I.- PRESENTACION

La Autoridad Nacional de Protección de Datos Personales -APDP- del Ministerio de Justicia y Derechos Humanos, de conformidad con lo dispuesto por la segunda disposición complementaria final de la Ley N° 27933, ha tenido a su cargo la elaboración de una directiva de seguridad para poner al servicio de todos los titulares de bancos de datos personales un instrumento que facilite el cumplimiento de la Ley. Esa es la finalidad central de este documento y es por ello que no hemos querido hacer un documento con términos generales o lugares comunes que hubiera significado cumplir con esta obligación "formalmente" pero sin aportar nada concreto.

Consideramos que eso hubiera ocurrido si hubiéramos entregado una directiva limitada a la enumeración de obligaciones (que ya están en la ley) o si hubiéramos desarrollado criterios o disposiciones de modo previo a la vigencia del reglamento de la ley, con el riesgo de que el reglamento resultara con un contenido que dejara descolada a la directiva. No podíamos pues, poner la carreta delante de los caballos. Teniendo la ley y su reglamento vigentes plenamente, ya tenía sentido culminar esta directiva y así lo hemos hecho, lo más pronto que ha sido posible.

Para evitar que este documento sea repetitivo respecto de la ley o el reglamento y, por el contrario, constituya una herramienta útil de trabajo para quien requiera consultarla, ha sido necesario replicar las preguntas, las dudas, las necesidades y las circunstancias que pueden acompañar a los concernidos por la ley, para encontrarles respuestas y soluciones. Para ello ha sido preciso "cruzar" los criterios que pueden describir y caracterizar los bancos o tratamientos de datos, como son: el tipo de datos (generales o sensibles), el numero de datos de cada persona, el número de personas y el tiempo previsto o previsible de uso de la información, entre otros.

Este cruce, ordenado y sistematizado de criterios, permite ubicar las características de cada banco de datos, lo cual constituye el paso previo para relacionarlo con las medidas de seguridad indicadas o sugeridas como una suerte de "diseño a la medida" porque entendemos que lo que el administrado requiere es justamente pasar del texto general de la norma a un plan de adecuación para su caso concreto. Esperamos que esta directiva cumpla ese simple pero trascendental papel a favor de los administrados.

Para terminar quisiera dejar constancia de dos cosas:

Primero: Esta es una directiva, es decir una indicación de cómo pueden hacerse las cosas, un documento facilitador. Si los administrados encuentran que pueden cumplir las normas de seguridad con criterios o protocolos distintos pero igualmente eficientes deben recordar que su obligación es adecuarse a la ley y el reglamento no a la directiva, que es solo un documento facilitador.

Segundo: Este documento estará en permanente revisión, justamente porque debe considerarse un documento de trabajo, cuyo valor estará siempre dado por su utilidad.

José Alvaro Quiroga León

Director de la Autoridad Nacional de Protección de Datos Personales.

AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES

DIRECTIVA DE SEGURIDAD DE LA INFORMACIÓN

LEY N° 29733 - LEY DE PROTECCIÓN DE DATOS PERSONALES

INDICE

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS
DIRECCIÓN GENERAL DE PROTECCIÓN DE DATOS PERSONALES
J. A. Quiroga L.

V°B°
V. Sánchez

I. ESTRUCTURA

La presente directiva orienta sobre las condiciones, los requisitos, y las medidas técnicas que se deben tomar en cuenta para el cumplimiento de la Ley Nº 29733, Ley de Protección de Datos Personales y su reglamento, aprobado a través del Decreto Supremo Nº 003-2013-JUS, en materia de medidas de seguridad de los bancos de datos personales.

Las condiciones constituyen recomendaciones que facilitan o generan impacto favorable para la implementación de los requisitos, habilitando un entorno apropiado para la comprensión y desarrollo de las actividades necesarias.

Los requisitos corresponden a condiciones que deben ser demostrables, para considerar que se ha cumplido la presente directiva.

Las medidas técnicas son aquellas que se consideran coherentes para cumplir con los requisitos.

Tanto los requisitos como las medidas a implementar pueden ser variables y por ello están segmentadas atendiendo a criterios, como –por ejemplo- el tipo de tratamiento.

Así tenemos que, se asigna un color para facilitar la identificación en los cuadros mostrados:

Básico	
Simple	
Intermedio	
Complejo	
Crítico	

La categorización se describe en el apartado 1.1.

El numeral 3 describe de manera general el procedimiento para desarrollar la presente directiva.

El numeral 4 incluye disposiciones complementarias que pueden facilitar el proceso de implementación de la presente directiva y con ello el cumplimiento de la Ley Nº 29733, Ley de Protección de Datos Personales, y su reglamento.

Finalmente se presentan tres anexos de apoyo:
Anexo A: Glosario de términos aplicables en la lectura de la presente directiva.
Anexo B: Orientación para bancos de datos personales de tipo *básico* o *simple.*
Anexo C: Orientación para bancos de datos personales de tipo *complejo* o *crítico.*

II. OBJETIVO

a) Objetivo General:

Garantizar la seguridad de los datos personales contenidos o destinados a ser contenidos en bancos de datos personales, mediante medidas de seguridad que protejan a los bancos de datos personales, de conformidad con la Ley Nº 29733 y su reglamento.

b) Objetivos Específicos:

a. Brindar lineamientos para determinar las condiciones de seguridad en el tratamiento de datos personales a cumplir por el titular del banco de datos personales.
b. Brindar lineamientos para determinar las medidas organizativas a cumplir por el titular del banco de datos personales.
c. Brindar lineamientos para determinar las medidas legales a cumplir por el titular del banco de datos personales.
d. Brindar lineamientos para determinar medidas técnicas a cumplir por el titular del banco de datos personales.
e. Brindar lineamientos para determinar las medidas de seguridad que resulten apropiadas, en función a las características de cada caso concreto, a partir de considerar criterios de diferenciación basados en las características del tratamiento de datos personales que se vaya a efectuar y en las características de datos personales que se tratan.

III. BASE LEGAL

a) Constitución Política del Perú.
b) Ley N° 29733, Ley de Protección de Datos Personales.
c) Decreto Supremo 003-2013-JUS, aprueba el Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales.
d) Decreto Supremo 011-2012-JUS, aprueba el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos
e) Resolución Ministerial Nº 246-2007-PCM, aprueba la Norma Técnica Peruana "NTP ISO/IEC 17799:2007 EDI, Técnicas de seguridad, Código de Buenas Prácticas para la gestión de seguridad de la información. 2a Edición"
f) Resolución Ministerial 129-2012-PCM, aprueba el uso obligatorio de la norma técnica peruana "NTP-ISO/IEC 27001:2008 EDI Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información en todas las entidades integrantes del Sistema Nacional de Informática".

J. A. Quiroga L.

IV. ALCANCE

La presente directiva es aplicable a los bancos de datos personales de administración pública o privada de acuerdo a lo establecido en la Ley N° 29733 y su reglamento.

V. RESPONSABILIDAD

En el marco de la presente directiva, se tiene en cuenta la atribución de responsabilidades, desde el origen hasta la disposición de los datos personales, que

V. Sánchez

debe tomarse en cuenta para mantener la coherencia y la concordancia de la actuación de quienes participan en la protección de los datos personales con los objetivos y medidas de seguridad a implementar.

a) Titular de datos personales

Es responsable de sus propios datos personales, debe tomar en cuenta que su consentimiento para el tratamiento de sus datos personales debe ser libre, previo e informado y verificar que su consentimiento sea registrado en los términos en que expresa e inequívocamente lo ha dado. Es responsable de conocer y ejercer los derechos conferidos por la Ley N° 29733, Ley de Protección de Datos Personales.

b) Titular del banco de datos personales

a. Es responsable de otorgar y mantener el nivel suficiente de protección a los datos personales contenidos en el banco de datos personales que tenga bajo su titularidad.
b. Es responsable por la determinación y cumplimiento de la finalidad y del contenido del banco de datos personales bajo su titularidad.
c. Es responsable por el tratamiento de los datos personales contenidos en el banco de datos personales bajo su titularidad.
d. Es responsable de garantizar el cumplimiento de los derechos del titular de los datos personales conferidos en la Ley N° 29733, Ley de Protección de Datos Personales.

c) Autoridad Nacional de Protección de Datos Personales

a. Es responsable de realizar todas las acciones necesarias para el cumplimiento de la Ley N° 29733, Ley de Protección de Datos Personales, y su reglamento.
b. Es responsable de ejercer las funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras señaladas en la Ley N° 29733, Ley de Protección de Datos Personales, y su reglamento.
c. Es responsable de la administración del Registro Nacional de Protección de Datos Personales.
d. Es responsable del seguimiento y evaluación de la presente directiva.
e. Es responsable de la revisión de esta directiva de seguridad a fin de mantener su aplicabilidad e idoneidad. El periodo de revisión es, cuando menos, bianual.

J. A. Quiroga L

V°B°
V. Sánchez

MEDIDAS DE SEGURIDAD

1. DISPOSICIONES GENERALES

1.1 Categoría:

1.1.1 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 descrito en el artículo 7 de la Ley N° 29733 cuando no exista coincidencia exacta:

a) **Básico**, corresponde a la categoría de menor nivel e incluye a bancos de datos personales que:
- No contengan la información de más de cincuenta (50) personas.
- Número de datos personales no mayor a cinco (05). Por ejemplo nombres, apellidos, DNI, dirección y teléfono.
- No incluyen datos sensibles.
- Tienen como titular a una persona natural.

b) **Simple**, corresponde a bancos de datos personales que:
- No contengan la información de más de cien (100) personas.
- El periodo de tiempo del tratamiento para cumplir con la finalidad es inferior a un (01) año.
- No incluyen datos sensibles.
- Tiene como titular a una persona natural o jurídica.

c) **Intermedio**, corresponde a bancos de datos personales que:
- Contienen la información de hasta mil (1000) personas.
- Sirven para tratamiento de datos personales cuya finalidad se cumple en un plazo indeterminado o superior a un (01) año.
- Puede incluir datos sensibles.
- Tiene como titular a una persona natural o jurídica.

J. A. Quiroga L.

d) **Complejo**, corresponde a bancos de datos personales que:
- Sirven para el tratamiento de datos personales cuya finalidad se cumple en un plazo indeterminado o superior a un (01) año.
- Sirven para el tratamiento de datos personales que es realizado en múltiples localizaciones (Oficinas o dependencias diferentes en la misma ciudad o ciudades diferentes, servicios tercerizados o similares).
- Puede incluir datos sensibles.
- Tiene como titular a una persona jurídica o entidad pública.

e) **Crítico**, corresponde la categoría de mayor nivel e incluye a bancos de datos personales que:
- Sirven para el tratamiento de datos personales cuya finalidad está respaldada por una norma legal.
- Sirven para el tratamiento de datos cuya finalidad se cumple en un plazo indeterminado o superior a un (01) año.
- Sirven para el tratamiento de datos personales que es realizado en múltiples localizaciones (Oficinas o dependencias diferentes

V. S.

en la misma ciudad o ciudades diferentes, servicios tercerizados o similares)
- Puede incluir datos sensibles.
- Tiene como titular a una persona jurídica o entidad pública.

1.1.2 Justificación de los criterios

Los criterios que permiten categorizar los bancos de datos han sido determinados tomando en cuenta lo siguiente:

a) **Volumen de registros.-** Es importante considerar que existe una diferencia importante entre realizar el tratamiento manual de los datos personales de veinte (20) personas que de un millón, toda vez que se requiere mecanismos, procesos y herramientas diferentes.

El tratamiento de altos volúmenes de datos personales requiere, actualmente, el uso de tecnologías de la información. Lo cual, incorpora mejoras fundamentales en los tiempos de procesamiento, pero también incorpora un conjunto de vulnerabilidades asociadas a la tecnología utilizada, por lo que los niveles de protección deben ser adecuados y comúnmente son mayores a los de un tratamiento sin tecnologías de la información.

b) **Número de datos.-** El número de datos personales de cada titular de datos personales que se procesa es un criterio a considerar porque incluye un mayor nivel de detalle sobre el titular de los datos personales con o sin la inclusión de datos sensibles.

c) **Periodo de tiempo para la finalidad del tratamiento de datos personales.-** El tener un periodo de tiempo indeterminado o muy largo, para cumplir la finalidad del tratamiento, implica un aumento en el nivel de seguridad que debe observarse en el almacenamiento que se dé a los datos personales durante el periodo del tratamiento, así como en el nivel de impacto sobre el titular de los datos personales en caso de pérdida de la información, lo que puede conducir a la implementación de mecanismos de recuperación ante desastres o no.

J. A. Quiroga L.

d) **La titularidad del banco de datos personales.-** Proporciona un criterio de selección que principalmente separa los extremos de las categorías. Es decir, no se le puede asignar a una persona natural una categoría de altísimo nivel porque no dispone de los recursos necesarios, ni será necesario –como regla general- que implemente las medidas más complejas.

En el caso de las entidades públicas, se cuenta con la Resolución Ministerial 129-2012-PCM, que las obliga a implementar un sistema de gestión de seguridad de la información. Con lo cual, no se les puede asignar una categoría de menor nivel, debido a que la información que manejan impacta directamente en los titulares de datos personales. Sin embargo, para las categorías *simple*, *intermedio* y *complejo* se pueden tener combinaciones más acordes al tipo de tratamiento que se realice.

V. Sanchez

e) **Finalidad del tratamiento de datos personales respaldada por norma legal.-** Tiene especial impacto por ser obligatorio, esto determina el tipo *crítico*.

f) **Múltiples localizaciones**.- El acceso o tratamiento distribuido incorpora un nivel de atención especial porque incluye la transferencia de datos entre múltiples locales de tratamiento (ubicaciones diferentes, pueden ser inmuebles diferentes en la misma ciudad o ciudades diferentes), lo que genera complejidad y puede hacerlo *crítico*.

g) **Tratamiento de datos sensible.-** Al incluir estos datos se debe tomar medidas de protección como mínimo de categoría *intermedio*.

Así podemos hacer algunos cruces para explicar la categorización:

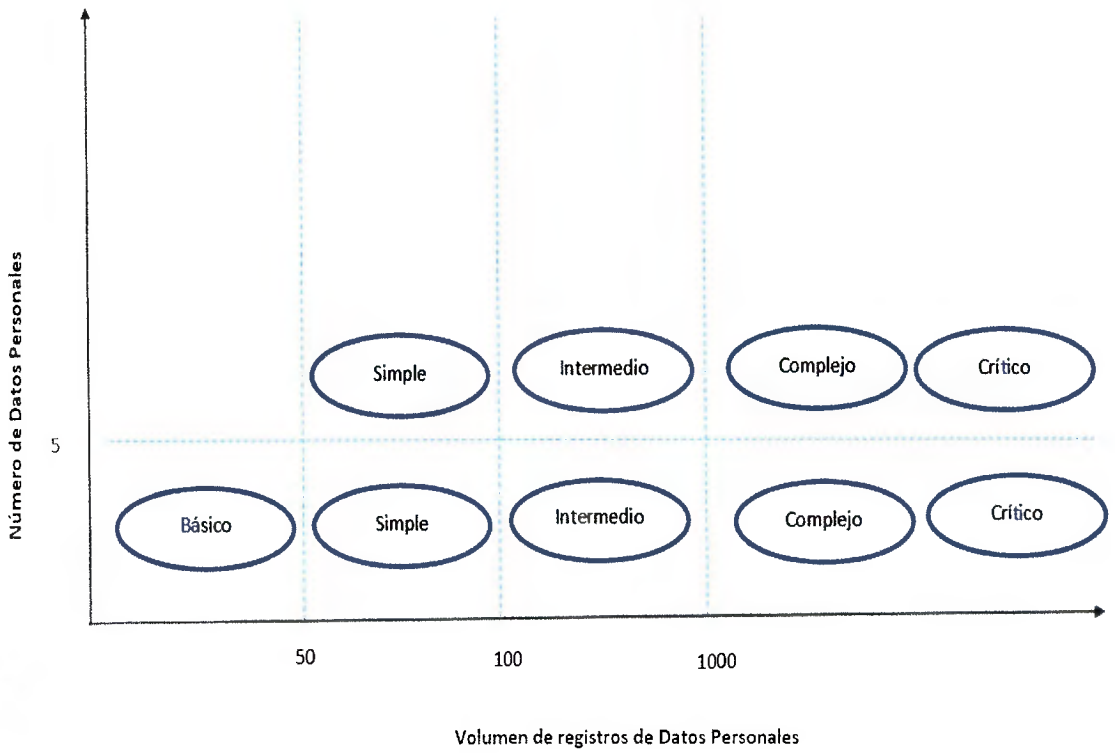


Figura 1: Volumen de datos / Número de datos

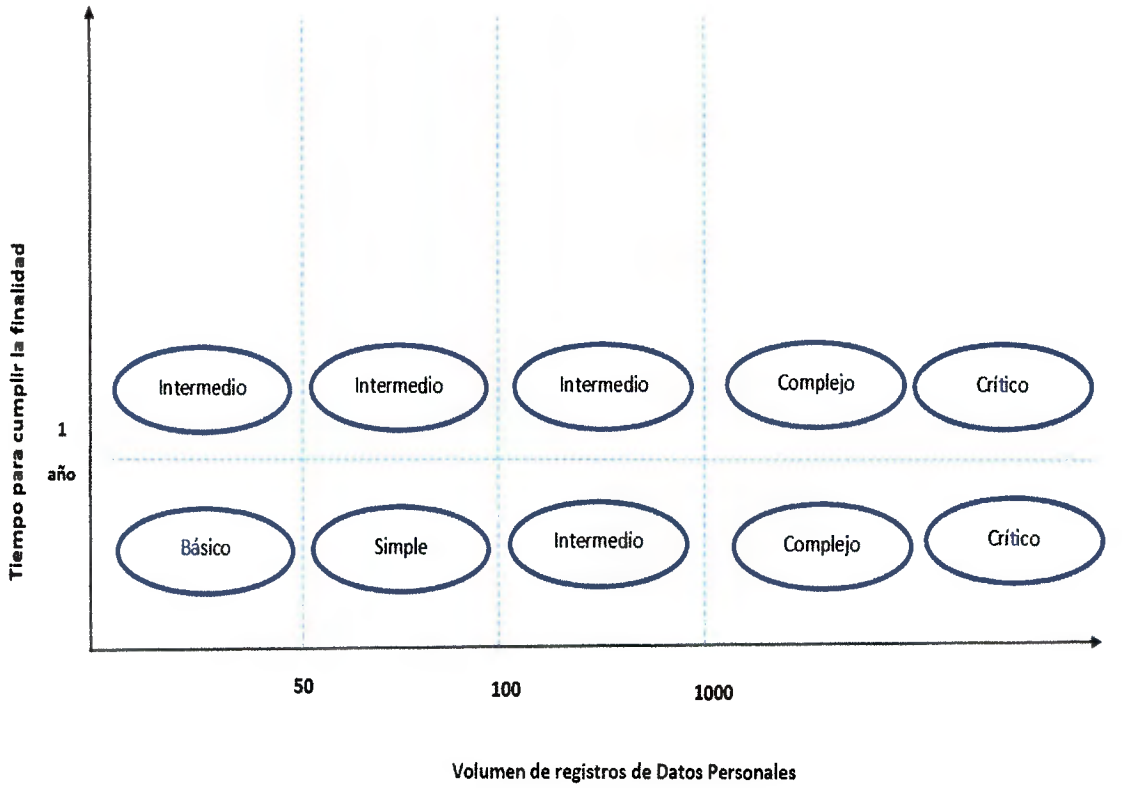


Figura 2: Volumen de registros / Tiempo para cumplir la finalidad.

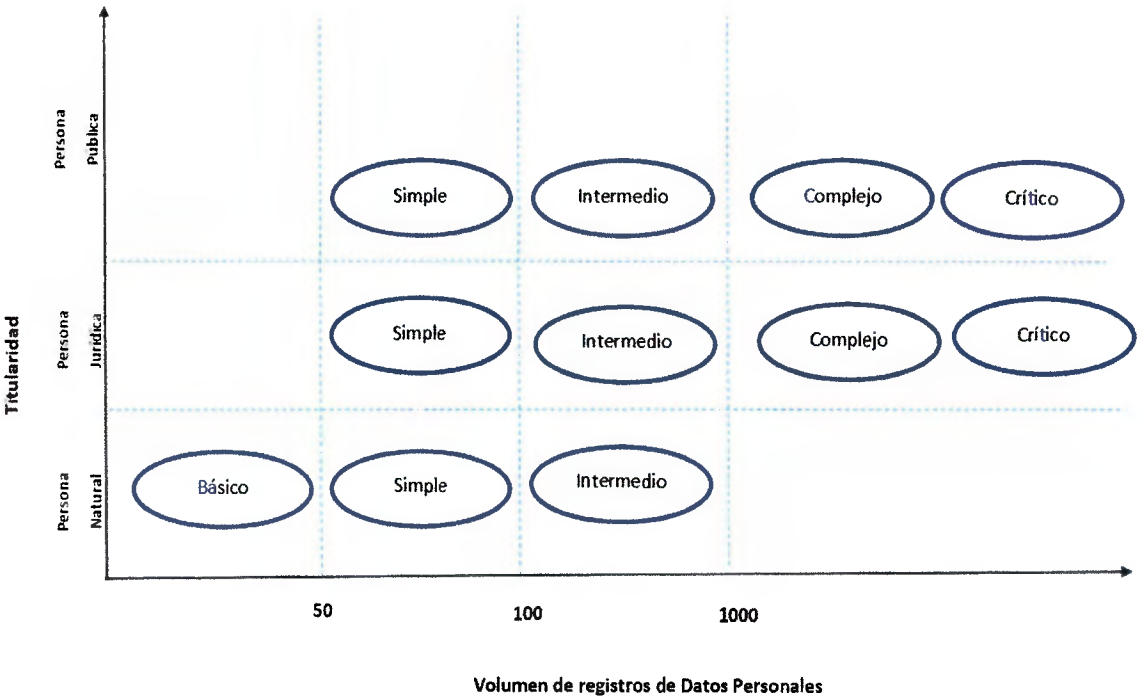


Figura 3: Volumen de registros / Titularidad del banco de datos personales.

1.1.3 Matriz de apoyo para la selección de categoría en el tratamiento de datos personales.

Ítem	Criterio	Básico	Simple	Intermedio	Complejo	Crítico
1	Volumen de registros, número de titulares de datos personales que consienten el tratamiento de sus datos. (Criterio utilizado para determinar las categorías)	**Hasta 50**	**Hasta 100**	**Hasta 1000**	**Indeterminado**	**Indeterminado**
2	Número de datos personales en banco de datos personales que no contienen datos sensibles. (Criterio utilizado para determinar el tipo *básico*)	**Hasta 5**	**Mas de 5**	**Más de 5**	**Más de 5**	**Más de 5**
3	Finalidad del tratamiento de datos personales respaldada por ley o similar. (Criterio utilizado para determinar el tipo *crítico*)	**No aplica**	**No aplica**	**No aplica**	**No aplica**	**Aplica**
4	Periodo mayor a un (01) año o indeterminado para cumplir la finalidad (tiempo de tratamiento de los datos personales).	**No aplica**	**No aplica**	**Aplica**	**Aplica**	**Aplica**
5	Tipo de Titular del banco de datos personales: persona natural. (Criterio utilizado para determinar el tipo entre *básico* a *intermedio*).	**Aplica**	**Aplica**	**Aplica**	**No aplica**	**No aplica**
6	Tipo de Titular del banco de datos personales: persona jurídica. (Criterio utilizado para determinar la categoría entre *simple* a *complejo*)	**No Aplica**	**Aplica**	**Aplica**	**Aplica**	**Aplica**

J. A. Quiroga L.

7	Titular del banco de datos personales del tipo persona jurídica o entidad pública con múltiples localizaciones desde las cuales se tiene acceso al banco de datos personales o se realiza tratamiento de los datos personales. (Criterio utilizado para determinar la categoría *complejo* o *crítico*)	**No aplica**	**No aplica**	**No aplica**	**Aplica**	**Aplica**
8	El banco de datos personales puede incluir datos sensibles. (Criterio utilizado para determinar la categoría entre *Intermedio* a *crítico*).	**No aplica**	**No aplica**	**Aplica**	**Aplica**	**Aplica**

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS
DIRECCIÓN GENERAL DE PROTECCIÓN DE DATOS PERSONALES

J. A. Quiroga L.

V. Sánchez

1.2 Condiciones de seguridad:

1.2.1 Condiciones de seguridad externas

a) Marco legal apropiado (leyes, reglamentos, o similares).
b) Conocimiento y conciencia (conocer la importancia de la protección de los datos personales, la Ley N° 29733, Ley de Protección de Datos Personales, y su reglamento).

1.2.2 Condiciones de seguridad internas

a) Compromiso del titular del banco de datos personales (para brindar los recursos y dirección en la protección de los datos personales).
b) Comprender el contexto institucional en el tratamiento y protección de los datos personales (Contexto organizativo, tecnológico, jurídico, legal, contractual, regulatorio, físico, etc.).
c) Determinar claramente las responsabilidades y roles organizacionales apropiados con la suficiente autoridad y recursos para liderar y hacer cumplir la política de seguridad para la protección de datos personales.
d) Enfoque de gestión del riesgo de los datos personales contenidos o destinados a ser contenidos en los bancos de datos personales.

1.3 Requisitos de seguridad:

1.3.1 Sin perjuicio de las condiciones de seguridad, se deben cumplir los requisitos de seguridad señalados a continuación:

		Aplica a la categoría de tratamiento :				
	Requisito	**Básico**	**Simple**	**Intermedio**	**Complejo**	**Crítico**
1.3.1.1	Determinar y dar a conocer una política de protección de datos personales: Una declaración breve y directa que demuestre el compromiso institucional y el involucramiento de sus autoridades con la protección de los datos personales en el tratamiento que se de a los datos personales contenidos en el banco de datos personales bajo su titularidad.	Pueden utilizar el modelo incluido en el Anexo B	Pueden utilizar el modelo incluido en el Anexo B	Incorporar ítem 1.4.1	Incorporar ítem 1.4.1	Incorporar ítem 1.4.1
1.3.1.2	Mantener la gobernabilidad completa de los procesos involucrados en el tratamiento de los datos personales, es decir conocer los procesos y procedimientos y tener control de las decisiones sobre los procesos involucrados en el tratamiento de datos personales cuando estos sean tercerizados o no.	Requerido	Requerido	Requerido	Requerido	Requerido
1.3.1.3	Implementación de las medidas de seguridad según las disposiciones específicas del numeral 2.	Implementar medidas de seguridad de tipo *básico*	Implementar medidas de seguridad de tipo *simple*	Implementar medidas de seguridad de tipo *intermedio*	Implementar medidas de seguridad de *complejo*	Implementar medidas de seguridad de tipo *crítico*
1.3.1.4	Implementar y mantener los siguientes procedimientos documentados.	Opcional	Incorporar ítem 1.4.2	Incorporar ítem 1.4.3	Incorporar ítem 1.4.3	Incorporar ítem 1.4.4
1.3.1.5	Adoptar un enfoque de riesgos y basar las decisiones en el plan de tratamiento de riesgos del banco de datos personales.	Opcional	Opcional	Requerido	Requerido	Requerido

J. A. Quiroga L.

V°B° V. Sánchez

1.3.1.6	Alineamiento a los requisitos según NTP-ISO/IEC 27001 o ISO/IEC 27001 en su edición vigente, incorporando dentro del alcance del SGSI los bancos de datos personales.	No aplica	Opcional	Opcional	Requerido	Requerido
1.3.1.7	Desarrollar y mantener un documento maestro de seguridad de la información del banco de datos personales.	Opcional (ver cuaderno de seguridad en el anexo B)	Opcional (ver cuaderno de seguridad en el anexo B)	Requerido	Requerido	Requerido
1.3.1.8	Desarrollar y mantener actualizado un documento de compromiso de confidencialidad en el tratamiento de datos personales (articulo 17 de la Ley N° 29733), aplicable al personal relacionado con el tratamiento de datos personales.	Declaración jurada simple indicando nombres, apellidos, DNI y firma (puede estar incluido en el cuaderno de seguridad (ver anexo B).	Declaración jurada simple indicando nombres, apellidos, DNI y firma (puede estar incluido en el cuaderno de seguridad (ver anexo B).	Incorporar el requisito dentro le los formatos, procedimientos o procesos apropiados en la organización.	Incorporar el requisito dentro le los formatos, procedimientos o procesos apropiados en la organización.	Incorporar el requisito dentro le los formatos, procedimientos o procesos apropiados en la organización.

J. A. Quiroga L.

V. Sánchez

1.4 Información complementaria sobre requisitos (para aplicar según cuadro de requisitos)

1.4.1 La política de protección de datos personales es una declaración formal de compromiso y debe considerar:

a) Ser clara y comprensible, tanto para el personal involucrado en el tratamiento como para los titulares de datos personales que hayan consentido el tratamiento.
b) Ser apropiada para los objetivos de la organización
c) Proporciona un lineamiento de alto nivel organizacional y objetivos claros que sirven de dirección para la implementación de las condiciones, requisitos y medidas de seguridad apropiadas.
d) Incluir un compromiso de cumplimiento de los requisitos de seguridad aplicables.
e) Incluir compromiso de respeto a los principios de la Ley N° 29733, Ley de Protección de Datos Personales.
f) Incluir un compromiso de mejora continua.
g) Comunicarse oportuna y claramente al interior de la organización.

1.4.2 Se debe lograr la implementación y el mantenimiento de los siguientes procedimientos documentados:

a) Control de documentos y registros.
b) Registros de personal con acceso autorizado.
c) Registro de incidentes y medidas adoptadas.

1.4.3 Se debe lograr la implementación y mantener los siguientes procedimientos documentados

a) Control de documentos y registros.
b) Registros de acceso.
c) Registro de auditorías.
d) Registro de incidentes y problemas.

1.4.4 Incluidos en el Sistema de Gestión de la Seguridad de la Información -SGSI, incluyendo además un registro de control de acceso, según el artículo 39 del reglamento de la Ley N° 29733.

2. DISPOSICIONES ESPECÍFICAS

a) Para los tratamientos determinados como *complejos* o *críticos*, se deben implementar los controles adecuados de un sistema de gestión de seguridad de la información bajo los requisitos y controles de la NTP-ISO/IEC 27001 EDI en su edición vigente, incorporando a los bancos de datos personales dentro del alcance del SGSI, asegurando como mínimo el cumplimiento de las medidas indicadas a continuación y que los riesgos asociados al banco de datos personales sean adecuadamente gestionados.
b) El titular del banco de datos personales debe designar un responsable de seguridad del banco de datos personales, quien coordinará en la institución la aplicación de la presente directiva. El rol de responsable de seguridad del banco de datos personales debe asignarse a una persona que tenga las capacidades y autoridad necesaria para el desarrollo de sus funciones. Cuando dicha designación no exista, se entiende que el rol de responsable de seguridad del banco de datos personales recae en el titular del banco de datos personales.
c) Las referencias a documentos o registros pueden estar en cualquier formato o tipo de medio (Hoja impresa, cuaderno, página web, afiche, registro de video, entre otros).

d) Limitar los bancos de datos personales a los datos estrictamente necesarios para cumplir la finalidad para la cual fueron acopiados.
e) Evaluar la posibilidad de implementar mecanismos de anonimización o disociación aplicables.

2.1 Medidas de Seguridad Organizativas

		Aplica a la categoría de tratamiento :				
Ítem	**Medidas de seguridad**	**Básico**	**Simple**	**Intermedio**	**Complejo**	**Crítico**
2.1.1	Desarrollar una estructura organizacional con roles y responsabilidades de acuerdo a la proporcionalidad de los datos a proteger.	Solo considera al titular del banco de datos personales y al o a los encargados del tratamiento de datos personales. (Cuando el tratamiento no lo realice exclusivamente el titular del banco de datos personales)	Solo considera al titular del banco de datos personales y al o a los encargados del tratamiento de datos personales. (Cuando el tratamiento no lo realice exclusivamente el titular del banco de datos personales)	Requerido	Requerido	Requerido
2.1.2	Compromiso documentado de respeto a los principios de la ley.	Puede utilizar el modelo citado en el Anexo B	Puede utilizar el modelo citado en el Anexo B	Requerido	Requerido	Requerido
2.1.3	Llevar un control y registro de los operadores con acceso al banco de datos personales con el objetivo de poder identificar al personal con acceso en determinado momento (Trazabilidad).	Opcional	Opcional	Opcional	Requerido	Requerido
2.1.4	Revisar periódicamente la efectividad de las medidas de seguridad adoptadas y registrar dicha verificación en un documento adjunto al banco de datos personales.	Requerido. (dichas revisiones pueden estar registradas en el cuaderno de seguridad citado en el anexo B)	Requerido. (dichas revisiones pueden estar registradas en el cuaderno de seguridad citado en el anexo B)	Requerido	Requerido	Requerido
2.1.5	Adecuación de los sistemas de gestión u aplicaciones existentes que intervengan en el tratamiento de datos personales, conforme a la Ley N° 29733, Ley de Protección de Datos Personales, y su reglamento.	Opcional	Opcional	Opcional	Requerido	Requerido

2.1.6	Adecuación de los procesos del negocio involucrados en el tratamiento de datos personales a los requisitos establecidos en la Ley N° 29733, Ley de Protección de Datos Personales, y su reglamento.	Opcional	Opcional	Opcional	Requerido	Requerido
2.1.7	Desarrollar procedimientos documentados adecuados para el tratamiento de datos personales.	Opcional	Opcional	Requerido	Requerido	Requerido
2.1.8	Desarrollar un programa de creación de conciencia y entrenamiento en materia de protección de datos personales.	Opcional	Opcional	Requerido	Requerido	Requerido
2.1.9	Desarrollar un procedimiento de auditoría respecto de las medidas de seguridad implementadas, teniendo como mínimo una auditoría anual.	Opcional	Opcional	Requerido	Requerido	Requerido
2.1.10	Desarrollar un procedimiento de gestión de incidentes para la protección de datos personales.	Opcional	Opcional	Requerido	Requerido	Requerido
2.1.11	Desarrollar un procedimiento de asignación de privilegios de acceso al banco de datos personales y su correspondiente registro de acceso.	Opcional	Requerido	Requerido	Requerido	Requerido

2.2 Medidas de Seguridad Jurídicas

		Aplica a la categoría de tratamiento :				
Ítem	**Medidas de seguridad**	**Básico**	**Simple**	**Intermedio**	**Complejo**	**Crítico**
2.2.1	Mantener los formatos de consentimiento para el tratamiento de datos personales, adecuados y de conformidad con la finalidad para la cual son acopiados.	Requerido (pueden estar registradas en el cuaderno de seguridad citado en el anexo B)	Requerido (pueden estar registradas en el cuaderno de seguridad citado en el anexo B)	Requerido	Requerido	Requerido
2.2.2	Adecuación de los contratos del personal relacionado con el tratamiento de datos personales, incluyendo la coherencia con el requisito 1.3.1.8.	Opcional	Opcional	Requerido	Requerido	Requerido
2.2.3	Adecuación de los contratos con terceros, incluyendo la coherencia con el requisito 1.3.1.8.	Opcional	Opcional	Requerido	Requerido	Requerido

2.3 Medidas de Seguridad Técnicas

2.3.1 Medidas de Seguridad Técnicas relacionadas al acceso no autorizado al banco de datos personales

Medidas generales

2.3.1.1 Gestión y uso de contraseñas cuando el tratamiento se realice con medios informáticos.

Se debe controlar la asignación y el uso de las contraseñas de los usuarios de los sistemas de información que realizan tratamiento de datos personales mediante la adopción de las siguientes medidas:

a) Solicitar a los usuarios que mantengan en secreto las contraseñas asignadas.
b) Cuando se utilice un servidor de autenticación, este debe almacenar las contraseñas de manera cifrada.
c) Permitir que el usuario cambie la contraseña asignada cuando lo considere necesario.
d) Requerir el uso de contraseñas que contengan al menos 8 dígitos y que sean alfanuméricas (mayúsculas, minúsculas y números) y al menos incluyan un caracter especial.
e) Cuando el acceso al sistema este expuesto en entornos públicos (intranet, internet o similares) se debe bloquear al usuario luego de cinco (05) intentos fallidos de autenticación consecutivos.

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS
DIRECCIÓN GENERAL DE PROTECCIÓN DE DATOS PERSONALES
V°B° Quiroga L

2.3.1.2 Revisión y registro de los privilegios de acceso

Se debe revisar periódicamente que los privilegios de acceso a los datos personales correspondan al personal autorizado. Esta revisión debe generar un registro de revisión que evidencie la realización de dicha revisión.

El periodo de revisión depende de las políticas organizacionales y el tipo de datos personales que contenga el banco de datos personales. Esta debe realizarse por lo menos semestralmente.

V°B°
V. Sánchez

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.

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.

J. A. Quiroga L.

V. Sánchez

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.

J. A. Quiroga L.

2.3.1.5 El titular del banco de datos personales, o quien este designe, debe autorizar o retirar el acceso de usuarios que realicen tratamiento de datos personales. Dicha autorización debe registrarse.

Aplica a la categoría de tratamiento :				
Básico	**Simple**	**Intermedio**	**Complejo**	**Crítico**
Se debe mantener un registro actualizado de usuarios con acceso autorizado para el tratamiento de datos personales y al banco de datos personales. (Puede registrarse en el cuaderno de seguridad citado en el anexo B)	Se debe mantener un registro actualizado de usuarios con acceso autorizado para el tratamiento de datos personales. (Puede registrarse en el cuaderno de seguridad citado en el anexo B)	El titular, o quien este designe, debe autorizar o retirar el acceso de usuarios a los datos personales contenidos en el banco de datos personales, dicha operación debe ser registrada. Los datos personales a registrar deben incluir como mínimo: • Usuario (en sistemas informáticos el identificador de usuario) • Fecha y hora de asignación y/o retiro de autorización del usuario. • Usuario que autoriza.	El titular, o quien este designe, debe autorizar o retirar el acceso de usuarios a los datos personales contenidos en el banco de datos personales, dicha operación debe ser registrada. Los datos a registrar deben incluir como mínimo: • Usuario (en sistemas informáticos el identificador de usuario). • Fecha y hora de asignación y/o retiro de autorización del usuario. • Usuario que autoriza.	El titular, o quien este designe, debe autorizar o retirar el acceso de usuarios a los datos personales contenidos en el banco de datos personales. Dicha operación debe ser registrada. Los datos a registrar deben incluir como mínimo: • Usuario (en sistemas informáticos el identificador de usuario) • Fecha y hora de asignación y/o retiro de autorización del usuario. • Usuario que autoriza.

2.3.1.6 Identificar los accesos realizados a los datos personales para su tratamiento.

Aplica a la categoría de tratamiento :				
Básico	**Simple**	**Intermedio**	**Complejo**	**Crítico**
Opcional	Opcional	Implementar un registro de accesos al banco de datos personales, el cual debe contener al menos los siguientes campos: • Fecha y hora del acceso. • Persona o personas que realiza el acceso. • Identificador del titular de los datos personales a tratar (mediante mecanismo de disociación aplicado). • Motivo del acceso.	Implementar un registro de accesos al banco de datos personales, el cual debe contener al menos los siguientes campos: • Fecha y hora del acceso. • Persona o personas que realiza el acceso. • Identificador del titular de los datos personales a tratar (mediante mecanismo de disociación aplicado). • Motivo del acceso.	Implementar un registro de accesos al banco de datos personales, el cual debe contener al menos los siguientes campos: • Fecha y hora del acceso. • Persona o personas que realiza el acceso. • Identificador del titular de los datos personales a tratar (mediante mecanismo de disociación aplicado). • Motivo del acceso.

J. A Quiroga L

2.3.2 Medidas de Seguridad Técnicas relacionadas a la alteración no autorizada del banco de datos personales

2.3.2.1 Autorización para el retiro o traslado de datos personales.

Todo traslado de datos personales hacia lugares fuera de los ambientes en donde se ubica el banco de datos personales debe contar con la autorización del titular del banco de datos personales o quien éste designe para ello.

2.3.2.2 Traslado de datos personales.

Todo traslado de datos personales debe considerar:

a) Los datos en soporte físico deben estar contenidos en un contenedor que evite su acceso y legibilidad, así como un mecanismo de verificación de la no vulneración del contenedor.
b) Los datos contenidos en soporte informático deben transportarse previa encriptación y un mecanismo de verificación de la integridad (checksum MD5, firma digital o similar).

2.3.2.3 Eliminación de la información contenida en medios informáticos removibles

Cuando se requiera eliminar la información contenida en un medio informático removible se deben utilizar mecanismos seguros de eliminación que incluyan el borrado total de la información y/o la destrucción del medio; de forma tal que, no permitan la recuperación de los datos.

El titular del banco de datos personales debe designar a las personas autorizadas a eliminar la información de datos personales contenida en los medios informáticos removibles.

J. A. Quiroga L.

2.3.2.4 Seguridad en la copia o reproducción de documentos.

Cuando sea necesario, el titular del banco de datos personales debe designar a las personas autorizadas a generar y/o eliminar las copias o reproducciones de los datos personales.

Se deben implementar las siguientes medidas para preservar la confidencialidad de los datos personales:

a) Utilizar impresoras, fotocopiadoras, scanner u otros equipos de reproducción autorizados.
b) Supervisar el proceso de copia o reproducción de los documentos. No dejar desatendido el equipo.
c) Retirar los documentos originales y las copias del equipo inmediatamente después de finalizada la copia o reproducción.

Se deben registrar las copias o reproducciones de los documentos con datos personales realizadas indicando como mínimo:

V. Sánchez

J. A. Quiroga L.

a) Nombre de la persona que solicita la copia
b) Nombre de la persona autorizada a realizar copias.
c) Descripción de los datos personales copiados.
d) Número de copias.
e) Motivo.
f) Nombre de la persona que recibe la copia.
g) Lugar de destino.
h) Periodo de validez de la copia.

Las copias o reproducciones de los documentos deben tener una marca que identifique el periodo de validez de las mismas.

2.3.2.5 El titular del banco de datos personales, o quien este designe, debe asignar o retirar el privilegio o privilegios (datos a tratar o tarea a realizar) para el tratamiento de datos personales a usuarios autorizados.

Aplica a la categoría de tratamiento :				
Básico	**Simple**	**Intermedio**	**Complejo**	**Crítico**
Se debe mantener un registro actualizado de usuarios con privilegios para el tratamiento de datos personales y acceso al banco de datos personales.(pueden estar registradas en el cuaderno de seguridad citado en el anexo B)	Se debe mantener un registro actualizado de usuarios con privilegios para el tratamiento de datos personales y acceso al banco de datos personales.(pueden estar registradas en el cuaderno de seguridad citado en el anexo B)	El titular, o quien este designe, debe asignar o retirar privilegios a los usuarios con acceso a los datos personales contenidos en el banco de datos personales. Dicha operación debe ser registrada. Los datos a registrar deben incluir como mínimo: * Usuario (en sistemas informáticos el Identificador de usuario). * Privilegio asignado o retirado al usuario. * Fecha y hora de asignación y/o retiro de privilegios del usuario. * Usuario que realiza la asignación y/o retiro de privilegios (en sistemas informáticos el identificador de usuario).	El titular, o quien este designe, debe asignar o retirar privilegios a los usuarios con acceso a los datos personales contenidos en el banco de datos personales. Dicha operación debe ser registrada. Los datos a registrar deben incluir como mínimo: * Usuario (en sistemas informáticos el identificador de usuario) * Privilegio asignado o retirado al usuario. * Fecha y hora de asignación y/o retiro de privilegios del usuario. * Usuario que realiza la asignación y/o retiro de privilegios (en sistemas informáticos el identificador de usuario).	El titular, o quien este designe, debe asignar o retirar privilegios a los usuarios con acceso a los datos personales contenidos en el banco de datos personales. Dicha operación debe ser registrada. Los datos a registrar deben incluir como mínimo: * Usuario (en sistemas informáticos el identificador de usuario) * Privilegio asignado o retirado al usuario * Fecha y hora de asignación y/o retiro de privilegios del usuario. * Usuario que realiza la asignación y/o retiro de privilegios (en sistemas informáticos el identificador de usuario).

J. A. Quiroga

2.3.3 Medidas de Seguridad Técnicas relacionadas a la pérdida del banco de datos personales

		Aplica a la categoría de tratamiento :				
Ítem	**Medidas de seguridad**	**Básico**	**Simple**	**Intermedio**	**Complejo**	**Crítico**
2.3.3.1	Se deben realizar copias de respaldo de los datos personales para permitir su recuperación en caso de pérdida o destrucción.	Opcional	Opcional	Implementar ítem 2.3.5.1	Implementar ítem 2.3.5.1	Implementar ítem 2.3.5.1
2.3.3.2	Toda recuperación de datos personales, desde su copia de respaldo, debe contar con la autorización del encargado del banco de datos personales.	Opcional	Opcional	Requerido	Requerido	Requerido
2.3.3.3	Se deben realizar pruebas de recuperación de los datos personales respaldados para comprobar que las copias de respaldo pueden ser utilizadas en caso de ser requerido.	Opcional	Opcional	Implementar ítem 2.3.5.2	Implementar ítem 2.3.5.2	Implementar ítem 2.3.5.2

2.3.4 Medidas de Seguridad Técnicas relacionadas al tratamiento no autorizado del banco de datos personales

Medidas Generales

2.3.4.1 El banco de datos personales no automatizado debe mantener los datos personales independizados de forma individual, de modo que pueda referirse unívocamente a un titular de datos personales sin exponer información de otro.

2.3.4.2 El titular del banco de datos personales debe informar al titular de datos personales los incidentes que afecten significativamente sus derechos patrimoniales o morales, tan pronto se confirme el hecho.

La información mínima que se debe proporcionar incluye:

a) Naturaleza del incidente.
b) Datos personales comprometidos.
c) Recomendaciones al titular de datos personales.
d) Medidas correctivas implementadas.

J. A. Quiroga L.

Medidas específicas

		Aplica a la categoría de tratamiento :				
Ítem	**Medidas de seguridad**	**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

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS
DIRECCIÓN GENERAL DE PROTECCIÓN DE DATOS PERSONALES
J. A. Quiroga L.

V. Sánchez

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

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS
DIRECCIÓN GENERAL DE PROTECCIÓN DE DATOS PERSONALES

J. A. Quiroga L.

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.

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS
DIRECCIÓN GENERAL DE PROTECCIÓN DE DATOS PERSONALES
J. A. Quiroga L.

V. Sánchez

2.3.5.1 Sobre pérdida del banco de datos personales, en complemento al requisito 2.3.3.1

Toda copia de respaldo de los datos personales debe estar protegida mediante técnicas de cifrado y almacenada en un local seguro y distante al ambiente principal de tratamiento de datos, para garantizar su disponibilidad frente a un desastre en el ambiente principal (considerar el almacenamiento en una localización diferente o remota).

La frecuencia y el periodo de conservación de los respaldos deben ser acorde con la finalidad del tratamiento a realizar y el impacto de la pérdida en los derechos del titular de los datos personales.

Cuando sea pertinente, se debe incorporar mecanismos que garanticen la continuidad del tratamiento de datos personales, principalmente cuando la finalidad tenga un alto impacto en relación con los titulares de datos personales o el bien común.

2.3.5.2 Sobre pérdida del banco de datos personales, en complemento al requisito 2.3.3.3

Estas pruebas deben realizarse por lo menos en forma semestral y se deben documentar los resultados de las pruebas incluyendo:

a) Fecha y hora de la prueba.
b) Nombre de la persona que realizó la prueba.
c) Banco de datos personales recuperado.
d) Archivo recuperado y fecha de los datos recuperados.
e) Tiempo de recuperación.
f) Resultados de las pruebas.
g) Acciones tomadas en caso de pruebas insatisfactorias.

2.3.5.3 Sobre el tratamiento no autorizado del banco de datos personales complemento al requisito 2.3.4.6

J. A. Quiroga L.

a) Transporte electrónico de datos personales en forma cifrada, lo cual puede realizarse mediante el cifrado de la información antes de su transmisión o mediante el uso de protocolos de comunicación cifrados (Ejemplo: VPN, correo electrónico cifrado, FTP seguro, entre otros).
b) Uso de firmas digitales para validar la identidad del emisor de la información.

2.3.5.4 Sobre el tratamiento no autorizado del banco de datos personales complemento al requisito 2.3.4.7

El receptor o importador de datos personales debe implementar las medidas de seguridad definidas por el emisor o exportador de datos personales en el documento de seguridad.

La aceptación de la implementación de las medidas de seguridad por parte del receptor o importador de datos personales debe establecerse por escrito

V. Sanchez

mediante cláusulas contractuales u otro instrumento jurídico.

2.3.5.5 Sobre el tratamiento no autorizado del banco de datos personales complemento al requisito 2.3.4.8

Se debe tomar en cuenta:

a) Que el proveedor no tenga acceso a la información de datos personales que utilicen su infraestructura.
b) Que el proveedor no brinde acceso a terceros a los datos personales que utilicen su infraestructura.
c) La destrucción o imposibilidad de recuperación de los datos alojados en el servicio una vez concluida la relación con el proveedor.
d) Uso de canales seguros para la transferencia de datos personales.
e) Garantizar el cumplimiento de las medidas de seguridad en todos los lugares en donde se encuentre distribuida la infraestructura del proveedor.

2.3.5.6 Sobre el tratamiento no autorizado del banco de datos personales complemento al requisito 2.3.4.9

El encargado del banco de datos personales o quien sea designado por el titular del banco de datos personales deberá coordinar las acciones requeridas para analizar y responder en forma rápida y efectiva a los incidentes de seguridad presentados.

Se deben registrar los incidentes de seguridad relacionados con los bancos de datos personales, incluyendo como mínimo:

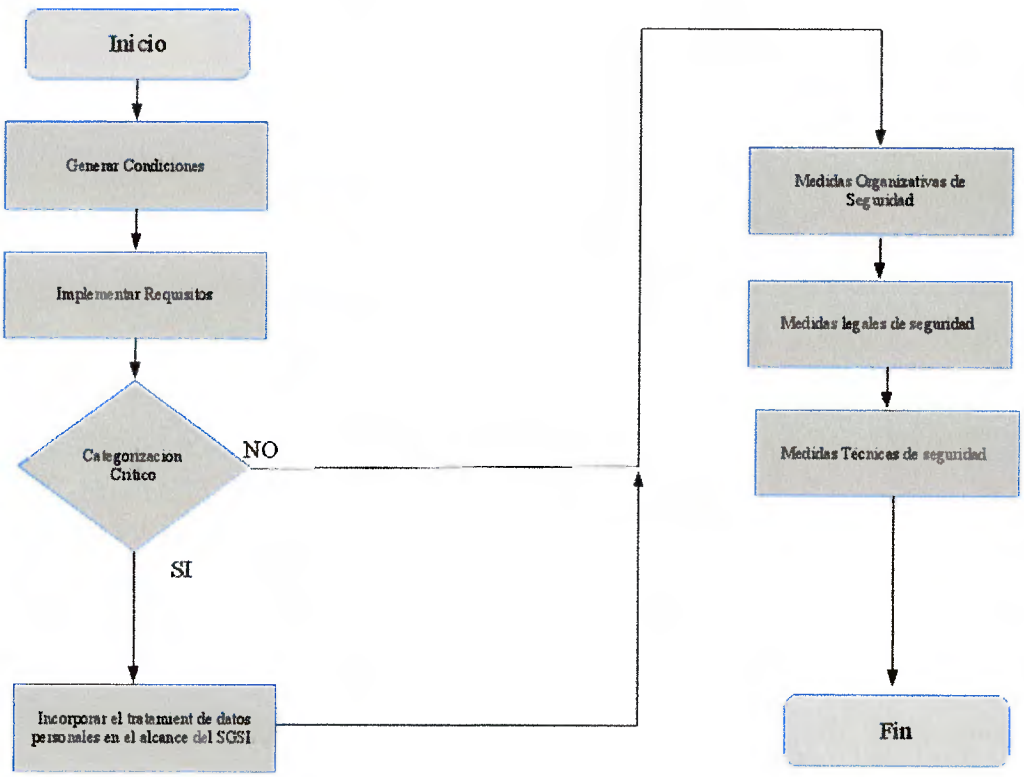
a) Fecha y hora del incidente.
b) Nombre de la persona que lo reporta.
c) Naturaleza del incidente
d) Datos personales comprometidos
e) Nombres de las personas involucradas en la resolución del incidente.
f) Consecuencias del incidente.
g) Medidas correctivas implementadas.
h) Recomendaciones para el titular de datos personales. (Si aplica)
i) Recuperación de datos.
j) En caso de haber realizado recuperación de datos, se debe registrar:

- Nombre de la persona que realizó la recuperación.
- Descripción y fecha de los datos restaurados.
- Descripción de los datos restaurados en forma manual. (Si aplica).

3. PROCEDIMIENTO

3.1 Generar las condiciones apropiadas habilita un entorno favorable para la implementación de la presente directiva.
3.2 Alinear los requisitos, identificar el tipo de tratamiento de datos personales y los requisitos aplicables.
3.3 Cuando el tratamiento de datos personales corresponda al tipo *crítico*, incorporar los bancos de datos personales dentro del alcance del sistema de gestión de seguridad de la información e implementar los controles apropiados.
3.4 Implementar medidas organizacionales de seguridad de acuerdo al tipo de tratamiento de datos personales aplicable.
3.5 Implementar medidas jurídicas de seguridad de acuerdo al tipo de tratamiento de datos personales aplicable.
3.6 Implementar medidas técnicas de seguridad de acuerdo al tipo de tratamiento de datos personales aplicable.

Flujograma:



4. DISPOSICIONES COMPLEMENTARIAS

J. A. Quiroga L.

Con el objetivo de conseguir el logro de los objetivos de la presente directiva, se deben considerar también las siguientes disposiciones:

4.1 Desarrollar programas de información en el ámbito de su responsabilidad, dirigido a titulares de datos personales sobre "consentimiento", "derechos del titular de datos personales" y "finalidad".

4.2 Los encargados del tratamiento por tercerización deben asegurar y mantener los mecanismos de auditoría, verificación y toma de decisiones del titular del banco que contrata.

V. Sánchez

ANEXO A: GLOSARIO

Para los efectos de la aplicación de la presente directiva, sin perjuicio de las definiciones contenidas en la Ley Nº 29733, Ley de Protección de Datos Personales, y su reglamento, se señalan las siguientes definiciones a tener en cuenta:

1. **Medio informático removible:** Dispositivo de almacenamiento de información. Incluye disquetes, CD's, DVD's, cintas de respaldo, memorias USB, disco duro externo, entre otros.

2. **Responsable de seguridad:** Rol asignado a una persona que coordina y controla la implementación de las medidas de seguridad en un banco de datos personales.

3. **Usuarios de sistemas de información:** Persona natural que tiene acceso a un sistema de información que realiza tratamiento de datos personales. Puede ser el administrador del sistema, administrador de banco de datos, operadores, personal de soporte o el titular de los datos personales.

4. **Gestión de Riesgos:** Proceso ordenado y continuo para medir y mantener los riesgos por debajo de los umbrales definidos organizacionalmente.

ANEXO B: ORIENTACIÓN PARA BANCOS DE DATOS DE TIPO *BÁSICO* O *SIMPLE*

Con el objetivo de orientar en el cumplimiento de la directiva de seguridad de la información administrada por los bancos de datos personales, se presenta lo siguiente:

1.- Política de seguridad de datos personales

Con conocimiento de los ocho (08) principios señalados en la Ley N° 29733, Ley de Protección de Datos Personales, para fines de cumplimiento, los bancos de datos personales de tipo *básico* o *simple* podrán colocar un aviso en un lugar visible, que contenga la siguiente información:

Aquí protegemos los datos personales.

Respetamos los principios de protección de datos personales:

- Principio de legalidad
- Principio de consentimiento
- Principio de finalidad
- Principio de proporcionalidad
- Principio de calidad
- Principio de disposición de recurso
- Principio de nivel de protección adecuado

Ley N° 29733- Ley de Protección de Datos Personales y su reglamento, aprobado mediante Decreto Supremo N° 003-2013-JUS

J. A. Quiroga L.

2.- Cuaderno de seguridad de datos personales (Documento maestro de seguridad de la información del banco de datos personales)

Para fines de cumplimiento, los bancos de datos de tipo *básico* pueden utilizar un cuaderno simple que contenga de manera ordenada todos los requisitos documentados y registros señalados en la directiva de seguridad de la información administrada por los bancos de datos personales.

Este cuaderno debe estar protegido del acceso no autorizado, por ejemplo en un gabinete o cajón de mueble protegido por una cerradura con llave o candado.

V. Sánchez

ANEXO C: ORIENTACIÓN PARA BANCOS DE DATOS DE TIPO *COMPLEJO* O *CRÍTICO*

Con el objetivo de orientar en el cumplimiento de la directiva de seguridad de la información administrada por los bancos de datos personales, se presenta lo siguiente:

- Las entidades públicas pertenecientes al Sistema Nacional de Informática tienen la obligatoriedad de implementar la NTP-ISO/IEC 27001 según la Resolución Ministerial 129-2012-PCM. Por lo que, al incorporar los bancos de datos personales dentro del alcance del SGSI, el sistema de gestión ayudará al cumplimiento de la mayor parte de los requisitos y medidas señaladas en la directiva de seguridad de la información administrada por los bancos de datos personales, incluso a mayor nivel del definido en la directiva. Siendo necesario identificar cuáles son los aspectos que el SGSI no cubre y que la directiva señala.
- Las personas jurídicas pueden implementar el ISO/IEC 27001 en su edición vigente incorporando, en el alcance del SGSI, a los bancos de datos personales. Con lo cual, el sistema de gestión ayudará al cumplimiento de la mayor parte de los requisitos y medidas señaladas en la directiva de seguridad de la información administrada por los bancos de datos personales, incluso a mayor nivel del definido en la directiva. Siendo necesario identificar cuáles son los aspectos que el SGSI no cubre y que la directiva señala.
- Las instituciones pueden utilizar el ISO 31000 o ISO/IEC 27005 como referencias de gestión del riesgo.
- Las instituciones pueden utilizar un Análisis de Impacto en la Privacidad (PIA por sus siglas en inglés) como insumo u orientación en la fase de planificación y gestión del riesgo.
- Las instituciones pueden utilizar el enfoque de "Privacidad por Diseño" como referencia en la evaluación de sus procesos y herramientas que determinen deban incorporarse o modificarse para el cumplimiento de la Ley N° 29733, Ley de Protección de Datos Personales.
  Ver: http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-spanish.pdf