Ingeniería de Sistemas

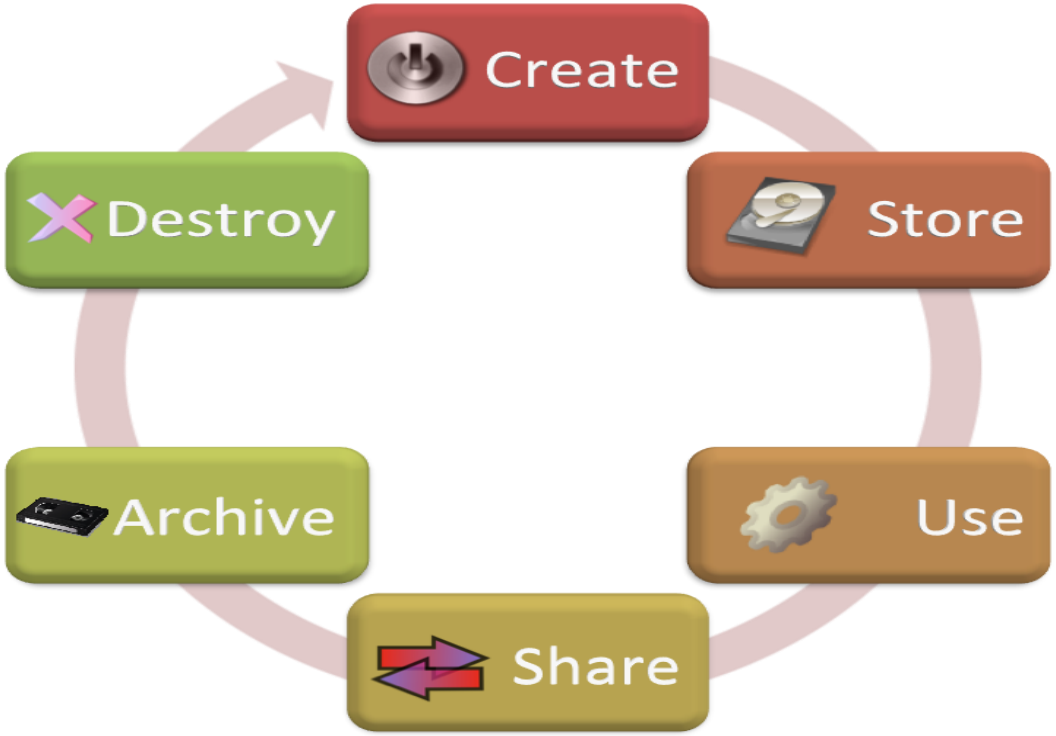
Protección de datos personales

Seguridad de Sistemas de TI

2022-1

UNIVERSIDAD DE LIMA

El Ciclo de vida de la seguridad de los datos



El ciclo de vida incluye seis fases, desde la creación a la destrucción. Aunque se muestra como una progresión secuencial, una vez creados, los datos pueden moverse entre fases sin restricciones, y puede que no pasen por todas las etapas (por ejemplo, no todos los datos son finalmente destruidos).

Referencia: http://www.securosis.com/blog/data-security-lifecycle-2.0

El Ciclo de vida de la seguridad de los datos

- **Creación**: es la generación de nuevo contenido digital, o la alteración, actualización o modificación de contenido existente.
- **Almacenamiento**: es el acto de ubicar los datos digitales en algún tipo de repositorio de almacenamiento y normalmente ocurre de forma prácticamente simultánea a su creación.
- **Uso**. los datos son visualizados, procesados, o utilizados de otro modo en algún tipo de actividad, no incluyendo su modificación.
- **Compartición**: la información se hace accesible a otros, tales como otros usuarios, clientes, y colaboradores.
- **Archivo**: los datos dejan de ser usados activamente y entran en un almacenamiento de largo plazo.
- **Destrucción**: los datos son destruidos de forma permanente usando medios físicos o digitales (por ejemplo, *crypto shredding).*

UNIVERSIDAD DE LIMA

Protección de datos personales

- **¿Qué son los datos personales?**

  Los **datos personales** son cualquier información que permite identificar a una persona. El nombre, los apellidos, la fecha de nacimiento, la dirección del domicilio, la dirección de correo electrónico, el número de teléfono, el número de RUC, el número de la placa del vehículo, la huella digital, el ADN, una imagen, el número del seguro social, etc. son datos que identifican a una persona, ya sea directa o indirectamente.

UNIVERSIDAD DE LIMA

Datos sensibles

- Dentro de los datos personales hay una categoría denominada "*datos sensibles*" que están constituidos por:
  - Los datos biométricos que por sí mismos pueden identificar a la persona, como la huella digital, la retina, el iris
  - Datos referidos al origen racial y étnico
  - Ingresos económicos
  - Opiniones o convicciones políticas, religiosas filosóficas o morales
  - la afiliación sindical;
  - Información relacionada a la salud
  - Etc.

Estos datos requieren de especial protección y solamente pueden ser objeto de tratamiento con el consentimiento **expreso y por escrito** del titular de los datos.

Gracias a la Constitución y a las Leyes de protección de datos personales tienes derecho a:

- Conocer, antes de entregar tus datos personales, cómo serán tratados mediante un aviso de privacidad.
- Tus datos sean tratados sólo para la finalidad que te informaron en el aviso de privacidad;
- Cuiden y protejan tus datos personales para que estén seguros
- Guardar la confidencialidad de tus datos…

Protección de datos personales

- **A**cceder a sus datos personales que estén en posesión de empresas o del gobierno;
- **R**ectificar sus datos cuando sean erróneos;
- **C**ancelar los datos que ya no son necesarios;
- **O**ponerse a que sus datos se traten para usos específicos, como mandarte publicidad.

Gracias a la constitución, Ley de PDP Nº 29733 , y su reglamento DS-003-2013-JUS , LOS CIUDADANOS PUEDEN

Principios que deben regir el uso de los datos personales

Legalidad

El tratamiento de los datos personales se hace conforme a lo establecido en la LPDP. Se prohíbe la recopilación de los datos personales por medios ilícitos.

Consentimiento o Autorización

Para realizar el tratamiento de los datos personales se debe contar con el consentimiento o la autorización de la persona, titular de los datos personales.

Finalidad

Los datos personales no deben ser tratados para una finalidad distinta a la establecida al momento de su recopilación.

Proporcionalidad

Todo tratamiento de datos personales debe ser apropiado a la finalidad para la que éstos hubiesen sido recopilados, usando la información que sea imprescindible y suficiente, sin excesos.

Calidad

Los datos personales que se tratan deben ser veraces, exactos y adecuados.

Seguridad

El titular del banco de datos personales y el encargado del tratamiento deben adoptar las medidas necesarias para garantizar la seguridad y confidencialidad de los datos personales que administran.

Directiva de Seguridad para el tratamiento de los DP

La Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales, aprobada por Resolución Directoral Nº019-2013-JUS/DGPDP, de la **Autoridad Nacional de Protección de Datos Personales**, órgano especializado del Ministerio de Justicia y Derechos Humanos, es un instrumento que posibilita un accionar ajustado a derecho de aquellas personas, sean naturales o jurídicas, que realizan tratamiento de datos personales y es que, como la propia Directiva lo señala, ésta orienta sobre las condiciones, requisitos y las medidas técnicas que deben tomar en cuenta para el cumplimiento de la ley.

Ministerio de Justicia y Derechos Humanos

UNIVERSIDAD DE LIMA

OE1: Brindar lineamientos para determinar las condiciones de seguridad en el tratamiento de datos personales a cumplir por el titular del banco de datos personales.

RESPONSABILIDAD

Titular de datos personales

Titular del banco de datos personales

Autoridad Nacional de Protección de Datos Personales

MEDIDAS DE SEGURIDAD

Para efectos de la presente directiva, se debe considerar la siguiente clasificación de categorías en el tratamiento de datos personales y el principio de proporcionalidad

Básico	Simple	Intermedio	Complejo	Crítico

UNIVERSIDAD DE LIMA

Criterios que permiten categorizar los bancos de datos:

Figura 1: Volumen de datos / Número de datos

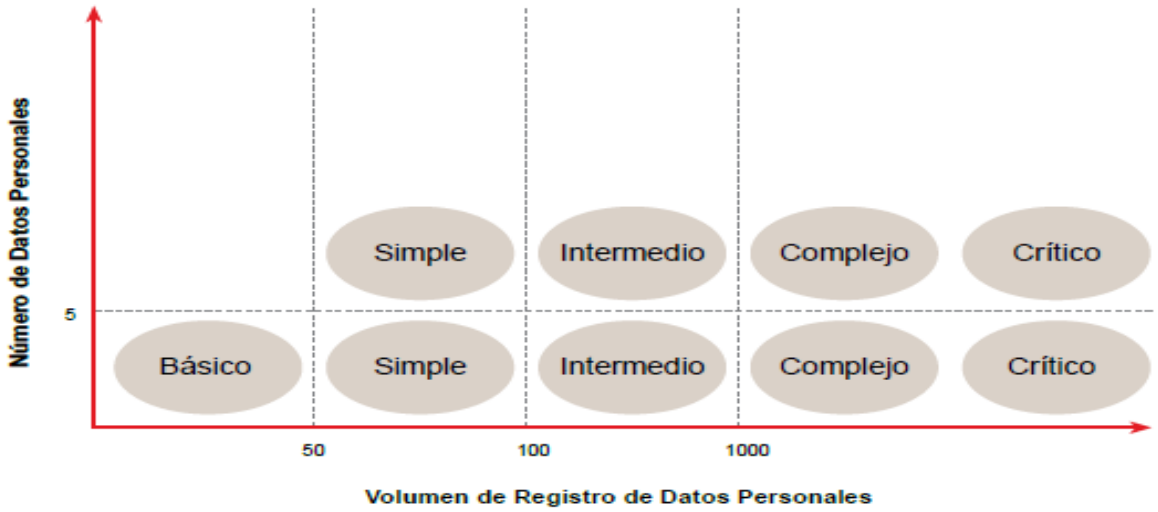
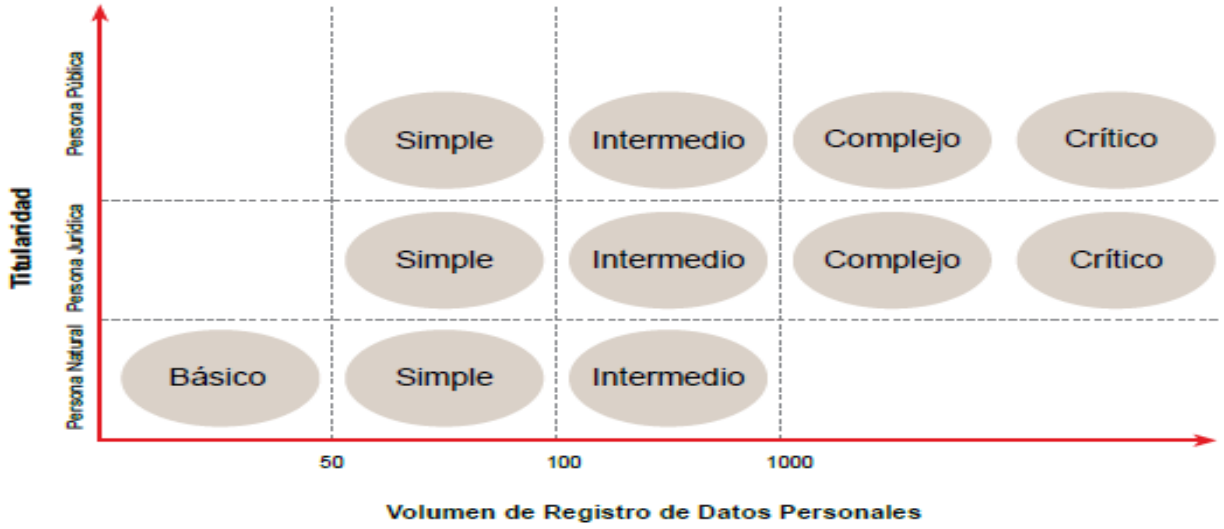


Figura 3: Volumen de registros / Titularidad del banco de datos personales



DE LIMA

2.3.1.3: Proteger el banco de datos personales contra acceso físico no autorizado mediante algún mecanismo de bloqueo físico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados (en caso de banco de datos personales no autorizado).

APLICA A LA CATEGORÍA DE TRATAMIENTO:				
BÁSICO	SIMPLE	INTERMEDIO	COMPLEJO	CRÍTICO
Ubicar el banco de datos personales en un gabinete, caja, cajón de un mueble, gaveta o similar siempre y cuando tenga una cerradura con llave o similar, la cual será responsabilidad del operador del banco de datos personales.	Ubicar el banco de datos personales en un gabinete, caja, cajón de un mobiliario, gaveta o similar siempre y cuando tenga una cerradura con llave o similar, la cual será responsabilidad del operador del banco de datos personales.	Cuando se contengan datos sensibles, ubicar el banco de datos personales en un ambiente aislado protegido por cerradura o similar mecanismo, donde la responsabilidad del mecanismo de acceso recae en el titular del banco de datos personales o un responsable delegado por el titular del banco de datos personales.	Cuando se contengan datos sensibles, ubicar el banco de datos personales en un ambiente aislado protegido por cerradura o similar mecanismo, donde la responsabilidad del mecanismo de acceso recae en el titular del banco de datos personales o un responsable delegado por el titular del banco de datos personales.	Cuando se contengan datos sensibles, ubicar el banco de datos personales en un ambiente aislado protegido por cerradura o similar mecanismo, donde la responsabilidad del mecanismo de acceso recae en el titular del banco de datos personales o un responsable delegado por el titular del banco de datos personales.

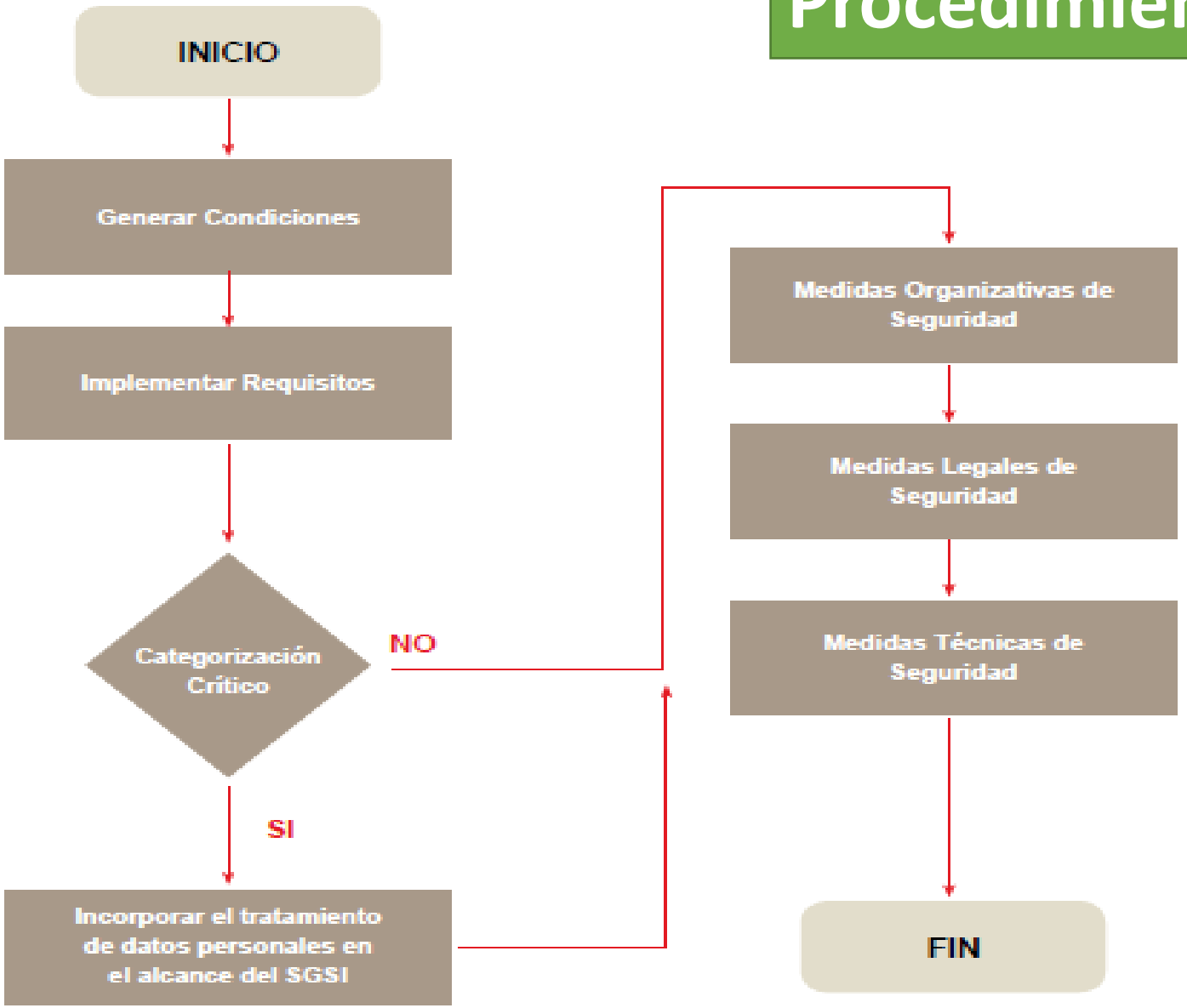
2.3.1.4 Cuando se utilicen mecanismos informáticos para el tratamiento de datos personales se debe proteger el banco de datos personales contra acceso lógico no autorizado mediante algún mecanismo de bloqueo lógico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados.

APLICA A LA CATEGORÍA DE TRATAMIENTO:				
BÁSICO	**SIMPLE**	**INTERMEDIO**	**COMPLEJO**	**CRÍTICO**
Cada usuario con acceso a los datos personales o al banco de datos personales debe estar claramente identificado y utilizar como mínimo una validación de acceso mediante el uso de usuario/ contraseña independiente para cada persona que tenga acceso.	Cada usuario con acceso a los datos personales o al banco de datos personales debe estar claramente identificado y utilizar como mínimo una validación de acceso mediante el uso de usuario/ contraseña independiente para cada persona que tenga acceso.	Los usuarios deben tener un identificador único de acceso asociado a perfiles de usuarios y los accesos autorizados para cada uno de ellos. Asimismo, se debe contar con mecanismos de restricción para evitar el acceso a recursos no autorizados. La autenticación de usuarios puede estar basada en contraseñas o mecanismos de fuerte autenticación como el uso de toquen, dispositivos biométricos, firmas digitales, tarjetas inteligentes, tarjetas de coordenadas, entre otros.	Los usuarios deben tener un identificador único de acceso asociado a perfiles de usuarios y los accesos autorizados para cada uno de ellos. Asimismo, se debe contar con mecanismos de restricción para evitar el acceso a recursos no autorizados.La autenticación de usuarios puede estar basada en contraseñas o mecanismos de fuerte autenticación como el uso de toquen, dispositivos biométricos, firmas digitales, tarjetas inteligentes, tarjetas de coordenadas, entre otros.	Los usuarios deben tener un identificador único de acceso asociado a perfiles de usuarios y los accesos autorizados para cada uno de ellos Asimismo, se debe contar con mecanismos de restricción para evitar el acceso a recursos no autorizados. La autenticación de usuarios puede estar basada en contraseñas o mecanismos de fuerte autenticación como el uso de toquen, dispositivos biométricos, firmas digitales, tarjetas inteligentes, tarjetas de coordenadas, entre otros.

Medidas Específicas

		APLICA A LA CATEGORÍA DE TRATAMIENTO:				
ÍTEM	CRITERIO	BÁSICO	SIMPLE	INTERMEDIO	COMPLEJO	CRÍTICO
2.3.4.3	Los equipos utilizados para el tratamiento de los datos personales deben recibir mantenimiento preventivo y correctivo de acuerdo a las recomendaciones y especificaciones del proveedor para asegurar su disponibilidad e integridad. El mantenimiento de los equipos debe ser realizado por personal autorizado.	Opcional	Opcional	Requerido	Requerido	Requerido
2.3.4.4	Los equipos utilizados para el tratamiento de los datos personales deben contar con software de protección contra software malicioso (virus, troyanos, spyware, etc.), para proteger la integridad de los datos personales. El software de protección debe ser actualizado frecuentemente de acuerdo a las recomendaciones y especificaciones del proveedor.	Opcional	Opcional	Requerido	Requerido	Requerido
2.3.4.5	Toda información electrónica que contiene datos personales debe ser almacenada en forma segura empleando mecanismos de control de acceso y cifrada para preservar su confidencialidad.	Opcional	Opcional	Requerido	Requerido	Requerido
2.3.4.6	La información de datos personales que se transmite electrónicamente debe ser protegida para preservar su confidencialidad e integridad.	Opcional	Implementar ítem 2.3.5.3	Implementar ítem 2.3.5.3	Implementar ítem 2.3.5.3	Implementar ítem 2.3.5.3
2.3.4.7	Seguridad en el flujo transfronterizo de datos personales.	No aplica	Implementar ítem 2.3.5.4	Implementar ítem 2.3.5.4	Implementar ítem 2.3.5.4	Implementar ítem 2.3.5.4
2.3.4.8	Seguridad en servicios de tratamiento de datos personales por medios tecnológicos tercerizados.	No aplica	Implementar ítem 2.3.5.5	Implementar ítem 2.3.5.5	Implementar ítem 2.3.5.5	Implementar ítem 2.3.5.5
2.3.4.9	Todo evento identificado que afecte la confidencialidad, integridad y disponibilidad de los datos personales, o que indique un posible incumplimiento de las medidas de seguridad establecidas, debe ser reportado inmediatamente al encargado del banco de datos personales.	Registrar el incidente con una descripción detallada del mismo y las medidas correctivas adoptadas (pueden estar registradas en el cuaderno de seguridad citado en el anexo B).	Implementar ítem 2.3.5.7	Implementar ítem 2.3.5.7	Implementar ítem 2.3.5.7	Implementar ítem 2.3.5.7
2.3.4.10	Restringir el uso de equipos de fotografía, video, audio u otra forma de registro en el área de tratamiento de datos personales salvo autorización del titular del banco de datos personales.	Opcional	Requerido	Requerido	Requerido	Requerido
2.3.4.11	Se debe realizar una auditoría sobre el cumplimiento de la presente directiva, bajo responsabilidad del titular del banco de datos personales.	Opcional	Opcional	Verificar de manera interna la existencia de los requisitos y registros aplicables	Se debe realizar una auditoría externa para la verificación del cumplimiento de la presente directiva, a fin de asegurar imparcialidad en los resultados.	Se debe realizar una auditoría externa para la verificación del cumplimiento de la presente directiva, a fin de asegurar imparcialidad en los resultados.
2.3.4.12	Acciones correctivas y mejora continúa.	Opcional	Opcional	Los resultados de la auditoría deben iniciar la implementación de acciones correctivas.	Los resultados de la auditoría deben iniciar la implementación de acciones correctivas.	Los resultados de la auditoría deben iniciar la implementación de acciones correctivas.

Procedimiento



UNIVERSIDAD DE LIMA

Referencias

https://www.minjus.gob.pe/material-informativo-dp/

http://www.securosis.com/blog/data-security-lifecycle-2.0

Directiva de Seguridad - Autoridad Nacional de Protección de Datos Personales APDP (2013)

Guías de seguridad de áreas críticas en cloud computing v3.0 – CSA ©2011 cloud security alliance

El Derecho Fundamental a la Protección de Datos Personales, Guía para el ciudadano, octubre 2013

Ley de Protección de Datos Personales LEY Nº 29733 (Julio 2011)

Reglamento de Ley N° 29733 , DS-003-2013 (marzo 2013)

UNIVERSIDAD DE LIMA