DEBERES	CONCEPTO
Artículo 32 LPDPPSO	**Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.**
Artículo 33 LPDPPSO	**Las medidas de seguridad adoptadas por el responsable deberán considerar:** **I. El riesgo inherente a los datos personales tratados;** **II. La sensibilidad de los datos personales tratados;** **III. El desarrollo tecnológico;** **IV. Las posibles consecuencias de una vulneración para los titulares;** **V. Las transferencias de datos personales que se realicen;** **VI. El número de titulares;** **VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y** **VIII. 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.**
Artículo 34 LPDPPSO	**Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:** **I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;** **II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;** **III. Elaborar un inventario de datos personales y de los sistemas de tratamiento de datos personales;** **IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;** **V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;** **VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;** **VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y** **VIII. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.**

Artículo 35 LPDPPSO	**Con relación a la fracción I del artículo anterior de la presente Ley, el responsable deberá incluir en el diseño e implementación de las políticas internas para la gestión y tratamiento de los datos personales al menos lo siguiente:** **I. Los controles para garantizar que se valida la confidencialidad, integridad y disponibilidad de los datos personas;** **II. Las secciones para restaurar la disponibilidad y el acceso a los datos personales de manera oportuna en caso de un incidente físico o técnico;** **III. Las medidas correctivas en caso de identificar una vulneración o incidente en los tratamientos de datos personales; IV. El proceso para evaluar periódicamente las políticas, procedimientos y planes de seguridad establecidos, a efecto de mantener su eficacia;** **V. Los controles para garantizar que únicamente el personal autorizado podrá tener acceso a los datos personales para las finalidades concretas, lícita, explícitas y legítimas que originaron su tratamiento, y** **VI. Las medidas preventivas para proteger los datos personales contra su destrucción accidental o ilícita, su pérdida o alteración y el almacenamiento, tratamiento, acceso o transferencias no autorizadas o acciones que contravengan las disposiciones de la presente Ley y demás que resulten aplicables.**
Artículo 36 LPDPPSO	**Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.** **Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia.**
Artículo 37 LPDPPSO	**De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:** **I. El inventario de datos personales y de los sistemas de tratamiento;** **II. Las funciones y obligaciones de las personas que traten datos personales;** **III. El análisis de riesgos;** **IV. El análisis de brecha;** **V. El plan de trabajo;** **VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y** **VII. El programa general de capacitación.**
Artículo 38 LPDPPSO	**El responsable deberá actualizar el documento de seguridad cuando ocurran los siguientes eventos:** **I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;** **II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;** **III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, e** **IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.**
Artículo 39 LPDPPSO	**En caso de que ocurra una vulneración a la seguridad, el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.**

Artículo 40 LPDPPSO	**Además de las que señalen las leyes respectivas y la normatividad aplicable, se consideran como vulnerables de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:** **I. La pérdida o destrucción no autorizada;** **II. El robo, extravío o copia no autorizada;** **III. El uso, acceso o tratamiento no autorizado, o** **IV. El daño, la alteración o modificación no autorizada.**
Artículo 41 LPDPPSO	**El responsable deberá llevar una bitácora de las vulnerabilidades a la seguridad ocurridas en la que se describa ésta, la fecha en la que ocurrió, el motivo de la misma y las acciones correctivas implementadas de forma inmediata y definitiva.**