

### 4.3 ISO/IEC 27005:2008, Information Technology - Security techniques – Information security risk management.

**Introducción.** Este estándar proporciona lineamientos para la gestión de riesgos de seguridad de la información. Su finalidad es apoyar la implementación de seguridad de la información con base en un enfoque de gestión de los riesgos.

| N°                 | Requerimiento normativo  | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones | Identificador y nombre Objetivo de Control               | Descripción   |
|--------------------|--|--------------------|-----------------------|----------------------------|--|---|
| <b>RESPONSABLE</b> |  |                    |                       |                            |  |   |
| <b>1</b>           | Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley. | Art. 6             | Art. 9                | 1. Recomendación General.  | 7 Establecimiento del Contexto.                          | Información de la organización que sea relevante para el establecimiento de la gestión de riesgos de seguridad de la información. |
|                    |  |                    |                       |                            | 8 Evaluación del Riesgo de Seguridad de la Información.  | Actividades para la identificación, evaluación, y priorización de los riesgos de seguridad de la información.                     |
|                    |  |                    |                       |                            | 9 Tratamiento del Riesgo de Seguridad de la Información. | Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información.                                    |
|                    |  |                    |                       |                            | 10 Aceptación del Riesgo de Seguridad de la Información. | Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.                                    |

| N°                       | Requerimiento normativo  | Referencia LFPDPPP | Referencia Reglamento         | Referencia Recomendaciones                       | Identificador y nombre Objetivo de Control                            | Descripción  |
|--------------------------|--|--------------------|-------------------------------|--|---|--|
|                          |  |                    |                               |  | 11 Comunicación y Consulta del Riesgo de Seguridad de la Información. | Acciones para comunicar los riesgos de la organización a las partes interesadas. |
|                          |  |                    |                               |  | 12 Monitoreo y revisión del Riesgo de Seguridad de la Información.    | Acciones para monitorear los riesgos y sus factores en la organización.          |
| <b>LICITUD Y LEALTAD</b> |  |                    |                               |  |   |  |
| 2                        | <p>Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos.</p> <p>La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.</p> | Art. 7             | Art. 7<br>Art. 10<br>Art. 44  | Paso 1. Alcance y Objetivos.                     | NO APLICA   | NO APLICA  |
| <b>CONSENTIMIENTO</b>    |  |                    |                               |  |   |  |
| 3                        | <p>El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley.</p> <p>Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular.</p>   | Art. 8             | Art. 11<br>Art. 12<br>Art. 15 | Paso 2. Política de Gestión de Datos Personales. | NO APLICA   | NO APLICA  |

| N° | Requerimiento normativo  | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones  | Identificador y nombre Objetivo de Control | Descripción |
|----|--|--------------------|-----------------------|---|--|-------------|
|    | Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.   |                    |                       |   |  |             |
| 4  | El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.   | Art. 8             | Art. 16               | Paso 2. Política de Gestión de Datos Personales.  | NO APLICA                                  | NO APLICA   |
| 5  | Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento.<br><br>No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado. | Art. 9             | Art. 56               | Paso 2. Política de Gestión de Datos Personales.  | NO APLICA                                  | NO APLICA   |
| 6  | Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.   |                    | Art. 20               | Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad. | NO APLICA                                  | NO APLICA   |

| N°                 | Requerimiento normativo  | Referencia<br>LFPDPPP | Referencia<br>Reglamento       | Referencia<br>Recomendaciones  | Identificador y<br>nombre<br>Objetivo de Control | Descripción |
|--------------------|--|-----------------------|--------------------------------|--|--|-------------|
| <b>INFORMACIÓN</b> |  |                       |                                |  |  |             |
| 7                  | <p>A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento.</p> <p>Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre.</p> <p>Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.</p> | Art. 15               | Art. 14<br>Art. 23<br>Art. 112 | Paso 2. Política de Gestión de Datos Personales.   | NO APLICA  | NO APLICA   |
| 8                  | <p>Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.</p>  | Art. 3, I<br>Art. 17  | Art. 27                        | <p>Paso 7.<br/>Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.<br/>Cumplimiento Cotidiano de Medidas de Seguridad.</p> | NO APLICA  | NO APLICA   |

| N°             | Requerimiento normativo   | Referencia LFPDPPP | Referencia Reglamento         | Referencia Recomendaciones  | Identificador y nombre Objetivo de Control | Descripción |
|----------------|---|--------------------|-------------------------------|---|--|-------------|
| 9              | El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios. | Art. 18            | Art. 14<br>Art. 29<br>Art. 32 | Paso 7.<br>Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.<br>Cumplimiento Cotidiano de Medidas de Seguridad  | NO APLICA                                  | NO APLICA   |
| 10             | Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.   |                    | Art. 31                       | Paso 7.<br>Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.<br>Cumplimiento Cotidiano de Medidas de Seguridad. | NO APLICA                                  | NO APLICA   |
| <b>CALIDAD</b> |   |                    |                               |   |  |             |
| 11             | El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.   | Art. 11            | Art. 36                       | Paso 2. Política de Gestión de Datos Personales.  | NO APLICA                                  | NO APLICA   |

| N° | Requerimiento normativo   | Referencia LFPDPPP    | Referencia Reglamento | Referencia Recomendaciones  | Identificador y nombre Objetivo de Control | Descripción |
|----|---|-----------------------|-----------------------|---|--|-------------|
| 12 | <p>Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos.</p> <p>El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.</p> | Art. 3 III<br>Art. 11 | Art. 37               | Paso 2. Política de Gestión de Datos Personales.  | NO APLICA                                  | NO APLICA   |
| 13 | El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.  |                       | Art. 38               | Paso 2. Política de Gestión de Datos Personales.  | NO APLICA                                  | NO APLICA   |
| 14 | Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.   |                       | Art. 39               | Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad. | NO APLICA                                  | NO APLICA   |

| N°                      | Requerimiento normativo   | Referencia LFPDPPP | Referencia Reglamento         | Referencia Recomendaciones                       | Identificador y nombre Objetivo de Control | Descripción |
|-------------------------|---|--------------------|-------------------------------|--|--|-------------|
| <b>FINALIDAD</b>        |   |                    |                               |  |  |             |
| 15                      | <p>El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.</p> <p>Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular.</p> <p>El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.</p> | Art. 12            | Art. 40<br>Art. 42<br>Art. 43 | Paso 2. Política de Gestión de Datos Personales. | NO APLICA                                  | NO APLICA   |
| <b>PROPORCIONALIDAD</b> |   |                    |                               |  |  |             |
| 16                      | El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.   | Art. 13            | Art. 45<br>Art. 46            | Paso 2. Política de Gestión de Datos Personales. | NO APLICA                                  | NO APLICA   |
| <b>CONFIDENCIALIDAD</b> |   |                    |                               |  |  |             |
| 17                      | El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el  | Art. 21            | Art. 9                        | Paso 2. Política de Gestión de Datos Personales. | NO APLICA                                  | NO APLICA   |

| N°                     | Requerimiento normativo   | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones                       | Identificador y nombre Objetivo de Control   | Descripción   |
|------------------------|---|--------------------|-----------------------|--|--|---|
|                        | titular o, en su caso, con el responsable.  |                    |                       |  |  |   |
| <b>RESPONSABILIDAD</b> |   |                    |                       |  |  |   |
| 18                     | <p>El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias.</p> <p>El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.</p> | Art. 14            | Art. 47               | Paso 2. Política de Gestión de Datos Personales. | <p>7 Establecimiento del Contexto.</p> <p>8 Evaluación del Riesgo de Seguridad de la Información.</p> <p>9 Tratamiento del Riesgo de Seguridad de la Información.</p> <p>10 Aceptación del Riesgo de Seguridad de la Información.</p> <p>11 Comunicación y Consulta del Riesgo de Seguridad de la Información.</p> <p>12 Monitoreo y revisión del Riesgo de Seguridad de la Información.</p> | <p>Información de la organización que sea relevante para el establecimiento de la gestión de riesgos de seguridad de la información</p> <p>Actividades para la identificación, evaluación, y priorización de los riesgos de seguridad de la información.</p> <p>Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información.</p> <p>Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.</p> <p>Acciones para comunicar los riesgos de la organización a las partes interesadas.</p> <p>Acciones para monitorear los riesgos y sus factores en la organización.</p> |

| N° | Requerimiento normativo   | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones                                      | Identificador y nombre Objetivo de Control               | Descripción  |
|----|---|--------------------|-----------------------|---|--|--|
| 19 | Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad. | Art. 14            | Art. 48               | Paso 5. Realizar el Análisis de Riesgo de los Datos Personales. | 7.1 Consideraciones generales.                           | Factores de la organización que inciden en la gestión de riesgos de seguridad de la información.   |
|    |   |                    |                       |   | 7.2 Criterios básicos.                                   | Establecimiento de criterios y enfoque para la gestión de seguridad de la información.   |
|    |   |                    |                       |   | 8.2 Identificación del Riesgo.                           | Identificación de las fuentes de riesgo aplicables a la organización.  |
|    |   |                    |                       |   | 8.3 Análisis del Riesgo.                                 | Actividades para la conducción de un análisis de riesgos de seguridad de la información.   |
|    |   |                    |                       |   | 8.4 Evaluación del Riesgo.                               | Actividades para llevar a cabo decisiones sobre los riesgos de seguridad de la información tomando en cuenta el contexto de la organización. |
|    |   |                    |                       |   | 9 Tratamiento del Riesgo de Seguridad de la Información. | Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información.   |
| 20 | Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.   |                    | Art. 48 - I           | Paso 2. Política de Gestión de Datos Personales.                | NO APLICA  | NO APLICA  |
| 21 | Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales. |                    | Art. 48 - II          | Paso 9. Mejora Continua y Capacitación. Capacitación.           | NO APLICA  | NO APLICA  |

| N° | Requerimiento normativo   | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones  | Identificador y nombre Objetivo de Control                         | Descripción   |
|----|---|--------------------|-----------------------|---|--|---|
| 22 | Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.  |                    | Art. 48 - III         | Paso 8. Revisiones y Auditoría.   | 12 Monitoreo y revisión de Riesgos de Seguridad de la Información. | Acciones para monitorear los riesgos y sus factores en la organización.                                     |
|    |   |                    |                       |   | 12.1 Monitoreo y revisión de factores de riesgo.                   | Actividades para el monitoreo y revisión de los factores de riesgo en la organización.                      |
|    |   |                    |                       |   | 12.2 Monitoreo, revisión, y mejora de la gestión del riesgo.       | Actividades para determinar lo adecuado y efectivo de la gestión del riesgo en la organización.             |
| 23 | Destinar recursos para la instrumentación de los programas y políticas de privacidad.   |                    | Art. 48 - IV          | Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales. | NO APLICA  | NO APLICA   |
| 24 | Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos. |                    | Art. 48 - V           | Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.                 | 7.2 Criterios básicos.   | Establecimiento de criterios y enfoque para la gestión de seguridad de la información.                      |
|    |   |                    |                       |   | 7.3 Límites y alcance.   | Factores a considerar para la definición de límites y alcance de la gestión de seguridad de la información. |
|    |   |                    |                       |   | 7.4 Organización para la Gestión del Riesgo de Seguridad de la     | Organización y responsabilidades para la gestión del riesgo de seguridad                                    |

| N° | Requerimiento normativo | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones | Identificador y nombre Objetivo de Control                            | Descripción  |
|----|-------------------------|--------------------|-----------------------|----------------------------|---|--|
|    |                         |                    |                       |                            | Información.  | de la información.   |
|    |                         |                    |                       |                            | 8.2 Identificación del Riesgo.  | Identificación de las fuentes de riesgo aplicables a la organización.  |
|    |                         |                    |                       |                            | 8.3 Análisis del Riesgo.  | Actividades para la conducción de un análisis de riesgos de seguridad de la información.   |
|    |                         |                    |                       |                            | 8.4 Evaluación del Riesgo.  | Actividades para llevar a cabo decisiones sobre los riesgos de seguridad de la información tomando en cuenta el contexto de la organización. |
|    |                         |                    |                       |                            | 9 Tratamiento del Riesgo de Seguridad de la Información.              | Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información.   |
|    |                         |                    |                       |                            | 10 Aceptación del Riesgo de Seguridad de la Información.              | Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.   |
|    |                         |                    |                       |                            | 11 Comunicación y Consulta del Riesgo de Seguridad de la Información. | Acciones para comunicar los riesgos de la organización a las partes interesadas.   |

| N° | Requerimiento normativo  | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones  | Identificador y nombre Objetivo de Control                         | Descripción   |
|----|--|--------------------|-----------------------|---|--|---|
|    |  |                    |                       |   | 12 Monitoreo y revisión del Riesgo de Seguridad de la Información. | Acciones para monitorear los riesgos y sus factores en la organización.                         |
| 25 | Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran. |                    | Art. 48 - VI          | Paso 8. Revisiones y Auditoría.   | 12 Monitoreo y revisión de Riesgos de Seguridad de la Información  | Acciones para monitorear los riesgos y sus factores en la organización.                         |
|    |  |                    |                       |   | 12.1 Monitoreo y revisión de factores de riesgo                    | Actividades para el monitoreo y revisión de los factores de riesgo en la organización.          |
|    |  |                    |                       |   | 12.2 Monitoreo, revisión, y mejora de la gestión del riesgo        | Actividades para determinar lo adecuado y efectivo de la gestión del riesgo en la organización. |
| 26 | Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.        |                    | Art. 48 - VII         | Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad. | NO APLICA  | NO APLICA   |

| N°               | Requerimiento normativo  | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones  | Identificador y nombre Objetivo de Control | Descripción |
|------------------|--|--------------------|-----------------------|---|--|-------------|
| 27               | Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.   |                    | Art. 48 - VIII        | Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.  | NO APLICA                                  | NO APLICA   |
| 28               | Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.                               |                    | Art. 48 - IX          | Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.  | NO APLICA                                  | NO APLICA   |
| 29               | Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.   |                    | Art. 48 - X           | Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.  | NO APLICA                                  | NO APLICA   |
| 30               | Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización. | Art. 30            |                       | Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad. | NO APLICA                                  | NO APLICA   |
| <b>SEGURIDAD</b> |  |                    |                       |   |  |             |
| 31               | Todo responsable que lleve a cabo tratamiento de datos personales deberá   | Art. 19            | Art. 4<br>Art. 9      | Paso 6. Identificación de las   | NO APLICA                                  | NO APLICA   |

| N° | Requerimiento normativo  | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones                                      | Identificador y nombre Objetivo de Control   | Descripción   |
|----|--|--------------------|-----------------------|---|--|---|
|    | <p>establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.</p> <p>No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información.</p> <p>Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.</p> |                    | Art. 57               | medidas de seguridad y Análisis de Brecha.                      |  |   |
| 32 | <p>El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.</p> <p>De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos:</p> <p>I. El número de titulares;</p> <p>II. Las vulnerabilidades previas ocurridas en</p>   | Art. 19            | Art. 60               | Paso 5. Realizar el Análisis de Riesgo de los Datos Personales. | <p>7.2 Criterios básicos.</p> <p>7.3 Límites y alcance.</p> <p>7.4 Organización para la Gestión del Riesgo de Seguridad de la Información.</p> | <p>Establecimiento de criterios y enfoque para la gestión de seguridad de la información.</p> <p>Factores a considerar para la definición de límites y alcance de la gestión de seguridad de la información.</p> <p>Organización y responsabilidades para la gestión del riesgo de seguridad de la información.</p> |

| N° | Requerimiento normativo   | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones | Identificador y nombre Objetivo de Control   | Descripción   |
|----|---|--------------------|-----------------------|----------------------------|--|---|
|    | <p>los sistemas de tratamiento;</p> <p>III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y</p> <p>IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.</p> |                    |                       |                            | <p>8.2 Identificación del Riesgo.</p> <p>8.3 Análisis del Riesgo.</p> <p>8.4 Evaluación del Riesgo.</p> <p>9 Tratamiento del Riesgo de Seguridad de la Información.</p> <p>10 Aceptación del Riesgo de Seguridad de la Información</p> | <p>Identificación de las fuentes de riesgo aplicables a la organización.</p> <p>Actividades para la conducción de un análisis de riesgos de seguridad de la información.</p> <p>Actividades para llevar a cabo decisiones sobre los riesgos de seguridad de la información tomando en cuenta el contexto de la organización.</p> <p>Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información</p> <p>Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.</p> |

| N° | Requerimiento normativo  | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones  | Identificador y nombre Objetivo de Control                            | Descripción  |
|----|--|--------------------|-----------------------|---|---|--|
|    |  |                    |                       |   | 11 Comunicación y Consulta del Riesgo de Seguridad de la Información. | Acciones para comunicar los riesgos de la organización a las partes interesadas.                               |
|    |  |                    |                       |   | 12 Monitoreo y revisión del Riesgo de Seguridad de la Información.    | Acciones para monitorear los riesgos y sus factores en la organización.  |
| 33 | Elaborar un inventario de datos personales y de los sistemas de tratamiento.   |                    | Art. 61 - I           | Paso 4. Elaborar un Inventario de Datos Personales.                             | 8.2.2 Identificación de activos                                       | Proceso de identificación de los activos para facilitar el análisis de riesgos de seguridad de la información. |
| 34 | Determinar las funciones y obligaciones de las personas que traten datos personales.   |                    | Art. 61 - II          | Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales. | NO APLICA   | NO APLICA  |
| 35 | Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales. |                    | Art. 61 - III         | Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.                 | 8.2 Identificación del Riesgo.  | Identificación de las fuentes de riesgo aplicables a la organización.  |
|    |  |                    |                       |   | 8.3 Análisis del Riesgo.  | Actividades para la conducción de un análisis de riesgos de seguridad de la información.                       |

| N° | Requerimiento normativo  | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones   | Identificador y nombre Objetivo de Control                            | Descripción  |
|----|--|--------------------|-----------------------|--|---|--|
|    |  |                    |                       |  | 8.4 Evaluación del Riesgo.  | Actividades para llevar a cabo decisiones sobre los riesgos de seguridad de la información tomando en cuenta el contexto de la organización. |
|    |  |                    |                       |  | 9 Tratamiento del Riesgo de Seguridad de la Información.              | Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información.   |
|    |  |                    |                       |  | 10 Aceptación del Riesgo de Seguridad de la Información.              | Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.   |
|    |  |                    |                       |  | 11 Comunicación y Consulta del Riesgo de Seguridad de la Información. | Acciones para comunicar los riesgos de la organización a las partes interesadas.   |
|    |  |                    |                       |  | 12 Monitoreo y revisión del Riesgo de Seguridad de la Información.    | Acciones para monitorear los riesgos y sus factores en la organización.  |
| 36 | Establecer las medidas de seguridad aplicables a los datos personales e identificar aquellas implementadas de manera efectiva. |                    | Art. 61 - IV          | Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha. | 8.2.2 Identificación de activos.                                      | Proceso de identificación de los activos para facilitar el análisis de riesgos de seguridad de la información.                               |
|    |  |                    |                       |  | 8.2.3 Identificación de amenazas.                                     | Identificación de amenazas aplicables a la organización y su probabilidad de ocurrencia.   |

| N° | Requerimiento normativo | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones | Identificador y nombre Objetivo de Control     | Descripción   |
|----|-------------------------|--------------------|-----------------------|----------------------------|--|---|
|    |                         |                    |                       |                            | 8.2.4 Identificación de controles existentes.  | Identificación y documentación de controles existentes incluyendo su efectividad.   |
|    |                         |                    |                       |                            | 8.2.5 Identificación de vulnerabilidades.      | Consideraciones para identificar las vulnerabilidades que pueden ser explotadas en la organización.   |
|    |                         |                    |                       |                            | 8.2.6 Identificación de consecuencias.         | Consideraciones para identificar las consecuencias de las vulnerabilidades en términos de la integridad, confidencialidad, y disponibilidad de los activos de información de la organización. |
|    |                         |                    |                       |                            | 8.3.2 Evaluación de consecuencias.             | Identificación de escenarios de impacto al negocio por incidentes de seguridad.   |
|    |                         |                    |                       |                            | 8.3.3 Evaluación de probabilidad de incidente. | Determinación de la probabilidad de un incidente de seguridad.  |
|    |                         |                    |                       |                            | 8.4 Evaluación del Riesgo.                     | Actividades para llevar a cabo decisiones sobre los riesgos de seguridad de la información tomando en cuenta el contexto de la organización.  |

| N° | Requerimiento normativo  | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones   | Identificador y nombre Objetivo de Control               | Descripción   |
|----|--|--------------------|-----------------------|--|--|---|
|    |  |                    |                       |  | 9 Tratamiento del Riesgo de Seguridad de la Información. | Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información.  |
|    |  |                    |                       |  | 10 Aceptación del Riesgo de Seguridad de la Información. | Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.  |
| 37 | Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales. |                    | Art. 61 - V           | Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha. | 8.2.2 Identificación de activos                          | Proceso de identificación de los activos para facilitar el análisis de riesgos de seguridad de la información   |
|    |  |                    |                       |  | 8.2.3 Identificación de amenazas.                        | Identificación de amenazas aplicables a la organización y su probabilidad de ocurrencia.  |
|    |  |                    |                       |  | 8.2.4 Identificación de controles existentes.            | Identificación y documentación de controles existentes incluyendo su efectividad.   |
|    |  |                    |                       |  | 8.2.5 Identificación de vulnerabilidades.                | Consideraciones para identificar las vulnerabilidades que pueden ser explotadas en la organización.   |
|    |  |                    |                       |  | 8.2.6 Identificación de consecuencias.                   | Consideraciones para identificar las consecuencias de las vulnerabilidades en términos de la integridad, confidencialidad, y disponibilidad de los activos de información de la |

| N° | Requerimiento normativo   | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones  | Identificador y nombre Objetivo de Control          | Descripción  |
|----|---|--------------------|-----------------------|---|---|--|
|    |   |                    |                       |   |   | organización.  |
|    |   |                    |                       |   | 8.3.2 Evaluación de consecuencias.                  | Identificación de escenarios de impacto al negocio por incidentes de seguridad   |
|    |   |                    |                       |   | 8.3.3 Evaluación de probabilidad de incidente.      | Determinación de la probabilidad de un incidente de seguridad.   |
|    |   |                    |                       |   | 8.4 Evaluación del Riesgo.                          | Actividades para llevar a cabo decisiones sobre los riesgos de seguridad de la información tomando en cuenta el contexto de la organización. |
| 38 | Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha. |                    | Art. 61 - VI          | Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes. | 9.1 Descripción general del Tratamiento del Riesgo. | Lineamientos para el tratamiento del riesgo.   |
|    |   |                    |                       |   | 9.2 Modificación del Riesgo.                        | Medidas para modificar el riesgo.  |
|    |   |                    |                       |   | 9.3 Retención del Riesgo.                           | Lineamientos para la retención del riesgo.   |
|    |   |                    |                       |   | 9.4 Cancelación del Riesgo.                         | Lineamientos para la cancelación del riesgo.   |

| N° | Requerimiento normativo   | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones                            | Identificador y nombre Objetivo de Control                            | Descripción   |
|----|---|--------------------|-----------------------|---|---|---|
|    |   |                    |                       |   | 9.5 Transferencia del Riesgo.   | Lineamientos para la transferencia del riesgo.  |
|    |   |                    |                       |   | 10 Aceptación del Riesgo de Seguridad de la Información.              | Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.  |
|    |   |                    |                       |   | 11 Comunicación y Consulta del Riesgo de Seguridad de la Información. | Acciones para comunicar los riesgos de la organización a las partes interesadas.                |
| 39 | Llevar a cabo revisiones o auditorías.  |                    | Art. 61 - VII         | Paso 8. Revisiones y Auditoría.                       | 12 Monitoreo y revisión de Riesgos de Seguridad de la Información.    | Acciones para monitorear los riesgos y sus factores en la organización.                         |
|    |   |                    |                       |   | 12.1 Monitoreo y revisión de factores de riesgo.                      | Actividades para el monitoreo y revisión de los factores de riesgo en la organización.          |
|    |   |                    |                       |   | 12.2 Monitoreo, revisión, y mejora de la gestión del riesgo.          | Actividades para determinar lo adecuado y efectivo de la gestión del riesgo en la organización. |
| 40 | Capacitar al personal que efectúe el tratamiento de datos personales.         |                    | Art. 61 - VIII        | Paso 9. Mejora Continua y Capacitación. Capacitación. | NO APLICA   | NO APLICA   |
| 41 | Realizar un registro de los medios de almacenamiento de los datos personales. |                    | Art. 61 - IX          | Paso 5. Realizar el Análisis de Riesgo                | 8.2.2 Identificación de activos.                                      | Proceso de identificación de los activos para facilitar el análisis                             |

| N°                                  | Requerimiento normativo  | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones  | Identificador y nombre Objetivo de Control                         | Descripción   |
|-------------------------------------|--|--------------------|-----------------------|---|--|---|
|                                     |  |                    |                       | de los Datos Personales.  |  | de riesgos de seguridad de la información.  |
| 42                                  | Contar con una relación de las medidas de seguridad.   |                    | Art. 61               | 3. Acciones a implementar para la seguridad de los datos personales documentadas. | 8.2.4 Identificación de controles existentes.                      | Identificación y documentación de controles existentes incluyendo su efectividad.               |
| 43                                  | <p>Actualizar las medidas de seguridad cuando:</p> <p>I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable.</p> <p>II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo.</p> <p>III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento.</p> <p>IV. Exista una afectación a los datos personales distinta a las anteriores.</p> <p>En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.</p> |                    | Art. 62               | Paso 8. Revisiones y Auditoría.   | 12 Monitoreo y revisión de Riesgos de Seguridad de la Información. | Acciones para monitorear los riesgos y sus factores en la organización.                         |
|                                     |  |                    |                       |   | 12.1 Monitoreo y revisión de factores de riesgo.                   | Actividades para el monitoreo y revisión de los factores de riesgo en la organización.          |
|                                     |  |                    |                       |   | 12.2 Monitoreo, revisión, y mejora de la gestión del riesgo.       | Actividades para determinar lo adecuado y efectivo de la gestión del riesgo en la organización. |
| <b>VULNERACIONES A LA SEGURIDAD</b> |  |                    |                       |   |  |   |

| N° | Requerimiento normativo   | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones   | Identificador y nombre Objetivo de Control | Descripción   |
|----|---|--------------------|-----------------------|--|--|---|
| 44 | Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.   | Art. 20            | Art. 63<br>Art. 64    | Paso 8. Revisiones y Auditoría.<br>Vulneraciones a la Seguridad de la Información. | 8.2.5 Identificación de vulnerabilidades.  | Consideraciones para identificar las vulnerabilidades que pueden ser explotadas en la organización.   |
|    |   |                    |                       |  | 8.2.6 Identificación de consecuencias.     | Consideraciones para identificar las consecuencias de las vulnerabilidades en términos de la integridad, confidencialidad, y disponibilidad de los activos de información de la organización. |
| 45 | En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente:<br><br>I. La naturaleza del incidente.<br>II. Los datos personales comprometidos.<br>III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses.<br>IV. Las acciones correctivas realizadas de forma inmediata.<br>V. Los medios donde puede obtener más |                    | Art. 65               | Paso 8. Revisiones y Auditoría.<br>Vulneraciones a la Seguridad de la Información. | 8.2.5 Identificación de vulnerabilidades.  | Consideraciones para identificar las vulnerabilidades que pueden ser explotadas en la organización.   |
|    |   |                    |                       |  | 8.2.6 Identificación de consecuencias.     | Consideraciones para identificar las consecuencias de las vulnerabilidades en términos de la integridad, confidencialidad, y disponibilidad de los activos de información de la organización. |

| N°               | Requerimiento normativo   | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones   | Identificador y nombre Objetivo de Control  | Descripción   |
|------------------|---|--------------------|-----------------------|--|---|---|
|                  | información al respecto.  |                    |                       |  |   |   |
| 46               | En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita. |                    | Art. 66               | Paso 8. Revisiones y Auditoría.<br>Vulneraciones a la Seguridad de la Información. | 8.2.5 Identificación de vulnerabilidades.<br><br>8.2.6 Identificación de consecuencias.<br><br>8.3.2 Evaluación de consecuencias. | Consideraciones para identificar las vulnerabilidades que pueden ser explotadas en la organización.<br><br>Consideraciones para identificar las consecuencias de las vulnerabilidades en términos de la integridad, confidencialidad, y disponibilidad de los activos de información de la organización.<br><br>Identificación de escenarios de impacto al negocio por incidentes de seguridad. |
| <b>ENCARGADO</b> |   |                    |                       |  |   |   |
| 47               | El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable:  |                    | Art. 50               | 1. Recomendación General.  | NO APLICA   | NO APLICA   |

| N°                       | Requerimiento normativo   | Referencia<br>LFPDPPP | Referencia<br>Reglamento | Referencia<br>Recomendaciones | Identificador y<br>nombre<br>Objetivo de Control | Descripción |
|--------------------------|---|-----------------------|--------------------------|-------------------------------|--|-------------|
|                          | <p>I. Tratar únicamente los datos personales conforme a las instrucciones del responsable.</p> <p>II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.</p> <p>III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables.</p> <p>IV. Guardar confidencialidad respecto de los datos personales tratados.</p> <p>V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.</p> <p>VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.</p> |                       |                          |                               |  |             |
| <b>SUBCONTRATACIONES</b> |   |                       |                          |                               |  |             |

| N° | Requerimiento normativo  | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones   | Identificador y nombre Objetivo de Control | Descripción |
|----|--|--------------------|-----------------------|--|--|-------------|
| 48 | La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.   |                    | Art. 51               | Paso 7.<br>Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad. | NO APLICA                                  | NO APLICA   |
| 49 | <p>Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último.</p> <p>Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido.</p> <p>En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente.</p> <p>La obligación de acreditar que la subcontratación se realizó con autorización</p> |                    | Art. 54<br>Art. 55    | Paso 7.<br>Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad. | NO APLICA                                  | NO APLICA   |

| N°                        | Requerimiento normativo  | Referencia<br>LFPDPPP | Referencia<br>Reglamento | Referencia<br>Recomendaciones  | Identificador y<br>nombre<br>Objetivo de Control | Descripción |
|---------------------------|--|-----------------------|--------------------------|--|--|-------------|
|                           | del responsable corresponderá al encargado.  |                       |                          |  |  |             |
| <b>CÓMPUTO EN LA NUBE</b> |  |                       |                          |  |  |             |
| 50                        | <p>Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente:</p> <p>a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento;</p> <p>b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;</p> <p>c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y</p> <p>d) Guardar confidencialidad respecto de los</p> |                       | Art. 52 - I              | <p>Paso 7.<br/>Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.<br/>Cumplimiento Cotidiano de Medidas de Seguridad.</p> | NO APLICA  | NO APLICA   |

| N° | Requerimiento normativo  | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones   | Identificador y nombre Objetivo de Control | Descripción |
|----|--|--------------------|-----------------------|--|--|-------------|
|    | datos personales sobre los que se preste el servicio.  |                    |                       |  |  |             |
| 51 | <p>Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para:</p> <p>a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;</p> <p>b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;</p> <p>c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio;</p> <p>d) Garantizar la supresión de los datos</p> |                    | Art. 52 - II          | <p>Paso 7.<br/>Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.<br/>Cumplimiento Cotidiano de Medidas de Seguridad.</p> | NO APLICA                                  | NO APLICA   |

| N°                    | Requerimiento normativo  | Referencia LFPDPPP | Referencia Reglamento                    | Referencia Recomendaciones   | Identificador y nombre Objetivo de Control | Descripción |
|-----------------------|--|--------------------|--|--|--|-------------|
|                       | <p>personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y</p> <p>e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.</p>  |                    |  |  |  |             |
| <b>TRANSFERENCIAS</b> |  |                    |  |  |  |             |
| 52                    | <p>Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento.</p> <p>El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.</p> | Art. 36            | Art. 68<br>Art. 71<br>Art. 72<br>Art. 74 | Paso 7.<br>Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad. | NO APLICA                                  | NO APLICA   |

| N° | Requerimiento normativo  | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones  | Identificador y nombre Objetivo de Control   | Descripción   |
|----|--|--------------------|-----------------------|---|--|---|
| 53 | Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.  |                    | Art. 69               | Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad. | NO APLICA  | NO APLICA   |
| 54 | En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable. |                    | Art. 70               | 1. Recomendación General  | <p>7.2.1 Enfoque de la Gestión del Riesgo.</p> <p>7.2.2 Criterios de evaluación del Riesgo.</p> <p>7.2.3 Criterio para el Impacto.</p> <p>7.2.4 Criterio para aceptación del Riesgo.</p> | <p>Desarrollo de un enfoque de la gestión del riesgo para abordar los criterios de evaluación, impacto, y aceptación de riesgos.</p> <p>Factores de la organización a considerar para la evaluación del riesgo.</p> <p>Factores de la organización a considerar para determinar el impacto de los riesgos.</p> <p>Definición de escalas y niveles de aceptación del riesgo.</p> |

| N° | Requerimiento normativo  | Referencia LFPDPPP | Referencia Reglamento | Referencia Recomendaciones  | Identificador y nombre Objetivo de Control                            | Descripción  |
|----|--|--------------------|-----------------------|---|---|--|
|    |  |                    |                       |   | 11 Comunicación y consulta del Riesgo de Seguridad de la Información. | Acciones para comunicar los riesgos de la organización a las partes interesadas. |
| 55 | La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales. |                    | Art. 73<br>Art. 75    | Paso 7.<br>Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.<br>Cumplimiento Cotidiano de Medidas de Seguridad. | NO APLICA   | NO APLICA  |