

Conozca las responsabilidades de su rol de acuerdo a la Ley de Protección de Datos Personales.

Privacidad de Datos Personales. Roles y responsabilidades.

Una de las implicaciones de las regulaciones para los responsables del tratamiento de la Ley de Privacidad de los Datos Personales, se encuentra en la **designación formal de una función específica** y la incorporación de estas responsabilidades en la operación cotidiana del negocio. Esto permite atender las solicitudes respecto a estos datos por parte de sus dueños, y **fomentar la protección de los mismos en la organización como parte de una cultura corporativa.**

En los diferentes procesos de una organización, **los datos personales son obtenidos, utilizados, transmitidos, almacenados, destruidos, y su existencia puede darse por varios medios** (electrónicos, físicos, verbales y/o visuales), lo que implica que **las decisiones sobre su tratamiento y protección sean generadas a partir de la participación de diferentes funciones** en la organización relacionadas con cada fase y uso de los datos.

Si bien se requiere que todos los sectores de una compañía generen un tratamiento adecuado de datos personales, hay dos áreas vitales:

Jurídica/Legal.

Infraestructura Tecnológica y Seguridad.

Área Jurídica/Legal.

La participación del área responsable de los asuntos legales o jurídicos en la función de datos personales, puede seguir las siguientes medidas:

- ◆ Favorecer activamente el entendimiento de los requerimientos de las regulaciones de privacidad para toda la organización.

- ◆ Apoyar en la definición de iniciativas de mecanismos de cumplimiento de las regulaciones y protección de los Datos Personales de acuerdo a los términos de la normatividad.
- ◆ Asumir responsabilidad en la ejecución de procedimientos y mecanismos para atender las interacciones con las autoridades y dueños de Datos Personales según los términos de las regulaciones.
- ◆ Participar en la evaluación del nivel de riesgo aceptable relativo a los impactos para la organización por incidentes relacionados a Datos Personales.
- ◆ Asegurar la validez en términos de las regulaciones de los mecanismos de atención a solicitudes de los dueños de Datos Personales y protección de los mismos.
- ◆ Verificar de forma permanente los cambios en la normatividad aplicable a la privacidad de la información y las afectaciones al negocio en su contexto de operación para clasificar la información y seleccionar los mecanismos de control que permitan lograr el nivel de riesgo aceptable más rápido (más impacto, más probabilidades, más costo), con un sentido de negocio.

Área de Infraestructura Tecnológica y Seguridad.

La participación activa de las áreas responsables de la gestión tecnológica y seguridad de la información, tienen una participación directa a partir de aquellos requerimientos en las regulaciones que pueden implicar la implantación de un control técnico y el soporte a la operación del negocio. De esta forma, aconsejamos:

Identificar e implantar los controles técnicos de la información e infraestructura que favorecen el cumplimiento de las regulaciones de privacidad, como también el nivel de protección definido por la organización y los requerimientos de las autoridades correspondientes.

Apoyar en la definición de iniciativas de mecanismos técnicos de cumplimiento de las regulaciones y protección de los Datos Personales de acuerdo a los términos de la normatividad.

Asumir la responsabilidad en la ejecución de procedimientos y mecanismos para atender las interacciones con las autoridades y dueños de datos personales según los términos de las regulaciones, tales como:

- ◆ Respaldos de información.
- ◆ Gestión y control de incidentes de seguridad (brechas o fugas de información).
- ◆ Disociación de información.
- ◆ Destrucción y borrado de información.
- ◆ Control de acceso a los recursos de infraestructura y datos personales.
- ◆ Monitoreo de actividades en los recursos de infraestructura.
- ◆ Gestión de bitácoras y eventos de seguridad.
- ◆ Control de vulnerabilidades técnicas.

Participar en la obtención del nivel de riesgo aceptable relativo a los impactos para la organización por incidentes relacionados a Datos Personales.

Verificar de forma permanente los cambios en la normatividad aplicable a privacidad de la información y las afectaciones al esquema tecnológico de la organización en su contexto de operación.

Logre un tratamiento óptimo de la Ley de Privacidad de Datos Personales.

Solicite una consultoría personalizada de IBM