RESOLUCIÓN de GERENCIA GENERAL

N° 022-2019-GG/ZED ILO

Ilo; 2019 Mayo 07.

VISTOS:

El Informe N° 030-2019-DOI/ZED ILO, de la Dirección de Operaciones e Infraestructura de ZED ILO, y;

CONSIDERANDO:

Que, la Zona Especial de Desarrollo Ilo - ZED ILO, es un Organismo Público con autonomía administrativa, técnica, económica, financiera y operativa, en virtud a lo dispuesto en el artículo 2° de la Ley N° 28569 "Ley que otorga autonomía a los CETICOS", hoy ZED ILO conforme a lo establecido en la Ley N° 30446; adscrita al Gobierno Regional de Moquegua, en virtud a la Ley N° 29014;

Que, mediante el Informe del Vistos de fecha 06 de Mayo del presente año, la Dirección de Operaciones e Infraestructura de la Entidad remite en diez (10) folios la Directiva de seguridad de la Información en el ámbito de la Protección de Datos Personales, indicando que la misma servirá para el desarrollo de las actividades del área de Informática de la institución, así como para los términos de referencia para la contratación del servicio de nube para la Entidad. Por lo cual solicita a la Gerencia General la aprobación de la citada Directiva mediante acto administrativo.

Que la finalidad de la Directiva de seguridad de la Información en el ámbito de la Protección de Datos Personales es constituir un instrumento que oriente sobre las condiciones, requisitos y medidas técnicas que se deben tomar en cuenta en ZED ILO para el cumplimiento de la Ley N° 29733 Ley de Protección de Datos Personales y su Reglamento, en materia de seguridad de los datos personales. Asimismo su objetivo general es garantizar la seguridad de los datos personales contenidos o destinados a ser contenidos en bancos de datos personales y su manejo por las diferentes áreas de ZED ILO.

Por lo que; de conformidad con lo establecido en el Artículo 8 de la Ley N° 28569 "Ley que otorga Autonomía a los CETICOS" sus modificatorias Ley N° 28854, Ley N° 29479, Ley N° 30446, Ley N° 29733 Ley de protección de datos Personales y su Reglamento; y con el visto bueno de la Oficina de Asesoría Legal, Dirección de Operaciones e Infraestructura y Oficina General de Administración de ZED ILO;

SE RESUELVE:

ARTICULO PRIMERO- *Aprobar la Directiva N° 05-2019/ZED ILO Directiva de seguridad de la Información en el ámbito de la Protección de Datos Personales de la Zona Especial de Desarrollo Ilo – ZED ILO, la misma que consta de diez (10) folios.*

ARTICULO SEGUNDO- *Remitir copia de la presente Resolución a la Oficina General de Administración, Oficina de Asesoría Legal, Dirección de Operaciones e Infraestructura, Dirección de Promoción y Desarrollo y Órgano de Control Institucional de ZED ILO.*

REGÍSTRESE, COMUNIQÚESE Y NOTIFIQUESE.

Abog. JORGE PACORA FUENTES
Gerente General

DIRECTIVA DE SEGURIDAD DE LA INFORMACION EN EL AMBITO DE LA PROTECCIÓN DE DATOS PERSONALES

DIRECTIVA N° 05-2019/ZED ILO

I. FINALIDAD

Constituir un instrumento que oriente sobre las condiciones, requisitos y medidas técnicas que se deben tomar en cuenta en ZED ILO para el cumplimiento de la Ley Nº 29733 y su Reglamento, en materia de seguridad de los datos Personales.

II. OBJETIVO

2.1 OBJETIVO GENERAL

Garantizar la seguridad de los datos personales contenidos o destinados a ser contenidos en bancos de datos personales y su manejo por las diferentes áreas de ZED ILO.

2.2 OBJETIVO ESPECIFICO

- ✓ Determinar las condiciones de seguridad en el tratamiento de datos personales.
- ✓ Determinar las medidas organizativas y técnicas a cumplir por los responsables del banco de datos personales.
- ✓ Establecer las medidas de seguridad apropiadas para el manejo y conservación de base de datos los datos personales en ZED ILO.

ZED ILO ANALISTA DE SISTEMAS

III. ALCANCE

La presente Directiva es de aplicación y cumplimiento obligatorio por todos los órganos y unidades orgánicas de ZED ILO.

ZED ILO Dirección de Operaciones e Infraestructura

IV. BASE LEGAL

- La Ley N° 29733, Ley de Protección de Datos Personales y sus modificatorias. Modificada por el El Decreto Legislativo N° 1353 el 07 de Enero de 2017.
- Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales y su Tercera Disposición Complementaria Modificatoria del Reglamento aprobado por el Artículo 1 del Decreto Supremo N° 019-2017-JUS, publicado el 15 septiembre 2017.

DIRECTIVA DE SEGURIDAD DE LA INFORMACION EN EL AMBITO DE LA PROTECCIÓN DE DATOS PERSONALES

DIRECTIVA N° xxxxxx-2019/ZED ILO

05

I. FINALIDAD

Constituir un instrumento que oriente sobre las condiciones, requisitos y medidas técnicas que se deben tomar en cuenta en ZED ILO para el cumplimiento de la Ley Nº 29733 y su Reglamento, en materia de seguridad de los datos Personales.

II. OBJETIVO

2.1 OBJETIVO GENERAL

Garantizar la seguridad de los datos personales contenidos o destinados a ser contenidos en bancos de datos personales y su manejo por las diferentes áreas de ZED ILO.

2.2 OBJETIVO ESPECIFICO

- ✓ Determinar las condiciones de seguridad en el tratamiento de datos personales.
- ✓ Determinar las medidas organizativas y técnicas a cumplir por los responsables del banco de datos personales.
- ✓ Establecer las medidas de seguridad apropiadas para el manejo y conservación de base de datos los datos personales en ZED ILO.

ZED ILO ANALISTA DE SISTEMAS

III. ALCANCE

La presente Directiva es de aplicación y cumplimiento obligatorio por todos los órganos y unidades orgánicas de ZED ILO.

IV. BASE LEGAL

- La Ley N° 29733, Ley de Protección de Datos Personales y sus modificatorias. Modificada por el El Decreto Legislativo N° 1353 el 07 de Enero de 2017.
- Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales y su Tercera Disposición Complementaria Modificatoria del Reglamento aprobado por el Artículo 1 del Decreto Supremo N° 019-2017-JUS, publicado el 15 septiembre 2017.

ZED ILO Dirección de Operaciones e Infraestructura

- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado y sus modificatorias. Modificada por el Decreto Legislativo N° 1446, Ley 30039, Ley 27899, Ley N° 27842 y Ley N° 27852.
- Decreto Legislativo N° 1353, Decreto Legislativo que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la Regulación de la Gestión de Intereses. Modificado por el Decreto Legislativo N° 1416.
- Decreto Supremo N° 004-2019-JUS, publicado el 25 enero 2019.
- Ordenanza Regional N° 02-2017-CR/GRN, Reglamento de Organización y Funciones de la Zona Especial de Desarrollo de Ilo – ZED ILO.
- Ordenanza Regional 17-2008-CR/GRM, Cuadro para asignación de personal CAP.
- Resolución Ministerial N° 246-2007-PCM que aprueba el uso de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 23. Edición".
- Resolución Ministerial N° 004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a Edición". Modificada por el Artículo 3 de la Resolución Ministerial N° 166-2017-PCM, publicada el 21 junio 2017, por el Artículo 2 de la Resolución Ministerial N° 087-2019-PCM, publicada el 22 marzo 2019.
- Ley 27806, Ley de Transparencia y Acceso a la Información Pública.
- Constitución Política del Perú

ZED ILO ANALISTA DE SISTEMAS

V. DEFINICIONES

1. **Banco de datos personales.** Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.
2. **Banco de datos personales de administración pública.** Banco de datos personales cuya titularidad corresponde a una entidad pública.
3. **Datos personales**. Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

ZED ILO Dirección de Operaciones e Infraestructura

4. **Datos sensibles.** Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.
5. **Encargado del banco de datos personales.** Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales.
6. **Entidad pública.** Entidad comprendida en el artículo I del Título Preliminar de la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces.
7. **Flujo transfronterizo de datos personales.** Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.
8. **Fuentes accesibles para el público.** Bancos de datos personales de administración pública o privada, que pueden ser consultados por cualquier persona, previo abono de la contraprestación correspondiente, de ser el caso. Las fuentes accesibles para el público son determinadas en el reglamento.
9. **Nivel suficiente de protección para los datos personales.** Nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de esta Ley, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de que se trate.
10. **Procedimiento de anonimización.** Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.
11. **Procedimiento de disociación.** Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es reversible.
12. **Titular de datos personales**. Persona natural a quien corresponde los datos personales.
13. **Titular del banco de datos personales.** Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.
14. **Transferencia de datos personales.** Toda transmisión, suministro o manifestación de datos

ZED ILO
ANALISTA
DE SISTEMAS

ZED ILO
Dirección de
Operaciones e
Infraestructura

personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.

15. **Tratamiento de datos personales**. Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación¿ o interconexión de los datos personales.

VI. DISPOSICIONES GENERALES

6.1 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 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.

6.2 ZED ILO para efectos de la organización y demás actos relacionados con los datos deberá crear bancos de Datos Personales y determinar su finalidad y contenido así como su tratamiento y las medidas de seguridad a implementar, conforme a las normas legales aplicables.

ZED ILO ANALISTA DE SISTEMAS

6.3 La clasificación de la información que contienen los bancos de datos, se presentan en cinco (5) categorías, teniendo en consideración lo siguiente: el volumen de registros, número de datos, período durante el cual se realiza el tratamiento, finalidad del tratamiento de los datos personales, múltiples localizaciones, tratamientos de datos sensibles:

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

ZED ILO Dirección de Operaciones e Infraestructura

b. ***Simple,*** *corresponde a bancos de datos personales que:*

- ✓ Contengan la información de hasta 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.

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.
- ✓ Puede incluir datos sensibles.
- ✓ Tiene como titular a una persona jurídica o entidad pública.
- ✓ No incluyen datos sensibles.
- ✓ Tiene como titular a una persona natural o jurídica.

ZED ILO ANALISTA DE SISTEMAS

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.
- ✓ Puede incluir datos sensibles.
- ✓ Tiene como titular a una persona jurídica o entidad pública.

ZED ILO Dirección de Operaciones e Infraestructura

6.4 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 aplique 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.

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.

ZED ILO
ANALISTA DE SISTEMAS

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.

ZED ILO
Dirección de Operaciones e Infraestructura

g) Tratamiento de datos sensible.- Al incluir estos datos se debe tomar medidas de protección como mínimo de categoría intermedio. Para determinar dicha categoría analizar los cruces de categorización de Volumen de datos/Número de datos, Volumen de registros/Tiempo para cumplir la finalidad y Volumen de registros/Titularidad del banco de datos personales

VII. 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 debe ser designado por la Gerencia General; El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.

c) 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.

ZED ILO ANALISTA DE SISTEMAS

d) 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).

e) Limitar los bancos de datos personales a los datos estrictamente necesarios para cumplir la finalidad para la cual fueron acopiados.

VIII. PARA EFECTOS DE LA INSCRIPCIÓN DE LOS RESPECTIVOS BANCOS DE DATOS PERSONALES DE ZED ILO, SE PROPORCIONARÁ LA SIGUIENTE INFORMACIÓN:

1. La denominación y ubicación del banco de datos personales, sus finalidades y los usos previstos.
2. La identificación del titular del banco de datos personales, y la identificación del encargado del tratamiento.
3. Tipos de datos personales sometidos a tratamiento en cada Banco.
4. Procedimientos de obtención y el sistema de tratamiento de los datos personales.
5. La descripción técnica de las medidas de seguridad.
6. Los destinatarios de transferencias de datos personales.

ZED ILO Dirección de Operaciones e Infraestructura

IX. TRATAMIENTO Y DEMÁS ACTUACIONES SOBRE LOS DATOS PERSONALES

El titular de datos personales tiene derecho a obtener la información que sobre sí mismo sea objeto de tratamiento en bancos de datos en el ZED ILO, a la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación y a solicitud de quién se realizó la recopilación, así como las transferencias realizadas o que se prevén hacer de ellos. Los derechos de información, acceso, rectificación, cancelación, oposición y tratamiento objetivo de datos personales sólo pueden ser ejercidos por el titular de datos personales.

El ejercicio de alguno o algunos de los derechos no excluye la posibilidad de ejercer alguno o algunos de los otros, ni puede ser entendido como requisito previo para el ejercicio de cualquiera de ellos.

X. CONDICIONES DE SEGURIDAD

Para efectos del tratamiento de los datos personales en el ZED ILO, los encargados responsables de los Bancos de Datos del ZED ILO, deben tener en cuenta tanto las condiciones de seguridad externa como interna:

ZED ILO ANALISTA DE SISTEMAS

10.1 Condiciones de Seguridad Externa

- ✓ Se debe tener en cuenta el marco legal aplicable (leyes, reglamentos, o similares).
- ✓ Conocimiento y conciencia de la importancia de la protección de los datos personales, la Ley N° 29733, Ley de Protección de Datos Personales, y su Reglamento.

10.2 CONDICIONES DE SEGURIDAD INTERNA

- ✓ La Gerencia General dispone las medidas correspondientes, a propuesta de los encargados responsables de los Bancos de Datos para la implementación y operación de la protección de datos personales (para brindar los recursos y dirección en la protección de los datos personales), así corno cada servidor asume 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, conforme a las funciones.

ZED ILO Dirección de Operaciones e Infraestructura

- ✓ Para la presente directiva se aplica el enfoque de gestión del riesgo de los datos personales contenidos o destinados a ser contenidos en los bancos de datos personales elaborando formatos para dicho fin o tomando como referencia el tratamiento de datos personales de otras entidades del estado Peruano.

10.3 REQUISITOS DE SEGURIDAD

Los Bancos de Datos Personales deben cumplir requisitos de seguridad, que varían dependiendo de la categoría de tratamiento de datos (básico, simple, intermedio, complejo o crítico).

En tal sentido, las categorías de tratamiento de datos deben cumplir (en mayor o menor medida) los siguientes requisitos:

a. Mantener la gobernabilidad completa de los procesos involucrados en el tratamiento de los datos personales.
b. Implementar medidas de seguridad según lo indicado en el numeral **X** de la presente directiva.
c. Mantener procedimientos documentados (procedimientos de seguridad de la información determinados por el SGSI según la ISO/IEC 27001 en su edición vigente).
d. Adoptar un enfoque de riesgos y el plan de tratamiento de riesgos del Banco de Datos Personales que se desprende del mismo, servirá como base para la implementación de controles.
e. Alinear los controles indicados en la NTP-ISO/IEC 27001 o ISO/IEC 27001 en su edición vigente, en caso las categorías de tratamiento sean complejas o críticas.
f. Desarrollar y mantener una lista maestra de registro de los bancos de datos personales de la institución.
g. Desarrollar y mantener actualizado un documento o cláusulas de compromiso de confidencialidad de seguridad en el tratamiento de datos personales. Para lo cual se deberá desarrollar y mantener actualizado un documento de compromiso de confidencialidad en el tratamiento de datos personales (artículo 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).

ZED ILO ANALISTA DE SISTEMAS

ZED ILO Dirección de Operaciones e Infraestructura

10.4 INFORMACIÓN COMPLEMENTARIA SOBRE REQUISITOS DE SEGURIDAD

En materia de requisitos de seguridad, las categorías de tratamiento de datos personales, según corresponda, deben implementar los siguientes procedimientos documentados:

a. Control de documentos y registros
b. Registro de accesos
c. Registros de personal con acceso autorizado
d. Registro de incidentes y medidas adoptadas
e. Registro de auditorías.

ZED ILO
ANALISTA DE SISTEMAS

ZED ILO
Dirección de Operaciones e Infraestructura