



PROCEDIMIENTO PARA LA GESTIÓN DE RIESGOS DE PROTECCIÓN DE DATOS PERSONALES

1. OBJETIVO

Establecer la documentación de los pasos a seguir a partir de la identificación de una situación que pone o puede poner en riesgo los datos personales de los titulares.

2. ALCANCE

El alcance del procedimiento de gestión de riesgos de privacidad de datos personales abarca la creación y mantenimiento de la documentación necesaria para guiar las acciones de la organización a partir de la identificación de situaciones que representen o puedan representar un riesgo para los datos personales de los titulares. Esto incluye la identificación de riesgos potenciales, la evaluación de su impacto y probabilidad, la implementación de medidas de mitigación, y la supervisión continua para asegurar la protección de los datos personales.

3. GLOSARIO

- **ÁREA O CARGO RESPONSABLE DE LA GESTIÓN.** Rol encargado de la gestión de la protección de datos, también conocido como Oficial de protección de datos.
- **ANÁLISIS DE RIESGO:** Proceso que permite comprender la naturaleza del riesgo y establecer el nivel de riesgo
- **CAUSALES DE INCIDENTE DE SEGURIDAD:** Un causal de incidente de seguridad se refiere a aquellas causas bajo las cuales se puede realizar la clasificación de un incidente de seguridad de datos personales
- **CONTROL:** Se interpretan como las medidas que transforman el riesgo. Los controles contienen los procesos, procedimientos, políticas, prácticas y dispositivos que cambian los riesgos
- **EVALUACIÓN DE RIESGOS:** Proceso de identificación, análisis y estimación de riesgos
- **GESTIÓN DE INCIDENTES DE SEGURIDAD:** La gestión de incidentes de seguridad se refiere a la documentación de los pasos a seguir una vez se ha detectado un incidente de seguridad de datos personales.
- **IMPACTO:** Se concibe como las consecuencias que puede originar o causar la materialización del riesgo
- **OFICIAL DE PDP.** Corresponde al área, cargo o persona responsable de la gestión de la protección de datos personales.
- **PDP.** Protección de datos personales
- **PLAN DE TRATAMIENTO DE RIESGOS:** Contempla las herramientas que determina las actuaciones o acciones para mitigar los riesgos de seguridad de la información y establecer los controles preciso para salvaguardar lo mismo.



- **RIESGO:** Posibilidad de que una amenaza, aproveche o explote una vulnerabilidad para causar una pérdida o daño en un activo de información. Esto suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias
- **RIESGO INHERENTE:** Dicta el nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.
- **RIESGO RESIDUAL:** El riesgo restante que permanece tras el tratamiento del riesgo que mitiga una pérdida o daño
- **SITUACIÓN DE RIESGO:** Una situación de riesgo corresponde a un evento, comportamiento, falta de control o acción que puede dar lugar a la materialización de un incidente de seguridad de datos personales.

3. DESCRIPCIÓN DEL PROCEDIMIENTO

Paso	Actividad	Descripción	Responsable	Registros
1	Validación y/o Identificación de riesgos	Realizar en el instrumento de valoración de riesgo la validación y/o identificación de riesgos que puedan presentarse como parte de la gestión y tratamiento de datos personales. Una vez hayan sido identificadas esas situaciones de riesgo potencial <u>continuar con el paso 2.</u>	Área, Cargo o persona responsable de la gestión y/o designado para el desarrollo de la actividad	Instrumento de Valoración de Riesgos
2	Validación y/o Identificación de causas de riesgo	Realizar en el instrumento de valoración de riesgo la validación y/o identificación de causas o situaciones que potencian o facilitan la materialización del riesgo que ha sido identificado. Una vez hayan sido validadas o identificadas <u>continuar con el paso 3</u>	Área, Cargo o persona responsable de la gestión y/o designado para el desarrollo de la actividad	Instrumento de Valoración de Riesgos
3	Calificación de probabilidad e impacto	Teniendo en cuenta las tablas 1 y 2 de la metodología para la gestión de riesgo realice en el instrumento de valoración de riesgo la calificación de la probabilidad de ocurrencia y del impacto que causaría la materialización de cada una de las causas identificadas. Una vez hayan calificado la	Área, Cargo o persona responsable de la gestión y/o designado para el	Instrumento de Valoración de Riesgos



¡Nosotros investigamos por ti, Y EN TIEMPO RÉCORD!

Leguizamón Asesorías SAS

probabilidad y el impacto para cada una de las causas identificadas continuar con el paso 4

desarrollo
de la
actividad

Cra. 13 #N° 51-25 Oficina 312, (Bogotá - Colombia)

3112754465 - 3203602262

leguizamonsas@leguizamonasas.com

4	Verificación de resultados riesgo inherente	Teniendo en cuenta las tablas 3 y 4 de la metodología para la gestión de riesgo establezca la zona en el que se encuentran tanto los riesgos como sus causas que ha identificado y calificado. Esto será visible en la pestaña [Mapa Inherente] del instrumento de valoración de riesgo. Una vez hayan verificado el estado de los riesgos inherentes <u>continuar con el paso 5</u>	Área, Cargo o persona responsable de la gestión y/o designado para el desarrollo de la actividad	Instrumento de Valoración de Riesgos
5	Identificación de controles	Identifique que controles actualmente aplica y que le pueden ayudar a evitar que el riesgo se materialice. Tenga en cuenta las causas que identifico para el riesgo como base para identificación de los controles. Una vez hayan identificado los controles <u>continuar con el paso 6</u>	Área, Cargo o persona responsable de la gestión y/o designado para el desarrollo de la actividad	Instrumento de Valoración de Riesgos
6	Calificación de controles	Teniendo en cuenta la tabla 5 de la metodología para la gestión de riesgos realice la calificación de los aspectos asociados a cada control, aspectos que permiten identificar la efectividad de un control. Una vez hayan realizado la calificación de los controles <u>continuar con el paso 7</u>	Área, Cargo o persona responsable de la gestión y/o designado para el desarrollo de la actividad	Instrumento de Valoración de Riesgos
7	Verificación de resultados riesgo Residual	Teniendo en cuenta las tablas 3 y 4 de la metodología para la gestión de riesgo establezca la zona en el que se encuentran tanto los riesgos como sus causas que ha identificado y calificado. Esto será visible en la pestaña [Mapa Residual] del instrumento de valoración de riesgo. Una vez hayan verificado el estado de los riesgos inherentes <u>continuar con el paso 8</u>	Área, Cargo o persona responsable de la gestión y/o designado para el desarrollo de la actividad	Instrumento de Valoración de Riesgos



¡Nosotros investigamos por ti, Y EN TIEMPO RÉCORD!

8	Verificación del informe de resultado	Verifique el nivel de riesgo residual de cada uno de los riesgos identificados y evaluados de acuerdo con las calificaciones suministradas. Una vez hayan verificado el nivel de los riesgos residuales <u>continuar con el paso 9</u>	Área, Cargo o persona responsable de la gestión y/o designado para el desarrollo de la actividad	Instrumento de Valoración de Riesgos
9	Identificar los riesgos que requieren planes de tratamiento	Teniendo en cuenta la tabla 4 de la metodología de gestión de riesgos, identifique cuales de los riesgos han quedado en una zona de riesgo critica o moderada y que por lo tanto son riesgos a los cuales se les debe definir un plan de tratamiento. Una vez identificados los riesgos <u>continuar con el paso 10</u>	Área, Cargo o persona responsable de la gestión y/o designado para el desarrollo de la actividad	Instrumento de Valoración de Riesgos
10	Definición de acciones de tratamiento	Documente las actividades o acciones que espera llevar a cabo en el corto, medio y largo plazo para mitigar o reducir el nivel de los riesgos que han quedado en una zona de riesgo critica o moderada. Una vez identificadas las actividades o planes de tratamiento <u>continuar con el paso 11 y 12</u>	Área, Cargo o persona responsable de la gestión y/o designado para el desarrollo de la actividad	Instrumento de Valoración de Riesgos
11	Monitoreo y Seguimiento	Realizar monitoreo y seguimiento a la ejecución de cada una de las actividades definidas para mitigar o reducir el nivel de los riesgos que han quedado en una zona de riesgo critica o moderada.	Área, Cargo o persona responsable de la gestión y/o designado para el desarrollo de la actividad	Instrumento de Valoración de Riesgos
12	Socialización	Realizar la socialización con cada una de las partes interesadas en la organización del resultado de la identificación y valoración de los riesgos. Una vez realizada la socialización <u>continuar con el paso 13</u>	Área, Cargo o persona responsable de la gestión y/o	Instrumento de Valoración de Riesgos. Informe o

Cra. 13 #N° 51-25 Oficina 312, (Bogotá - Colombia)
3412754465 - 3203602262
leguizamonsas@leguizamonesorias.com



¡Nosotros investigamos por ti, Y EN TIEMPO RÉCORD!

Leguizamón
Asesorías SAS

designado
para el
desarrollo
de la
actividad

presentación
de
socialización

13

Aprobación y
Respaldo

Realice la aprobación y almacenamiento del resultado de la identificación y valoración de riesgos realizada junto con el plan de tratamiento o actividades a realizar de la vigencia en la cual fue realizado.

Área, Cargo
o persona
responsable
de la gestión
y/o
designado
para el
desarrollo
de la
actividad

Instrumento
de
Valoración
de Riesgos
del ejercicio
realizado.

Cra. 13 #Nº 51-25 Oficina 312, (Bogotá - Colombia)
3112754465 - 3203602262
leguizamonsas@leguizamonasessorias.com