

MANUAL PARA PROTECCIÓN DE DATOS PERSONALES



CÓDIGO: DOCUMENTO 1

REVISIÓN:

FECHA: AGOSTO 2023

Página 1 de 31

ANTECEDENTES

Antecedentes

Del 23 y 27 de marzo de 2015 durante su 86º período ordinario de sesiones celebrado en su sede en Río de Janeiro, Brasil, el Comité Jurídico Interamericano (CJI) adoptó por consenso el informe sobre “Protección de Datos Personales” preparado por el Dr. David P. Stewart, Relator para el tema de acceso a la información pública y la protección de datos personales. Esto dio paso a lo que se conocerá como la **Ley Modelo sobre Protección de Datos Personales**.

El 20 de junio del año 2017, quedaron aprobados los **Estándares de Protección de Datos Personales** por los países miembros de la **Red Iberoamericana de Protección de Datos** (RIPD), de la cual Ecuador es miembro.

El 9 de julio del año 2018, el Ministerio de Telecomunicaciones y de la Sociedad de la Información, realizó el lanzamiento del Libro Blanco de la Sociedad de la Información y del Conocimiento (LBSIC), dicho libro es una guía para informar a la ciudadanía sobre las estrategias y líneas de acción que servirán para desarrollo de la Sociedad de la Información y del Conocimiento en Ecuador, a fin de impulsar el crecimiento económico, la equidad e inclusión y la eficiencia de la administración pública. **Una de sus ejes estratégicos es la Protección de Datos Personales**.

El 22 de octubre del año 2018, bajo el acuerdo ministerial No. 016-2018, se aprueba el **Plan Nacional de la Sociedad de la Información y del Conocimiento** (PNSIC), el cual en su capítulo 5 describe los programas del plan nacional. El 6^{to} programa describe, en tres proyectos, las acciones para garantizar la protección de datos personales. De este programa se desprende la acción estratégica clave para el Gobierno de “**Promulgar una Ley Orgánica de Protección de Datos Personales para garantizar el derecho constitucional**”

El 26 de mayo del año 2021 se publicó La **Ley Orgánica de Protección de Datos Personales** (LOPD), en Ecuador. El texto fue aprobado por la Asamblea Nacional y sancionado por el señor Presidente de la República. Desde esa fecha las empresas cuentan con un **período de adaptación de dos años** con el objetivo de poder adecuar todos sus procesos a lo exigido por esta nueva normativa.

Por tanto, el 26 de mayo del año 2023 **todo responsable del tratamiento de datos** y encargados de tratamiento de deben tener registros y pruebas de haber cumplido con las obligaciones listadas en el Capítulo VII, artículo 47 en sus numerales del 1 al 15.

OBJETO

El objeto y finalidad de este manual es servir de referencia de la ruta transitada para lograr la documentación de las políticas de protección de datos personales y el plan inicial para protección de datos personales bajo los requisitos de la Ley orgánica para protección de datos personales del Ecuador (LOPDP:2021).

Para lograrlo el manual presenta 1 documento que servirá de muestra de cómo procedimientos, rutinas, comunicados, infografías y ejercicios técnicos han sido redactados, diseñados y realizados. El manual servirá de apoyo para capacitaciones, uso durante auditorías internas (primera parte) y auditorías contratadas (segunda parte), evitando subjetividades.

OBJETIVOS

1. Satisfacer el capítulo VIII, artículo 52, de la Ley de Protección de Datos Personales, que solicita Responsabilidad Proactividad y demostrada por parte del responsable del Tratamiento de los datos Personales.
2. Describir la secuencia de actividades realizadas para definir y redactar las políticas de protección de datos personales que servirán de marco regulatorio para llevar a cabo las acciones, medidas y herramientas en las áreas jurídicas, organizativas, administrativas, técnicas y físicas descritas en el plan inicial para protección de datos personales bajo los requisitos de la LOPDP:2021
3. Describir la estrategia definida para la culminación del proyecto PDP-Royaltex, la cual posee las siguientes dos etapas:
 - a. Etapa I:
 - i. Fase 1: Documentación de la política PDP y el plan inicial PDP
 - ii. Fase 2: Implementación del plan inicial PDP
 - iii. Fase 3: Activación de la mejora continua y la gestión de riesgos
 - b. Etapa II:
 - i. Fase 1: Primer plan de mejora continua
 - ii. Fase 2: Gestión de riesgos
4. Satisfacer los requisitos de documentación que permitan no ser sujetos a sanciones descritas en el régimen sancionatorio de la LOPDP:2021
5. Articular toda la documentación que permita a los usuarios del manual poder implantar y administrar el esquema de protección de datos personales.

ALCANCE

El manual recoge la documentación desarrollada para completar la fase I de la primera etapa del proyecto PDP-Megabrokers. Específicamente, el plan inicial de protección de datos personales (PIPDP) y las políticas para protección de datos personales (PPDP), para cada una de las cinco áreas donde la LOPDP:2021, solicita medidas y herramientas

MANUAL PARA PROTECCIÓN DE DATOS PERSONALES



OBJETO, OBJETIVOS, ALCANCE y LIMITANTES DEL ESQUEMA SKILLMAN- PDP

CÓDIGO: DOCUMENTO 2

REVISIÓN:

FECHA: AGOSTO 2023

Página 3 de 31

que mitiguen los riesgos identificados en la realización de las actividades de tratamiento con datos personales (ATD).

El esquema de seguridad se enfoca en los puestos de trabajo donde se traten datos personales (PATD) y la ruta que los trabajadores de esos puestos, utilizan para realizar las actividades de tratamiento de datos personales bajo su responsabilidad. Un ejemplo de la caracterización de un PATD se muestra en la siguiente figura:

CARACTERIZACIÓN DE PUESTOS CON ACTIVIDADES DE TRATAMIENTO											
PUESTO DE TRABAJO	TRATAMIENTO	TIEMPO	FINALIDAD	DATOS QUE SE UTILIZAN	MÉTODO DE ANONIMIZACIÓN	BASES DE LEGITIMACIÓN	SERVIDOR	RUTA DIGITAL	ETD CONTRATO	DDP LICITUD	DERECHOS AREE Y CONSERVACIÓN DATOS

LISTADO DE AMENAZAS:

PUESTO DE TRABAJO CON ACTIVIDAD DE TRATAMIENTO DE DATOS PERSONALES



LIMITANTES

En el desarrollo de este manual se encontraron algunas circunstancias limitantes que no están bajo el control de la organización. Sin embargo, listándolas en este manual se podrán superar en el momento que las circunstancias cambien y se den las condiciones para satisfacer los requisitos que a la fecha no pueden ser atendidos ni satisfechos. Dentro de ellos se puede mencionar que el régimen sancionatorio de la LOPDP ecuatoriana entró en vigencia el 26 de mayo del 2023 y a la fecha aún existen los siguientes vacíos:

1. Cap VI, art 39 (PDP desde el diseño y por defecto): se debe realizar bajo los términos del reglamento.
2. Cap VI, art 43 (Notificación de vulneración de la seguridad): se debe informar a la Autoridad de PDP y a la agencia de regulación y control de las telecomunicaciones, en menos de cinco (5), días y aún no está nombrada el superintendente de PDP
3. Cap VII, art 47 #1, #2, #8, #11, #12 (RNDP), #14 y #15: No hay autoridad PDP, no hay reglamento, no hay normativa ni regulación emitida por la autoridad PDP, en esta materia.
4. Cap VII, art 48 (DPDP), #2, #3 (reglamento), #4 (2do párrafo): No hay autoridad PDP, no hay reglamento, no hay normativa ni regulación emitida por la autoridad PDP, en esta materia.
5. Cap VII, art 49 (funciones DPDP), #1, #2, #4, #5: No hay autoridad PDP, no hay reglamento, no hay normativa ni regulación emitida por la autoridad PDP, en esta materia. (la evaluación de riesgo, controles e impacto quedan como preliminares)
6. Cap VII, art 51 (registro nacional de PDP): no está creado y depende de la Autoridad PDP
7. Cap VIII, art 53 (códigos de conducta): no hay reglamento, ni modelos aprobados por la autoridad, ni normativa emitida por la autoridad.
8. Cap VIII, art 54 (entidades de certificación): no hay ninguna acreditada por la Autoridad PDP para que realicen auditorías de segunda parte que activen el régimen sancionatorio.
9. Cap. IX (Transferencia Internacional DP), art 56 (transferencia a países "liberados"): No hay reglamento, No hay autoridad PDP, no hay listado de países.
10. Cap. IX (Transferencia Internacional DP), art 57 (transferencias mediante garantías adecuadas): No hay reglamento, No hay autoridad PDP (RTD debe cubrir los requisitos que están bajo su radio de control)
11. Cap. IX (Transferencia Internacional DP), art 58 (Normas corporativas vinculantes): No hay reglamento, No hay autoridad PDP que defina los formatos, Sin embargo, el RTD debe cubrir los requisitos que están bajo su radio de control (hasta el primer párrafo del numeral 11)



MANUAL PARA PROTECCIÓN DE DATOS PERSONALES

CÓDIGO: DOCUMENTO 2

REVISIÓN:

OBJETO, OBJETIVOS, ALCANCE y LIMITANTES
DEL ESQUEMA SKILLMAN- PDP

FECHA: AGOSTO 2023

Página 5 de 31

12. Cap. IX (Transferencia Internacional DP), art 59 (Autorización para trans. Intnl): No hay reglamento, No hay autoridad que otorgue la autorización.
13. Cap. IX (Transferencia Internacional DP), art 61 (control continuo) No hay reglamento, No hay autoridad PDP que entregue información actualizada sobre listados de países “autorizados” y “no autorizados”
14. Cap. X (procedimiento administrativo), art 62, art 63 y art. 64: No hay autoridad PDP que acompañe y de trámite a los reclamos por parte del titular de los datos

El primer paso para iniciar la documentación de un sistema de gestión es la caracterización de los procesos que permitirán dar seguimiento a las actividades críticas que deben completarse en cada uno de esos procesos y así garantizar la entrega a tiempo del resultado esperado dentro de los estándares de calidad estipulados.

En el caso de un sistema de gestión para garantizar protección de datos personales el enfoque de la caracterización recae sobre las actividades en las que se realizan tratamiento de datos personales (ATD), no sobre los procesos donde estas actividades se encuentran inmersas.

El beneficio de hacerlo de esta manera, es ganar tiempo evitando la revisión de la documentación de los procesos y los manuales de procedimientos existentes ya que, en muchas ocasiones, lo que está escrito en esos manuales no tiene relación con la realidad de la operación. Resulta, entonces, más sencillo identificar todas aquellas actividades en donde se solicitan datos personales a los titulares de los datos o se logra acceder a bases de datos (físicas o digitales), que contengan datos personales.

Estas actividades suelen realizarse en cuatro ámbitos:

Ámbito WEB: Si la empresa posee portal donde por el giro de negocio solicite a los internautas datos personales o si dentro de las actividades de busca de clientes se visitan páginas WEB para descargar nombres, direcciones o números telefónicos para contactar a los titulares de esos datos personales.

Ámbito digital: Es la infraestructura digital de las organizaciones para conservar bases de datos digitales que contengan datos personales de trabajadores, proveedores, clientes y otras partes interesadas.

Ámbito físico-estático: Los puestos de trabajo donde se realizan actividades rutinarias con manejo de datos e información y para lo cual se accede a archivadores físicos y digitales o se comparten bases de datos con otros puestos de trabajo. Todas estas opciones deben ser identificadas y listadas.

Ámbito físico-móvil: En muchas organizaciones el equipo de trabajo es portátil (laptop, Tablet, smartphone, otros), e incluso permiten que se conserven datos e información en memorias portátiles (pen drive, hard drives portátiles, otros), o una práctica más reciente el acceso a bases de datos en lo que se conoce como "La nube".

Para cada uno de estos ámbitos se deben identificar y listar las actividades donde se utilizan datos personales. para la realización de esta actividad se puede utilizar un formato similar al que se muestra en la siguiente figura:

INVENTARIO DE ACTIVIDADES DE TRATAMIENTO

NOMBRE	CARGO	DESCRIPCIÓN DE CARGO	SOLICITA DATOS PERSONALES	ACCEDE A BASE DE DATOS PERSONALES
			SI NO	SI NO
BASES DE DATOS FÍSICAS		TIENEN CONTROL DE ACCESO (CLAVE, LLAVES, BIOMÉTRICO, OTRO)		COMPARTE ARCHIVOS CON DATOS PERSONALES (EXCEL, WORD, PDF, IMÁGENES, OTROS)
	SI NO	SI NO		SI NO
BASES DE DATOS DIGITALES	DISTINTAS PLATAFORMAS O SERVIDORES (ERP'S, CRM'S, NUBE PÚBLICA, OTROS)	TODAS CUENTAN CON CONTROL DE ACCESO (CLAVE, LLAVES, BIOMÉTRICO, OTRO)		COMPARTE ARCHIVOS CON DATOS PERSONALES (EXCEL, WORD, PDF, IMÁGENES, OTROS)
	SI NO	SI NO	SI NO	SI NO



ACTIVIDADES CON DATOS PERSONALES	DATOS QUE SE RECOGEN	FINALIDAD	TIEMPO	TIPO DE REGISTRO	REPOSITORIO
•				IMPRESO DIGITAL	CARPETA EXCEL PLATAFORMA
•				IMPRESO DIGITAL	CARPETA EXCEL PLATAFORMA
•				IMPRESO DIGITAL	CARPETA EXCEL PLATAFORMA
•				IMPRESO DIGITAL	CARPETA EXCEL PLATAFORMA

Con esta información se logra identificar que actividades con datos personales realiza cada uno de los trabajadores de un departamento. El responsable del portal WEB de la organización debe incluir en su departamento las actividades donde desde el portal se solicitan datos personales a los internautas o si dentro de las actividades de alguno de los puestos de trabajo está la búsqueda de datos personales en portales WEB de acceso público.

Luego de listadas las actividades de tratamiento el siguiente paso es identificar las bases de licitud que son un requisito de la LOPDP:2021 en su artículo 7. Para este fin se puede utilizar un formato como el que muestra la siguiente imagen:

PRIORIZACIÓN DE ACTIVIDADES DE TRATAMIENTO DE DATOS PERSONALES

- a.- GIRO DE NEGOCIO
- b.- OBLIGATORIAS
- c.- ENCARGADAS
- d.- DESTINATARIOS
- e.- OPERATIVAS DATOS ESPECIALES
- f.- OPERATIVAS DIVERSAS

TRATAMIENTO	PUESTO DE TRABAJO	TRATANTE	DATOS QUE SE SOLICITAN	BASE LEGITIMACIÓN 1	BASE LEGITIMACIÓN 2	BASE LEGITIMACIÓN 3
Ventas en tiendas			Nombre, apellido, #cedula, dirección domicilio, firma personal	LOPDP 7.2 (ley régimen tributario)	LOPDP 7.5 Contrato compra-venta	LOPDP 7.1 Consentimiento del titular
Ventas en la WEB (facturación)			Nombre, apellido, #cedula, dirección domicilio, firma personal	LOPDP 7.2 (ley régimen tributario)	LOPDP 7.5 Contrato compra-venta	LOPDP 7.1 Consentimiento del titular
Ventas en la WEB (envíos)			Nombre, apellido, dirección de entrega, #telefónico, correo electrónico	LOPDP 7.2 (ley régimen tributario)	LOPDP 7.8 (Interés legítimo de cumplimiento servicio)	LOPDP 7.1 Consentimiento del titular
Ventas en la WEB (promoción)			Fechas conmemorativas	LOPDP 7.1 Consentimiento del titular		
Ventas empleados			Nombre, apellido, #cedula, dirección domicilio, firma personal	LOPDP 7.2 (ley régimen tributario)	LOPDP 7.5 Contrato compra-venta	LOPDP 7.1 Consentimiento del titular
Pasarelas – videos (modelos de ropa)			Nombre, apellido, #cedula, dirección domicilio, firma personal	LOPDP 7.2 (ley régimen tributario)	LOPDP 7.5 Contrato servicios	LOPDP 7.1 Consentimiento del titular
Campañas tik-toc con empleados			Imágenes	LOPDP 7.1 Consentimiento del titular		
Ejercicio de derechos AREO			Los que solicite el titular de los datos	LOPDP 7.2 (Art. 13-14-15-16)		

tener identificadas mas de una base de licitud es una herramienta importante para redactar los comunicados de información previa que es un derecho de los titulares de los datos y una condición para que el consentimiento que otorgue el titular para que se realicen actividades de tratamiento con sus datos, no quede viciado.

El artículo 5 de la LOPDP:2021 lista a los integrantes del sistema de protección de datos personales ecuatoriano. Este listado toma importancia al momento que el sistema toma vida y ritmo operativo. Las interacciones en este “ecosistema PDP” están reguladas por la LOPDP:2021, su reglamento, la normativa aplicable por sector económico y las mejores prácticas reconocidas internacionalmente. En este sentido, tener identificados a los organismos con los que la organización deba interactuar es muy relevante y evita infracciones y quedar expuesto a sanciones.

Para identificar y documentar a todos los integrantes se puede utilizar un formato como el que se muestra en la siguiente imagen:

 <p>MANUAL PARA PROTECCIÓN DE DATOS PERSONALES</p> <p>TRATAMIENTOS Y LEGITIMACIÓN</p>			CÓDIGO: INFOGRAFÍA 5 REVISIÓN: FECHA: MAYO 2023 Página: 1 - 1
FIGURA RESPONSABLE DE TRATAMIENTO (RTD)	DESIGNADO	CORREO ELECTRONICO	FIGURA REGISTRO NACIONAL BASES DE DATOS (RNBD)
FIGURA ENCARGADO DEL TRATAMIENTO (ETD)	DESIGNADO	CORREO ELECTRONICO	FIGURA ENTIDADES CERTIFICADORAS ACREDITADAS (ECA)
FIGURA DESTINATARIO (DTD)	DESIGNADO	CORREO ELECTRONICO	FIGURA REGISTRO NACIONAL INCUMPLIDOS (RNI)
FIGURA DELEGADO DE PROTECCIÓN DATOS (DPD)	DESIGNADO	CORREO ELECTRONICO	FIGURA PAISES AUTORIZADOS PARA TRANSFERENCIA (PATr)
FIGURA AUTORIDAD DE PROTECCIÓN DE DATOS (APDP)	DESIGNADO SIN DESIGNAR	CORREO ELECTRONICO	FIGURA OTRAS ENTIDADES INTERESADAS (EIBD)

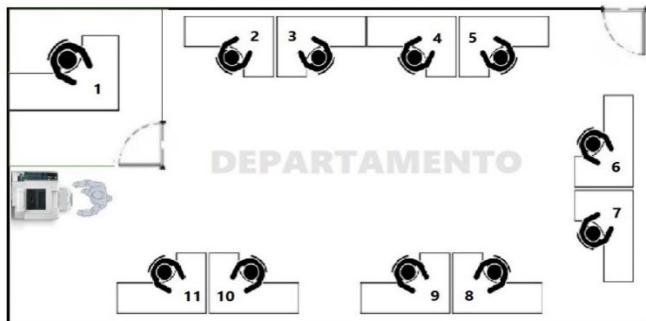
UBICACIÓN Y CARACTERIZACIÓN DE PATD

Como se menciona en el documento 3, en la descripción del ámbito físico-estático, identificar los puestos de trabajo donde se realizan actividades donde se tratan datos personales o se accede a bases de datos donde existen datos personales (PATD), es relevante para definir rutinas que garanticen la seguridad y protección de los datos personales y de las bases de datos.

La caracterización de los PATD también facilita la identificación de la ruta de los datos personales y la identificación de las herramientas digitales que están instaladas para proteger los ordenadores y la plataforma digital de ser alcanzadas por intrusos, virus u otros malwares que puedan significar una vulneración a la seguridad de la información o de los datos.

La siguiente imagen muestra un ejemplo de como se puede caracterizar un PATD y como documentar una carpeta donde se enumeren y se ubiquen los PATD de una organización mediante un croquis o esquemático de las oficinas.

IDENTIFICACIÓN DE PUESTOS CON ACTIVIDAD DE TRATAMIENTO DE DATOS PERSONALES



PUESTO DE TRABAJO CON ACTIVIDAD DE TRATAMIENTO DE DATOS PERSONALES



PRIORIZACIÓN DE ACTIVIDADES DE TRATAMIENTO DE DATOS PERSONALES

- a.- GIRO DE NEGOCIO
- b.- OBLIGATORIAS
- c.- ENCARGADAS
- d.- DESTINATARIOS
- e.- OPERATIVAS DATOS ESPECIALES
- f.- OPERATIVAS DIVERSAS

TRATAMIENTO	PUESTO DE TRABAJO	TRATANTE	DATOS QUE SE SOLICITAN	BASE LEGITIMACIÓN 1	BASE LEGITIMACIÓN 2	BASE LEGITIMACIÓN 3
Ventas en tiendas			Nombre, apellido, dirección de correo electrónico, firma personal	LOPD 7.2 (ley régimen tributario)	LOPD 7.5 Contrato compraventa	LOPD 7.1 Consentimiento: otorgador
Ventas en la WEB (facturación)			Nombre, apellido, dirección de correo electrónico, firma personal	LOPD 7.2 (ley régimen tributario)	LOPD 7.5 Contrato compra venta	LOPD 7.1 Consentimiento: otorgador
Ventas en la WEB (envío)			Dirección de entrega # facturación, correo electrónico	LOPD 7.2 (ley régimen tributario)	LOPD 7.0 Interés legítimo: no cumplimiento de servicio	LOPD 7.1 Consentimiento: otorgador
Ventas en la WEB (promoción)			Itinerarios	LOPD 7.1 Consentimiento: otorgador		
Ventas empleados			NOMBRE, apellido, dirección doméstica, firma personal	LOPD 7.2 (ley régimen tributario)	LOPD 7.5 Contrato compraventa	LOPD 7.1 Consentimiento: otorgador
Passarelas - videos (modelos de ropa)			NOMBRE, apellido, dirección doméstica, firma personal	LOPD 7.2 (ley régimen tributario)	LOPD 7.5 Contrato servicios	LOPD 7.1 Consentimiento: otorgador
Campañas lik-toe con empleados			Imagenes	LOPD 7.1 Consentimiento: otorgador		
Ejercicio de derechos AREEQ			Lote que solicita el titular de los datos	LOPD 7.2 (ley 15/2012)		

MANUAL PARA PROTECCIÓN DE DATOS PERSONALES



UBICACIÓN Y CARACTERIZACIÓN DE PATD

CÓDIGO: DOCUMENTO 5

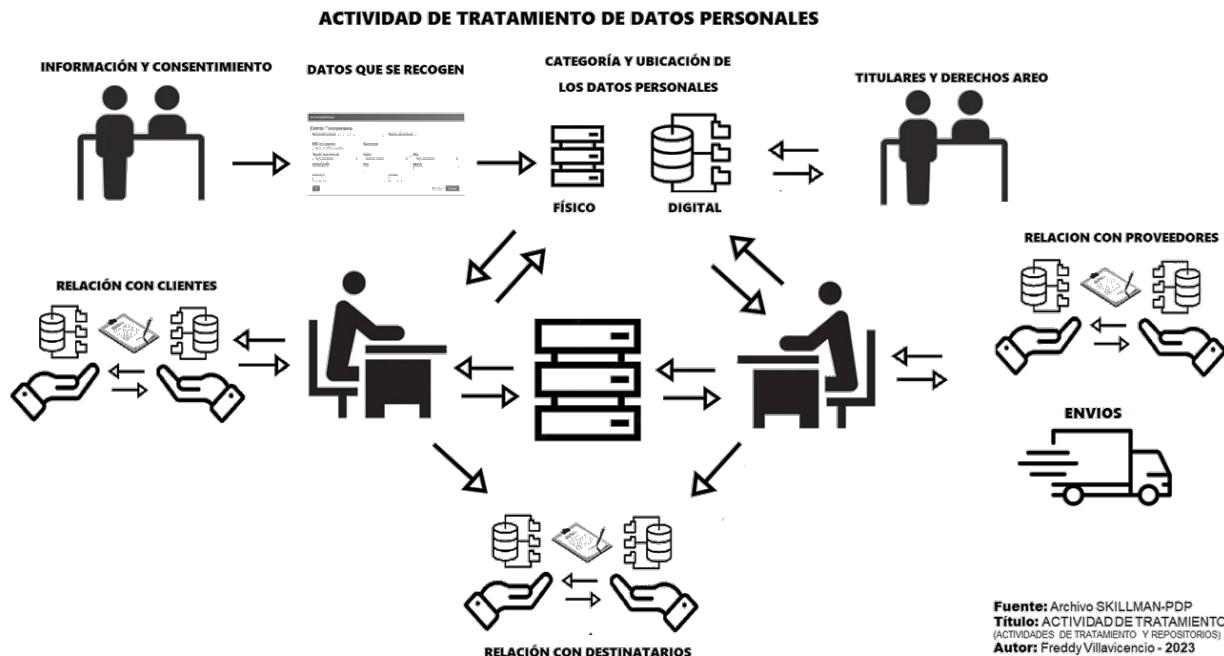
REVISIÓN:

FECHA: septiembre
2023

Página 11 de 31

Otra caracterización importante de un PATD es la manera de como se obtienen los datos personales requeridos por la actividad de tratamiento específica. Esta manera o ruta de acceso poseen algunas variantes que se muestran en las siguientes imágenes.

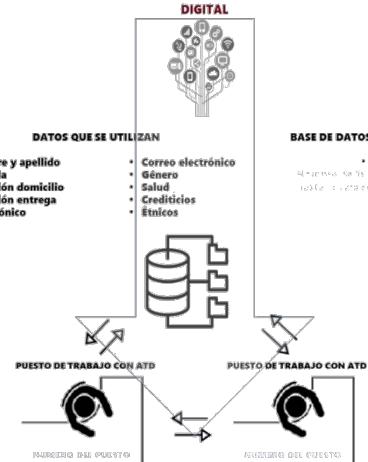
Esta imagen muestra de manera general todas las posibles variantes de rutas de datos



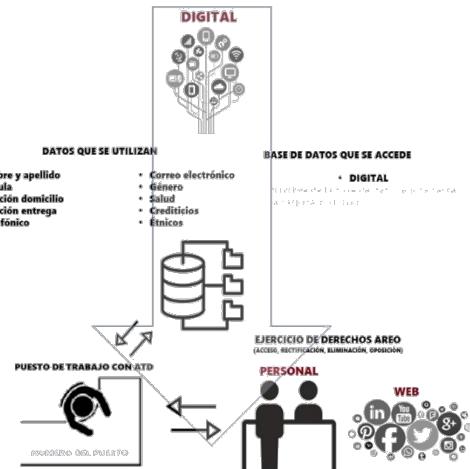
Las siguientes imagines muestran desde que ámbito se recogen los datos y con quien se encargan o transfieren los datos personales para completar la actividad de tratamiento



OPERACIONES INTERNAS CON DATOS PERSONALES



EJERCICIO DE DERECHOS ARO



MANUAL PARA PROTECCIÓN DE DATOS PERSONALES

CÓDIGO: DOCUMENTO 5



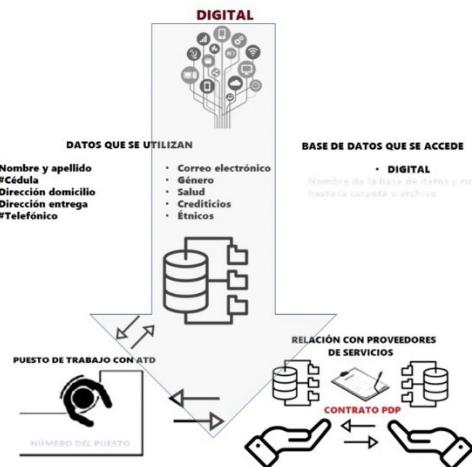
REVISIÓN:

FECHA: septiembre
2023

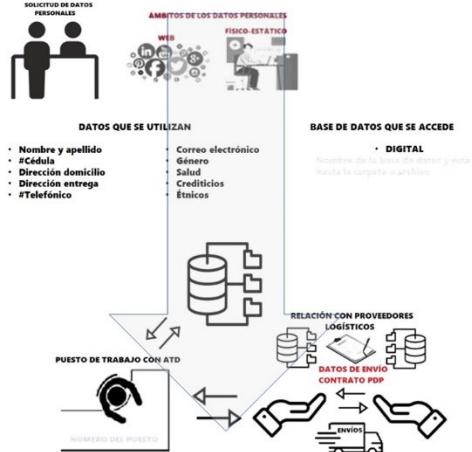
UBICACIÓN Y CARACTERIZACIÓN DE PATD

Página 12 de 31

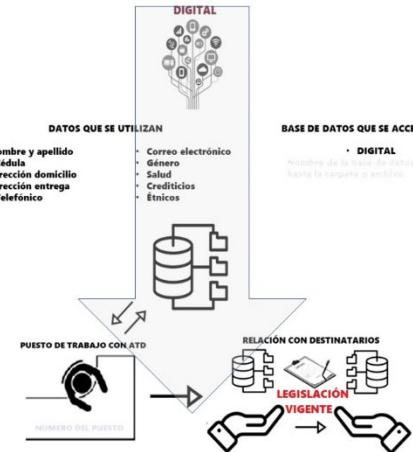
RUTA DE LOS DATOS CON ETD



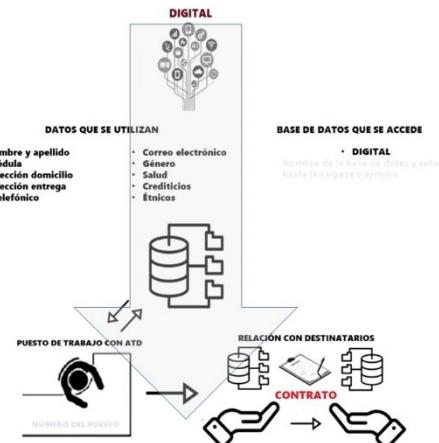
SERVICIOS LOGÍSTICOS DE ENTREGA



RELACIÓN CON ECOSISTEMA PDP DESTINATARIOS



COMUNICACIÓN A PARTES INTERESADAS OTROS DESTINATARIOS





MANUAL PARA PROTECCIÓN DE DATOS PERSONALES

CÓDIGO: DOCUMENTO 6

CATÁLOGO DE CATEGORÍAS Y TIPOS (DATOS, ECOSISTEMA PDP, ATD's, PATD's, RUTAS DE ACCESO POR ATD)

REVISIÓN:

FECHA: OCTUBRE 2023

Página 13 de 31

La LOPDP:2021 en el capítulo IV, lista y describe las categorías especiales de datos personales y determina como los datos personales de estas categorías deben ser tratados. Los datos personales que no estén dentro de estas categorías serán categorizados como datos personales "comunes" y aquellos que no sean datos personales serán categorizados como "otro tipo de datos", dentro de los cuales podrán figurar los datos técnicos, datos estadísticos, datos contables, datos de producto y muchos otros tipos de datos.

Al igual que los datos las interacciones que se llevan a cabo dentro del ecosistema PDP de las organizaciones diversifican los tipos de actividades de tratamiento, tipos de puestos de trabajo, tipos de ruta de acceso y entrega de los datos y algunas otras tipologías que deben ser listadas, descritas y documentadas.

Se recomienda agrupar esta documentación en un documento que puede ser titulado como el catálogo de categorías y tipos. En este catálogo que servirá de referencia rápida para poder realizar un mejor análisis de los riesgos que entrañan las actividades de tratamiento.

CATEGORIZACIÓN Y TIPOLOGÍA DE ELEMENTOS INTERNOS

	CATEGORÍA	TIPOS
DATOS	• Especiales	Biométricos, niños y adolescentes, de salud, crediticios, sensibles
	• Comunes	De identidad, de dirección, de contacto telefónico, de contacto en redes sociales,
	• Otros	Estadísticos, de producto, contables, financieros, otros
PUESTOS DE TRABAJO	• Sin tratamiento a datos personales	
	• Con tratamiento a datos personales	
RUTAS DE ACCESO BASES DE DATOS	• Bases de datos personales - especiales	
	• Bases de datos personales - comunes	
	• Otras bases de datos	
ACTIVIDADES DE TRATAMIENTO	• Obligatorias	Plataforma IESS, Min. Trabajo, UAFE, SRI,
	• Giro del negocio	Solicitud de consentimiento, facturación, entregas a domicilio,
	• Operativas - interés legítimo	Control de asistencia, pago de nómina, vinculación, desvinculación
	• Operativas - beneficios	Descuentos en comercios, viajes y hospedajes, becas de estudio
	• Otras operativas	Productividad, programación de jornadas, evaluación de desempeño

Para un correcto seguimiento a un proyecto de donde se debe diseñar, documentar, implantar, mantener y evaluar de manera periódica la eficiencia del mismo, lo más recomendable es dividir al proyecto en etapas y a cada una de esas etapas definirle fases y a cada una de estas fases un plan de trabajo con revisiones frecuentes. De no hacerlo así, existe un alto riesgo que perdamos el control de los avances, lo cual degenera en sobrecostos y retrasos.

Para el proyecto PDP, Royaltex diseño la estrategia que muestra la siguiente imagen:

PROYECTO PDP ROYALTEX



Estratégicamente se decide dividir al proyecto en dos etapas. La etapa I tiene como objetivo activar la mejora continua (requisito LOPDP:2021, art. 47.3), activar la gestión de riesgos (requisito LOPDP:2021, art. 47.7) y en el proceso de avance capacitar y facultar a los equipos de administren esos procesos con la ayuda del delegado de protección de datos (requisito LOPDP:2021, art. 48).

En la etapa II los equipos de auditores internos y el comité de crisis, inician el trabajo de seguimiento a los indicadores de gestión definidos en el plan de mejora resultante de la primera auditoría interna.

La declaración de aplicabilidad es el compromiso de la dirección con respecto a las acciones, medidas y herramientas que permitan mitigar el efecto negativo de los riesgos que entrañan el contexto organizacional sobre la adecuada evolución del proyecto PDP y de los riesgos que entrañan las actividades de tratamiento de datos de manera particular.

En resumen, en la etapa I el compromiso de la dirección será invertir lo mínimo necesario para completar las tres fases de la etapa I. de esta manera quedarían cubiertos todas las obligaciones de responsable del tratamiento descritos en el capítulo VII de la LOPDP:2021, en el artículo 47 y específicamente en 47.1 y 47.2

la declaración de aplicabilidad está al inicio de la carpeta donde se conservan los registros del ejercicio de análisis del contexto organizacional y la evaluación de riesgos a los PATD. La misma tiene el formato que muestra la siguiente imagen:

DECLARACIÓN DE APLICABILIDAD

Declaración de aplicabilidad de controles y acciones mitigadoras de los riesgos identificados:

1. El proyecto está separado en dos etapas.
 2. La etapa I está dividida en tres fases: Documentación + implantación + activación mejora continua y gestión del riesgo
 3. El equipo de documentación no es el designado para completar las fases 2 y 3
 4. El plan inicial PDP está diseñado para asegurar que se completen las 3 fases de la etapa I
 5. Las rutinas iniciales PDP en cada PATD, representan la herramienta sistemática para mantener vigiladas a las actividades de tratamiento de datos personales.
 6. Luego de completada la fase 3, la medida prioritaria de la etapa II, será la inclusión de controles adicionales a las rutinas PDP de cada PATD, tomados de la norma INEN ISO/IEC 27002:2022
 7. Esta declaración de aplicabilidad describe como serán aplicados los controles iniciales (mitigación de riesgos que impidan completar las tres fases) y los controles complementarios (Controles tomados de la norma INEN ISO/IEC 27002:2022) para fortalecer las rutinas PDP y la gestión de riesgos en la etapa II
- 8. Controles, medidas y herramientas iniciales:**
- a. Se debe realizar una evaluación de impacto sobre el ejercicio de derechos a las acciones, medidas y herramientas seleccionados para evitar que el contexto organizacional impida la implantación del esquema PDP bajo los requisitos de la LOPDP:2021
 - b. Con el resultado de la evaluación de impacto inicial se priorizará que actividades de tratamiento deberán ser revisadas, modificadas o eliminadas luego de culminada las tres fases de implantación del esquema PDP bajo los requisitos de la LOPDP:2021.
 - c. Los que mitigen los riesgos inducidos por el contexto interno de la organización con respecto a la culminación de las fases del proyecto PDP
 - d. Los que mitigen los riesgos inducidos por el contexto externo de la organización con respecto a la culminación de las fases del proyecto PDP
 - e. Los que mitigen los riesgos asociados al régimen sancionatorio en cada una de las cinco áreas donde la LOPDP:2021 solicita controles, medidas y herramientas
 - f. Los que mitigen los riesgos inherentes a los puestos con actividades de tratamiento de datos personales (PATD)
 - Cumplir el plan progresivo de activación de los PATD priorizados por la tipología y ámbito de las actividades de tratamiento (giro de negocio, encargadas, obligatorias, comunicadas, operativas, otras)
 - Cumplir con el plan progresivo de seguridad física
 - Cumplir con el plan progresivo de ciber seguridad
 - g. Estas acciones se completan en las fases 2 y 3
- 9. Controles, medidas y herramientas complementarios:**
- a. Realizar un revisión punto a punto de la norma INEN ISO/IEC 27002:2022 sobre cada uno de los PATD
 - b. Realizar una selección de los controles aplicables a cada PATD
 - c. Realizar una evaluación de impacto sobre el ejercicio de derechos a los controles seleccionados a cada una de las acciones de tratamiento de datos personales en cada PATD
 - d. Estas acciones se iniciaran con el primer plan de mejora continua



MANUAL PARA PROTECCIÓN DE DATOS PERSONALES

CÓDIGO: DOCUMENTO 9

REVISIÓN:

COMUNICADOS, CLÁUSULAS, CUESTIONARIO PDP,
RESPUESTAS AL ECOSISTEMA PDP

FECHA: OCTUBRE 2023

Página 16 de 31

Una vez que el ecosistema PDP comience a interactuar será necesario tener documentada la manera de responder a solicitudes que realicen titulares de datos personales, encargados de tratamiento, destinatarios y otras partes interesadas pertenecientes al ecosistema PDP Royaltex.

Incluso, la organización debe tener preparado los comunicados que deseé utilizar para comunicar al ecosistema PDP que está en la ruta para implantar un esquema PDP bajo los requisitos de la LOPDP:2021. Dentro de esta documentación están las cláusulas de confidencialidad y cláusulas PDP que debe incluir en los contratos de nuevos vinculados y en los trabajadores que ocupen PATD lo cual es un requisito de la LOPDP:2021, descrito en el artículo 47.10.

También se encuentra el cuestionario que se suele utilizar para hacer una aproximación de la auditoría documental, lo que denominaremos como "Cuestionario PDP" y es la manera técnica-elegante de solicitar a encargados de tratamiento y destinatarios por contrato/convenio un estatus de su esquema PDP. Este es el primer paso para cumplir con el requisito LOPDP:2021 descrito en el artículo 47.11

A continuación, se presentan ejemplos de cómo deberían de ser redactados alguno de estos comunicados:



ROYALTEX S.A.

MANUAL PARA PROTECCIÓN DE DATOS PERSONALES

CÓDIGO: DOCUMENTO 9

COMUNICADOS, CLÁUSULAS, CUESTIONARIO PDP,
RESPUESTAS AL ECOSISTEMA PDP

REVISIÓN:

FECHA: OCTUBRE 2023

Página 17 de 31

COMUNICADO DE INICIO DE PROYECTO PDP-ROYALTEX

Quito, XX de septiembre de 2023

Comunicado a nuestros clientes, proveedores y empleados

Comunicamos a todos nuestros clientes, proveedores y otras partes interesadas que ROYALTEX s.a., ha iniciado el proceso de implantación de la ley orgánica de protección de datos personales (LOPDP), por tal motivo los datos personales que nos confíen estarán debidamente protegidos bajo las directrices definidas en nuestras **Políticas de Protección de Datos Personales** y cuyos lineamientos están incorporados dentro de nuestro **Esquema de Protección de Datos personales** (EPDP).

La confidencialidad, integridad, disponibilidad, pertinencia, minimización, configuración y restricción de acceso, a los datos personales que nos confíen, quedarán garantizadas y su tratamiento será realizado bajo la base de licitud que se les comunicará de manera previa para que otorguen su consentimiento.

ROYALTEX s.a. continúa adaptando sus procesos para brindarles a sus clientes, proveedores y trabajadores la mejor experiencia durante nuestra relación.



ROYALTEX S.A.

MANUAL PARA PROTECCIÓN DE DATOS PERSONALES

CÓDIGO: DOCUMENTO 9

COMUNICADOS, CLÁUSULAS, CUESTIONARIO PDP,
RESPUESTAS AL ECOSISTEMA PDP

REVISIÓN:

FECHA: OCTUBRE 2023

Página 18 de 31

COMUNICADO DE INFORMACIÓN PREVIA A LA SOLICITUD DE DATOS PERSONALES AL TITULAR DE LOS DATOS EN PUNTOS DE VENTA

Es nuestra obligación informarle que en los próximos pasos estaremos solicitándole datos personales como parte de los requisitos de formalización de la compra-venta de prendas de vestir.

Sus datos estarán protegidos y seguros ya que contamos con un esquema de protección riguroso. Usted tiene el derecho de solicitar acceso a sus datos cuando lo desee, tenemos la obligación de atender esa solicitud en un lapso de hasta 15 días.

Esta gestión podrá realizarla de manera personal en el punto de venta, vía telefónica utilizando los números del punto de venta, mediante correo electrónico pdpairo@royaltex.com o utilizando el portal web.

Los datos que deberá entregar son de identificación, datos de localización, datos de contacto y datos de fechas de cumpleaños.

La finalidad de la solicitud es poder facturar bajo los requisitos del SRI, entregar oportuna y de manera precisa su mercadería adquirida en el portal web, compartir información de promociones y así brindarle una experiencia satisfactoria. El tiempo de uso de sus datos será el que usted otorgue al momento de compartirlos. Al final de ese tiempo sus datos serán eliminados de nuestras bases de datos o los mantendremos si así lo desea al realizar nuevas compras.

Por lo anteriormente expuesto le solicitamos que sea lo más preciso y exacto al momento de informarnos. Sería lamentable no poder completar alguna de las actividades por datos inexactos.

Gracias y esperamos que una vez informado y que haya entendido los próximos pasos, continue con el proceso que permita completar su deseo de compra.

Firma del solicitante

El análisis del contexto organizacional es un ejercicio que ha tomado mucha fuerza en los últimos 10 años. En las normativas internacionales para el diseño, documentación e implantación de sistemas de gestión, dentro de los cuales las normas emitidas por ISO son las más aceptadas internacionalmente, este ejercicio es el paso inicial para realizar el análisis de riesgos.

Para el caso de la LOPDP:2021 se presenta como algo novedoso e innovador que, de manera explícita, la ley solicite que el esquema de protección de datos personales tenga las características de un sistema de gestión (LOPDP:2021, art. 37, párrafo 2 y art. 47.3).

Otra particularidad de la LOPDP:2021, es que solicita que se apliquen los requisitos, medidas y herramientas en cinco áreas específicas: Jurídica. Técnica. Administrativa. Organizativas y Físicas (Capítulo VII, art. 47: Obligaciones del responsable de tratamiento en 47.2, 47.3 y 47.7 y capítulo XI, art. 68: Infracciones graves del responsable del tratamiento en 68.1), para el diseño del esquema de protección de datos personales.

La solicitud expresa obliga a las organizaciones a presentar el análisis del contexto interno separado, al menos, en estas cinco áreas, no hacerlo de esta manera expone a las organizaciones a ser sancionados por no cumplir con el requisito y, además, tipificado como: Infracción grave.

La decisión de separar el proyecto LOPDP de Royaltex en dos etapas, permite que el análisis de contexto organizacional tome preponderancia en la etapa I, debido a que supone el mayor riesgo. La razón es que probará la capacidad de la organización a comprometerse con la culminación de las fases de implantación y en la etapa II, mostrar el compromiso de mantenerlo, evaluarlo y fortalecerlo.

Existen muchas variables que conforman al contexto interno y externo de las organizaciones. Royaltex eligió el siguiente conjunto para cada uno de los contextos:

Contexto Interno: Temas jurídicos, Esquema organizacional, Esquema administrativo, Esquema técnico y Esquema físico

Contexto Externo: Ecosistema PDP, Situación política, Situación económica, Operativos externos (Cliente, proveedores y servicios logísticos de entrega)

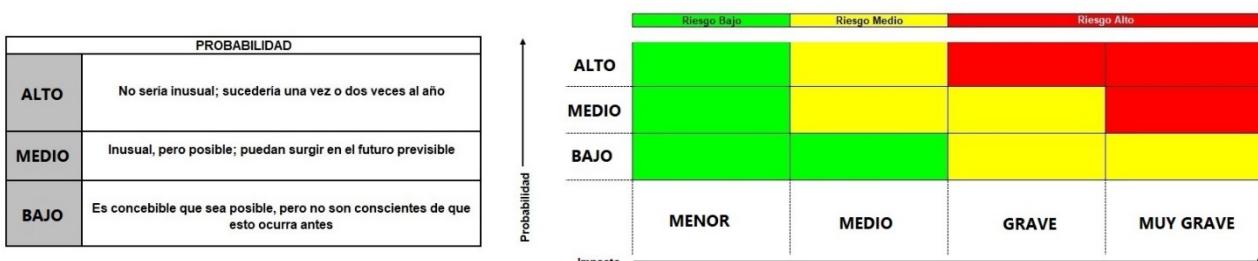
A continuación, un extracto del ejercicio:



CRITERIOS DE PONDERACIÓN DEL RIESGO

IMPACTO				
	DERECHOS Y LIBERTADES DE LOS TITULARES	REPUTACIÓN ORGANIZACIONAL	CONTINUIDAD DEL NEGOCIO	CONTINUIDAD DEL PROYECTO PDP
MENOR	No existe impacto sobre el ejercicio de derechos de los titulares de los datos	Impacto negativo menor en la imagen / reputación de la empresa en el ámbito local.	el impacto de las desviaciones no generan consecuencias que creen intermitencia en la operación	El impacto sobre el desarrollo del proyecto PDP son retrasos que no representan más de 30 días
MODERADO	El impacto se centra en una cantidad de personas específicas de un área o actividad con alcance definido y las bases de datos personales vulneradas no conservan datos de categoría especial .	Impacto moderado negativo en la imagen / reputación de la empresa, impacto negativo en la relación de las partes interesadas se extiende más allá del ámbito local,	el impacto de las desviaciones generan consecuencias que creen intermitencia en la operación. Estas pueden ser: acciones correctivas e infracciones leves sin multa asociada, o sanciones previas sin cese de las actividades de tratamiento.	El impacto sobre el desarrollo del proyecto está sobre la correcta implantación de las acciones descritas en el plan inicial PDP. La no realización del plan de concientización del
GRAVE	El impacto se centra en una cantidad de personas específicas de un área o actividad con alcance definido y las bases de datos personales vulneradas conservan datos de categoría especial .	Impacto negativo grave en la imagen / reputación de la empresa, el impacto negativo en la relación de las partes interesadas se extiende más allá del entorno regional.	el impacto de las desviaciones generan intermitencia en la operación. Estas pueden ser: infracciones leves con multa asociada, o sanciones previas con cese de ciertas actividades de tratamiento.	No tener un esquema organizacional documentado que propicie la revisión de indicadores claves, evitará que el proyecto tenga continuidad.
CATASTÓFICO	Son vulneradas múltiples bases de datos personales que contienen datos las distintas categorías.	Impacto negativo catastrófico y mundial sobre la imagen / reputación de la empresa, el impacto negativo de la relación entre las partes interesadas se prolonga por varios años.	el impacto de las desviaciones detienen la operación por un periodo definido de tiempo. Estas pueden ser: sumatoria de infracciones leves y graves con multa asociada, o sanciones previas con cese de la operación y/o de varias actividades de tratamiento	tener un esquema de trabajo por REACCIÓN, donde las decisiones son tomadas sin analizar datos o tendencias puede provocar que se decida abortar el proyecto o no continuar con las fases siguientes.

Fuente: Archivo SKILLMAN-PDP
Título: GESTIÓN DEL RIESGO (CRITERIOS DE PONDERACIÓN DEL RIESGO)
Autor: Freddy Villavicencio - 2023



CONTEXTO ORGANIZACIONAL

RESULTADOS DE LA PONDERACIÓN DE LOS RIESGOS INDUCIDOS POR EL CONTEXTO INTERNO ESQUEMA ORGANIZACIONAL

Esquema administrativo

Factor interno	REQUISITO	DESAFIOS	RIESGOS ASOCIADOS
Incorporar PDP al esquema de mejora continua actual	<ul style="list-style-type: none"> Tener un esquema organizacional documentado y entendido Tener implantado la mejora continua PDP 	<ul style="list-style-type: none"> Existe la posición de hacer lo mínimo necesario con respecto al proyecto PDP Que se completen las tres fases de implantación del sistema de gestión 	<ul style="list-style-type: none"> La mala interpretación de mínimo necesario puede convertirse en una amenaza al proyecto PDP Con la primera fase de implantación, sería complejo incorporar PDP a la mejora continua vigente El enfoque de temporada no permitiría mayor asignación de recursos al proyecto PDP
Definir indicadores PDP	<ul style="list-style-type: none"> Identificar actividades de tratamiento críticas Definir transiciones críticas en la ruta de los datos para las ATD críticas Definir rango de trabajo de las variables críticas Definir plan de muestreo y alarmas 	<ul style="list-style-type: none"> Lograr desarrollar un piloto dentro del 4Q2023 o 1Q2024 Que se completen las tres fases de implantación del sistema de gestión 	<ul style="list-style-type: none"> Con la primera fase (documentación), sería complejo incorporar PDP a la mejora continua vigente El enfoque de temporada no permitiría mayor asignación de recursos al proyecto PDP
Incorporar gestión de riesgos al esquema de mejora continua	<ul style="list-style-type: none"> Definir esquema de auditoría para rutinas PDP (plan de muestreo) Definir esquema de auditoría al plan inicial PDP 	<ul style="list-style-type: none"> Lograr desarrollar un piloto dentro del 4Q2023 o 1Q2024 Que se completen las tres fases de implantación del sistema de gestión 	<ul style="list-style-type: none"> Con la primera fase (documentación), sería complejo incorporar PDP a la mejora continua vigente El enfoque de temporada no permitiría mayor asignación de recursos al proyecto PDP

Listado de riesgos

- Entender que significa "mínimo necesario". Creer que la documentación es todo lo que solicita la LOPDP
- El último trimestre del año (Temporada alta), limita la capacidad de recurso humano para conformar equipo interno PDP. No conformar al equipo interno PDP
- Toda la organización enfocada en la temporada pone en riesgo el cumplimiento del cronograma de implantación

Acciones, medidas y herramientas

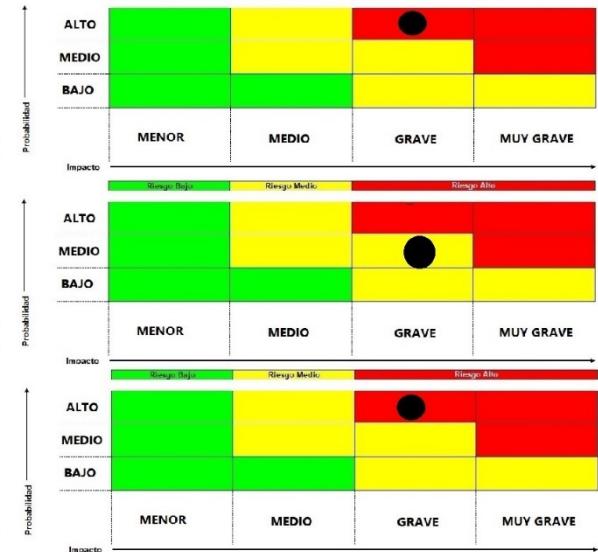
- Aclarar que un requisito de la LOPDP-2021 (Art. 47.3), "Aplicar implementar procesos de verificación, evaluación, valoración periódica de la eficiencia, eficacia y efectividad de los requisitos y herramientas técnicas, jurídicas, administrativas, organizativas y físicas implementadas"
- Determinar los recursos con los que podría apoyar a la continuidad del proyecto PDP
- Aprovechar la coyuntura política que brinda hasta 9 meses de tiempo para que aparezca la autoridad de PDP, esto permite reiniciar en enero 2024

Riesgo residual

Perdida de interés sobre la culminación del proyecto y otras actividades tomen prioridad.

Ponderación de probabilidad e impacto de las amenazas identificadas

AMENAZA IDENTIFICADA	Probabilidad	ÁREAS DE IMPACTO				Impacto		
		baja	media	alta	menor	medio	grave	Muy grave
Creer que la documentación es todo lo que solicita la LOPDP					DERECHOS Y LIBERTADES DE LOS TITULARES			
					REPÚBLICA ORGANIZACIONAL			
					CONTINUIDAD DEL NEGOCIO			
					CONTINUIDAD DEL PROYECTO PDP			



Fuentes: Archivo SKILLMAN-PDP
Título: GESTIÓN DEL RIESGO
(CRITERIOS DE PONDERACIÓN DEL RIESGO)
Autor: Freddy Villavicencio - 2023



Contexto organizacional externo

Ecosistema PDP Royaltex

Factor externo	REQUISITO	DESAFÍOS	RIESGOS ASOCIADOS
Super intendencia PDP (Requisitos LOPDP:2021)	<ul style="list-style-type: none"> • Listado de ATD's en cuatro ámbitos: WEB, Digital y Físico • Análisis del contexto organizacional en las 5 áreas • Evaluación de riesgo • Evaluación de impacto • Políticas PDP en las 5 áreas • Plan inicial PDP las 5 áreas • Procedimientos PDP 	<ul style="list-style-type: none"> • Implantar las rutinas PDP en cada puesto de trabajo con ATD • Mantener activo al equipo del proyecto PDP en el 4Q23 	<ul style="list-style-type: none"> • No implantar las rutinas PDP en los puestos de trabajo con ATD • No hacer pilotos de los procedimientos PDP para perfeccionarlos • No incluir actividades al equipo de proyecto PDP en el 4Q23
Otras partes interesadas (Requisitos LOPDP:2021)	<ul style="list-style-type: none"> • Normativa aplicable y base de licitud • Contrato vigente y en funciones 	<ul style="list-style-type: none"> • Definir la ATD y la ruta de datos para satisfacer lícitamente la transferencia de datos 	<ul style="list-style-type: none"> • No definir esta actividad rutinaria y obligatoria como una ATD • No asociar la base de licitud y tener el consentimiento expreso viciado • No incluir actividades al equipo de proyecto PDP en el 4Q23

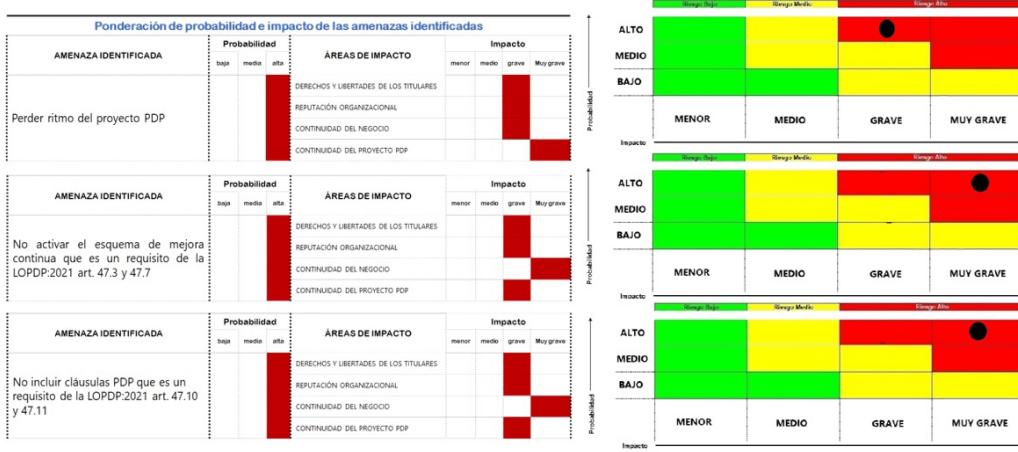
Factor externo	REQUISITO	DESAFÍOS	RIESGOS ASOCIADOS
Titulares, encargados y destinatarios (Requisitos LOPDP:2021)	<ul style="list-style-type: none"> • Listado de ATD's y bases de licitud • Ecosistema PDP documentado • Contrato con cláusula PDP • Comunicados, respuestas y acuerdos PDP 	<ul style="list-style-type: none"> • Mantener activo al equipo del proyecto PDP en el 4Q23 	<ul style="list-style-type: none"> • Perder seguimiento a los comunicados enviados al ecosistema PDP • No incluir actividades al equipo de proyecto PDP en el 4Q23

Listado de riesgos

- 1.- Perder ritmo del proyecto PDP
- 2.- No activar el esquema de mejora continua que es un requisito de la LOPDP:2021 art. 47.3 y 47.7
- 3.- No incluir cláusulas PDP que es un requisito de la LOPDP:2021 art. 47.10 y 47.11

RESULTADOS DE LA PONDERACIÓN DE LOS RIESGOS INDUCIDOS POR EL CONTEXTO EXTERNO

ECOSISTEMA PDP ROYALTEX



Acciones, medidas y herramientas

- 1.- Aprovechar la coyuntura política que brinda hasta 9 meses de tiempo para que aparezca la autoridad de PDP, esto permite reiniciar en enero 2024
- 2.- Determinar los recursos con los que podría mantener la continuidad del proyecto PDP
- 3.- Reducir al equipo de documentación a una persona que mantenga activo al proyecto PDP durante el 4Q23

Riesgo residual

Perdida de interés sobre la culminación del proyecto y otras actividades tomen prioridad



MANUAL PARA PROTECCIÓN DE DATOS PERSONALES

CÓDIGO: DOCUMENTO 11

REVISIÓN:

RIESGOS Y ESQUEMA PDP POR PATD
PATD y CIBERSEGURIDAD
PATD y RUTINAS PDP

FECHA: OCTUBRE 2023

Página 23 de 31

La LOPDP:2021 solicita en el capítulo VI (Seguridad de datos personales), artículo 40, que se debe considerar, para el análisis de riesgos, las particularidades de la actividad de tratamiento, las particularidades de las partes involucradas y las categorías y el volumen de los datos asociados al tratamiento.

Esto aunado a la solicitud que se apliquen los requisitos, medidas y herramientas en cinco áreas específicas: Jurídica. Técnica. Administrativa. Organizativas y Físicas (Capítulo VII, art. 47: Obligaciones del responsable de tratamiento en 47.2, 47.3 y 47.7 y capítulo XI, art. 68: Infracciones graves del responsable del tratamiento en 68.1).

La solicitud obliga a las organizaciones a presentar las acciones, medidas y herramientas mitigadoras, resultantes del análisis de riesgos, para cada una de estas cinco áreas. No hacerlo de esta manera expone a las organizaciones a ser sancionadas por no cumplir con el requisito tipificado como: Infracción grave, en los artículos 68.4 y 68.6 de la LOPDP:2021.

Para satisfacer las tres condiciones el análisis de riesgos se realizará en cada PATD, ya que es allí donde se ubican todos los requisitos que solicita el artículo 40 de la LOPDP:2021. La siguiente imagen muestra el formato que se utiliza para realizar el análisis de riesgos por PATD.

PUESTO DE TRABAJO



CARACTERIZACIÓN DE PUESTOS CON ACTIVIDADES DE TRATAMIENTO

TRATAMIENTO	TIEMPO	FINALIDAD	DATOS QUE SE UTILIZAN	MÉTODO DE ANONIMIZACIÓN	BASES DE LEGITIMACIÓN	SERVIDOR	RUTA DIGITAL	ETD CONTRATO	DDP LICITUD	DERECHOS AREE Y CONSERVACIÓN DATOS

LISTADO DE RIESGOS:

Acciones, medidas y herramientas

Riesgo residual



MANUAL PARA PROTECCIÓN DE DATOS PERSONALES

CÓDIGO: DOCUMENTO 12

REVISIÓN:

SELECCIÓN DE CONTROLES, DECLARACIÓN DE APPLICABILIDAD Y PLAN INICIAL PDP

FECHA: OCTUBRE 2023

Página 24 de 31

El resultado de los ejercicios de análisis del contexto organizacional y de la evaluación de riesgos que entrañan las actividades de tratamiento de datos personales, es el plan inicial para protección de datos personales (PIPDP). Todo sistema de gestión bajo esquema SL de ISO solicita un plan inicial resultante de la evaluación de los riesgos y políticas que sirvan de marco regulatorio para la implantación y ejecución del plan inicial.

Con estos dos elementos se procede a implantar las acciones que están listadas y priorizadas en el plan inicial. Se debe considerar el requisito de la LOPDP:2021, capítulo VI (Seguridad de datos personales), artículo 37, párrafo primero para seleccionar y priorizar las acciones inscritas en el plan inicial.

Una práctica común luego de realizada el análisis del contexto y la evaluación de riesgos es seleccionar las acciones, medidas y herramientas, mitigadoras de los riesgos, amenazas y vulnerabilidades identificados. No siempre es factible implantar todos los controles, por eso se estila redactar un documento que lleva por nombre "*Declaración de aplicabilidad*" y es el compromiso de la organización sobre la implantación de los controles que considere importantes, viables en inversión de recursos (Tiempo, espacios, tecnología, talentos y económicos) y críticos desde lo que se desea proteger.

A continuación, se presenta la declaración de aplicabilidad Royaltex:

DECLARACIÓN DE APPLICABILIDAD

Declaración de aplicabilidad de controles y acciones mitigadoras de los riesgos identificados:

1. El proyecto está separado en dos etapas.
2. La etapa I está dividida en tres fases: Documentación + implantación + activación mejora continua y gestión del riesgo
3. El equipo de documentación no es el designado para completar las fases 2 y 3
4. El plan inicial PDP está diseñado para asegurar que se completen las 3 fases de la etapa 1
5. Las rutinas iniciales PDP en cada PATD, representan la herramienta sistemática para mantener vigiladas a las actividades de tratamiento de datos personales.
6. Luego de completada la fase 3, la medida prioritaria de la etapa II, será la inclusión de controles adicionales a las rutinas PDP de cada PATD, tomados de la norma INEN ISO/IEC 27002:2022
7. Esta declaración de aplicabilidad describe como serán aplicados los controles iniciales (mitigación de riesgos que impidan completar las tres fases) y los controles complementarios (Controles tomados de la norma INEN ISO/IEC 27002:2022) para fortalecer las rutinas PDP y la gestión de riesgos en la etapa II

8. Controles, medidas y herramientas iniciales:

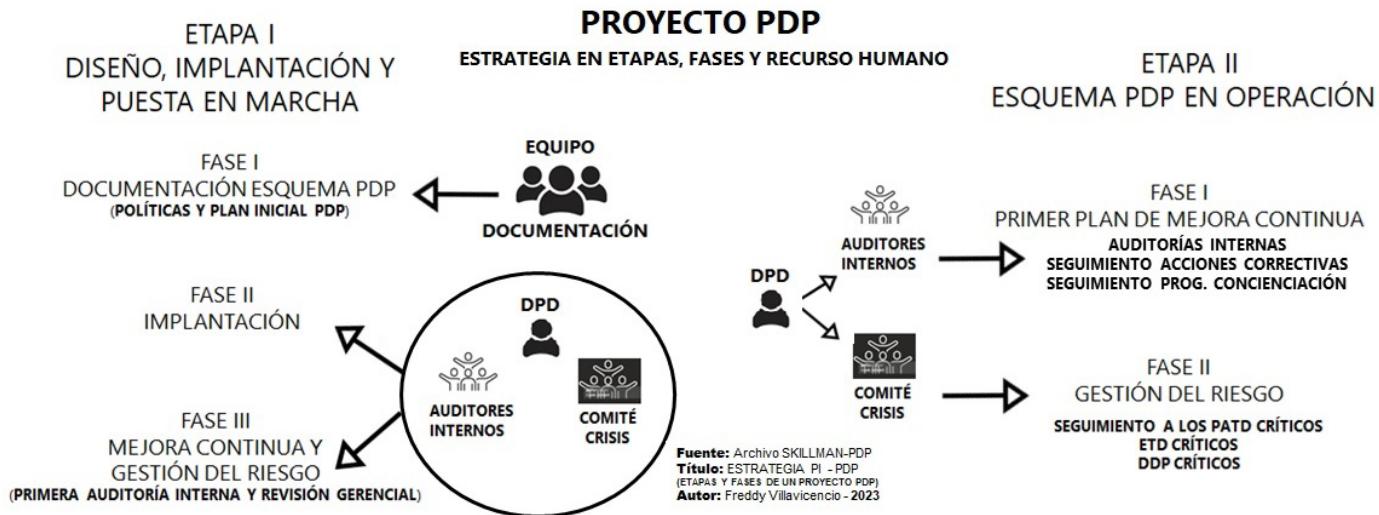
- a. Se debe realizar una evaluación de impacto sobre el ejercicio de derechos a las acciones, medidas y herramientas seleccionados para evitar que el contexto organizacional impida la implantación del esquema PDP bajo los requisitos de la LOPDP:2021
- b. Con el resultado de la evaluación de impacto inicial se priorizará que actividades de tratamiento deberán ser revisadas, modificadas o eliminadas luego de culminadas las tres fases de implantación del esquema PDP bajo los requisitos de la LOPDP:2021.
- c. Los que mitigan los riesgos inducidos por el contexto interno de la organización con respecto a la culminación de las fases del proyecto PDP
- d. Los que mitigan los riesgos inducidos por el contexto externo de la organización con respecto a la culminación de las fases del proyecto PDP
- e. Los que mitigan los riesgos asociados al régimen sancionatorio en cada una de las cinco áreas donde la LOPDP:2021 solicita controles, medidas y herramientas
- f. Los que mitigan los riesgos inherentes a los puestos con actividades de tratamiento de datos personales (PATD)
 - Cumplir el plan progresivo de activación de los PATD priorizados por la tipología y ámbito de las actividades de tratamiento (giro de negocio, encargadas, obligatorias, comunicadas, operativas, otras)
 - Cumplir con el plan progresivo de seguridad física
 - Cumplir con el plan progresivo de ciber seguridad
- g. Estas acciones se completan en las fases 2 y 3

9. Controles, medidas y herramientas complementarios:

- a. Realizar un revisión punto a punto de la norma INEN ISO/IEC 27002:2022 sobre cada uno de los PATD
- b. Realizar una selección de los controles aplicables a cada PATD
- c. Realizar una evaluación de impacto sobre el ejercicio de derechos a los controles seleccionados a cada una de las acciones de tratamiento de datos personales en cada PATD
- d. Estas acciones se inicien con el primer plan de mejora continua

También es valioso para la selección y priorización de los controles que se defina una estrategia para completar el proyecto PDP. La estrategia del proyecto que se describió en el documento 7 de este manual presenta la siguiente ruta:

PROYECTO PDP ROYALTEX



Como ya se ha mencionado a lo largo de este manual, la LOPDP:2021 tiene como requisito que las acciones, medidas y herramientas definidas para proteger los datos personales deben presentarse para cada una de las cinco áreas mencionadas en los artículos 37 y 47 de la ley.

De la declaración de aplicabilidad se desprende que la prioridad para la etapa I es mitigar la amenaza que puede representar el contexto organizacional sobre la culminación de la etapa I. Por ese motivo el Plan inicial tiene un primer enfoque en cubrir o controlar las amenazas identificadas en el análisis del contexto interno y externo de Royaltex.

A continuación, se presenta una muestra de como estará documentado el plan inicial PDP-Royaltex



MANUAL PARA PROTECCIÓN DE DATOS PERSONALES

CÓDIGO: DOCUMENTO 12

REVISIÓN:

SELECCIÓN DE CONTROLES, DECLARACIÓN DE APPLICABILIDAD Y PLAN INICIAL PDP

FECHA: OCTUBRE 2023

Página 26 de 31

Extracto de las medidas que deben implantarse para asegurar la culminación de la etapa I

PLAN INICIAL PARA PROTECCIÓN DE DATOS PERSONALES MEDIDAS, ACCIONES Y CONTROLES MITIGADORES

ABREVIATURAS: PERS= PERSONAS TECN = TECNOLOGÍA INFR. = INFRAESTRUCTURA DINE = DINERO



PLAN INICIAL DE PROTECCIÓN DE DATOS PERSONALES

ÁREA LOPDP:2021	MEDIDAS, HERRAMIENTAS Y CONTROL PARA MITIGAR EL IMPACTO	RECURSOS NECESARIOS				FECHA PROBABLE	INVERSIÓN ESTIMADA	COMENTARIOS
		PERS.	TECN.	INFR.	DINE			
Contexto organizacional	Determinar los recursos con los que podría apoyar a la continuidad del proyecto PDP							<ul style="list-style-type: none"> Es un requisito de la LOPDP:2021 (Art. 47.3), "Aplicar implementar procesos de verificación, evaluación, valoración periódica de la eficiencia, eficacia y efectividad de los requisitos y herramientas técnicas, jurídicas, administrativas, organizativas y físicas implementadas"
	Aprovechar la coyuntura política que brinda hasta 9 meses de tiempo para que aparezca la autoridad de PDP, esto permite reiniciar en enero 2024							<ul style="list-style-type: none"> La documentación en si misma, no es suficiente si no queda demostrado (en un plan de implantación), que el objetivo es implantar un esquema PDP que sea evaluado periódicamente
	Crear un documento que permita dar seguimiento a los integrantes del ecosistema PDP (ETD, TDP y DDT), para saber el estatus de la inclusión de la cláusula PDP en los contratos, además de, la identificación de la ruta de los datos							<ul style="list-style-type: none"> Se pueden utilizar entre 9 y 12 meses para completarlo
	De manera preventiva proyectar la búsqueda de opciones que brinden protección de datos personales							<ul style="list-style-type: none"> Los valores son referenciales, se debe realizar una gestión de procura y compra

Extracto de las medidas por cada área LOPDP:2021 (Organizacionales):

PLAN INICIAL PARA PROTECCIÓN DE DATOS PERSONALES MEDIDAS, ACCIONES Y CONTROLES MITIGADORES

ABREVIATURAS: PERS= PERSONAS TECN = TECNOLOGÍA INFR. = INFRAESTRUCTURA DINE = DINERO



PLAN INICIAL DE PROTECCIÓN DE DATOS PERSONALES

ÁREA LOPDP:2021	MEDIDAS, HERRAMIENTAS Y CONTROL PARA MITIGAR EL IMPACTO	RECURSOS NECESARIOS				FECHA PROBABLE	INVERSIÓN ESTIMADA	COMENTARIOS
		PERS.	TECN.	INFR.	DINE			
Organizativas (FASE II – Implementación)	Actualizar el organigrama anexando el mapa de PATD como estructura del esquema de protección de datos personales							<ul style="list-style-type: none"> La reinicio del proyecto PDP fase 2 consiste en seleccionar el comité de crisis, al equipo de auditores internos y la contratación del delegado de protección de datos.
	Actualizar el listado maestro de documentos incluyendo el mapa de PATD, listado de las actividades de tratamiento, el ecosistema PDP, el catálogo de categorías y tipologías, el glosario de términos, las políticas PDP, el plan de concienciación PDP general (Titulares internos, clientes y proveedores), el plan de concienciación PDP para miembros PDP (Comité de crisis y PATD), el plan de capacitación equipo interno PDP y el plan inicial PDP							<ul style="list-style-type: none"> Completar las fases 2 y 3 del sistema de gestión PDP requiere de la inversión mostrada como referencia estimada
	Actualizar las descripciones de cargos incluyendo las rutinas PDP en las PATD							<ul style="list-style-type: none"> Este proyecto puede durar hasta 6 meses.
	Seleccionar al equipo interno PDP para 4Q23 y 1Q24 al 4Q24							<ul style="list-style-type: none"> Será imprescindible un diagnóstico para darle prioridad a las acciones a seguir Seleccionar la mejor opción de ayuda será clave de éxito Este proyecto es de alta complejidad ya que asocia cultura, organización y gestión
	Seleccionar al auditor líder y equipo de auditores internos							<ul style="list-style-type: none"> Los valores son referenciales, se debe realizar una gestión de procura y compra
	Completar la activación de todos los PATD							

El hecho de que la LOPDP:2021 en el capítulo VII (Obligaciones del responsable de tratamiento de datos personales), artículos 47.1, 47.2 y 47.4, sea específica en solicitar acciones, medidas y herramientas en cinco áreas, para mitigar el impacto de los riesgos, amenazas y vulnerabilidades identificadas en los ejercicios de análisis del contexto organizacional y evaluación de riesgos, obliga a los responsables de tratamiento a definir políticas para protección de datos personales en cada una de esas áreas.

Las políticas son el marco regulatorio interno para ejecutar los controles seleccionados y declarados aplicables. Estas políticas, entonces, serán presentadas de manera diferenciada de la siguiente manera:

1. **Políticas del área jurídica:**

- a. Contratos
- b. Comunicados
- c. Acuerdos
- d. Diseño de actividades de tratamiento
- e. Respuestas al ecosistema PDP

2. **Políticas del área organizativas:**

- a. Inventario de actividades de tratamiento
- b. Mapeo de los puestos de trabajo
- c. Ecosistema PDP de la organización
- d. Catálogo de categorías y tipologías
- e. Glosario de términos
- f. Procedimientos documentados
- g. Despliegue de infografías
- h. Maestro de documentos
- i. Plan de concienciación PDP
- j. Descripción de cargos
- k. Comité de crisis y equipo interno PDP

Se pueden incluir otras políticas organizativas. Un ejemplo puede ser el código de sanciones y recompensas por gestión PDP.

3. Políticas del área administrativa:

- a. Mejora continua
- b. Evaluación de la eficacia del SGPD
- c. Gestión de riesgos

4. Políticas del área técnica:

- a. Inventario de activos de los datos
- b. Ciberseguridad
- c. Trabajo remoto
- d. Encargo de datos + comunicación de datos
- e. Anonimización de los datos
- f. Gestión de claves y usuarios
- g. Dispositivos móviles y almacenadores digitales de datos
- h. Gestión de respaldos

5. Políticas del área física:

- a. Selección de proveedores
- b. Categorización de condiciones deseadas
- c. Ventana de inversión
- d. Categoría de los bienes

Hay muchas maneras de redactar políticas, lo importante es que tengan tono de comunicado de carácter mandatorio. Las políticas no son procedimientos, son reglas, es la normativa sobre la ejecución de actividades estratégicas de la organización. A continuación, se entrega una muestra de una política:

1.1.1 Contratos con titulares de datos

i. **Titulares empleados del responsable del tratamiento (RTD)**

- 1. El contrato debe incluir la cláusula de protección de datos personales.
 - a. La cláusula debe incluir el acuerdo y compromiso de confidencialidad si tiene acceso a datos personales de terceros.
 - b. La cláusula debe incluir una mención a los principios que el RTD debe practicar para garantizar la protección de datos personales
 - c. La cláusula debe incluir una mención de los derechos que el RTD debe respetar y que son irrenunciables por el titular
 - d. La cláusula debe incluir una mención separada de los derechos de acceso a los datos, rectificación de los datos, eliminación de los datos y de oposición al tratamiento de los datos que tiene el titular.
 - e. La cláusula debe incluir un listado de las actividades de tratamiento, su finalidad, tiempo de utilización, datos que se solicitan y sus categorías.
 - f. La cláusula debe mencionar que la organización tiene un esquema de protección de datos personales bajo requisitos LOPDP:2021
- 2. La persona responsable de formalizar el contrato debe asegurarse que el nuevo contratado lea o escuche cada una de las cláusulas del contrato en especial las de protección de datos personales.
- 3. El modelo de cláusula PDP está en el **anexo 1**

Todo sistema de gestión cuenta con un número definido de procedimientos obligatorios que reciben el nombre de "Procedimientos documentados". Estos procedimientos garantizan el correcto funcionamiento del sistema. Para el caso de la LOPDP:2021, que funciona como sistema de gestión y esto queda expresado como requisito en el capítulo VII (Obligaciones del responsable de tratamiento de datos personales), artículos 47.1, 47.2, podemos listar el siguiente grupo de procedimientos:

- a. Ejercicio de Derechos AREO (**LOPDP:2021, capítulo III**)
- b. Procedimiento administrativo (**LOPDP:2021, capítulo X**)
- c. Garantías de transferencia internacional (**LOPDP:2021, capítulo IX**)
- d. Notificación de brecha a la autoridad (**LOPDP:2021, capítulo VI, art. 43**)
- e. Notificación de brecha a los titulares (**LOPDP:2021, capítulo VI, art. 46**)
- f. Actualización del registro nacional de bases de datos (**LOPDP:2021, capítulo VII, art. 47.12**)
- g. Metodología para evaluación de riesgos (**LOPDP:2021, capítulo VI, art. 40**)
- h. Selección de controles y declaración de aplicabilidad (**LOPDP:2021, capítulo VI, art. 41**)
- i. Metodología para evaluación de impacto (**LOPDP:2021, capítulo VI, art. 42**)
- j. Protocolo de crisis y resiliencia del esquema PDP (**LOPDP:2021, capítulo VI, art. 44**)
- k. Metodología para PDP desde el diseño y por defecto (**LOPDP:2021, capítulo VI, art. 39**)
- l. Programa de auditorías internas y revisiones gerenciales (**LOPDP:2021, capítulo VII, art. 47.3**)
- m. Formato de informe del DPD @ APDP

MANUAL PARA PROTECCIÓN DE DATOS PERSONALES		CÓDIGO:
		REVISIÓN:
DERECHOS AREO (ACceso + RECtificación + ELIMINACIÓN + oPOSICIÓN)		FECHA:
ALCANCE		Página 1 de 1

ALCANCE
Los derechos a solicitar acceso a los datos personales, rectificación de los datos personales, eliminación de los datos personales y oposición al tratamiento de datos personales, aplica a todos los titulares de datos personales que estén en las bases de datos personales del responsable del tratamiento de los datos.
El responsable de tratamiento debe establecer los mecanismos y métodos razonables que permitan el ejercicio de estos derechos. El responsable del tratamiento tiene hasta 15 días para responder a estas solicitudes.

ACCION DE TRATAMIENTO: Solicitud de acceso por titular de los datos	SÍMBOLOS ASME					DESCRIPCIÓN DE LA ACCIÓN
	OFRACÓN	INSPECCIÓN	ARCHIVO	TRANSPORTE	RETASCO	
Llenar formato de solicitud (WEB o Físico)	Titular de los datos	x				
Entregar al DPD (WEB o Físico)	Titular de los datos	x		x		
Emitir comunicado de recibido e inicio de trámite	dpd	x				
Realización del trámite (10 días)	dpd	x	x	x	x	
Comunicado de trámite completado	dpd	x		x		
Retiro del documento	Titular de los datos	x				

Los procedimientos serán redactados bajo la normativa ASME para diagramas de flujo. Existen muchas metodologías para redacción y de todas esta fue la elegida.

Una práctica útil y, sin embargo, no masificada al momento de ensamblar un manual técnico, donde se incluirán términos de distintas áreas de conocimiento, es agregar un glosario de términos al manual. El glosario de términos es un instrumento del sistema de gestión para asegurar la interpretación homogénea de las instrucciones, abreviaturas y conceptos que se mencionan en la documentación del sistema de gestión.

Una utilidad muy valiosa de este instrumento es cuando se recibe a un auditor de segunda parte. Al momento de existir una discrepancia entre lo que el auditado menciona en sus argumentos y lo que el auditor interpreta desde sus preconceptos, acudir a un glosario es la salida idónea.

En el diseño y documentación de un sistema de gestión para protección de datos personales, se utiliza un grupo de normativa referente, metodologías y técnicas que reciben diversas interpretaciones, ya que las mismas, son redactadas en lenguaje genérico y, en ocasiones, tienden a ser interpretados según la base de conocimiento de los individuos que interactúen en el proceso.

Royaltex incluye en su manual PDP, un glosario de términos para facilitar la interacción con auditores de segunda parte, con personal interno durante las auditorias de primera parte y como alineador de criterios durante las sesiones de capacitación del esquema de protección de datos personales y las sesiones de concienciación sobre las particularidades el ejercicio de libertades y derechos de los titulares de los datos personales, entre lo mas relevante de su uso.

Este glosario reúne términos tomados de distintas normativas referentes para el diseño y documentación del sistema de gestión para protección de datos bajo los requisitos de la LOPDP:2021. Entre ellos se incluyen:

- Ley orgánica para protección de datos personales del Ecuador
- Acuerdo ministerial No. 012-2019, vigente desde el 15 de agosto del año 2019
- RGPD:2018 de la comunidad europea
- Norma NTE ISO 19011:2018
- Norma NTE ISO/IEC 27000:2018
- Interpretaciones y comentarios recogidos de diversas fuentes.

La siguiente imagen muestra el formato del glosario de términos.

GLOSARIO DE TERMINOS PDP

SKILLMAN-PDP

CÓDIGO: QUICK RE
VERSIÓN: 2021



GLOSARIO y REFERENCIAS RÁPIDAS PARA PROTECCIÓN DE DATOS PERSONALES

GLOSARIO
Página 10 de 1

GLOSARIO

Para efecto del presente manual de protección de datos personales, todos los términos aquí recogidos son los que tendrán validez al momento de recibir a un auditor externo o interno.

Este glosario integra las definiciones y términos que se expresan en los siguientes documentos:

- Ley orgánica para protección de datos personales, vigente en Ecuador desde el 26 de mayo del año 2021
 - Acuerdo ministerial No. 012-2019, vigente desde el 15 de agosto del año 2019
 - Norma INEN ISO 19011:2018
 - Norma INEN ISO 27000:2018
 - Interpretaciones y comentarios recogidos de diversas fuentes.
- a) Las palabras que se encuentran en letra cursiva y subrayadas con doble línea, son términos que se encuentran definidos en este Glosario.
- b) Las frases o párrafos que se encuentran subrayados con doble línea, son interpretaciones resultantes de la investigación y lectura de diversas fuentes. Tienen como objetivo ampliar la definición que se encuentra en los documentos listados anteriormente.

A

Acceso restringido: Para efectos de este manual es la clasificación que reciben todas la BDP, por diseño y por defecto. Las BDP deben contar desde el diseño con una ruta de acceso desde posiciones de tratamiento de datos personales (PTDP), vigente en los activos de los datos (**GLOSARIO SKILLMAN-PDP:2021**)

Actividad de tratamiento (ATDP): Para efectos de este manual es el término que puede sustituir a Tratamiento de datos sin que esto represente un error. Ambos términos utilizarán las siglas ATDP en la documentación del manual Skillman-PDP, para referirse a la autoridad (**GLOSARIO SKILLMAN-PDP:2021**)

Activos de los datos (AcDP): Para efectos de este manual es el inventario de Posiciones de tratamiento de datos personales (PTDP), ordenadores asociados a esa PTDP, dueño del PTDP (DPTD), listado de ATDP de la posición, listado de BDP de la posición y listado de las rutinas de seguridad y protección de la PTDP. Esta información se muestra en la infografía "Ciclo de vida y ruta de los datos" (**GLOSARIO SKILLMAN-PDP:2021**)

AEPD-EUROPA: Agencia Española de Protección de Datos, cuya misión tiene tres pilares: 1. Difundir y garantizar el derecho fundamental a la protección de los datos personales. 2. Velar por el cumplimiento de la legislación sobre protección de datos. 3. Impulsar una labor proactiva que permita detectar el impacto que los nuevos desarrollos tecnológicos puedan tener en la privacidad de los ciudadanos. (**GLOSARIO SKILLMAN-PDP:2021**)

AEPD-SUDAMÉRICA: Asociación Ecuatoriana de Protección de Datos, cuyos fines quedan expresados en 9 objetivos relacionados con la protección de datos personales, la privacidad, intimidad y tecnologías de la información, además de promover el estudio y brindar asesorías técnica y legal en la materia. (**GLOSARIO SKILLMAN-PDP:2021**)

Análisis de riesgos: Proceso para comprender la naturaleza del rriesgo y para determinar el nivel de riesgo. El análisis de riesgos proporciona la base para la evaluación de riesgos y las decisiones sobre el tratamiento de riesgos. El análisis de riesgos incluye la estimación de riesgos. (**INEN ISO 27000: 2018**)

B

Base de datos: Conjunto estructurado de datos cualquiera que fuera la forma, modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento, localización o acceso, centralizado, descentralizado o repartido de forma funcional o geográfica. (**Ley Orgánica de Protección de Datos Personales - 2021**)

Bases de datos personales (BDP): Conjunto estructurado de datos personales, categorizados y legitimados para cada tratamiento específico, cualquiera que fuera la forma, modalidad de creación, conservación, organización, tipo de soporte, tipos de tratamientos, procesamiento, localización o acceso, centralizado, descentralizado, repartido de forma funcional o geográfica, físico o digital y que deben contar con un esquema de protección y seguridad, de los datos contenidos, que mitiguen el efecto de los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades del titular de los datos (TDP). (**GLOSARIO SKILLMAN-PDP:2021**)

Bases de datos personales en custodia (BDP-C): Conjunto estructurado de datos personales, físico o digital, cuyo tiempo de tratamiento haya concluido y que por disposición legal o normativa aplicada exija al RTD mantener una copia por un período de tiempo determinado. Las BDP-C deben contar con un esquema de protección y seguridad, de los datos contenidos, que mitiguen el efecto de los riesgos de diversa probabilidad y gravedad que entraña la actividad de custodia, para los derechos y libertades del titular de los datos (TDP). (**GLOSARIO SKILLMAN-PDP:2021**)

C

Canales: Estructuras o medios de difusión de los contenidos y servicios; incluyendo el canal presencial, el telefónico y el electrónico, así como otros que existan en la actualidad o puedan existir en el futuro (dispositivos móviles, TDT, etc.). (**Acuerdo Ministerial No. 012-2019**)

Canal electrónico: todo canal de transmisión de datos por medios electrónicos, ópticos o radiofrecuencias. (**Acuerdo Ministerial No. 012-2019**).

Categoría de los clientes: Para efectos de este manual, es la diferenciación y jerarquización de clientes que permite a un RTD ingresar sus datos en una base de datos apropiada. Las categorías son: 1. Comparte BDP, 2. No comparte BDP, 3. Persona natural, 4. Otros (**GLOSARIO SKILLMAN-PDP:2021**)

Categoría de los datos: Para efectos de este manual, es la diferenciación y jerarquización de los datos personales que permitirá clasificarlos y tratarlos de manera diferenciada. (**GLOSARIO SKILLMAN-PDP:2021**)

Categoría de los proveedores: Para efectos de este manual, es la diferenciación y jerarquización de proveedores que permite a un RTD ingresar sus datos en una base de datos apropiada. Las categorías son: 1. Comparte BDP, 2. Recibe BDP, 3. Persona natural, 4. Otros. (**GLOSARIO SKILLMAN-PDP:2021**)

Categorías especiales de datos: Para efectos de este manual las categorías especiales y su tratamiento son las descritas en la LOPDP:2021, en el capítulo IV, desde el artículo 25 al 32, inclusive. (**GLOSARIO SKILLMAN-PDP:2021**)

F

Fuente accesible al público: Bases de datos que pueden ser consultadas por cualquier persona, cuyo acceso es público, incondicional y generalizado. (**Ley Orgánica de Protección de Datos Personales - 2021**)

G

Gestión de los riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Para ahondar en el detalle de como gestionar los riesgos, se debe leer la definición de Proceso para la gestión de riesgos. (**INEN ISO 27000: 2018**)