Guía para la implementación de la ley 1581 de 2012 de protección de datos personales en las empresas

Christian Fabián Delgado Anaya

1095840288

Manual para la implementación de la ley 1581 de 2012 de protección de datos personales en las empresas

UNIDADES TECNOLÓGICAS DE SANTANDER

Facultad Ciencias Naturales e Ingenierías

Ingeniería de sistemas

Bucaramanga, 15/06/2023

Guía para la implementación de la ley 1581 de 2012 de protección de datos personales en las empresas.

A continuación, describiré una serie de pasos que pueden ser de utilidad a la hora de implementar un sistema de gestión y protección de datos personales en las empresas, tal y como muestran los resultados de la investigación realizada en este proyecto de investigación.

El modelo de protección de datos personales consta de varias etapas, en cada una de las etapas se incluye una orientación para comprender el cumplimiento frente a la ley 1581 de 2012.

ETAPA 1: DIAGNOSTICO

DETERMINAR LA RESPONSABILIDAD DE LA PROTECCIÓN DE DATOS PERSONALES.

Defina un oficial de protección de datos o un equipo responsable de proteger los datos personales dentro de su organización. Este individuo o equipo garantiza la protección de los datos personales, pero la responsabilidad recae en todos los empleados de la empresa.

DETERMINA LA FINALIDAD DE LA RECOLECCIÓN DE DATOS PERSONALES Y ESTABLECE LA POLÍTICA DE PRIVACIDAD

Determina los datos personales que tu empresa recolecta o desea recolectar, así como el uso que darás a estos datos. Esta información será clave para que puedas establecer la política de tratamiento de datos personales, que será el corazón de tu sistema de protección de datos personales.

DESCRIBIR LA BASE DE DATOS

Identificar bases de datos que contengan información personal, ya sea privada, confidencial o pública. Una base de datos no significa necesariamente un software o un sistema de información. Una base de datos es como un archivador que almacena los currículos de los empleados de su empresa.

Si su organización cuenta con más de 100.000 UVT en total, debe registrar sus bases de datos en el Registro Nacional de Bases de Datos (RNBD) bajo el Reglamento 090 de 2018.

Tabla 1. Descripción Base de datos

Datos								
Procesos	**Subproceso**	**Nombre de la base de datos**	**Cantidad de usuarios**	**Finalidad de la base de datos**	**Norma del tratamiento de datos**	**Tipo de norma**	**Número de la norma**	**Año de expedición de la norma**
Proceso al que pertenece la base de datos	Subprocesos donde se le da uso a la base de datos	Nombre de la base de datos	Total de usuarios con acceso a la base de datos	Describir el uso que se le da a la base de datos	Registre si conoce alguna normatividad diferente a la ley 1581 de 2012 la cual nos obligue a realizar el tratamiento de los datos de la base de datos	Si existe alguna otra norma, especificar el nombre de la norma	Especificar el número de la norma	Especificar el año de expedición de la norma

Fuente: Autor

DEFINIR EL TRATAMIENTO DE LOS DATOS RECOLECTADOS

Tabla 2. Tratamiento de datos

Tratamiento de los datos			
Tipo de Base de datos	**Aplicativo**	**Tiempo de almacenamiento de los datos**	**Propósito de guardar los datos**
Describir si la base de datos es física o automatizada	¿En qué aplicación se encuentra la base de datos?	Describir el tiempo por el cual se almacenará la información	Tener claro el porqué de guardar la información

Fuente: Autor

IDENTIFICAR LOS DATOS PERSONALES

Datos Personales			
Publico	**Semiprivado**	**Privado**	**Sensible**
Para su recolección y tratamiento no requiere autorización del titular. **Ej.** Nombre, dirección.	Información que no es de naturaleza privada, ni publica su divulgación interesa a un grupo de personas en general **Ej.** Estado Financiero	Dato de carácter privado. Solo es de interés del titular de la información Para su tratamiento requiere de su expresa autorización **Ej.** Nivel de estudios, foto, correo.	Dato relacionado con la intimidad del titular, su tratamiento puede generar discriminación por lo que requiere autorización expresa. **Ej.** Estado salud, Origen étnico, huella.

ETAPA 2: PLANIFICACION

DEFINIR LAS OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO DE LOS DATOS PERSONALES

Una vez que las bases de datos que coinciden con las características del controlador de la información han sido identificadas en la Etapa 1, las obligaciones que se implementarán dentro de la organización deben validarse contra el artículo 18 "Obligaciones del controlador de la información" para planificar su implementación y cumplimiento según las medidas sugeridas en la Tabla 4.

Tabla 4. Medidas Articulo 18

Deberes del encargado de la información	***Acciones***
Debe garantizar que el titular siempre ejerza plenamente y efectivamente sus derechos de hábeas data.	Se requieren procedimientos de consulta y quejas.
Almacenar la información bajo las condiciones de seguridad necesarias para evitar su alteración, pérdida, inspección, uso y acceso no autorizado.	Se deben cumplir las condiciones de seguridad especificadas en el manual RNBD
Actualizar, rectificar o suprimir oportunamente los datos de conformidad con lo dispuesto en la presente ley.	Esto debe asegurarse en los procedimientos de consulta y denuncia.
Actualizar cualquier información reportada por su proveedor de atención primaria dentro de los 5 días hábiles posteriores a la recepción.	Esto debe asegurarse en los procedimientos de consulta y denuncia.
Tramitar las solicitudes y reclamaciones de los propietarios en los términos y condiciones previstos en esta Ley.	Esto debe asegurarse en los procedimientos de consulta y denuncia.
Adopción de manuales internos para asegurar el adecuado cumplimiento de esta ley, incluyendo políticas y procedimientos específicos para atender las solicitudes y reclamos de los propietarios.	El cumplimiento de las responsabilidades como controlador de información debe estar especificado en el manual interno para el tratamiento de datos personales.
Registrar los "pendiente" en la base de datos en la forma regulada por esta ley	Debe implementarse en bases de datos tanto físicas como digitales, tal como se indica en los registros de solicitudes y reclamos.
Incluir en la base de datos la "Información sobre deliberaciones judiciales" tan pronto como haya sido notificado por la autoridad competente de procedimientos judiciales relacionados con la calidad de sus datos personales.	Debe implementarse en bases de datos tanto físicas como digitales, tal como se indica en los registros de solicitudes y reclamos.

Tabla 4. Continuación

No difundir información que haya sido cuestionada por el propietario y ordenada a ser bloqueada por la Oficina de Industria y Comercio.	Se deben cumplir las condiciones de seguridad especificadas en el manual RNBD
Sólo permitir el acceso a la información a quienes tengan acceso a ella.	Se deben cumplir las condiciones de seguridad especificadas en el manual RNBD
Notificar a la Oficina de Industria y Comercio sobre violaciones al código de seguridad y riesgos en el manejo de la información del propietario	Esto debe asegurarse en los procedimientos de consulta y denuncia.
Seguir las instrucciones y requisitos de la Superintendencia de Industria y Comercio.	Su cumplimiento debe asegurarse consultando los documentos publicados por la SIC en su sitio web.

Fuente: Autor

ETAPA 3: IMPLEMENTACION

Según la propuesta presentada en virtud de la Ley 1581 de 2012 en el artículo 18 se detallan los siguientes pasos a seguir:

Establecer un mecanismo para recibir solicitudes de asesoramiento, actualizaciones, correcciones, reclamaciones, etc. respecto de sus datos personales. Para ello, configure canales como formularios web, buzones de correo, líneas telefónicas y direcciones de correo electrónico

DEFINIR LAS MEDIDAS DE SEGURIDAD DE LA INFORMACION

Tal como lo recomienda la SIC, se recomienda seguir las condiciones de seguridad del manual RNBD. Cabe señalar que la implementación de medidas de seguridad depende de las necesidades, presupuesto y capacidades de cada organización.

Tabla 9. Seguridad de la información personal

#	Seguridad de la información personal	Explicación	ISO 27001
1	¿Cuenta con un documento de seguridad de la información personal o general aprobado?	Un documento de seguridad de datos personales es un documento que contiene instrucciones y/o principios administrativos, humanos y técnicos que todas las áreas de la organización y cada uno de sus integrantes deben adoptar para cumplirlos durante el tratamiento de datos personales. Con el principio de seguridad especificado en la Ley 1581 de 2012, que está redactado textualmente en el artículo 4: "Principio de seguridad: La información especificada en esta ley procesada debe ser procesada con las medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad del archivo para evitar su falsificación, pérdida, investigación, uso o acceso no autorizado o fraudulento".	A.5
2	¿Ha documentado sus procesos de seguridad de datos personales?	Esto se refiere a la presencia de documentos que documenten los procesos relacionados con la seguridad de la información relacionada con los datos personales.	A.5
3	¿Tiene procedimientos para compartir responsabilidades y autorización para tratar datos personales?	Esto se refiere a si la(s) persona(s) responsable(s) del tratamiento de los datos personales en cada etapa del proceso y/o los procedimientos relacionados con ese tratamiento están documentados por escrito o de cualquier forma.	A.6
4	¿Tiene acuerdos de confidencialidad con cualquier persona que tenga acceso a la información personal?	Esto se relaciona con el principio de confidencialidad establecido en la Ley 1581 de 2012, que establece: El suministro o comunicación de datos personales sólo es posible en relación con la extinción de la relación con la empresa objeto del tratamiento y en atención al desarrollo de las actividades permitidas por esta Ley y su reglamento.	A.13
5	¿Existen controles de seguridad cuando se subcontratan servicios de procesamiento de datos personales?	Aborda los controles implementados en los procesos o tratamientos de datos realizados por terceros ajenos a la organización correspondientes a los responsables del tratamiento de datos personales.	A.15

Fuente: Autor

Tabla 10. Sistemas de seguridad de la información

#	Sistemas de seguridad de la información	Explicación	ISO 27001
1	¿Ha implementado herramientas de gestión de riesgos al procesar datos personales?	Las herramientas de gestión de riesgos son sistemas, controles y herramientas diseñadas para facilitar el proceso de prevención, contención y preparación en la capacidad de una organización para evitar, reducir o redirigir los efectos adversos o impactos de amenazas identificadas, métodos, etc. Análisis ambiental y su naturaleza en cada etapa del ciclo de datos. Los Responsables son libres de utilizar las herramientas y metodologías que necesiten, en función de sus necesidades y de las posibilidades de su organización. La metodología utilizada para la evaluación de riesgos debe estar documentada.	Dominio. 6.1;8,2;8, 3
2	¿Cuenta con un sistema de gestión de la seguridad de la información o un programa completo de gestión de datos personales?	En general, un sistema de gestión de seguridad de la información es La información o SGSI es un conjunto de directrices y/o políticas, gestión de personal y de información técnica. Este concepto se utiliza en varios estándares, principalmente en ISO/IEC 27001. Con respecto al Programa de Gestión Integral de Datos Personales PIGDP, es la implementación de medidas apropiadas y efectivas dentro de la organización para cumplir con las obligaciones establecidas en el artículo 6 de la Ley 1581/2012. El Decreto N° 1074 establece el principio de responsabilidad probada para el tratamiento de datos personales, y la	A.5
		Cámara de Comercio e Industria ha publicado una guía sobre la implementación del principio de responsabilidad probada en las organizaciones, disponible en el sitio web de la SIC www.sic.gov.co está abierto al público. A través de un SGSI o PIGDP, una organización diseña, implementa y mantiene un conjunto de procesos para gestionar de manera eficiente el acceso y uso de la información en general o de los datos personales en particular, con base en principios de seguridad. Dependiendo de la clasificación y naturaleza de los datos, aseguramos la confidencialidad, integridad y disponibilidad para minimizar los riesgos asociados al procesamiento de la información.	

Fuente: Autor

Tabla 11. Seguridad de la información personal en torno al recurso humano

#	Seguridad de la información personal en torno al recurso humano	Explicación	ISO 27001
1	¿Cuenta con controles de seguridad para los datos personales de recursos humanos antes de unirse y después de irse?	Políticas y controles relacionados con los recursos humanos asociados a la organización que tienen acceso a los datos personales antes, durante y después del desempeño de sus funciones. Por ejemplo, acuerdos de confidencialidad de la información, investigación de seguridad precontractual, ejecución pos contractual y control de perfiles de acceso a la información.	A.7

Fuente: Autor

Tabla 12. Control de acceso a la información personal

#	Control de acceso a la información personal	Explicación	ISO 27001
1	¿Cuenta con políticas para controlar el acceso a los datos personales tanto a nivel de instalación física como técnico?	Se deben implementar medidas o controles para regular el acceso a los datos personales. Estas políticas deben abordar tanto el acceso físico (a las instalaciones) como el acceso lógico (software, aplicaciones, usuarios, IP, contraseñas, etc.). Define quién tiene acceso a los datos personales y qué puede hacer exactamente con ellos.	A.9
2	¿Ha implementado políticas específicas para acceder a datos personales de bases de datos que contienen datos personales confidenciales?	Esto se relaciona con las directivas que regulan el acceso a los datos personales, pero los datos confidenciales (el uso indebido discrimina contra Se refiere específicamente al manejo de datos que puede dar lugar a Tipo de datos. Estas políticas deben abordar tanto el acceso físico (a la instalación) como el acceso lógico (software, aplicaciones, usuarios, IP, contraseñas, etc.) y definir, entre otras cosas, quién tiene permisos para esos datos.	A.8
3	¿Tiene una política para proteger la información personal?	Esto se refiere a si existe una política que especifique qué datos se respaldan. Esto depende de las definiciones de su organización de los tipos de datos, los períodos de retención, lo que se respalda, los medios de almacenamiento, la ubicación de las copias, las pruebas de recuperación, etc.	A.12

Fuente: Autor

Tabla 13.Procesamiento de información personal

#	Procesamiento de información personal	Explicación	ISO 27001
1	¿Cuenta con un procedimiento implementado para la validación de datos de entrada y procesamiento de la información personal, para garantizar que los datos recolectados y procesados sean correctos y apropiados, como confirmación de tipos, formatos, longitudes, pertinencia, cantidad, uso, etc.?	Esto tiene que ver con la exactitud de los datos y debe garantizarse en el momento de la recopilación. Por lo tanto, se deben utilizar técnicas de procesamiento y validación de datos de entrada para verificar el tipo, el formato, la longitud, la relevancia, la cantidad, el uso, etc., para minimizar el riesgo de errores y ataques de inyección de código.	A.14
2	¿Existen controles de seguridad de la información para validar los datos de salida?	Este control se relaciona con la precisión e integridad de los datos y tiene como objetivo garantizar y lograr los resultados esperados durante la recopilación y el procesamiento. Los datos de salida son los datos esperados. Entonces, si se acepta un campo con un tipo de datos definido, ese campo se conservará y otro campo no. relevancia de la información reportada según el propósito, similar al reporte; Así es como controlamos la exactitud, calidad y acceso no autorizado de la información.	A.9
3	¿Cuenta con procedimientos o controles establecidos con respecto a la disposición final de los datos personales (por ejemplo, eliminación, archivo, destrucción)?	Después de identificar los riesgos asociados con el procesamiento de datos en cada etapa, se deben implementar controles consistentes sobre el procesamiento final de la información. Se trata de la supresión (borrado seguro), destrucción o almacenamiento de datos de forma que no se utilicen o se expongan a un uso no autorizado, y suponga un riesgo tanto para el propietario como para el encargado del tratamiento.	A.8

DEFINIR MANUAL INTERNO EN PROTECCIÓN DE DATOS PERSONALES

De acuerdo al artículo 18 de la Ley 1581 de 2012, se propone incluir en el manual interno de una organización para el cumplimiento del tratamiento legal, los siguientes temas:

De acuerdo al artículo 18 de la Ley 1581 de 2012, se propone incluir en el manual interno de una organización para el cumplimiento del tratamiento legal, los siguientes temas:

- Procedimientos de consultas y quejas.
- Procedimientos implementados de gestión de Incidentes.
- Plan de sensibilización.
- Un proceso para auditar la seguridad de los datos personales. Esto permite la evaluación del cumplimiento, los resultados y la documentación de las medidas correctivas y/o preventivas relacionadas con el procesamiento de datos personales.
- Procedimiento o control implementado para la disposición final de la información personal (supresión, archivo, destrucción, etc.)
- Procedimientos de asignación de responsabilidades
- Control de acceso a la información personal, tanto en las instalaciones físicas como a nivel tecnológico.
- Proceso de respaldo de la información personal
- Proceso para el acceso remoto a la información personal
- Proceso para el tratamiento de la información en la recolección, uso, almacenamiento, transferencia y eliminación.
- Procedimientos para asegurar que la verificación de los datos ingresados y el tratamiento de los datos personales se lleven a cabo y que los datos recabados y tratados sean correctos y adecuados en cuanto a identificación de tipo, forma, cantidad, uso, etc.
- Proceso para validación de datos de salida.

ETAPA 4: EVALUACIÓN DE RIESGOS

IDENTIFICA Y GESTIONA LOS RIESGOS DE LOS DATOS PERSONALES

Identifique los riesgos potenciales que los datos personales pueden presentar para las actividades y procesos realizados por su organización. Analizarlos y evaluarlos para establecer planes de manejo y tratamiento para prevenir su ocurrencia. Por ejemplo, todos los contratos que firman las empresas (empleados, proveedores, alianzas) contienen cláusulas sobre confidencialidad y manejo de datos personales.

ETAPA 5: EVALUACIÓN DE DESEMPEÑO

AUDITORIA

Las organizaciones deben considerar planificar y realizar auditorías internas o externas para verificar el cumplimiento de manera objetiva y evitar conflictos de intereses en todo momento.

Se programarán periódicamente auditorías para garantizar que la organización cumpla con las políticas, los manuales de procesamiento de datos personales y los procedimientos definidos, y cumpla con todos los acuerdos de servicio y tecnología.

Es importante conservar la información documentada como prueba de los resultados de la auditoría y compartirla con la alta dirección. Los riesgos identificados a partir de los resultados de la auditoría se utilizan como observaciones que requieren una acción preventiva o correctiva inmediata, contribuyendo así al ciclo de mejora continua de la protección de datos personales de la organización.

ETAPA 6: MEJORA CONTINUA Y CAPACITACIÓN

Se deben tomar acciones correctivas y preventivas como resultado de la fase de evaluación de riesgos para lograr una mejora continua.

La mejora continua se puede dividir en dos tipos

- Acciones correctivas: Es una actividad para suprimir la causa del incidente y evitar que vuelva a ocurrir. Para abordar estas medidas, se debe considerar lo siguiente:

✓ Análisis y revisión del incidente.

✓ Causas que originen el incidente

✓ Acciones que adopta para evitar que el incidente se vuela a originar.

✓ Implementar dichas acciones.

✓ Documentar las consecuencias de las actividades implementadas.

✓ Evaluar la eficacia de las actividades implementadas

- Acciones preventivas: Son actividades encaminadas a suprimir las causas de incidentes relacionados con amenazas potenciales. Para abordar estas medidas, se debe considerar lo siguiente:

✓ Análisis de las amenazas

✓ Posibles incidentes que podrían generarse por una amenaza

✓ Acciones necesarias para evitar que el incidente ocurra

✓ Implementación de las actividades necesarias

✓ Documentar los resultados de las actividades

Estas acciones pueden implementarse periódicamente, según la importancia de la mejora y los recursos disponibles, o pueden abordarse tan pronto como se descubran, como antes de una auditoría externa.

CAPACITA A TODO EL PERSONAL

Si bien puede parecer excesivo capacitar a todos los empleados sobre la protección y el procesamiento de datos personales, la historia nos ha enseñado que esto es absolutamente necesario. Hay una triste historia de una gran empresa colombiana que tuvo que pagar millones de dólares en multas porque sus consultores de call center no proporcionaron información, proporcionaron información insuficiente o no cumplieron con los requisitos de servicio al cliente o área comercial. actualizar o corregir datos personales;