Cra. 13 #N° 51-25 Oficina 312, (Bogotá - Colombia)
3112754665 - 3203602262
l.leguizamon@leguizamonasesorias.com

Metodología para la Gestión de Riegos de Privacidad

1. OBJETIVO

Establecer la metodología sobre la cual se sustenta la gestión de riesgos asociados al tratamiento de datos personales que es requerida como parte de las obligaciones para el cumplimiento del artículo 26 del decreto 1377 de 2013 y la cual debe estar compuesta por las etapas de identificación, medición, control y monitoreo.

2. ALCANCE

Explicar y establecer las etapas y las variables sobre las cuales se desarrolla el sistema de administración de riesgo asociados al tratamiento de datos personales requerido como un aspecto fundamental dentro del cumplimiento de la responsabilidad demostrada.

3. DEFINICIONES

- Aceptación del Riesgo: Decisión informada de sumir un riesgo concreto.
- Activo: se refiere a cualquier información o elemento relacionado con el tratamiento de la seguridad de la información (sistemas, soportes, edificios, personas, etc.), que tenga valor para la entidad.
- Administración de Riesgos: Conjunto de actividades que permiten realizar la identificación, clasificación, análisis, evaluación, valoración, mitigación y monitoreo de los riesgos.
- Causa: Medios, circunstancias y o situaciones que llevan a la materialización de un riesgo
- Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de privacidad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- Impacto: El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.
- Plan de tratamiento de Riesgo: Documento que define las acciones para gestionar los riesgos de privacidad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- Probabilidad: Frecuencia de ocurrencia de un riesgo.
- Propiedad del Riesgo: Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.
- Riesgo: Posibilidad de que una causa concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo.
- Tratamiento de Riesgo: Proceso de modificar el impacto o probabilidad de ocurrencia de un riesgo, mediante la implementación de controles.

Cra. 13 #N° 51-25 Oficina 312, (Bogotá - Colombia)
3112754665 - 3203602262
l.leguizamon@leguizamonasesorias.com

- Valoración del Riesgo: Primera fase en la administración de riesgos, diagnóstico que consta de la identificación, análisis y determinación del nivel de riesgo.

4. GENERALIDADES

4.1. CONTEXTO ESTRATÉGICO

El responsable de la gestión de la protección de datos en compañía del recurso humano interno son los responsables de establecer un sistema que permita identificar, medir, controlar, y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que esta expuestos en desarrollo del cumplimiento de las normas de protección de datos personales.

4.2. IDENTIFICACIÓN DE LOS RIESGOS

La identificación de los riesgos se realiza con base a resultados de análisis de factores internos y externos, en donde se determinan o establecen los riesgos a que se ven expuestos los datos personales en desarrollo de su tratamiento.

4.3. MEDICIÓN DE LOS RIESGOS

La medición tiene por objeto determinar la posibilidad de ocurrencia de los riesgos relacionados con el tratamiento de datos personales y su impacto en caso de llegar a materializarse. Para realizar esta medición, se toman los valores de probabilidad e impacto relacionados en las siguientes tablas:

Niveles para Clasificar la Probabilidad			
Niveles de Probabilidad	**Descriptor**	**Descripción**	**Frecuencia**
5	Casi seguro	La causa ha ocurrido más de dos veces en el último año.	Mayor que 2 en 1 año
4	Probable	La causa ha ocurrido una vez en el último año	Igual a 1 en 1 año
3	Posible	La causa No ha ocurrido en el último año	Igual a 0 en 1 año
2	Improbable	La causa No ha ocurrido en un año y medio	Igual a 0 en 1 año y medio
1	Muy baja	La causa No ha ocurrido en dos años	Igual a 0 en 2 años

Tabla 1. Clasificación de la Probabilidad de ocurrencia

Niveles para Clasificar el Impacto		
Niveles para Clasificar	**Características de Seguridad**	**Impacto (consecuencias) Cualitativo**
Catastrófico	Integridad	Se genera más de un 80% de pérdida en la exactitud y completitud de los datos o información.
	Disponibilidad	Se imposibilita el uso o acceso a datos o información durante más de 8 horas.
	Confidencialidad	Se revela a individuos, entidades o procesos externos o internos no autorizados más de un 80% del total de los datos o la información.
Mayor	Integridad	Se genera más de un 60% y hasta un 80% de pérdida en la exactitud y completitud de los datos o información.
	Disponibilidad	Se imposibilita el uso o acceso a datos o información por más de 6 horas y hasta 8 horas.
	Confidencialidad	Se revela a individuos, entidades o procesos externos o internos no autorizados más del 60% y hasta un 80% del total de los datos o la información.
Moderado	Integridad	Se genera más de un 40% y hasta un 60% de pérdida en la exactitud y completitud de los datos o información.
	Disponibilidad	Se imposibilita el uso o acceso a datos o información por más de 4 horas y hasta 6 horas.
	Confidencialidad	Se revela a individuos, entidades o procesos externos o internos no autorizados más del 40% y hasta un 60% del total de los datos o la información.
Menor	Integridad	Se genera más de un 20% y hasta un 40% de pérdida en la exactitud y completitud de los datos o información.
	Disponibilidad	Se imposibilita el uso o acceso a datos o información por más de 2 horas y hasta 4 horas.
	Confidencialidad	Se revela a individuos, entidades o procesos externos o internos no autorizados más del 20% y hasta un 40% del total de los datos o la información.
Insignificante	Integridad	Se genera menos de un 20% de pérdida en la exactitud y completitud de los datos o información.
	Disponibilidad	La causa imposibilita el uso o acceso a datos o información por menos de 2 horas.
	Confidencialidad	Se revela a individuos, entidades o procesos externos o internos no autorizados hasta un 20% del total de los datos o la información.

Tabla 2 Clasificación del Impacto

Una vez determinado los valores de probabilidad e impacto que llegara a causar la materialización u ocurrencia del riesgo, se determina el nivel en el que se encuentra un determinado riesgo, multiplicando el valor de la probabilidad por el valor del impacto y ubicando el riesgo en su respectiva zona, conforme la matriz de calor que se describe a continuación:

Probabilidad	Valor	Evaluación				
Casi Seguro	5	51	52	53	54	55
Probable	4	41	42	43	44	45
Posible	3	31	32	33	34	35
Improbable	2	21	22	23	24	25
Muy Baja	1	11	12	13	14	15
	Valor	1	2	3	4	5
	Impacto	**Insignificante**	**Menor**	**Moderado**	**Mayor**	**Catastrófico**

Tabla 3 Matriz de evaluación y calificación de riesgos

El resultado de la medición de los riesgos determina en cuál de las cuatro (4) zonas de calor posibles se encuentra cada uno de los riesgos que han sido identificados y evaluados. De acuerdo con la zona de calor en la cual se encuentre un riesgo es el tratamiento o acciones que se deben adelantar así:

Valoración	Zona de Riesgo	Descripción Zona
Extrema	Zona de riesgo Critica	El riesgo debe ser tratado de manera inmediata, se deben implementar controles y actividades para mitigar el riesgo.
Alto	Zona de riesgo Alta	El riesgo debe ser tratado de manera prioritaria, se deben implementar controles y actividades para mitigar el riesgo.
Modera	Zona de riesgo moderada	El riesgo debe ser monitoreado, se recomienda establecer controles que lleven los riesgos en esta zona a una zona de riesgo moderado.
Bajo	Zona de riesgo tolerable	El riesgo es tolerable, se asume y se puede convivir con el sin desarrollar acciones o controles adicionales.

Tabla 4 Zonas del Riesgo

4.4. CONTROL DE LOS RIESGOS

El control de los riesgos se relaciona con la identificación de las acciones o controles que se ejecutan, ya sea que se encuentren documentados o no y que ayudan a disminuir la probabilidad y/o el impacto de la materialización de un riesgo. Para ello, es importante tener claridad sobre los controles existente, pues ello permite obtener información relevante para la toma decisiones y el tratamiento de los riesgos. La valoración de los controles se llevará a cabo a través de la revisión de los criterios establecidos y que se describen en la siguiente tabla.

Criterios	Opciones	Descripción	Puntaje
Tipo de Control	Detectivo	Permite identificar que algo ocurre	1
	Preventivo	Permite prevenir de algo ocurra	2

	Correctivo	Permite corregir algo que ocurrió	1
	Continuo	Se realiza todo el tiempo	3
Frecuencia	Periódico	Se realiza en momentos establecidos	2
	Esporádico	Se realiza pocas veces	1
Aplicación	Automático	El control no depende de nadie	3
	Semi-Automático	El control depende de la acción inicial de un sistema o una persona	2
	Manual o de Usuario	El control depende totalmente de una persona	1
Complejidad	Simple	El control requiere poco o nada de esfuerzo	3
	Moderado	El control requiere algo de esfuerzo	2
	Complejo	El control requiere mucho esfuerzo	1
Formalización	Está documentado	El control esta por escrito	3
	No está documentado	El control no está por escrito	1
Evidencia	Física / Electrónica	Siempre se puede saber si se realizó el control	3
	Informal	Se confía en que el control se realiza	2
	Ninguna	No hay forma de saber si el control se realizó	1
Recursos	Suficientes	Se cuenta con todo lo requerido para su optima ejecución	3
	Regulares	Se cuenta con parte de lo requerido para su optima ejecución	2
	Insuficientes	No se cuenta con lo requerido para su optima ejecución	1

Tabla 5 Criterios establecidos para la valoración de los controles

La anterior calificación de los controles define si el riesgo disminuye en probabilidad o impacto teniendo en cuenta que los controles preventivos reducen la probabilidad y los controles correctivos disminuyen el impacto, de acuerdo con los siguientes valores:

Puntaje de calificación de controles	Efectividad del control
6	18,33%
7	23,89%
8	29,44%
9	35,00%
10	40,56%
11	46,11%
12	51,67%
13	57,22%
14	62,78%
15	68,33%
16	73,89%
17	79,44%

Cra. 13 #N° 51-25 Oficina 312, (Bogotá - Colombia)
3112754665 - 3203602262
leguizamon@leguizamonasesorias.com

18		85,00%

Tabla 6 Efectividad de control de acuerdo con el puntaje de valoración

Con el resultado de la anterior valoración de los controles existentes se determina el riesgo residual, realizando el respectivo desplazamiento dentro de la matriz de evaluación y clasificación de los riesgos para realizar el respectivo tratamiento del riesgo.

4.5. TRATAR EL RIESGO

El objetivo de los controles es buscar la reducción de la probabilidad de ocurrencia o impacto de los riesgos. Dentro de las opciones a tener presentes para el tratamiento de los riesgos se encuentran:

- Evitar el riesgo: Tomar las medidas necesarias encaminadas a prevenir su materialización, esto se puede lograr cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas, que identifican en lo posible la causa raíz.
- Reducir el riesgo: Se puede lograr a través de la optimización de los procedimientos y la implementación de controles encaminados a disminuir el impacto y la probabilidad de ocurrencia.
- Compartir o transferir el riesgo: reduce su efecto buscando respaldo y compartir con otra parte el riesgo, por ejemplo, adquirir pólizas de seguros.
- Asumir o aceptar el riesgo: Se acepta la pérdida generada por el riesgo.

Una vez establecidas las opciones de tratamiento del riesgo, se determinan y evalúan los controles conforme al costo-beneficio, los mismos se documentan en la matriz de riesgos de privacidad de la información. Para realizar el respectivo seguimiento, se fijan las actividades a desarrollar para el cumplimiento de los controles, acciones a desarrollar (Aceptar, Mitigar, Evitar o Transferir), el plan de tratamiento, tipo de tratamiento, beneficios esperados, responsable, fecha de ejecución (Inicio y Fin).

4.6. IMPLEMENTAR Y MONITOREAR LOS CONTROLES

Una vez definidos los controles, se procede a implementar las actividades conforme a lo establecido en la Matriz de Riesgos de privacidad de la información, y se efectúa su respectivo monitorio dentro de los tiempos establecidos.

Se debe realizar un monitoreo constante con el fin de asegurarse que las acciones determinadas tengan el efecto esperado frente a la mitigación de los riesgos, o en caso contrario determinar las nuevas acciones necesarias para evitar situaciones o factores que puedan materializar el riesgo. Dicho seguimiento será registrado dentro de la matriz, en donde se dispondrán distintas casillas para su registro, evidenciando tanto el seguimiento, como las fechas de culminación de las actividades, así como posibles observaciones que se identifiquen.