acudiesen o hubieren acudido respetando SECRETO PROFESIONAL

PRINCIPIOS GENERALES

7. DEBER DE CONFIDENCIALIDAD

Secreto profesional sobre datos

en todas las fases de su tratamiento, incluso

una vez finalizada la relación con el responsable

de la BD

PRINCIPIOS GENERALES

8. CESION

Los DP solo pueden ser cedidos para cumplir con el interés legítimo del cedente y cesionario con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario

Excepción consentimiento: cesión entre dependencias de órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias

PRINCIPIOS GENERALES

9. TRANSFERENCIA INTERNACIONAL

Prohibido transferencia de DP hacia organismos que no presenten niveles de protección adecuados

Excepto colaboración judicial (PLA) internacional o transferencias bancarias o bursátiles

PRINCIPIOS GENERALES

SEGURIDAD DE LOS DATOS - Artículo N° 9

1. Responsable o usuario de BD debe adoptar medidas técnicas y organizativas para garantizar seguridad y confidencialidad de los datos personales, evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones.

2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

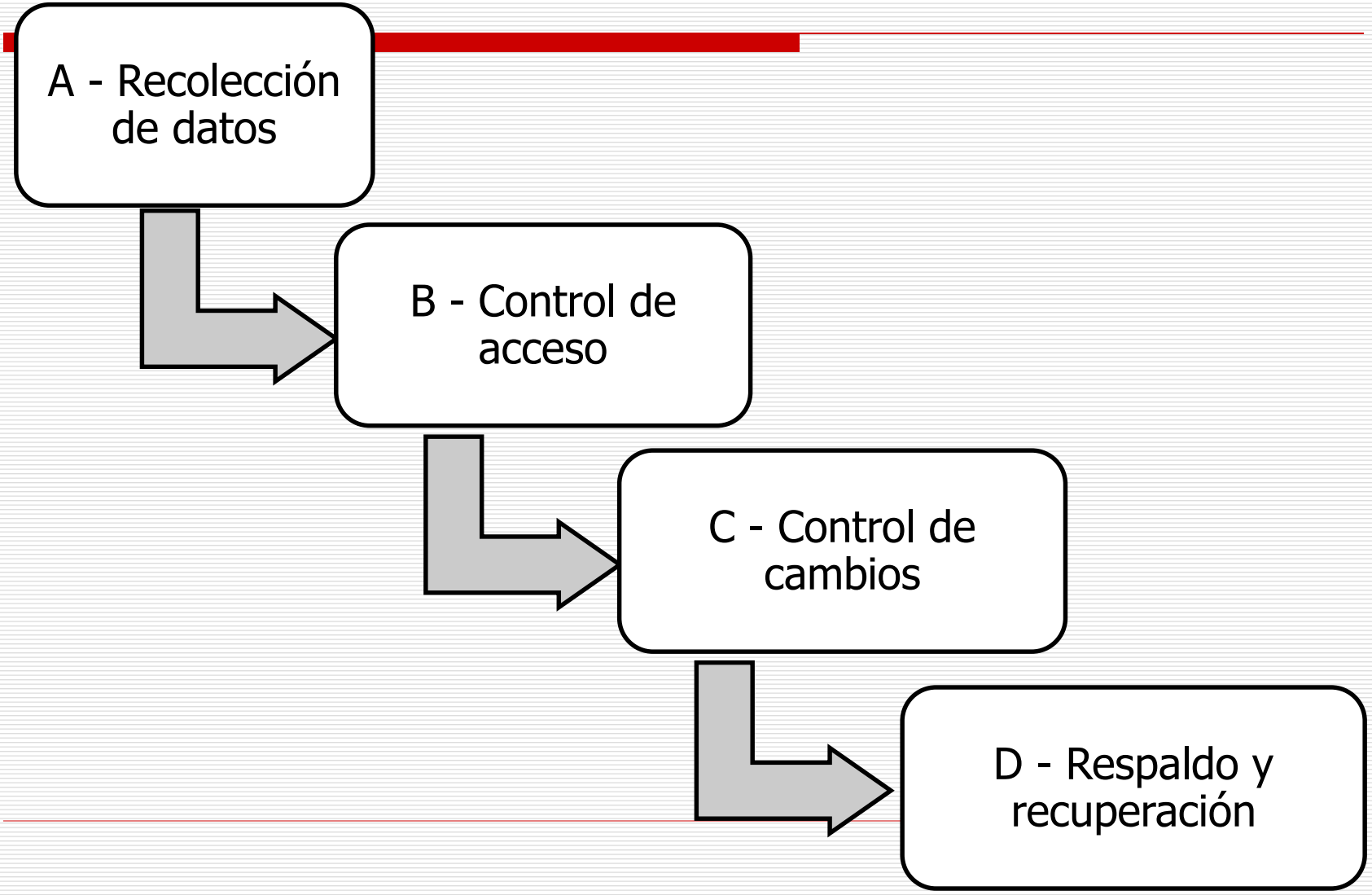
SEGURIDAD Resolución 47/2018

MEDIDAS DE SEGURIDAD RECOMENDADAS PARA EL TRATAMIENTO Y CONSERVACION DE LOS DATOS PERSONALES EN MEDIOS INFORMATIZADOS

MEDIDAS DE SEGURIDAD RECOMENDADAS PARA EL TRATAMIENTO Y CONSERVACION DE LOS DATOS PERSONALES EN MEDIOS NO INFORMATIZADOS

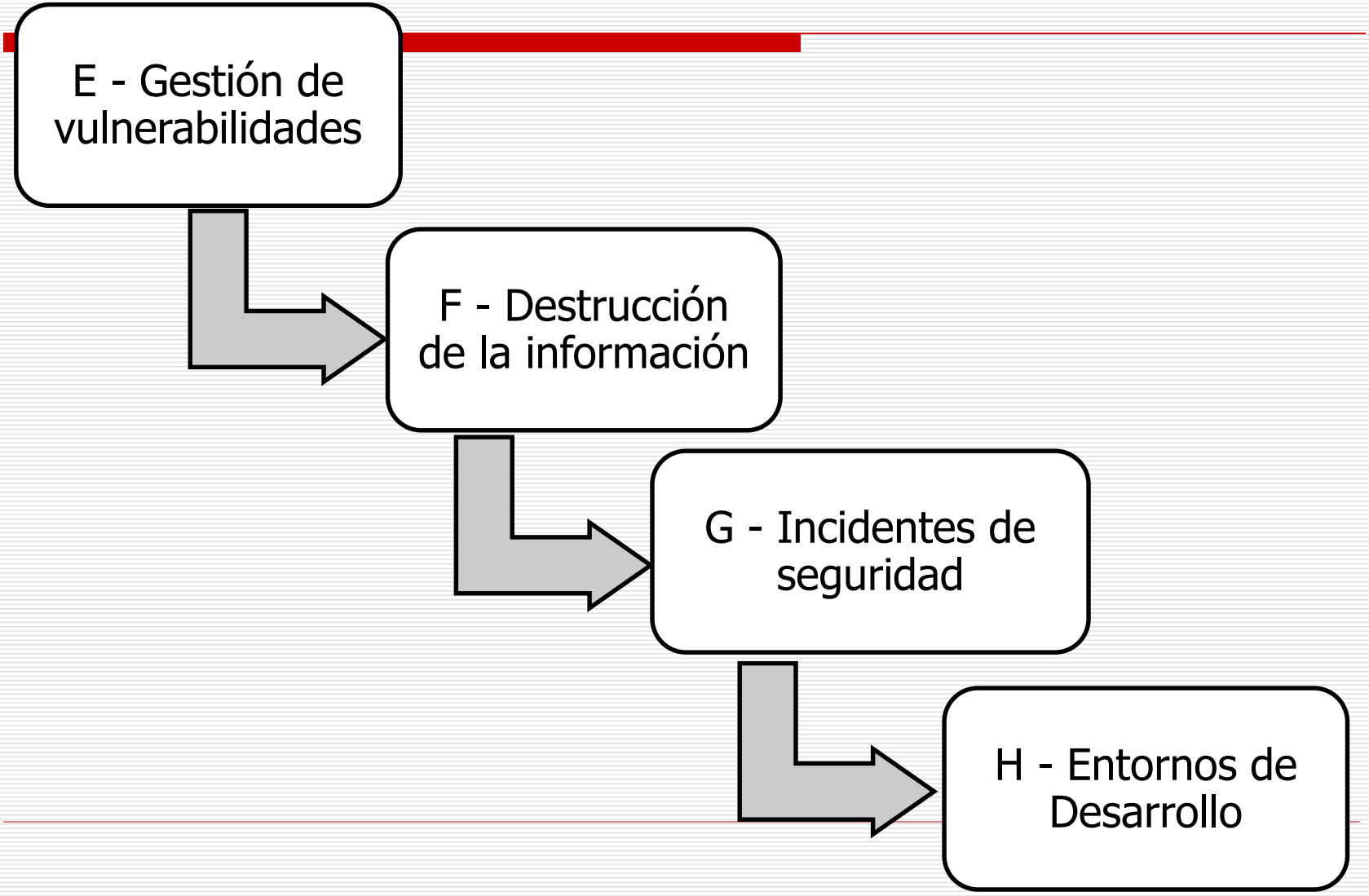
SEGURIDAD

MEDIDAS DE SEGURIDAD MEDIOS INFORMATICOS



SEGURIDAD

MEDIDAS DE SEGURIDAD MEDIOS INFORMATICOS



SEGURIDAD

MEDIDAS DE SEGURIDAD MEDIOS INFORMATICOS

A - RECOLECCIÓN DE DATOS

A.1. INTEGRIDAD

A.1.1. ASEGURAR COMPLETITUD

A.1.2. MINIMIZAR ERRORES DE INGRESO

A.2. CONFIDENCIALIDAD

A.2.1. ASEGURAR CONFIDENCIALIDAD DURANTE RECOLECCION

A.2.2. LIMITAR ACCESO A RECOLECCION DATOS

A.2.3. LIMITAR ACCESO NO AUTORIZADO DURANTE RECOPILACION

SEGURIDAD

MEDIDAS DE SEGURIDAD MEDIOS INFORMATICOS

B - CONTROL DE ACCESO

B.1. IDENTIFICACION DE ACTIVOS

B.1.1. IDENTIFICAR ACTIVOS

B.1.2. DEFINIR RESPONSABLES Y RESPONSABILIDADES

B.1.3. VERIFICAR APLICACIÓN DE CONTROLES

B.2. ACCESO A LOS DATOS

B.2.1. GESTIONAR ACCESOS A SISTEMAS

B.2.2. ASIGNAR PERMISOS

B.2.3. VERIFICAR IDENTIFICACION Y AUTORIZACION

B.2.4. CONTROLAR ACCESO FISICO AL CENTRO DE DATOS

B.2.5. MONITOREAR ACTIVIDADES

SEGURIDAD

MEDIDAS DE SEGURIDAD MEDIOS INFORMATICOS

C - CONTROL DE CAMBIOS

C.1. CONTROL DE CAMBIOS

C.1.1. ASEGURAR LOS CAMBIOS

D - RESPALDO Y RECUPERACIÓN

D.1. COPIAS DE RESPALDO Y PROCESO DE RECUPERACION

D.1.1. ASEGURAR PROCESO FORMAL DE RESPALDO Y RECUPERACION

D.1.2. ASEGURAR CONTROL DE ACCESO EN LOS MEDIOS

SEGURIDAD

MEDIDAS DE SEGURIDAD MEDIOS INFORMATICOS

E - GESTIÓN DE VULNERABILIDADES

E.1. GESTION DE VULNERABILIDADES

E.1.1. PREVENIR INCIDENTES DE SEGURIDAD DESDE EL DISEÑO

E.1.2. ASEGURAR PROTECCION ADECUADA

E.1.3. DETECTAR POSIBLES INCIDENTES DE SEGURIDAD

E.1.4. GARANTIZAR MEDIDAS EFICACES Y PERDURABLES

SEGURIDAD

MEDIDAS DE SEGURIDAD MEDIOS INFORMATICOS

F - DESTRUCCIÓN DE LA INFORMACIÓN

F.1. ASEGURAR DESTRUCCION INFORMACION

F.1.1. ESTABLECER FORMATO/MODELO DE DESTRUCCION

F.1.2. ESTABLECER MECANISMOS SEGUROS DE ELIMINACION

F.1.3. DESIGNAR RESPONSABLE DE DESTRUCCION

F.1.4. MONITOREAR PROCESO

SEGURIDAD

MEDIDAS DE SEGURIDAD MEDIOS INFORMATICOS

G - INCIDENTES DE SEGURIDAD

G.1. NOTIFICACION ANTE INCIDENTES DE SEGURIDAD

G.1.1. ESTABLECER RESPONSABILIDADES Y PROCEDIMIENTOS

G.1.2. ELABORAR INFORMES

G.1.3. ENVIAR NOTIFICACION

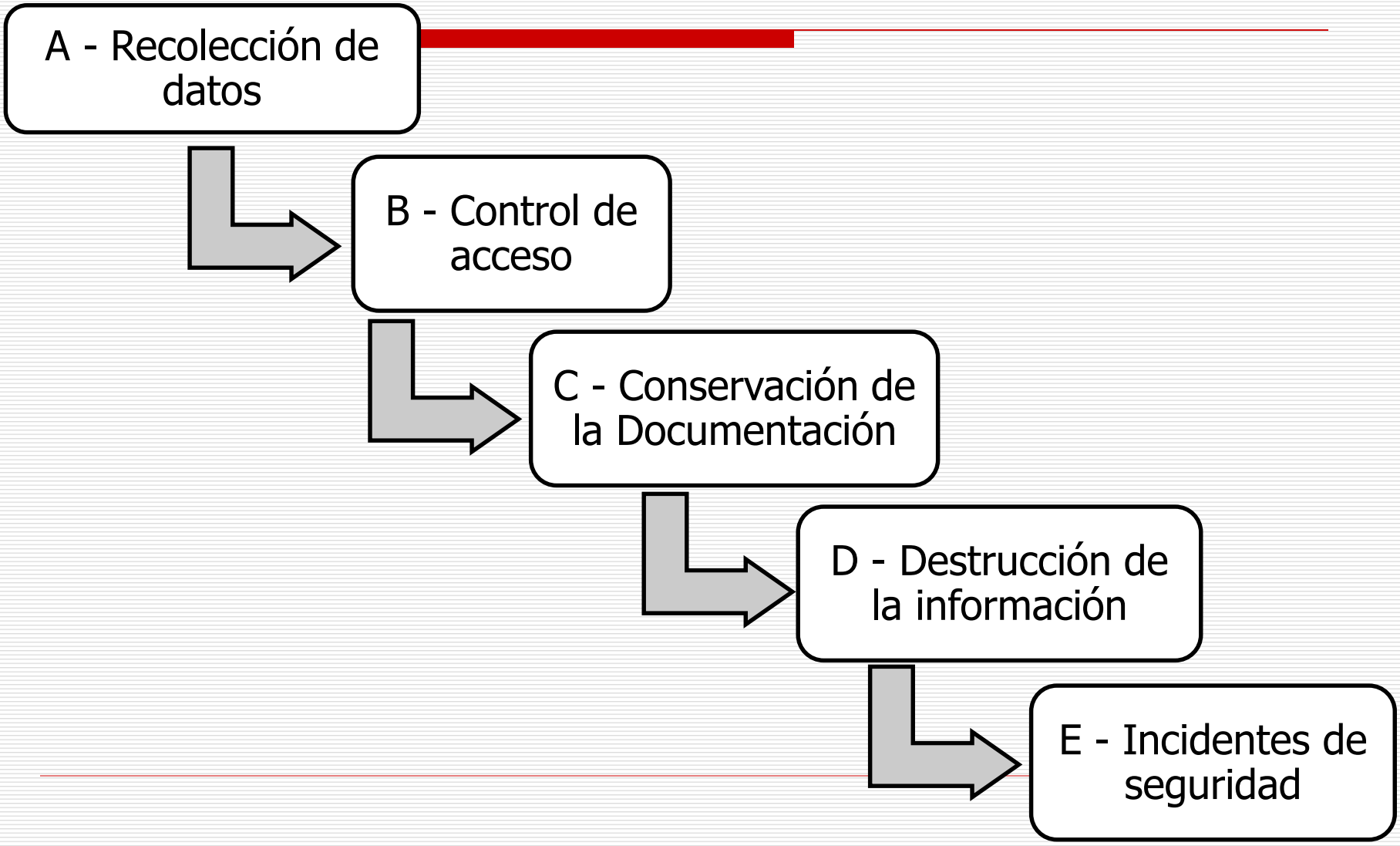
H - ENTORNOS DE DESARROLLO

H.1. SEGURIDAD EN ENTORNO DE DESARROLLO

H.1.1. IMPLEMENTAR POLITICA DE DESARROLLO SEGURO

SEGURIDAD

MEDIDAS DE SEGURIDAD MEDIOS NO INFORMATICOS



SEGURIDAD

MEDIDAS DE SEGURIDAD MEDIOS NO INFORMATICOS

A - RECOLECCIÓN DE DATOS

A.1. INTEGRIDAD

A.1.1. ASEGURAR COMPLETITUD

A.1.2. MINIMIZAR ERRORES DE INGRESO

SEGURIDAD

MEDIDAS DE SEGURIDAD MEDIOS NO INFORMATICOS

B - CONTROL DE ACCESO

B.1. IDENTIFICACION DE ACTIVOS

B.1.1. IDENTIFICAR ACTIVOS

B.1.2. DEFINIR RESPONSABLES Y RESPONSABILIDADES

B.1.3. VERIFICAR APLICACIÓN DE CONTROLES

B.2. ACCESO A LOS DATOS

B.2.1. GESTIONAR ACCESOS

B.2.2. ASIGNAR PERMISOS

B.2.3. VERIFICAR IDENTIFICACION Y AUTORIZACION

B.2..4. CONTROLAR ACCESO FISICO

B.3. COPIA O REPRODUCCION

B.3.1. CONTROLAR COPIAS REPRODUUCCION

B.4. TRASLADO DOCUMENTACION

B.4.1. CONTROLAR TRASLADO

B.4.2. ASEGURAR ELIMINACION

SEGURIDAD

MEDIDAS DE SEGURIDAD MEDIOS NO INFORMATICOS

C. CONSERVACION DE LA INFORMACION
C.1. CONTROL CONDICIONES AMBIENTALES
C.1.1. CONDICIONES AMBIENTALES
C.2. CONTROL DE INCENDIOS E INUNDACIONES
C.2.1. INCENDIOS E INUNDACIONES

D - DESTRUCCIÓN DE LA INFORMACIÓN
D.1. ASEGURAR DESTRUCCION INFORMACION
D.1.1. ESTABLECER FORMATO/MODELO DE DESTRUCCION
D.1.2. ESTABLECER MECANISMOS SEGUROS DE ELIMINACION
D.1.3. DESIGNAR RESPONSABLE DE DESTRUCCION
D.1.4. MONITOREAR PROCESO
D.1.5. DESCARTE DE ARCHIVOS

SEGURIDAD

MEDIDAS DE SEGURIDAD MEDIOS NO INFORMATICOS

E - INCIDENTES DE SEGURIDAD

E.1. NOTIFICACION ANTE INCIDENTES DE SEGURIDAD

E.1.1. ESTABLECER RESPONSABILIDADES Y PROCEDIMIENTOS

E.1.2. ELABORAR INFORMES

E.1.3. ENVIAR NOTIFICACION

INSPECCION Y CONTROL DNPDP

Disp. N° 5/2008

OBJETIVOS

- Mejorar gestión tratamiento datos personales
- Evaluar grado de cumplimiento ley 25.326.
- Recomendar mejor desempeño de responsables
- Verificar medidas técnicas y organizativas desarrolladas

INSPECCION Y CONTROL DNPDP

Disp. N° 5/2008

- CAPACITACION
- LEGALIDAD GESTION DATOS
- IDONEIDAD MEDIOS TRATAMIENTO DATOS
- CORRECTO TRATAMIENTO DATOS
- PUBLICIDAD
- ASESORIA LEGAL INFORMATICA

DERECHOS DE LOS TITULARES DE DATOS

1. DERECHO DE INFORMACION
2. DERECHO DE ACCESO
3. CONTENIDO DE LA INFORMACION
4. DERECHO DE RECTIFICACION, ACTUALIZACION O SUPRESION DE DATOS

DERECHOS DE LOS TITULARES DE DATOS

1. DERECHO DE INFORMACION

Al organismo de control referente a la existencia de bases de datos personales, finalidades y responsables

DERECHOS DE LOS TITULARES DE DATOS

2. DERECHO DE ACCESO

Para obtener información de datos personales incluidos en los bancos de datos públicos o privados

La información solicitada se debe proporcionar dentro de los DIEZ días corridos de la notificación. Si no se satisface el pedido, quedará expedita la acción de hábeas data.

DERECHOS DE LOS TITULARES DE DATOS

3. CONTENIDO DE LA INFORMACION

La información debe ser clara, amplia y completa.

DERECHOS DE LOS TITULARES DE DATOS

4. DERECHO DE RECTIFICACION, ACTUALIZACION O SUPRESION DE DATOS

El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales en el plazo máximo de CINCO días hábiles de recibido el reclamo

El incumplimiento de esta obligación dentro del término acordado habilitará a promover la acción de hábeas data.

REGISTRO NACIONAL DOCUMENTOS CUESTIONADOS

Creado por Disposición DNPDP N° 24/2010

Objetivo: mantener actualizado un registro informatizado de documentos de identidad denunciados por autoridades públicas competentes y/o sus titulares con motivo de pérdida, hurto, robo o cualquier otra alteración

REGISTRO NACIONAL NO LLAME

Creado por Ley 26.951

Objetivo: concentrar en un solo ámbito números telefónicos de titulares que decidan no ser contactados por las empresas que publiciten, oferten, vendan o regalen bienes o servicios mediante servicios de telefonía (cualquiera sea su modalidad), tales como telefonía básica, móvil, servicios de radiocomunicación móvil celular, comunicaciones móviles, SMS por IP, voz por IP, y cualquier otro servicio similar que la tecnología permita en el futuro.

ACCION DE HABEAS DATA

Quiénes pueden ejercerla?

Titular de datos

Sobre quiénes?

Responsables y Usuarios

PROCEDENCIA

Para qué?

Conocer datos personales almacenados en BD y su finalidad

En caso de inexactitud, falsedad, desactualización, exigir su rectificación, supresión o actualización

Caso de Estudio

Un cliente rescinde contrato de servicio de internet, la empresa asignó a un tercero homónimo la misma dirección de correo electrónico.

Analizar licitud del tratamiento de este dato y alcance de la Ley Nº 25.326

Caso de Estudio
Conclusión DNPDP

Finalizado el servicio el Denunciante dejó de ser el titular del correo electrónico, por lo que no cabe hacer lugar a la denuncia sustentada en la falta de su consentimiento para dicho tratamiento. Denunciada se le requiere política tratamiento de datos

Conclusiones

- ✓ Ley 25.326 es norma de orden público y alcance nacional.
- ✓ Responsables y usuarios tienen responsabilidad sobre tratamiento y gestión que realicen en los datos.
- ✓ Requiere adoptar medidas de seguridad, con condiciones técnicas de integridad y seguridad en los archivos de datos personales que se gestionen.
- ✓ Requiere observar y hacer observar a los miembros de la organización como a terceros con acceso a los datos el cumplimiento de las normas vigentes.
- ✓ Inspección incluye: tratamiento y gestión de datos personales, capacitación al personal, aspectos legales, acuerdos de confidencialidad, medidas implementadas de seguridad informática, documentación de sistemas y revisiones de auditoría.

Fin de la presentación

Muchas Gracias!!