Guía

de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales - Versión 2

Superintendencia de Protección de Datos Personales

Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales

2026

GUÍA DE GESTIÓN DE RIESGOS Y EVALUACIÓN DE IMPACTO DEL TRATAMIENTO DE DATOS PERSONALES

INTRODUCCIÓN

La Ley Orgánica de Protección de Datos Personales se fundamenta en la gestión de riesgos. En este contexto, la finalidad de la gestión de riesgos es reducir la incertidumbre de los responsables y encargados del tratamiento, con el propósito de que puedan tomar decisiones informadas para la protección efectiva y eficaz de los derechos y libertades de los titulares de datos personales. No obstante, tenemos que comprender que la gestión del riesgo no funciona por defecto, pues no se trata de elaborar listas de chequeo, estimar los niveles del riesgo sin fundamentos o escribir largos reportes sin sustancia desde una lógica de cumplimiento "en el papel". Al contrario, se trata de construir una cultura de la conformidad en riesgos; para lo cual, es fundamental aprender a utilizar datos confiables, calibrar las opiniones de expertos, construir métricas significativas y desarrollar modelos de riesgo adecuados.

La presente obra ha sido desarrollada con el fin de orientar a responsables y encargados del tratamiento hacia un cumplimiento real de la Ley Orgánica de Protección de Datos Personales (LOPDP), de una manera escalable. Consecuentemente, se establecen principios fundamentales para la gestión de riesgos y se exponen diversos métodos cuantitativos y cualitativos que pueden ser adaptados a las diferentes circunstancias de los responsables y encargados del tratamiento.

Los métodos expuestos para la evaluación de impacto del tratamiento de datos personales se fundamentan en la elaboración de escenarios de riesgos reales que pueden vulnerar los derechos y libertades de los titulares de datos personales.

La Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales tiene el agrado de presentar la **"Guía de gestión de riesgos y evaluación de impacto del tratamiento de datos personales – Versión 2"**. Este documento fue elaborado por Luis Enríquez Álvarez, Intendente General de Innovación Tecnológica y Seguridad de Datos Personales, y editado por Vanessa Hervás Novoa, asesora de la SPDP, con el apoyo del Superintendente de Protección de Datos Personales, Fabrizio Peralta-Díaz.

CONTENIDOS

I. PRINCIPIOS FUNDAMENTALES pág. 1

0. Definiciones aplicadas pág. 1

1. Gestión de riesgos para la protección de derechos y libertades pág. 4

1.1. Fundamentos
1.2. Objetivo
1.3. Etapas

2. Integración de los riesgos de seguridad de la información y la gestión de riesgos para la para la protección de derechos y libertades pág. 5

2.1. Interdependencias
2.2. Integración

3. Rol de los estándares de mejores prácticas pág. 6

3.1. Naturaleza
3.2. Objetivos
3.3. Beneficios
3.4. Advertencia

4. Justificación de todos los rationales pág. 8

4.1. Concepto
4.2. Rationales cuantitativos
4.3. Rationales cualitativos

5. Conformidad en riesgos pág. 9

5.1. Naturaleza
5.2. Rol de la gestión de riesgos
5.3. Protección de derechos
5.4. Principios para la estimación del riesgo

6. Auditorías pág. 11

6.1. Auditorías permanentes
6.2. Auditorías jurídicas
6.3. Auditorias organizacionales
6.4. Auditorías técnicas

7. Vulneraciones de la seguridad de datos personales pág. 13

7.1. Tipos de vulneraciones

7.2. Vulneraciones de confidencialidad
7.3. Vulneraciones de integridad
7.4. Vulneraciones de disponibilidad

II. PROCEDIMIENTOS SEGÚN CADA ETAPA DE LA GESTIÓN DE RIESGOS pág. 15

1. Establecimiento del Contexto pág. 16

1.1. Criterios de evaluación de riesgos para la protección de derechos y libertades
1.2. Criterios cualitativos de impacto
1.3. Criterios cuantitativos de impacto
1.4. Criterios de la probabilidad de ocurrencia
1.5. Integración en los criterios de evaluación de seguridad de la información
1.6. Aceptación del riesgo.
1.7. Integración entre el delegado de protección de datos y el departamento de seguridad de la información
1.8. Integración entre el delegado de protección de datos y el departamento jurídico
1.9. Integración entre el delegado de protección de datos y el departamento de gestión de riesgos

2. Identificación de riesgos de protección de datos personales pág. 25

2.1. Identificación de datos
2.2. Identificación de amenazas
2.3. Identificación de vulnerabilidades
2.4. Identificar escenarios de riesgo

3. Análisis de riesgos de protección de datos personales pág. 37

3.1. Modelar el riesgo
3.2. Análisis cuantitativo
3.3. Métodos cuantitativos de análisis
3.4. Modelos cuantitativos de riesgo
3.5. Representación cuantitativa del riesgo
3.6. Análisis cualitativo
3.7. Métodos cualitativos de análisis
3.8. Modelos calibración de opiniones
3.9. Representación cualitativa del riesgo

4. Evaluación de riesgos de protección de datos personales pág. 56

4.1 Evaluación de impacto del tratamiento de datos personales
4.2. Etapas previas
4.3. Contenidos
4.4. Integración de resultados
4.5. Integración en una evaluación holística de riesgos

5. Tratamiento de riesgos de protección de datos personales pág. 67

5.1. Etapas previas
5.2. Taxonomías de controles de riesgos
5.3. Retorno a la inversión en seguridad de datos
5.4. Interdependencias de controles
5.5. Calificadores frágiles e inestables
5.6. Modelos de tratamiento de riesgos
5.7. Monitoreo de manejo de variaciones de los controles de los riesgos
5.8. Modelos de tomas de decisiones
5.8. Estrategias

ANEXO: Ejemplo de formato de una evaluación de impacto del tratamiento de datos personales. pág. 75

ABREVIACIONES

CISO: Chief Information Security Officer.

CoBiT: Control Objectives for Information Technologies.

Cy-VaR: Cyber Value at Risk.

DAMA-DMBOK: Data Management Body of Knowledge.

DPD: Delegado de Protección de Datos Personales.

DOS: Denial of Service.

DDOS: Distributed Denial of Service.

EGSI: Esquema Gubernamental de Seguridad de la Información.

FAIR: Factor Analysis of Information Risk.

ISO: International Organization for Standardization.

LOPDP: Ley Orgánica de Protección de Datos Personales.

MAE: Mean Absolute Error.

MIPYMES: Micro, pequeñas y medianas empresas.

MITM: Man in the Middle.

NLP: Natural Language Processing.

NIST: National Institute of Standards and Technology.

OSI: Oficial de Seguridad de la Información.

OSINT: Open Source Intelligence.

OWASP: Open Web Application Security Project.

PCI-DSS: Payment Card Industry Data Security Standard.

Pd-VaR: Personal Data Value at Risk.

Pen testing: Test de penetración.

PERT: Program Evaluation and Review technique.

PYMES: Pequeñas y medianas empresas.

RAE: Real Academia Española.

RAT: Registro de actividades del tratamiento.

RGPD: Reglamento General de Protección de Datos (UE) 2016/679.

RLOPDP: Reglamento a la Ley Orgánica de Protección de Datos Personales.

ROSI: Retorno a la Inversión en Seguridad.

RPO: Recovery Point Objective.

RTO: Recovery Time Objective.

SOC: Security Operations Center.

SPDP: Superintendencia de Protección de Datos Personales.

TPRM: Third Party Risk Management.

VaR: Value at Risk.

I. PRINCIPIOS FUNDAMENTALES

Este primer título es de carácter obligatorio, cuya finalidad es cumplir con los principios fundamentales de la gestión de riesgos para la protección de los derechos y libertades de los titulares de datos. A continuación, se explican los fundamentos de la gestión de riesgos, los cuales son esenciales para reducir la incertidumbre inherente en diversos escenarios de riesgo, a partir del conocimiento y las mejores prácticas.

0. Definiciones aplicadas

Análisis de riesgos. La detallada calibración de los componentes del riesgo, incluyendo la evaluación de las probabilidades de ocurrencia de varios eventos y su impacto, con la finalidad de tomar decisiones informadas para proteger los derechos y libertades de los titulares de datos personales.

Amenaza. Potencial causa de un incidente que vulnere los derechos y libertades de los titulares de datos personales.

Analítica predictiva legal. Es el proceso de utilizar análisis de datos para comprender en profundidad los casos y decisiones jurídicas.

Calibración del riesgo. La calibración es un método para mejorar la capacidad de un individuo para hacer buenas estimaciones acerca de la probabilidad o frecuencia de ocurrencia y de la magnitud del impacto de un riesgo.

Comunidades de amenaza. Grupos de personas que pueden aprovecharse de una vulnerabilidad para materializar un riesgo que puede vulnerar los derechos y libertades de los titulares de datos.

Capacidad de la amenaza. Experiencia, conocimiento, y recursos de la amenaza que pueden aprovechar una vulnerabilidad para vulnerar los derechos y libertades de los titulares de datos.

Confidencialidad. Propiedad de que los datos personales no se pongan a disposición o se divulguen a personas, entidades no autorizadas por el titular de los datos u por otra causal que justifique la legitimidad del tratamiento de datos.

Disponibilidad. Propiedad de los datos para ser accesibles y utilizables bajo el control del titular de datos u otra causal que justifique la legitimidad del tratamiento de datos.

Evaluación de impacto del tratamiento de datos personales. Es la evaluación de los niveles de los riesgos en el tratamiento de datos personales que pueden vulnerar los derechos y libertades de los titulares de datos, y/o no cumplir con las obligaciones establecidas en la LOPDP. Para realizarla es fundamental haber cumplido con las etapas anteriores de establecimiento del contexto, identificación de riesgos y análisis de riesgos.

Frecuencia de ocurrencia. Cantidad de eventos estimados en un lapso determinado que puede vulnerar los derechos y libertades de los titulares de los datos personales.

Gestión de riesgos para la protección de los derechos y libertades. Es la identificación, análisis y priorización de riesgos para reducir la incertidumbre, con la finalidad de tomar decisiones informadas en la implementación de medidas de seguridad jurídicas,

organizacionales y técnicas para reducir la probabilidad de ocurrencia y el impacto de incidentes no deseados que pudiesen vulnerar los derechos y libertades de los titulares de datos personales.

Impacto. Consecuencias de la materialización de un riesgo en los derechos y libertades de los titulares de datos personales.

Impactos primarios. Consecuencias de la materialización de un riesgo en los derechos y libertades de los titulares de datos personales que afectan directamente al titular.

Impactos secundarios. Consecuencias de la materialización de un riesgo en los derechos y libertades de los titulares de datos personales que afectan directamente al titular, pero debido a las reacciones de otros interesados.

Incertidumbre aleatoria. Es un tipo de incertidumbre irreducible y random, por cuanto se debe a una probabilidad inherente de un elemento en un espacio de sampleo. Por ejemplo, al lanzar un dado, la probabilidad de que salga un '3' es de '1/6' por cada intento.

Incertidumbre epistemológica. Es un tipo de incertidumbre reducible y sistemática, originada por la falta de conocimiento sobre un sistema o proceso. Es el caso de la gestión de riesgos para la protección de derechos y libertades; en la cual, la incertidumbre puede ser reducida con mayor conocimiento en áreas como el derecho de protección de datos personales, la seguridad de la información, la gestión de riesgos, y sobre todo, el contexto interno de cada institución.

Integridad. Propiedad en la que los datos personales no han sido alterados sin autorización de los titulares de datos o por otra causal que justifique la legitimidad del tratamiento de datos.

Jurimetría. Estudio cuantitativo del derecho.

Metarregulación. Modelo regulatorio mediante el cual la Superintendencia de Protección de Datos Personales supervisa la autorregulación de los responsables y encargados del tratamiento de datos personales.

Modelos de aprendizaje automático. Metodologías de la inteligencia artificial que utilizan algoritmos entrenados con sets de datos para crear modelos que pueden tomar decisiones o clasificar información sin la intervención de humanos.

Opiniones de expertos. Opiniones de personas naturales experimentadas con un alto grado de conocimiento en derecho, seguridad y gestión de protección de datos personales.

Perfilamiento de amenazas. Comprensión de los métodos y características de las comunidades de amenaza para materializar un riesgo.

Probabilidad de ocurrencia. Probabilidad de que suceda un riesgo que puede vulnerar los derechos y libertades de los titulares de los datos en un lapso determinado. Se pueden estimar entre 0 y el 1, en percentiles y en porcentajes.

Rationale. Justificación de las métricas, modelos de riesgo y criterios utilizados para calibrar los componentes del riesgo.

Resiliencia. Grado o porcentaje de resistencia frente a eventos que pueden vulnerar los derechos y libertades de los titulares de datos. Estado de madurez de la conformidad a la LOPDP.

Riesgo. Una pérdida potencial, desastre u otro evento no deseado que puede vulnerar los derechos y libertades de los titulares de datos personales. Debe ser estimado con probabilidades y/o frecuencias de ocurrencia asignadas a impactos de varias magnitudes.

Riesgo inherente. Son los niveles de la probabilidad de ocurrencia y del impacto preexistente en un escenario de riesgo, sin la implementación de nuevas medidas de seguridad jurídicas, organizacionales y técnicas.

Riesgo residual. Son los niveles de la probabilidad de ocurrencia y del impacto en un escenario de riesgo, que permanecen una vez que se han implementado nuevas medidas de seguridad jurídicas, organizacionales y técnicas.

Ruido. Deficiente estimación de la probabilidad de ocurrencia, de los niveles y de la magnitud del riesgo.

Sesgo. Prejuicio que puede afectar la objetividad de una decisión.

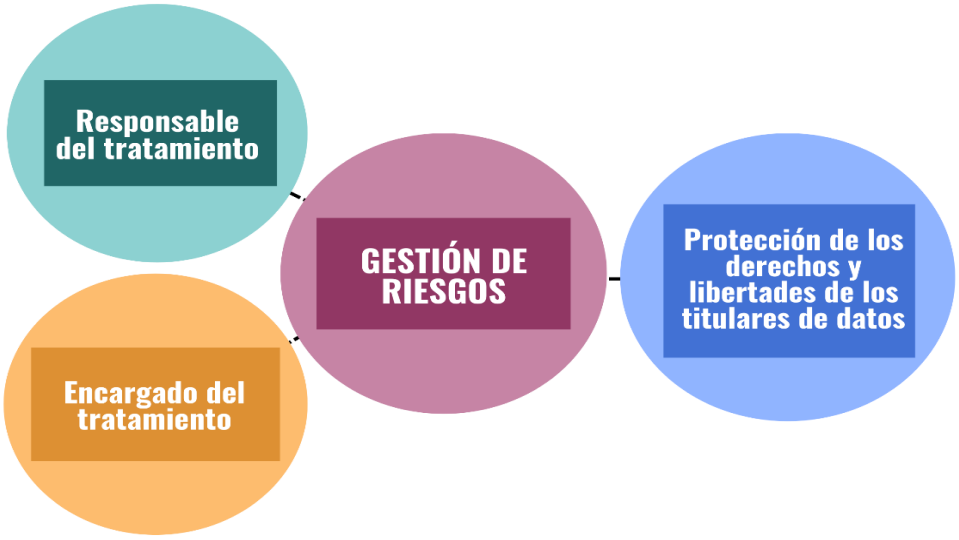
Vulnerabilidad. Debilidad de un activo o control que puede ser utilizada para que se produzca un evento con un efecto negativo, que puede vulnerar los derechos y libertades de los titulares de datos personales.

Vulnerabilidades jurídicas. Debilidades en el cumplimiento jurídico de conformidad a la normativa ecuatoriana de protección de datos personales que puede ser aprovechada por una amenaza para que se produzca un evento con un efecto negativo en los derechos y libertades de los titulares de datos personales.

Vulnerabilidades organizacionales. Debilidades de estrategias, procesos, políticas, operaciones y tácticas que pueden ser utilizadas para que se produzca un evento con un efecto negativo en los derechos y libertades de los titulares de datos personales.

Vulnerabilidades técnicas. Debilidades del software y/o del hardware las cuales usualmente no son visibles sin herramientas especializadas para identificarlas. Todas las vulnerabilidades del software pueden potencialmente vulnerar los derechos y libertades de los titulares de datos personales.

1. Gestión de riesgos para la protección de derechos y libertades



1.1. Fundamentos. La LOPDP[1] se fundamenta en la gestión de riesgos para la protección de los derechos y libertades de los titulares de los datos. Esto quiere decir que, para que los responsables y encargados del tratamiento cumplan con las obligaciones establecidas en la LOPDP, están obligados a reducir al máximo posible la probabilidad de ocurrencia y el impacto que pueden sufrir los titulares de los datos en diversos escenarios de riesgo relacionados al tratamiento de datos personales.

1.2. Objetivo. La gestión de riesgos debe ser entendida como un mecanismo indispensable para que los responsables y encargados del tratamiento puedan tomar decisiones informadas para proteger los derechos y libertades de los titulares de los datos. Un exitoso manejo de riesgos implica disminuir la incertidumbre para tomar decisiones informadas en la implementación de medidas de seguridad en el tratamiento de datos personales. Es obligación de los responsables y encargados del tratamiento, prevenir la materialización de potenciales riesgos que pudiesen vulnerar derechos y libertades de los titulares de datos, a través del desarrollo de modelos adecuados de riesgo, métricas significativas y comparaciones efectivas entre diversos escenarios de riesgo. Es fundamental comprender que en cualquier tipo de conflicto entre normas y principios, siempre deberá prevalecer la protección de derechos y libertades de los titulares de datos personales.

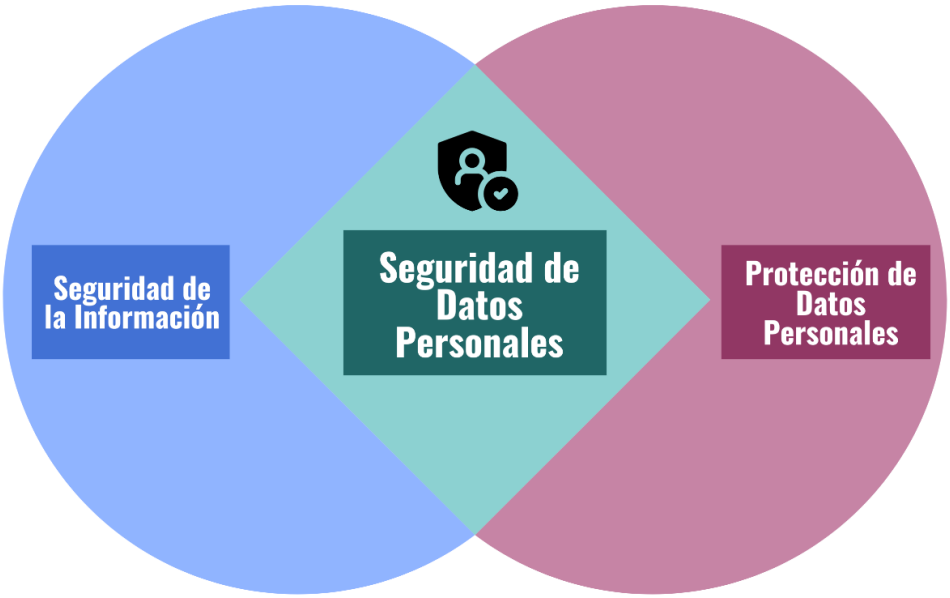
1.3. Etapas. Una gestión de riesgos incluye al menos cinco etapas: establecimiento del contexto, identificación de riesgos, análisis de riesgos, evaluación de riesgos y tratamiento de riesgos[2]. Es fundamental cumplir con estas cinco etapas de manera efectiva, pues la finalidad de la gestión de riesgos debe ser tomar decisiones informadas para proteger los derechos y libertades de los titulares de los datos, evitando a toda costa un ejercicio de conformidad superficial a la LOPDP. A estas cinco etapas se suman los objetivos de comunicación y de monitoreo.

---

[1] Al referirse a la conformidad a la LOPDP, se comprende a la normativa de protección de datos personales del Ecuador, incluyendo el Reglamento de la LOPDP y la normativa emitida por la Superintendencia de Protección de Datos Personales.

[2] Se recomienda seguir las directrices del Estándar ISO/IEC 27005:2022. Ver https://www.iso.org/standard/80585.html.

2. Integración de la gestión de riesgos para la protección de derechos y libertades con la gestión riesgos de seguridad de la información



2.1. Interdependencias. Los riesgos de seguridad de la información y los riesgos de conformidad a la LOPDP son interdependientes. Eso quiere decir que deben ser analizados de manera holística, integrando de manera efectiva riesgos jurídicos, riesgos de seguridad de la información y otros riesgos operacionales. A la luz de la LOPDP, todo riesgo de seguridad de la información vinculado al tratamiento de datos personales se convierte en un probable riesgo contra los derechos y libertades de los titulares de datos.

2.2. Integración. Es fundamental encontrar mecanismos de integración entre el área jurídica, el área de seguridad de la información y el área de gestión de riesgos. Se recomienda la interacción permanente entre Delegados de Protección de Datos, abogados, Oficiales de Seguridad de la Información y Oficiales de riesgo, con el fin de construir estrategias, operaciones y tácticas encaminadas a manejar de manera adecuada los riesgos de cumplimiento de la LOPDP.

3. Implementación de estándares de mejores prácticas

3.1. Naturaleza. Los estándares de mejores prácticas son útiles para el cumplimiento de las obligaciones establecidas en la LOPDP. Sin embargo, no existen estándares que sean específicos para la conformidad a la LOPDP. Consecuentemente, es necesario aprender a utilizarlos en función de las necesidades específicas de la protección de datos personales. No obstante, el EGSI, en el caso de instituciones públicas, y los marcos de gestión de riesgos empresariales ya existentes en instituciones privadas, pueden ser considerados adecuados para cumplir con los requisitos del Capítulo I, siempre que se complementen con un enfoque orientado a salvaguardar los derechos y libertades de los titulares de datos personales. Si se trata del EGSI, deberá cumplirse con los principios establecidos en el primer capítulo de esta guía.

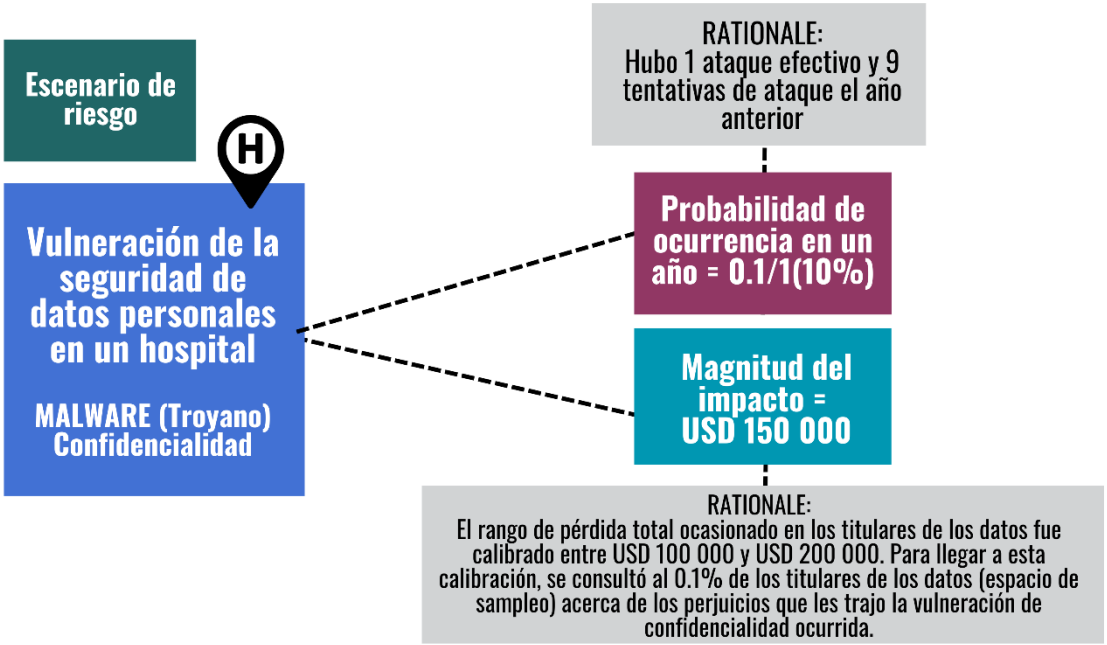
3.2. Objetivos. Los estándares de mejores prácticas cumplen con diferentes objetivos. Por ejemplo, la norma ISO/IEC 27701 es útil para la implementación de sistemas de gestión de privacidad. Las normas ISO/IEC 27001 y 27002 son útiles para la implementación de sistemas de gestión de seguridad de la información. La norma ISO/IEC 42001 para implementar sistemas de gestión de inteligencia artificial. La norma DAMA-DMBOK para gobernanza y gestión de datos. Otros estándares son útiles para áreas específicas, como el PCI-DSS para el tratamiento de pagos con tarjetas de crédito; o, el OWASP ASVS para la seguridad de aplicaciones Web.

3.3. Beneficios. Se recomienda la implementación de sistemas de gestión de seguridad de la información, sistemas de implementación de gestión de privacidad, sistemas de gestión de control de calidad y cualquier otro que ayude a implementar un proyecto de conformidad a estándares de mejores prácticas. Los estándares de mejores prácticas ayudan a tener orden en la gestión y tener la trazabilidad de las acciones realizadas por los responsables o encargados del tratamiento.

3.4. Advertencia. Hay que tomar en cuenta que conformarse a estándares de mejores prácticas es útil, pero no garantiza la conformidad a la LOPDP. Se trata más bien de guías para la implementación de proyectos de seguridad de la información, de privacidad y

taxonomías de controles de riesgos. Ellos no abarcan la conformidad jurídica directa con la LOPDP, no proveen el insumo de datos necesarios para la gestión de riesgos, no proveen métricas para protección de datos personales, ni tampoco proveen modelos de riesgos de protección de datos personales adaptados a contextos específicos. El capítulo II de esta guía contiene explicaciones detalladas en estos ámbitos. Por otro lado, se aclara que se trata de una obligación fundamentada en el principio de escalabilidad, considerando la cantidad y la criticidad de procesos que involucren el tratamiento de datos personales, el tamaño de la institución y su facturación anual.

4. Justificación de todos los rationales

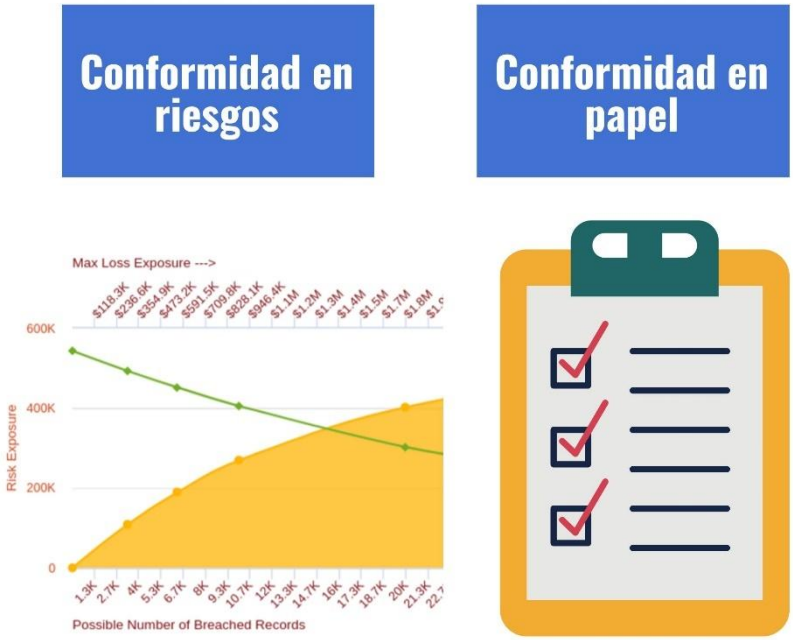


4.1. Concepto. Un *rationale* debe ser entendido como el razonamiento de respaldo que sustenta cualquier valor de entrada utilizado en una gestión de riesgos. Su propósito se fundamenta en evitar ingresar valores sin sustento que pueden distorsionar el análisis de riesgos para la protección de derechos y libertades de los titulares de datos. Los responsables y encargados del tratamiento están obligados a justificar cualquier estimación cuantitativa o cualitativa con respecto al probable impacto de una gestión de riesgos en los derechos y libertades de los titulares de datos.

4.2. Rationales cuantitativos. En el análisis cuantitativo, los *rationales* serán justificados en función de métodos frecuentistas, estadísticos, Bayesianos, de probabilidad condicional, análisis de Monte Carlo, *conformal prediction* y similares. Estos datos serán representados en distribuciones de probabilidades, curvas de superación de pérdidas, entre otros, que justifiquen en números las razones para estimar dicho valor.

4.3. Rationales cualitativos. En el análisis cualitativo, los *rationales* serán justificados en función de la opinión de expertos. Sin embargo, según el caso y los recursos disponibles, se recomienda utilizar métodos de calibración de opiniones de expertos, como el método Delphi, el modelo Lens o cualquier otro enfoque racional que respalde los datos de entrada y las etiquetas utilizadas en matrices de riesgos, registros de riesgos o métodos afines de representación del riesgo. En el caso de responsables y encargados del tratamiento pequeños como Pymes y MiPymes, contar con un sólo experto es factible cuando éste aprende a calibrar sus opiniones.

5. Conformidad en riesgos



5.1. Naturaleza. La LOPDP tiene obligaciones de diferente naturaleza, algunas de la cuales pueden cumplirse al llenar y enviar registros o llenar notificaciones en el plazo determinado por la LOPDP. Sin embargo, las obligaciones vinculadas al tratamiento de datos personales deben resolverse a través de la gestión de riesgos, es decir, modelar acerca de cómo el incumplimiento a la LOPDP puede impactar a los titulares de datos. Los responsables y encargados del tratamiento deben cumplir con el principio de responsabilidad proactiva y demostrada en los procesos de gestión de riesgos con respecto a todo tratamiento de datos personales.

5.2. Rol de la gestión de riesgos. La LOPDP requiere de la gestión de riesgos como el mecanismo para disminuir la incertidumbre para mitigar la probabilidad de ocurrencia y el impacto de materialización de riesgos que pudiesen vulnerar los derechos y libertades de los titulares de los datos y disminuir el impacto. El riesgo es dinámico y debe ser calibrado de manera constante. Por ello, no se trata de presentar grandes cantidades de papeles declarativos a la SPDP; sino, más bien, de justificar los procedimientos utilizados para mitigar los riesgos en el tratamiento de datos personales.[3]

5.3. Protección de derechos. La gestión de riesgos no pone en cuestión la protección al cien por ciento de los derechos y libertades de los titulares de los datos. Si bien el riesgo residual es inevitable, en riesgos operacionales como los de la seguridad de datos, los responsables y encargados del tratamiento están obligados a disminuir los niveles de riesgo en el tratamiento de datos al máximo posible.

[3] Para ampliar sus conocimientos sobre la conformidad en riesgos, se recomienda la siguiente obra: Gellert, R. (2020). *The Risk Based Approach to Data Protection,* Oxford University Press, Reino Unido.

5.4. Principios para la estimación del riesgo. La gestión de riesgos es fundamental para la toma de decisiones informadas. No obstante, para incrementar la confianza en las estimaciones sobre los niveles de riesgo, se recomienda considerar los siguientes criterios[4]:

a) Objetividad. Las estimaciones no deben sustentarse en opiniones no fundamentadas pues pueden contener sesgos (prejuicios) y ruido (entendido como problemas de estimación)[5]. Es preferible sustentarse en datos confiables, estadísticas y métricas. Sin embargo, cuando no se disponga de datos confiables, se recomienda recurrir a métodos de calibración de opiniones de expertos.

b) Rangos de acierto. Es conveniente realizar las estimaciones en rangos de acierto en lugar de valores precisos. Por ejemplo, el rango del impacto de un ataque de *ransomware* es mejor calibrarlo en rangos, como un rango entre $12 000 y $16 000, en lugar de estimar un valor preciso como $14 359.

c) Probabilidad sobre posibilidad. La probabilidad de que ocurra un riesgo es estimable e informativa, con resultados medibles en porcentajes o percentiles. La posibilidad es de naturaleza binaria, pues un riesgo es posible o simplemente no lo es. Por ejemplo, un escenario de riesgo de vulneración de la seguridad de datos personales es posible, aunque la probabilidad de ocurrencia sea de un valor bajo del 0.01%. Por lo tanto, la mitigación de riesgos funciona bajo una lógica de probabilidad y no de posibilidad.

d) Tipos de cumplimiento normativo. Hay tipos de cumplimiento en la LOPDP que pueden solucionarse bajo una lógica binaria; como cumplir con los plazos de notificaciones, cumplir con los registros obligatorios o cumplir con ciertos mecanismos para el ejercicio de derechos de los titulares de los datos. Sin embargo, en un entorno probabilístico como los riesgos de la seguridad de la información y los riesgos de la analítica predictiva, es necesario seguir todas las recomendaciones anteriormente establecidas para la estimación del riesgo. Es importante tener en cuenta que los responsables o encargados del tratamiento pueden estar sujetos a obligaciones adicionales impuestas por otras autoridades de control, como ocurre en sectores regulados como el financiero o el de las telecomunicaciones. Esta guía está enfocada específicamente en la gestión de riesgos vinculados a la protección de los derechos y libertades de los titulares de datos personales, así como al cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP). En caso de que existan obligaciones derivadas de normativa especializada, se deberá observar lo dispuesto en el artículo 11 de la LOPDP, que establece la aplicación complementaria de las disposiciones contenidas en dicha ley.

---

[4] Para ampliar su conocimiento sobre estos principios del manejo de riesgos, se recomienda la siguiente obra: Freund, J., Jones, J. (2015). *Measuring and Managing Information Risk: a FAIR Approach.* Butterworth-Heinemann, 1st edition.

[5] Para ampliar sus conocimientos sobre la influencia del sesgo y el ruido en la toma de decisiones, se recomienda la siguiente obra: Kahneman, D., Sibony, O., *et al*. (2021). *Noise A Flaw in Human Judgment*, Harper Collins Publishers.

6. Auditorías

6.1. Auditorías permanentes. Los responsables y encargados del tratamiento están obligados a realizar auditorías periódicas con respecto al tratamiento de datos personales. Auditar es verificar el cumplimiento en normas y riesgos con respecto a las obligaciones establecidas en la LOPDP para el tratamiento de datos. Es necesario realizar auditorías jurídicas, auditorías organizacionales y auditorías técnicas.

6.2. Auditorías jurídicas. Son las auditorías de cumplimiento a la LOPDP. El auditor debe constatar que se cumplan en la práctica los principios del tratamiento de datos personales, el ejercicio de los derechos de los titulares de los datos, las obligaciones de llenar los registros de la SPDP y demás establecidas en la LOPDP, su Reglamento y en las Resoluciones emitidas por la Superintendencia de Protección de Datos Personales. Por ejemplo, no se trata únicamente de constatar que existe una política de protección de datos personales, sino de que los titulares de los datos cuentan con mecanismos para ejercer sus derechos, tales como contar con los privilegios necesarios para controlar sus datos personales desde su espacio Web; o, al menos, un correo electrónico de contacto para poder ejercerlos con celeridad. Es obligatorio que los auditores jurídicos sean expertos en derecho de protección de datos personales.

6.3. Auditorías organizacionales. Son esenciales para el cumplimiento a la LOPDP. Para ello es muy útil la implementación de sistemas de gestión de privacidad y de seguridad de la información. Se recomienda que las políticas de seguridad de la información y de seguridad de datos personales se fundamenten en normas y modelos tales como la ISO/IEC27001, ISO/IEC 27702, ISO/IEC 27005, COBIT, FAIR, FAIR-CAM, entre otros, con el fin de abarcar las áreas necesarias de controles de riesgos. Sin embargo, lo esencial es el cumplimiento en el campo práctico. Las políticas de seguridad de la información deben ser adaptadas a la conformidad de la LOPDP. Es necesario que los auditores sean expertos en

seguridad organizacional en conformidad a estándares de mejores prácticas de seguridad de la información y de gobernanza de datos.

6.4. Auditorías técnicas. Consisten en identificar las vulnerabilidades del software; y, en algunos escenarios, también del hardware. Estas se encuentran en el código fuente, y en todo tipo de dependencias del software. Las vulnerabilidades técnicas no son visibles, por lo cual el auditor debe tener un conocimiento especializado en el campo, siendo recomendable contar con auditores expertos en áreas como el manejo de vulnerabilidades de software, desarrollo de *exploits*, hackeo ético, test de penetración, respuesta a incidentes e informática forense. Hacer la seguridad visible es un gran desafío, pues todo el software tiene vulnerabilidades que deben ser detectadas y corregidas en el menor tiempo posible.

7. Prevención de vulneraciones de la seguridad de datos personales

7.1. Tipos de vulneraciones. Las vulneraciones de la seguridad de datos personales son violaciones a cualquiera de las tres dimensiones de la seguridad de la información: vulneraciones de la confidencialidad, vulneraciones de la integridad y vulneraciones de la disponibilidad. Toda vulneración de seguridad de la información puede ocasionar la violación de los derechos y libertades de los titulares de los datos. Por ello, existe la obligación de los responsables y encargados del tratamiento de notificar a la SPDP ante cualquier sospecha de una vulneración de datos personales en el plazo de cinco días establecido en la LOPDP.

7.2. Vulneraciones de la confidencialidad. Las vulneraciones de seguridad de la confidencialidad de datos personales consisten en el acceso, distribución, y/o publicación de datos personales sin la autorización del titular de los datos; o, sin una base legal que así lo justifique. Cuando un incidente compromete las medidas de seguridad implementadas por responsables y encargados del tratamiento, puede existir una vulneración contra los derechos y libertades de los titulares de los datos. En dependencia del tipo de datos y sus circunstancias de tratamiento, pueden tener un impacto negativo irreversible en los derechos de las personas concernidas. Es fundamental construir escenarios de riesgos de la confidencialidad de datos personales.

7.3. Vulneraciones de la integridad. Las vulneraciones de seguridad contra la integridad de los datos consisten en alterar los datos personales de los titulares de datos. Estas vulneraciones pueden ser temporales cuando el responsable o encargado del tratamiento ha implementado las medidas necesarias para detectar y recuperar la integridad de los datos. Es fundamental construir escenarios de riesgo de la integridad de datos personales.

7.4. Vulneraciones de la disponibilidad. Las vulneraciones de seguridad contra la disponibilidad de datos personales consisten en impedir el acceso o eliminar los datos

personales de los titulares de datos. Estas vulneraciones pueden ser temporales cuando el responsable o encargado del tratamiento ha implementado las medidas necesarias para restaurar los datos. Es fundamental construir escenarios de riesgo de la disponibilidad de datos personales.

II. PROCEDIMIENTOS SEGÚN CADA ETAPA DE LA GESTIÓN DE RIESGOS

Este segundo capítulo tiene la finalidad de mostrar diferentes métodos y recursos para poder sustentar los *rationales* en una gestión de riesgos para la protección de derechos y libertades. Es importante considerar que la LOPDP establece, en el artículo 40, la obligación de responsables y encargados del tratamiento de realizar un análisis de riesgo, amenazas y vulnerabilidades. El establecimiento del contexto y la identificación de riesgos son etapas obligatorias para realizar un análisis de riesgos. Lo mismo sucede con la obligación para los responsables y encargados del tratamiento para implementar medidas de seguridad en el tratamiento de datos personales, que establece la LOPDP en el artículo 37. No se debe implementar medidas de seguridad en la etapa de tratamiento de riesgos, sin haber cumplido con las cuatro etapas anteriores.

Por otro lado, la obligación de los responsables del tratamiento para realizar una evaluación de impacto establecida en el artículo 42 de la LOPDP, tampoco puede cumplirse sin haber realizado las etapas anteriores de la gestión de riesgos. No se debe realizar una evaluación de impacto del tratamiento de datos personales sin haber realizado el establecimiento del contexto, la identificación y el análisis de riesgos.

Los responsables y encargados del tratamiento podrán utilizar y personalizar los métodos que les sean más efectivos y eficaces de manera opcional y escalable, de acuerdo con sus propias circunstancias. Esto no contradice que todos los conceptos fundamentales establecidos en el primer título deben de ser considerados para la gestión de riesgos de manera obligatoria; sino, más bien, que los regulados tengan conocimiento de varios métodos, métricas y modelos de riesgo que pueden utilizarse para conseguir estos objetivos. Los procesos establecidos en cada etapa de gestión de riesgos tienen dos enfoques. En primer lugar, un enfoque desde el probable impacto que pueden recibir los titulares de los datos. En segundo lugar, la integración de la gestión de riesgos para la protección de los derechos y libertades de los titulares de datos con la gestión de riesgos operacionales, jurídicos y financieros de conformidad a la LOPDP. Si bien esta guía se centra en el primer enfoque, muchos de estos métodos pueden también utilizarse en la integración entre la gestión de riesgos para la protección de derechos y libertades, con la gestión de riesgos de seguridad de la información.

1. Establecimiento del contexto

La primera etapa de una gestión de riesgos tiene como fines: establecer los criterios de evaluación de riesgos para la protección de derechos y libertades, determinación de las metodologías y modelos de riesgo a implementarse de acuerdo con el contexto de la institución; y, la interacción entre el delegado de protección de datos y otras áreas de la organización. Para establecer el contexto, es recomendable tener claro los fundamentos de la gestión de riesgos para la protección de los derechos y libertades de los titulares de los datos.

1.1. Criterios de evaluación de riesgos para la protección de derechos y libertades

El primer paso para la gestión de riesgos es establecer los criterios de evaluación del riesgo para la protección de los derechos y libertades de los titulares de los datos. Para ello, será necesario considerar especialmente los siguientes aspectos: a) tratamiento de categorías especiales de datos (como datos sensibles), b) vulnerabilidades de grupos especiales de titulares de datos, c) la cantidad de titulares de datos afectados, d) la naturaleza de la infracción o el tipo de vulneración de la seguridad de datos y e) el volumen de datos personales.

a) Tratamiento de categorías especiales de datos. En primer lugar, las categorías especiales están definidas en el artículo 25 de la LOPDP. Los responsables y encargados del tratamiento deben identificar los tipos de datos personales que procesan, previo al establecimiento de los criterios de evaluación con el fin de clasificar el impacto de manera adecuada; tomando en cuenta que, el tratamiento de ciertas categorías especiales de datos como los datos sensibles, proporcionalmente ocasionarán un mayor impacto en los derechos y libertades de los titulares de los datos.

b) Las vulnerabilidades de grupos especiales de titulares de datos. En segundo lugar, la LOPDP establece de manera específica a los menores de edad como un grupo de titulares de datos particularmente vulnerable; pero, establece de manera genérica, a cualquier otro grupo vulnerable en el artículo 40 (2). Los responsables del tratamiento deberán tomar en cuenta a grupos en función de la edad, género, nivel educativo, nivel socioeconómico, discapacidades, etnia y cualquier otro factor que pueda amplificar el impacto que pueda sufrir durante el tratamiento de datos o como consecuencia del tratamiento de datos personales.

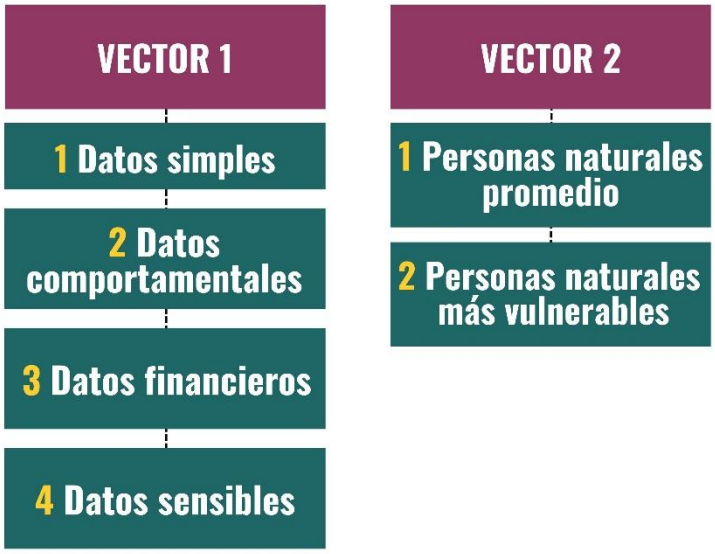
c) La cantidad de titulares de datos afectados. Otro factor importante para determinar el impacto en los derechos y libertades de los titulares de datos es la cantidad de afectados. En este contexto, es necesario considerar la categoría de la infracción o el tipo de vulneración de seguridad que se trate. Por ejemplo, un tratamiento ilegítimo de datos a la luz del artículo 7 de la LOPDP, vulnerará la confidencialidad de los datos personales de todos los titulares de los datos. De igual manera, una vulneración de la seguridad de una base de datos vulnerará la confidencialidad de los titulares de los datos que consten en ella.

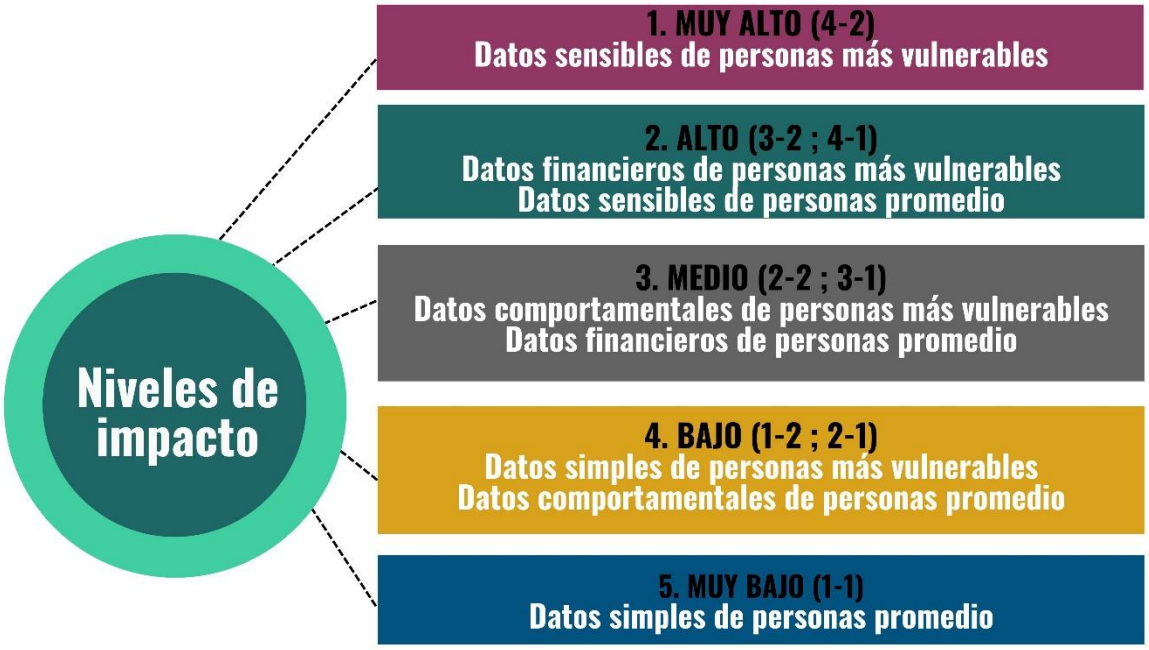
d) La naturaleza de la infracción o de la vulneración de la seguridad de datos. Es importante considerar que ciertos tipos de infracciones pueden tener un mayor impacto que otras, todo depende del escenario de riesgos planteado. Por ejemplo, una vulneración por consentimiento forzado que obligue al titular a compartir sus datos biométricos sin ninguna otra opción de autentificación podría tener un altísimo impacto en los derechos y libertades del titular, en el caso de que esos datos sean utilizados con fines de vigilancia masiva. Las vulneraciones de confidencialidad pueden ser irreversibles, sobre todo considerando si se trata de datos sensibles y de grupos especialmente vulnerables de titulares de datos. Las vulneraciones de la integridad y de la disponibilidad pueden ser temporales siempre y cuando los responsables y encargados del tratamiento cuenten con medidas adecuadas de seguridad tales como *backups* y planes de continuidad de negocios. Sin embargo, cabe considerar que, en escenarios de riesgos relacionados a daños y perjuicios, la disponibilidad y la integridad pueden ser muy costosas en ciertos casos; por cuanto, el titular, pierde el acceso a sus datos personales, o estos le causan un perjuicio por no estar actualizados o no ser íntegros. Por ello, todo depende del escenario de riesgo planteado. Los escenarios de riesgos relacionados a la confidencialidad, a la integridad y a la disponibilidad deben ser analizados en modelos de riesgo independientes.

e) El volumen de los datos personales. Es otro criterio útil para establecer criterios de evaluación de riesgos, considerando la cantidad de datos que pueden ocasionar vulneraciones de los derechos y libertades de los titulares. Por ejemplo, la cantidad de datos personales de un mismo titular que han sido filtrados puede complementar el criterio de la cantidad de titulares de datos afectados.

1.2. Criterios cualitativos de impacto. Los criterios de evaluación pueden ser respaldados en criterios cualitativos cuando los responsables y encargados del tratamiento no tengan datos confiables de entrada; o, simplemente, no tengan datos. Sin embargo, es fundamental establecer los niveles de evaluación del riesgo de la manera más objetiva posible, con el fin de eliminar sesgos (prejuicios) y ruido (entendido como una mala estimación del nivel de impacto) y de acuerdo con escenarios determinados de riesgo. Cabe considerar que, en la protección de datos personales, pueden establecerse criterios estáticos que establecen el nivel

de impacto del riesgo de manera predeterminada. El siguiente ejemplo[6] muestra un etiquetado de niveles fundamentado en criterios cualitativos en un escenario de riesgo de confidencialidad:

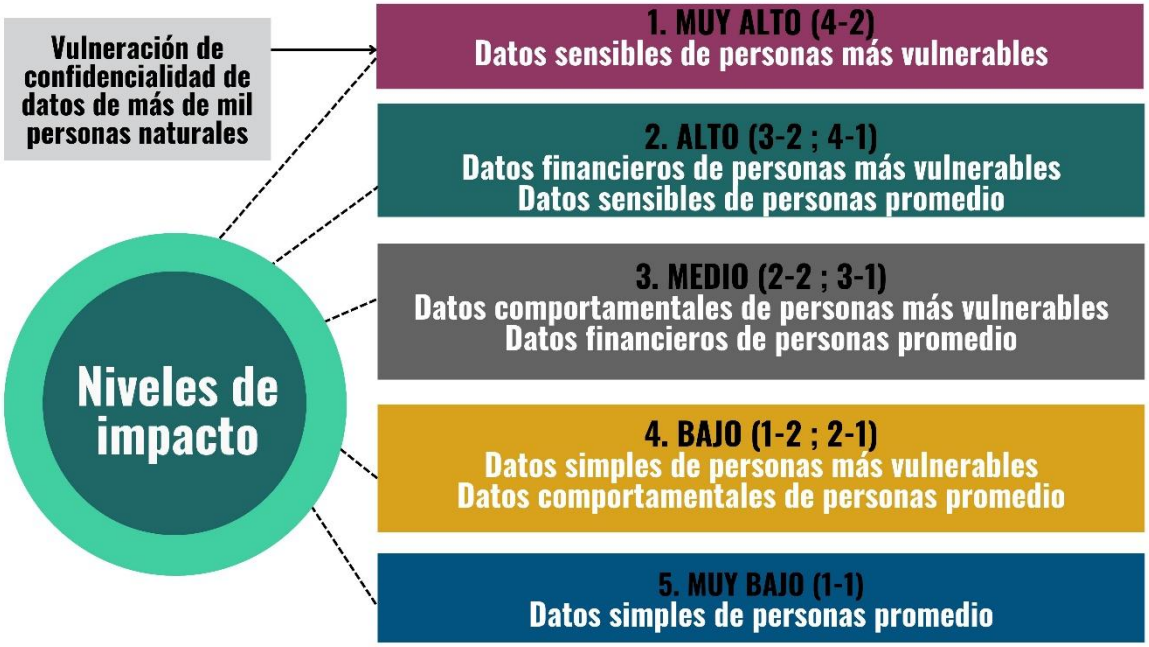




En los casos que amerita se pueden agregar o quitar criterios. En el presente ejemplo de criterios de evaluación de la confidencialidad, puede ser conveniente agregar un criterio acerca de la cantidad de personas cuyos datos han sido vulnerados u otros criterios

[6] Para este ejemplo se ha utilizado la metodología sobre la gravedad de las violaciones de datos de la Agencia Europea de Seguridad de la Redes y la Información (ENISA) Ver: European Network and Information Security Agency, *Recommendations for a methodology of the assessment of severity of personal data breaches*, working document v.1, Unión Europea, 2013.

relevantes. Por ejemplo, podemos agregar un criterio en el que una vulneración de datos que afecte a más de mil personas será considerada siempre de riesgo muy alto.

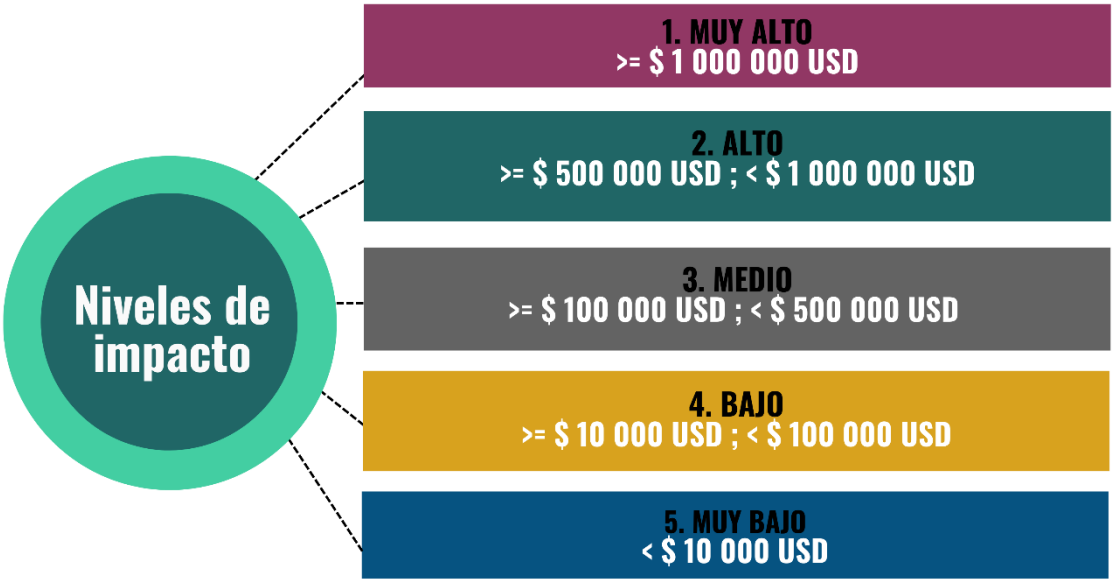


Sin embargo, cuando se utilizan criterios estáticos de evaluación de impacto, como los tradicionalmente establecidos en criterios jurídicos, es necesario estimar el nivel de la probabilidad o frecuencia de ocurrencia. La razón es considerar que la implementación de medidas de seguridad de prevención y de detección que disminuyan lo probabilidad de ocurrencia pueden reducir considerablemente la probabilidad de que el riesgo se materialice. También pueden implementarse medidas de seguridad reactivas que disminuyan el impacto.

1.3. Criterios cuantitativos de impacto. Los criterios de evaluación pueden ser respaldados en rangos cuantitativos de pérdidas financieras siempre y cuando se cuente con datos confiables, estadísticas y métricas significativas con respecto al impacto de una vulneración de los derechos y libertades en los titulares de los datos. No obstante, cuando se establecen criterios cuantitativos fundamentados en el impacto financiero, es conveniente utilizar criterios de evaluación de riesgos dinámicos, que calibren los niveles de riesgo en función de rangos.

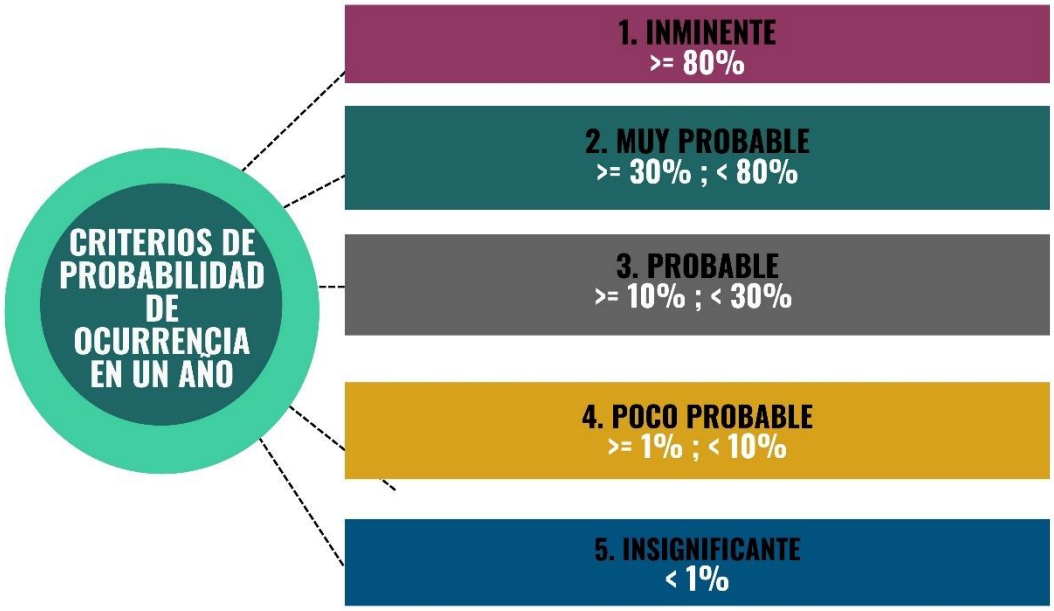
Los responsables y encargados del tratamiento pueden utilizar datos internos y externos. Ejemplo de datos internos son los datos provenientes de los SOC, en cuanto a incidentes de confidencialidad, integridad y disponibilidad de datos en la institución. Ejemplo de externos son los reportes de vulneraciones de la seguridad de datos personales, datos de los reportes de la SPDP y cualquier insumo cuantitativo relevante. También puede ser útil utilizar la jurimetría y la analítica legal con el fin de comprender la psicología sancionadora de la SPDP en cuanto a la valoración del impacto en los derechos y libertades de los titulares de los datos para establecer el monto de una sanción administrativa.

El siguiente ejemplo muestra un etiquetado de niveles de impacto fundamentado en criterios cuantitativos:



1.4. Criterios de la probabilidad de ocurrencia. Para elaborar los criterios de la probabilidad de ocurrencia es necesario considerar lo siguiente: a) estimar la probabilidad de ocurrencia en un lapso determinado, b) considerar que una frecuencia de ocurrencia de más de 1 afectará el nivel de impacto estimado, c) considerar la naturaleza multidimensional de los riesgos de seguridad de la información.

a) Estimar la probabilidad o frecuencia de ocurrencia. La probabilidad de ocurrencia se puede estimar entre 0 y 1, o en porcentajes. La frecuencia se la puede considerar en número de eventos. En ambos casos, es necesario estimarlos dentro de un lapso determinado. No es lo mismo estimar la probabilidad de ocurrencia de un incidente en una semana, en un mes o estimarla en un año. El siguiente ejemplo muestra los criterios de evaluación estimados en un año:

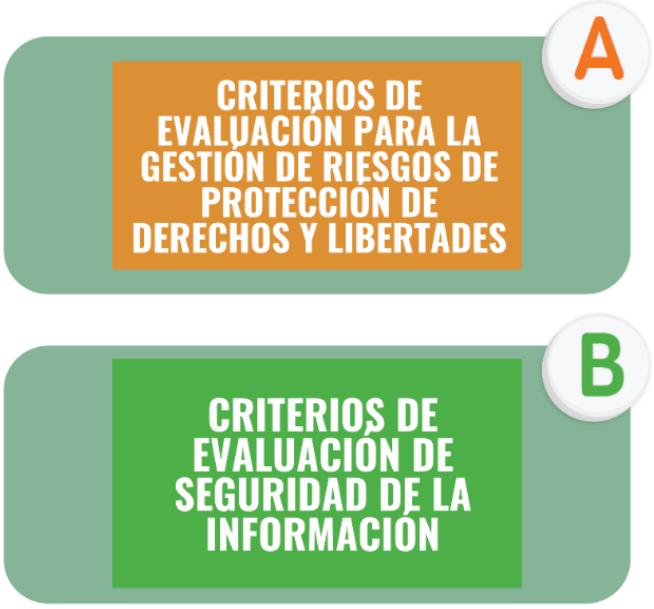


b) Considerar el nivel de aceptación de la probabilidad de ocurrencia en función del impacto. Está relacionado con el nivel de aceptación del impacto, sobre todo en un análisis cuantitativo. Por ejemplo, si el nivel de aceptación de la probabilidad de ocurrencia de un incidente es del 50% anual y el impacto de $10 000, esto equivale a una aceptación del riesgo de $5 000 por incidente.

c) Considerar la naturaleza multidimensional de los riesgos de seguridad de datos personales. En lo que concierne al tratamiento de datos personales, los riesgos de seguridad de la información también son riesgos contra los derechos y libertades de los titulares de los datos. Sin embargo, es importante tomar en cuenta que la probabilidad de ocurrencia del riesgo dependerá del nivel de resiliencia en cuanto a los controles de riesgos de protección de datos personales implementados. (Ejemplo: un acceso no consentido a una base de datos que está cifrada con algoritmos de cifrado seguro).

1.5. Integración en los criterios de evaluación de seguridad de la información

Los criterios de evaluación del impacto en contra de los derechos y libertades de los titulares de los datos serán tomados en cuenta en el establecimiento de los criterios de evaluación de seguridad de la información y otros riesgos operacionales. Es importante considerar que, desde una perspectiva de responsables y encargados del tratamiento, el impacto a los derechos y libertades de los titulares de datos se traduce en un riesgo de cumplimiento a la LOPDP. Se recomienda a los responsables y encargados del tratamiento a analizar las resoluciones, guías y precedentes sancionatorios de la SPDP para elaborar los criterios de evaluación. Es necesario ensamblar los criterios de evaluación desde una perspectiva de protección de los derechos y libertades de los titulares de los datos (a), con los criterios de evaluación desde una perspectiva organizacional del cumplimiento a la LOPDP (b).



En este contexto hay cuatro escenarios:

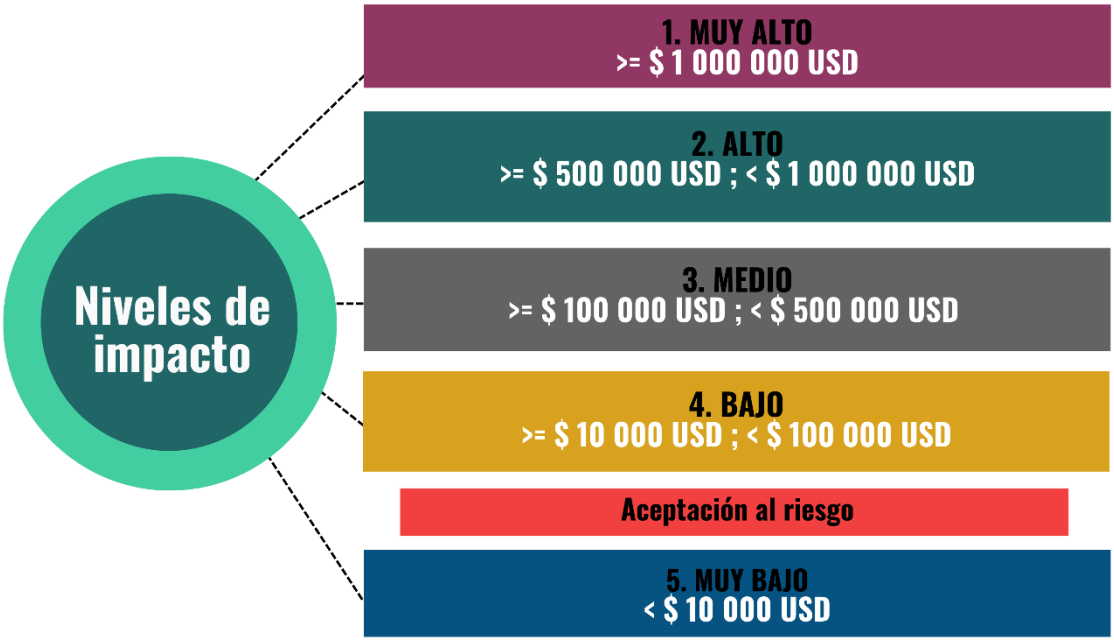
1.5.1. Cuantitativo (a) + cuantitativo (b). Los criterios cuantitativos son compatibles. Los responsables y encargados del tratamiento pueden evaluar de manera holística el impacto de una vulneración de seguridad de datos en los derechos y libertades de los titulares mediante métodos estadísticos y probabilísticos; o, a través de métodos jurimétricos y análisis legal que permitan analizar la psicología sancionadora de la SPDP. Es el caso de tener una lógica de Valor al Riesgo de protección de datos en donde el responsable del tratamiento estime de manera cuantitativa el impacto financiero de la conformidad a la LOPDP, calibrándolo en función del análisis de sanciones administrativas precedentes y las circunstancias actuales del riesgo. Estos métodos pueden servir para calibrar el impacto que sufren los titulares de datos. Los criterios cuantitativos facilitan la integración de la gestión de riesgos para la protección de derechos y libertades de los titulares de datos con la gestión de riesgos de seguridad de la información. Esto permite tener una visión clara del probable impacto por la conformidad a la LOPDP con otros tipos de pérdidas, tales como: pérdidas de productividad, respuesta de incidentes, reemplazo de activos, pérdida de ventaja competitiva, pérdida de reputación y otras pérdidas de índole jurídica.

1.5.2. Cualitativo (a) + cuantitativo (b). Es la forma más común de integración. Los criterios cualitativos y cuantitativos pueden ser compatibles siempre y cuando los responsables y encargados del tratamiento sepan interpretar de manera adecuada el impacto en los derechos y libertades de los titulares de los datos desde una perspectiva de cumplimiento a la LOPDP. El reto es aprender a calibrar las opiniones de quienes elaboren los criterios de evaluación del riesgo (por ejemplo: oficiales de riesgo, delegados de protección de datos, oficiales de seguridad de la información) con el fin de reducir los problemas de sesgo y de ruido.

1.5.3. Cualitativo (a) + cualitativo (b). También es posible que ambos tipos de criterios de evaluación sean cualitativos. Se requiere calibrar las estimaciones cualitativas de los expertos de manera rigurosa. Este aspecto no debe ser tomado a la ligera, por cuanto es obligatorio justificar los *rationales* que sustentan todo valor o criterio de entrada para un análisis de riesgos, con el fin evitar los análisis y evaluaciones de riesgos superficiales.

1.5.4. Cuantitativo (a) + cualitativo (b). Es inusual, pero aún posible, que los criterios de evaluación para la protección de derechos y libertades sean cuantitativos, aunque los criterios de evaluación de riesgos de seguridad de la información sean cualitativos. Es el caso de utilizar una lógica de Valor al Riesgo de protección de datos en donde el responsable del tratamiento estime de manera cuantitativa el impacto financiero de la conformidad a la LOPDP, calibrándolo en función del análisis de sanciones administrativas precedentes. Debe tenerse mucho cuidado al adaptar estos estimados cuantitativos en un análisis de riesgos de seguridad de la información cualitativo, sobre todo si se utilizan matrices de riesgo, pues estas pueden distorsionar el impacto en los derechos y libertades de las personas en ciertos escenarios de riesgo si es que hay una probabilidad de ocurrencia baja, pero un alto impacto.

1.6. Aceptación del riesgo. Desde una perspectiva de los titulares de datos, los derechos y libertades de los titulares de los datos deben ser protegidos al cien por ciento. No obstante, desde una perspectiva de los responsables y encargados del tratamiento, siempre existirá un riesgo residual en cualquier escenario de riesgo relacionado con el tratamiento de datos personales y la finalidad es reducirlo al máximo posible. Por ejemplo, un responsable del tratamiento puede calibrar su aceptación del riesgo residual de recibir una sanción administrativa menor a $10 000:



Se recomienda determinar el apetito al riesgo en función de: a) la capacidad al riesgo, b) la tolerancia al riesgo de la organización.

a) La capacidad al riesgo. Es de naturaleza cuantitativa y consiste en utilizar métricas objetivas para determinar el monto máximo de impacto financiero que puede recibir el responsable del tratamiento o el encargado debido a sanciones administrativas y otros tipos de impactos secundarios como la pérdida de reputación, la pérdida de productividad o las acciones por daños y perjuicios.

b) La tolerancia al riesgo. Es de naturaleza cualitativa y consiste en estimar el nivel de aceptación del riesgo de función de una estimación subjetiva. Se recomienda utilizar mecanismos de calibración de opiniones de expertos.

1.7. Integración entre el delegado de protección de datos y el departamento de seguridad de la información

Es fundamental comprender que la conformidad a la LOPDP requiere de un trabajo interdisciplinario. Esta facultad incluye la potestad de revisar la veracidad de las auditorías de seguridad de la información y de otros riesgos operacionales. Consecuentemente, es fundamental que el Delegado de Protección de Datos (DPD) audite y sugiera los controles de riesgo pertinentes en el ámbito de la seguridad de la información para mitigar al máximo posible la probabilidad de ocurrencia y el impacto que pueden sufrir los titulares de los datos durante el tratamiento de datos personales y como consecuencia del tratamiento de datos personales. Las metodologías de gestión de riesgos para la protección de derechos y libertades y de la gestión de riesgos de seguridad de la información deben ser compatibles y estar sincronizadas.

1.8. Integración entre el delegado de protección de datos y el departamento jurídico.

Es fundamental que el delegado de protección de datos audite los resultados de las auditorías jurídicas de cumplimiento a la LOPDP para poder solicitar controles de riesgos y recomendar cambios para mitigar al máximo posible la probabilidad de ocurrencia y el impacto que pueden sufrir los titulares de los datos durante el tratamiento de datos personales y como consecuencia del tratamiento de datos personales. El Delegado de Protección de Datos (DPD) puede auditar los informes de auditoría recibidos a través de las evaluaciones de impacto del tratamiento de datos personales; lo cual, implica pedir ajustes en controles de riesgos jurídicos, tales como las políticas de protección de datos personales, los convenios entre responsables y encargados del tratamiento, los mecanismos para el ejercicio de los derechos de los titulares de los datos personales, entre otros.

1.9. Integración entre el delegado de protección de datos y el departamento de gestión de riesgos.

En el caso de contar con departamento de gestión de riesgos, éste deberá considerar los criterios de evaluación de riesgos de seguridad de la información y los criterios de evaluación para la protección de derechos y libertades dentro de sus funciones. El objetivo es que sean compatibles e informativos.

2. Identificación de riesgos de protección de datos personales

Esta etapa es fundamental para poder estimar la probabilidad y/o frecuencia de ocurrencia de un riesgo en dos dimensiones: perfilamiento de amenazas e identificación de vulnerabilidades.

Es necesario utilizar métricas significativas para generar los valores de entrada tanto en el perfilamiento de amenazas como en la identificación de vulnerabilidades. Para comprender los riesgos de protección de datos personales se requiere un enfoque multidimensional entre riesgos jurídicos, riesgos operacionales y riesgos financieros.

En primer lugar, se trata de riesgos jurídicos que deben analizarse desde la perspectiva del titular de los datos (los riesgos contra sus derechos y libertades); y, desde la perspectiva de los responsables y encargados del tratamiento (los riesgos de conformidad a la LOPDP).

En segundo lugar, es necesario establecer escenarios de riesgos operacionales como los de seguridad de la información y de la analítica predictiva; los cuales, afectan a la vez, tanto a los responsables y encargados del tratamiento como a los titulares de los datos.

En tercer lugar, se recomienda estimar los riesgos financieros como consecuencia de la probable materialización del riesgo. Para ello, debe estimarse la materialización del riesgo en los derechos y libertades de las personas concernidas y las probables sanciones administrativas para los responsables y encargados del tratamiento que dicha materialización del riesgo podría generar. Se recomienda recopilar datos históricos de eventos que han atentado a la seguridad de datos del responsable del tratamiento o encargado o utilizar datos históricos de instituciones con características y objetos de negocio similares, de acuerdo con los reportes de violaciones de la seguridad de datos especializados e incluso en los reportes de actividades de la SPDP. A ello, deberá también considerarse las circunstancias actuales que podrían influir tanto en el perfil de amenazas, como en el incremento de vulnerabilidades; tales como riesgos macroeconómicos, inestabilidad política, pandemias, falta de electricidad, entre otros.

2.1. Identificación de datos. El primer paso en esta etapa es identificar los activos. Los datos personales pueden ser considerados como activos condicionales, por cuanto los titulares de los datos pueden oponerse al tratamiento consentido de sus datos en cualquier momento. No obstante, es de gran ayuda identificar las actividades de tratamiento de datos existentes, considerando que los datos personales están de manera omnipresente en muchas actividades y procesos. Se recomienda crear y mantener un registro de actividades del tratamiento (RAT), con el objeto de identificar de mejor manera las siguientes interrogantes: ¿En qué procesos hay tratamiento de datos personales? ¿Quién es el responsable del proceso? ¿Qué tipos de datos personales son tratados? ¿En dónde son guardados los datos personales? ¿Cuál es la cadena de dependencia de activos para guardar y tratar los datos personales identificados? Se recomienda también utilizar herramientas de descubrimiento electrónico y de recuperación de información para lograr identificar los atributos de los datos tratados e inferir si se trata de datos personales. Es importante considerar que los metadatos también pueden ser datos personales.

En este contexto, cabe considerar que la LOPDP define al dato personal como *"Dato que identifica o hace identificable a una persona natural, directa o indirectamente"*[7]. Para evitar problemas de interpretación se debe considerar que la identidad es definida por la RAE como el *"Conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás"*[8]. Consecuentemente, los rasgos genéticos, culturales, físicos, psíquicos, psicológicos son datos personales. Por ejemplo, los datos biométricos, los datos del ADN, o los datos de la salud son en sí mismos datos personales, aunque no estén relacionados de manera directa con números de registro de las personas naturales como los números de cédula de identidad o el pasaporte.

De igual manera, se debe considerar que, en ciertas áreas como la ciencia de datos, una persona natural no es identificable únicamente por sus datos biográficos o números de registro, sino por cualquier otro atributo que los distinga de un grupo de individuos, como su género, su edad, sus rasgos físicos, culturales o simplemente sus preferencias. En el siguiente ejemplo, podemos llegar a determinar el nombre de "Pedro", con base en su edad y sus preferencias musicales. Por ello, no basta ofuscar o seudonimizar su nombre, sino también identificar otros atributos que indirectamente lo pueden identificar en un determinado contexto.

In [21]:
```
# ANALIZAR ATRIBUTOS QUE INDIRECTAMENTE IDENTIFICAN AL TITULAR DE DATOS

import pandas as pd
df = {
    "Nombre": ["Lola", "Pedro", "Tito", "Fernando", "Luisa"],
    "Género": ["Femenino", "Masculino", "Masculino", "Masculino","Femenino"],
    "Edad": [20,51,20,20,20],
    "Música": ["Metal", "Pasillos", "Hiphop", "Hiphop", "Metal"],

}
df = pd.DataFrame(df)
```

In [24]:
```
Pedro = df.loc[(df['Edad'] > 50) & (df['Género'] == "Masculino")]
Pedro[[ "Edad", "Género", "Música"]]
```

Out[24]:

	Género	Edad	Música
1	Masculino	51	Pasillos

El ejemplo muestra que se puede llegar a la identidad de "Pedro" aunque no conste su nombre en el conjunto de datos. Es posible identificarlo a través de su edad (al ser el único del grupo mayor de 50 años) o de sus preferencias musicales (es el único del grupo que prefiere los pasillos).

2.2. Identificación de amenazas. En el contexto de la protección de datos personales, una amenaza puede ser definida como *algo o alguien que, a través de ataques y/o ciberataques, puede producir una vulneración de los derechos y libertades de los titulares de los datos*. Desde una perspectiva de los titulares de los datos, la comunidad de amenaza puede ser el

[7] LOPDP, artículo 4.
[8] Ver: RAE, https://dle.rae.es/identidad.

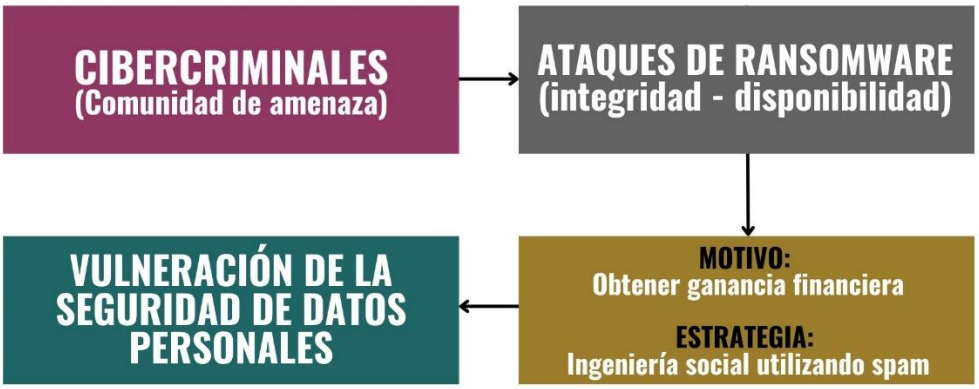
mismo responsable o encargado del tratamiento que trata sus datos personales sin una base legal que legitime el tratamiento a la luz del artículo 7 de la LOPDP. Además, son amenazas para los titulares de los datos, todas las comunidades de amenaza que pretenden vulnerar la seguridad de datos personales encomendada a los responsables del tratamiento. En este contexto, es fundamental comprender los conceptos de comunidades de amenaza, amenazas naturales, perfilamiento de la amenaza, capacidad de la amenaza y tipos de ataques y ciberataques.

a) Comunidades de amenaza (*¿Quién es la amenaza?*) Las comunidades de amenaza son grupos de personas que intencionalmente amenazan el derecho de protección de datos de los titulares. Cabe considerar que toda comunidad de amenaza en el contexto de la seguridad de la información es también una amenaza en el contexto de la protección de datos personales. Ejemplos de comunidades de amenaza son: cibercriminales, hacktivistas, empleados con privilegios, empleados sin privilegios, mercenarios auspiciados por gobiernos, terroristas o los mismos responsables y encargados del tratamiento cuando violan los derechos de los titulares de manera intencional. Es importante reflexionar acerca de las comunidades de amenaza en conexión con el tipo de organización que se trata. Por ejemplo, una entidad financiera podría tener mayor probabilidad de que las comunidades de amenaza sean cibercriminales por su interés en obtener ganancias a través del robo de credenciales de acceso y la generación de transacciones fraudulentas. Así mismo, una entidad pública podría tener una probabilidad mayor de comunidades de amenaza de mercenarios financiados por intereses políticos.

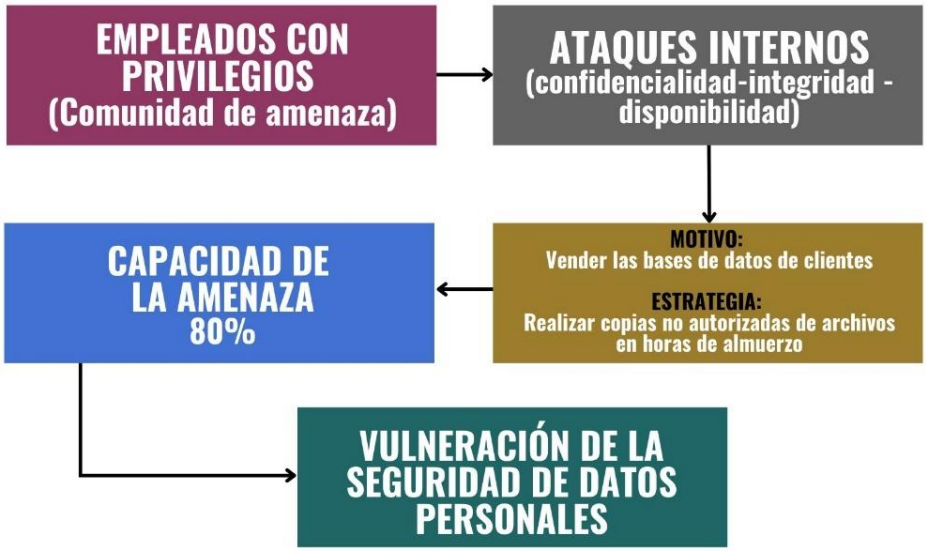
b) Amenazas naturales (¿Qué es la amenaza?) Los eventos de la naturaleza también constituyen una amenaza a los derechos y libertades de los titulares de datos. Ejemplos de amenazas naturales son inundaciones, terremotos, incendios. Este tipo de amenazas pueden usualmente provocar vulneraciones de disponibilidad de datos temporales o definitivas.

c) Perfilamiento de la amenaza. Perfilar amenazas es comprender sus objetivos y sus formas de ataque. Por ejemplo, hay grupos ciberdelincuenciales que pueden utilizar un tipo determinado de *malware* o un estilo particular de ejecutar extorsión al utilizar *ransomware*. Un grupo hacktivista podría utilizar una estrategia determinada para realizar ataques distribuidos de denegación de servicio (DDOS). Un grupo de empleados con privilegios podría actuar como intruso para filtrar información confidencial. Una empresa puede

vulnerar los derechos y libertades de los titulares de los datos a través de políticas de privacidad no transparentes o con mecanismos de consentimiento forzado para obligarlos a recibir publicidad.



d) Capacidad de la amenaza. La capacidad de la amenaza es la estimación de su nivel de conocimientos y efectividad. Para que la probabilidad o frecuencia de ocurrencia del riesgo sea alta es necesario que la capacidad de la amenaza sea superior al nivel de resiliencia de las medidas de seguridad implementadas en un sistema de tratamiento de datos personales.



e) Tipos de ataques y/o ciberataques. Es la manera conceptual, operativa y técnica utilizada para realizar un ataque y/o ciberataque. Los ataques y/o ciberataques usualmente caracterizan a una comunidad de amenazas para vulnerar la seguridad jurídica, organizacional o técnica de un responsable o encargado del tratamiento. Ejemplos de tipos de ciberataques incluyen: ataques de Denegación de Servicio (DoS), ataques de Hombre en el Medio (MITM), ataques dirigidos contra la inteligencia artificial, crackeo de contraseñas, ataques de ingeniería social como el phishing, ataques por *malware* (troyanos, virus, ransomware, rootkits), y la explotación de vulnerabilidades web, como *SQL Injection*. Los ataques también pueden ser no técnicos, tales como los ataques de empleados que filtran datos de para fines no autorizados (ataques internos), el aprovechamiento doloso de un

responsable del tratamiento para compartir datos personales sin la legitimidad en el tratamiento, impedir el ejercicio de los derechos de los titulares de los datos o el robo de dispositivos que almacenen datos personales. Se recomienda clasificar los vectores de ataque en función de la dimensión o las dimensiones de la seguridad de datos que pueden vulnerar; es decir, la confidencialidad, la integridad o la disponibilidad de los datos personales.

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Troyanos (Malware)	Ataques internos	Ataques distribuidos de denegación de servicio (DDOS)
Ataques de hombre en el medio (MITM)	Ransomware (Malware)	Ransomware (Malware)
SQL Injection	Ingeniería social	Robo de dispositivos de almacenamiento
Broken Access Control	Integrity failures	Cortes de electricidad
[...]	[...]	[...]

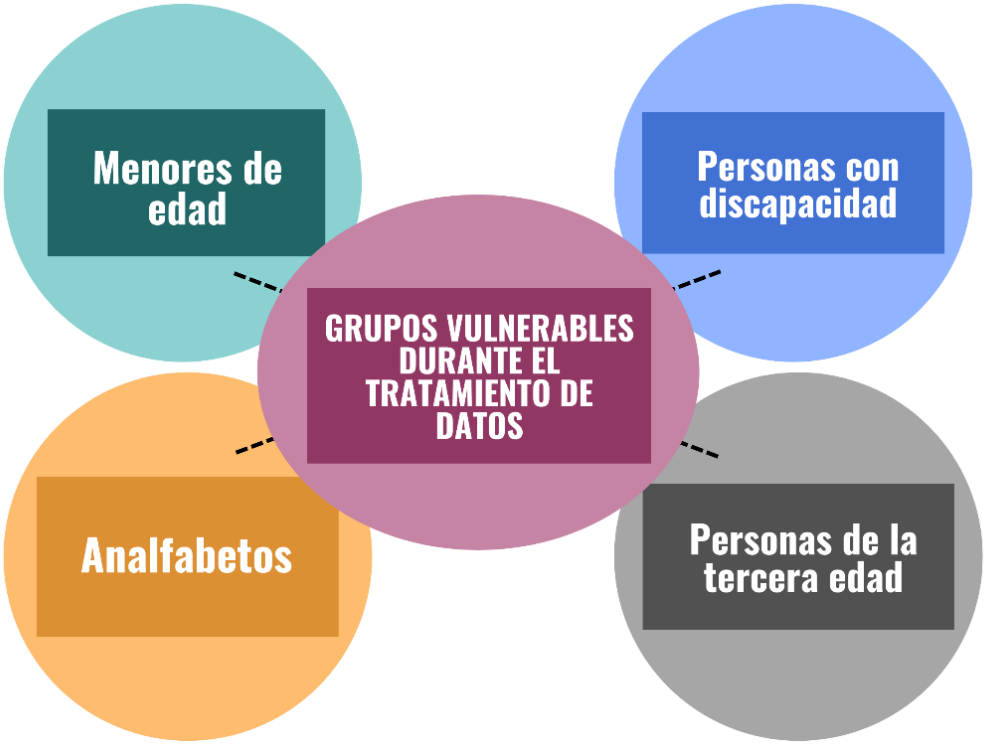
2.3. Identificación de vulnerabilidades. Las vulnerabilidades deben entenderse como debilidades en el tratamiento de datos personales que pueden ser aprovechadas por las amenazas. Es necesario realizar la identificación de vulnerabilidades jurídicas de cumplimiento a la LOPDP, la identificación de grupos vulnerables de titulares de datos, la identificación de vulnerabilidades organizacionales y la identificación de vulnerabilidades técnicas. Es obligatorio identificar las vulnerabilidades existentes para poder remediarlas o mitigarlas en la etapa de tratamiento de riesgos. Cabe considerar que mitigar vulnerabilidades incrementa la resiliencia para reducir la probabilidad de materialización del riesgo. Hay que cuidar que el nivel de resiliencia sea superior a la capacidad de ataque de las comunidades de amenaza.

a) Identificación de vulnerabilidades jurídicas. Desde una perspectiva de los responsables y encargados del tratamiento, las vulnerabilidades jurídicas corresponden a la falta de madurez en el cumplimiento de las obligaciones establecidas en la LOPDP; tales como: ausencia de legitimidad en el tratamiento de datos personales, la falta de mecanismos para que los titulares ejerzan sus derechos, la ausencia del delegado de protección de datos, no realizar las respectivas evaluaciones de impacto, no notificar las vulneraciones de la seguridad de datos en el plazo establecido, no cumplir con los requisitos para las transferencias internacionales de datos, no realizar los debidos registros ante la SPDP, no tener acuerdos de protección de datos con los encargados del tratamiento, entre otras. Para identificarlas es fundamental realizar auditorías jurídicas de cumplimiento a la LOPDP. Lo importante es el “SER” y no el “DEBER SER”, pues se trata de cumplir con la protección de datos personales en la práctica. Por ejemplo, en la política de tratamiento de datos personales, podría existir el siguiente compromiso:

> **"El responsable del tratamiento recolectará sólo los datos necesarios para cumplir con la apertura de cuenta del cliente".**

En el caso presentado, el responsable del tratamiento se compromete a recolectar los datos mínimos necesarios para los fines del tratamiento. Sin embargo, el auditor puede identificar que, en la práctica, la empresa solicita datos sin ninguna relevancia o pertinencia para cumplir con los fines del tratamiento; como la etnia, los datos de los hijos menores de edad del titular, los historiales crediticios, las cuentas de redes sociales o los datos médicos del titular. Una vez auditada la plataforma web, se identifica una violación del principio de pertinencia y minimización de datos personales establecido en el artículo 10 (e) de la LOPDP.

b) Identificación de grupos especialmente vulnerables de titulares de datos. Desde una perspectiva de los titulares de los datos, éstos pueden recibir un mayor impacto de acuerdo con ciertos factores como su condición social, racial, edad, género, discapacidades, pobreza y cualquier otra afín. Los responsables y encargados del tratamiento tienen que identificar a estos grupos más vulnerables en específicos escenarios de riesgo. En estos casos, es necesario implementar modelos de riesgo que permitan compensar las mayores vulnerabilidades de ciertos grupos de titulares de datos. Las vulnerabilidades pueden clasificarse en *"vulnerabilidades durante el tratamiento de datos personales y vulnerabilidades como consecuencia del tratamiento de datos personales"*[9]. Por ejemplo, en un escenario de riesgo relacionado al consentimiento para entregar datos de la salud, una política de protección de datos muy difícil de entender podría impactar a los siguientes grupos vulnerables:



[9] Para ampliar su conocimiento sobre las vulnerabilidades de ciertos grupos especiales de titulares de datos personales, se recomienda la siguiente obra: Malgieri, G. (2023). *Vulnerability and Data Protection Law*, Reino Unido, Oxford University Press.

No obstante, si existe una vulneración de la confidencialidad de datos personales, algunos grupos de titulares de datos afectados podrían sufrir un impacto mayor para conseguir un empleo:

c) Identificación de vulnerabilidades organizacionales. Son debilidades en los procesos de tratamiento de datos personales y de la seguridad del tratamiento. Esto incluye a todos los procesos de seguridad de la información y los procesos de seguridad de datos personales complementarios para la conformidad a la LOPDP. En ambos casos es recomendable utilizar, como guía, normas de buenas prácticas como la ISO/IEC 27001, ISO/IEC 27701. No obstante, si las finalidades del tratamiento de datos corresponden a actividades específicas es necesario implementar las políticas a la luz de éstas. Tal es el caso de los sistemas de gestión de la inteligencia artificial con el ISO/IEC 42001, el pago con tarjetas de crédito con el PCI-DSS o similares. Por ejemplo, la norma ISO/IEC 27001:2022 establece en su Anexo1 cláusula 8.13, la obligación del responsable del tratamiento para borrar la información cuando ya no sea requerida. El auditor debe verificar si la obligación se cumple en la práctica y la calidad de los procesos organizacionales para hacerlo.

El siguiente ejemplo muestra el principio del *mínimo privilegio* la cláusula 5.15 (a) de la norma ISO/IEC 27002:2022:

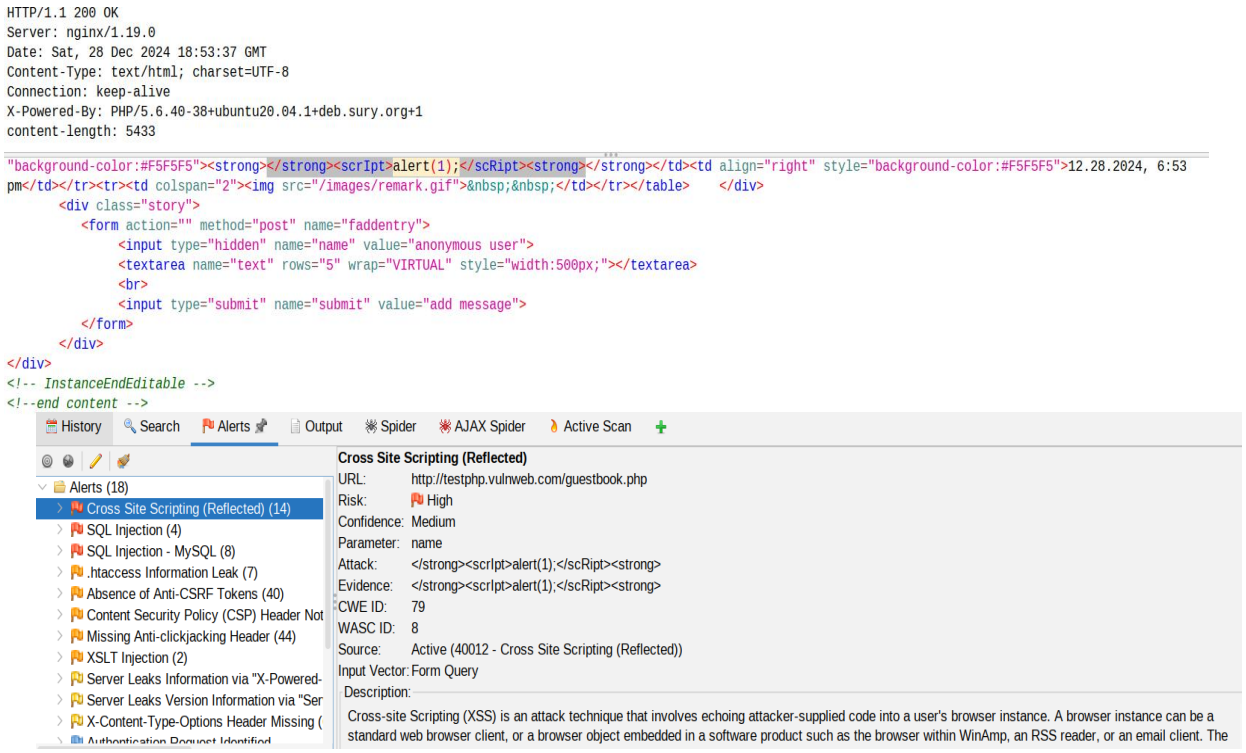
> **Establecer normas basadas en la premisa del menor privilegio: "Todo está generalmente prohibido a menos que esté expresamente permitido", en lugar de la norma más débil: "Todo está generalmente permitido a menos que esté expresamente prohibido."**

Sin embargo, si en la práctica los funcionarios de la institución tienen permisos de administrador sin necesitarlos, se está rompiendo el principio del mínimo privilegio. Consecuentemente, es una vulnerabilidad de seguridad organizacional. Estos problemas son muy comunes en instituciones públicas y privadas cuando se hace una copia de políticas de seguridad de la información de otra institución sin la necesaria gestión de riesgos o cuando los funcionarios no respetan las políticas de seguridad de la información.

Otros ejemplos de vulnerabilidades pueden ser la ausencia de políticas de control de acceso, la falta de capacitación al personal, falta de controles criptográficos; y, cualquier otra que no esté en conformidad con estas normas de buenas prácticas, cuando sean aplicables. Los derechos de los titulares de los datos también pueden ser vulnerados por negligencia humana. Esto es aplicable para comunidades de amenaza como empleados con privilegios, los cuales pueden publicar datos personales sin la debida legitimidad del tratamiento por negligencia. La negligencia no exime de responsabilidad; por el contrario, evidencia una vulnerabilidad derivada de la falta de capacitación de los empleados involucrados.

d) Identificación de vulnerabilidades técnicas. Las vulnerabilidades técnicas son las vulnerabilidades provenientes del software o del hardware. Estas vulnerabilidades son de naturaleza no visible; y, por ello, es fundamental contar con el personal humano especializado y las herramientas técnicas necesarias para el escaneo de puertos, redes, aplicaciones web, librerías de software y cualquier recurso de software. Se recomienda que el personal humano calificado sea experto en identificación de vulnerabilidades tales como hackers éticos y *penetration testers*. Se recomienda utilizar repositorios abiertos de vulnerabilidades conocidas y proyectos relevantes como el OWASP top ten.

El siguiente ejemplo muestra el escáner de vulnerabilidades *Zed Attack Proxy* utilizado para detectar vulnerabilidades de aplicaciones Web utilizando el OWASP top ten:



Es primordial utilizar bases de datos de vulnerabilidades conocidas[10] para poder investigar la vulnerabilidad detectada y remediarla. Sin embargo, cabe considerar que también pueden existir vulnerabilidades nuevas o *Zero Day*. Una vulnerabilidad de *Zero Day* no es conocida; y, por ello, los esfuerzos de auditar constantemente los sistemas de información por personal calificado o los programas abiertos de descubrimiento de vulnerabilidades (programas de *bug bounty*) pueden ser de gran ayuda en algunas circunstancias.

2.4. Identificar escenarios de riesgo. Un escenario de riesgo a aquel en donde existen datos personales en riesgo y la probabilidad de ocurrencia de que se materialice el riesgo, generando una consecuencia (por ejemplo, una violación de la confidencialidad de datos personales). Desde una perspectiva del titular de los datos, un daño puede ser primario cuando la materialización del riesgo produce daños directos en sus derechos y libertades, como en el caso de una vulneración a la seguridad de datos que viola la confidencialidad del titular exponiendo los datos de su salud. Un daño sería secundario cuando el daño se produce por la reacción de otras personas con respecto al evento principal; como, por ejemplo, ser discriminado por tener alguna enfermedad y que se disminuya su probabilidad de acceder a plazas de trabajo.

Desde una perspectiva de responsables y encargados del tratamiento, todo depende del enfoque. En un escenario de riesgos de vulneración de la seguridad de datos, un daño puede ser primario cuando la vulneración impacta a los sistemas de información del responsable del tratamiento, ocasionando "*pérdidas de productividad, pérdidas por respuesta al incidente, pérdidas por reemplazo de activos*". Los daños secundarios vendrían a ser

[10] Ver https://cve.mitre.org/.

producto de la reacción de otras personas naturales o jurídicas, como *las pérdidas de ventaja competitiva, pérdidas de reputación y pérdidas por sanciones administrativas y sentencias*[11].

Por ejemplo, un escenario de riesgo puede ser el riesgo de tener un accidente vehicular. Desde una perspectiva enfocada en un probable accidente:

Escenario de riesgo 1: Accidente de tránsito

Comunidad de amenaza: Otros conductores que pueden chocarnos el vehículo.

Perfil de la amenaza: Son los conductores que acostumbran a conducir con exceso de velocidad.

Vulnerabilidades: Una vulnerabilidad propia sería si nuestros frenos están en malas condiciones técnicas que nos impiden reaccionar de manera adecuada al riesgo.

En este caso, si la capacidad de la amenaza (conductores con exceso de velocidad) se aprovecha de nuestra vulnerabilidad (frenos en malas condiciones técnicas), se produce el accidente.

Impactos primarios: Daños en el vehículo, probables lesiones en el conductor del vehículo,

Impactos secundarios: pérdidas por litigios, como reacción al evento principal. Pérdida de puntos en la licencia.

Escenario de riesgo 2 (perspectiva de los titulares de datos personales): Vulneración de datos personales sensibles (confidencialidad) en un hospital, desde una perspectiva del impacto en los titulares de los datos.

[11] Para ampliar su conocimiento sobre estos principios del manejo de riesgos, se recomienda la siguiente obra: Freund, J., Jones, J. (2015). *Measuring and Managing Information Risk: a FAIR Approach.* Butterworth-Heinemann, 1st edition.

Comunidad de amenaza: Cibercriminales

Perfil de la amenaza: Motivado para vender datos a empresas de recursos humanos y seguros.

Vector de ataque: Ingeniería social y ataque de Malware (troyano).

Vulnerabilidades organizacionales: Falta de capacitación a los empleados. La vulnerabilidad del responsable del tratamiento se convierte en una vulnerabilidad del titular de los datos.

Vulnerabilidad técnica: Ausencia de antivirus eficaz.

Impacto primario: La vulneración de la seguridad de datos personales que viola el derecho de protección de datos personales del titular de los datos.

Impacto secundario: La violación de los datos personales del titular también violan su derecho al trabajo, por cuanto su empleador se entera de que tiene una enfermedad grave.

Escenario de riesgo 3 (perspectiva de los responsables del tratamiento de datos personales): Vulneración de datos personales (disponibilidad) desde una perspectiva del impacto del responsable del tratamiento o encargado de una empresa que vende productos online.

Comunidades de amenaza: Cibercriminales, empleados con privilegios.

Perfil de la amenaza: Cifrar la información y pedir el rescate en criptomonedas. El empleado desleal instala el ransomware gracias a sus privilegios.

Vector de ataque: Ataque interno y ataque de Malware (ransomware).

Vulnerabilidad organizacional: No haber implementado políticas de seguridad de la información para restricciones de acceso de empleados en las instalaciones de la empresa.

Vulnerabilidad técnica: No hay *backups* continuos ni planes de continuidad de negocio eficaces, perdiendo alrededor del 10% de los datos personales de los clientes.

Impacto primario: Pérdidas en productividad (144 horas fuera de línea hasta restaurar los sistemas de información gracias a que había *backups*), pérdidas por respuesta a incidentes (equipo de respuesta a incidentes, examinador digital forense), pérdidas por reemplazo del 10% de datos personales de clientes secuestrados.

Impacto secundario: Pérdida de reputación (pérdida de clientes), sanciones jurídicas (sanción administrativa de la autoridad de protección de datos), pérdida de ventaja competitiva (proveedores quitan privilegios en la cadena de abastecimiento).

3. Análisis de riesgos de protección de datos personales

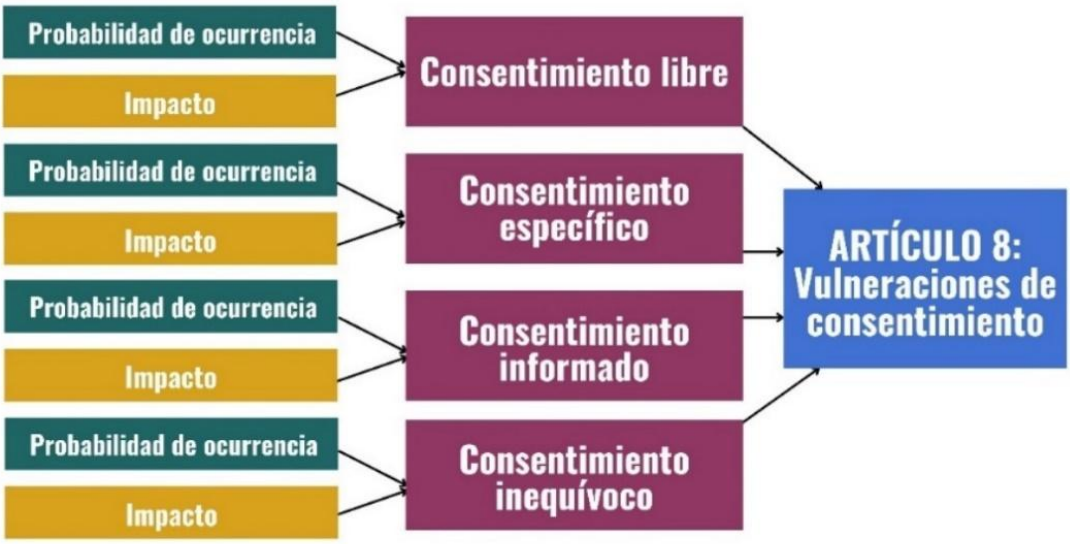
La finalidad de esta etapa es calibrar la probabilidad o frecuencia de ocurrencia y el impacto en función de diversos escenarios de riesgo. En este contexto, hay escenarios de riesgos primordialmente de cumplimiento jurídico y escenarios de riesgos operacionales (sobre todo de seguridad de la información) que son a la vez riesgos jurídicos de conformidad a la LOPDP. Ejemplos de riesgos, primordialmente de cumplimiento jurídico, son obligaciones como el cumplir con la legalidad del tratamiento, cumplir con los mecanismos adecuados para el ejercicio de los derechos de los titulares de los datos, cumplir con las obligaciones de registros o cumplir con los plazos establecidos para notificaciones.

En segundo lugar, los riesgos operacionales que son a la vez riesgos jurídicos constituyen una instancia metarregulatoria[12] de la LOPDP; en donde, únicamente, se establece el objetivo de proteger los derechos y libertades de los titulares en el tratamiento de sus datos, pero no los mecanismos específicos para lograrlo. En una metarregulación, la SPDP controla la autorregulación de los responsables y encargados del tratamiento. Es el caso de la protección de datos personales en las áreas de riesgos de seguridad de información, en donde la SPDP debe controlar los mecanismos de gestión de riesgos que utilizan los responsables y encargados del tratamiento para proteger los derechos y libertades de los titulares de los datos.

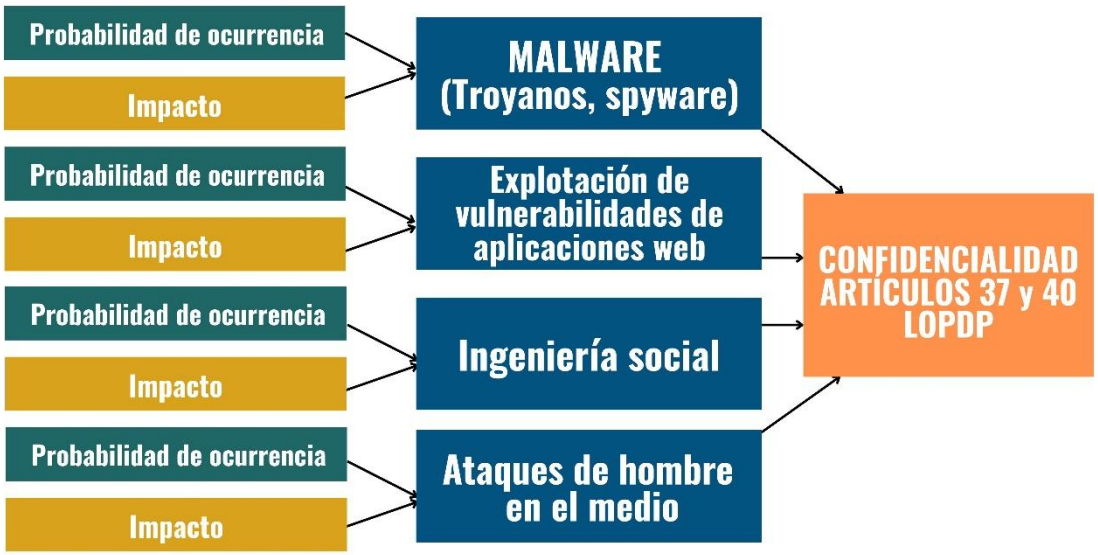
En tercer lugar, las probables consecuencias que resulten en caso de materializarse el riesgo pueden impactos mayores en grupos vulnerables de titulares de datos, lo cual puede ser resuelto al construir modelos de riesgo que permitan calibrar estos diferentes grados de vulnerabilidad.

a) Escenarios de riesgo primordialmente jurídico de cumplimiento a la LOPDP. Lo primero para el análisis es ubicarlos en escenarios de riesgos. Cuando se trata de un escenario de riesgos primordialmente jurídicos de conformidad a la LOPDP, se pueden utilizar escenarios de acuerdo con el artículo de la LOPDP implicado o la categoría de la infracción. Por ejemplo, en un escenario de riesgo de violación al consentimiento de los titulares de datos, el consentimiento debe cumplir con cuatro requisitos: ser libre, específico, informado e inequívoco[13]. A partir de ello, es necesario estimar en el análisis, cuál es la probabilidad o frecuencia de ocurrencia de que el tratamiento de datos no cumpla con estas cuatro condiciones, tanto en las políticas de protección de datos, como en la práctica (implementación). Es necesario también estimar el impacto que la probable vulneración de consentimiento podría tener en los titulares de los datos. A partir de este análisis, posteriormente se evaluará el nivel del riesgo en la etapa de evaluación de riesgos y se podrá implementar medidas de control al riesgo de manera informada.

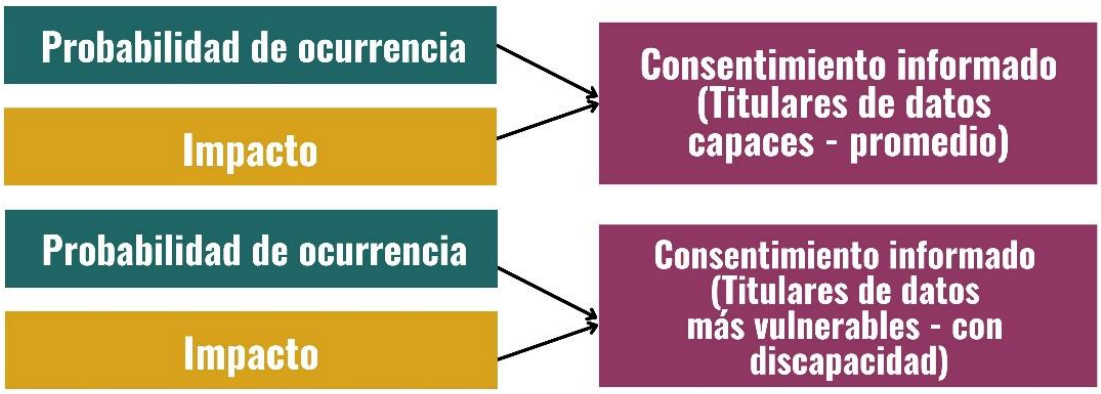
[12] Para ampliar su conocimiento sobre modelos regulatorios y gobernanza corporativa, se recomienda la siguiente obra: Parker, C. (2022). *The Open Corporation*, Cambridge University Press, Australia.
[13] LOPDP, artículo 8.



b) Escenarios de riesgos de seguridad de la información. Se recomienda descomponer los escenarios de riesgo. Por ejemplo, si el escenario de riesgo es el cumplimiento del artículo 37 de la LOPDP sobre seguridad de la información, este a su vez se divide en las tres dimensiones de la seguridad de datos; es decir, escenarios de riesgo contra la confidencialidad, contra la integridad y contra la disponibilidad. A su vez, varios escenarios de riesgo pueden implementarse dentro de cada una las dimensiones de la seguridad de datos. Por ejemplo, a continuación, se presenta un flujo en el que es necesario calibrar la probabilidad o frecuencia de ocurrencia y el impacto en cuatro escenarios de riesgos de seguridad de la información en la dimensión de la confidencialidad. Los resultados tendrán que ser posteriormente evaluados en la etapa de evaluación de riesgos para poder escoger e implementar las medidas de seguridad organizacionales y técnicas en la etapa de tratamiento de riesgos.



c) Calibración de las vulnerabilidades de los titulares de los datos. En ciertos casos será necesario incorporar, dentro de un escenario de riesgo de conformidad a la LOPDP, ciertas consideraciones particulares. Es el caso de grupos especialmente vulnerables ante un escenario de riesgo. En estas circunstancias es necesario calibrar las vulnerabilidades de grupos especiales de titulares de datos debido a circunstancias específicas como la pobreza, el género, las disparidades, la edad avanzada, entre otras. El siguiente ejemplo muestra una calibración de vulnerabilidades en razón del grupo más vulnerable de las personas con discapacidad:



3.1. Modelar de riesgo. Un modelo de riesgos debe incluir la estimación de la probabilidad o frecuencia de ocurrencia y del impacto. Los modelos para el análisis de riesgo pueden ser cuantitativos, cualitativos o híbridos. Se recomienda implementar una ontología o metodología que pueda descomponer el problema del riesgo en factores, determinar el nivel de confianza de las estimaciones y estimar rangos de acierto. Es fundamental comprender que un modelo de riesgos no es descriptivo, sino analítico. Es decir, lo fundamental es estimar y calibrar los valores de entrada y aplicar métricas y métodos para obtener una estimación sobre el nivel del riesgo o el valor al riesgo.

3.2. Análisis cuantitativo. Consiste en analizar la probabilidad o frecuencia de ocurrencia y el impacto en valores numéricos continuos. Son valores numéricos continuos: los números, los porcentajes, los percentiles, aplicados a la frecuencia de un evento, probabilidades o la materialización del impacto en pérdidas financieras. Un análisis cuantitativo implica que el *rationale* que justifica los valores de entrada sea cuantitativo, construir métricas significativas, realizar comparaciones efectivas de escenarios de riesgo e implementar modelos cuantitativos de análisis de riesgos[14].

Es importante considerar que utilizar escalas numéricas, como al estimar el nivel del riesgo del 1 al 3 no es análisis cuantitativo, pues los números pueden ser utilizados en los criterios de evaluación del riesgo como etiquetas subjetivas tales como 1 (riesgo bajo), 2 (riesgo medio), 3 (riesgo alto). Lo importante es que los *rationales* sean cuantitativos.

3.3. Métodos cuantitativos de análisis. Existen diversos métodos útiles para un análisis cuantitativo. Estos métodos usualmente requieren de datos de entrada, lo cual impone la necesidad de contar con datos confiables. Si los datos son erróneos o contienen considerables

[14] Para ampliar su conocimientos en análisis cuantitativo, se recomienda la siguiente obra: Hubbard, D., & Seiersen, R. (2016). *How to Measure Anything in Cybersecurity Risk*, John Wiley & sons Inc, Estados Unidos.

niveles de sesgo, los resultados también serán errados o sesgados. Además, cabe considerar que la gestión de riesgos para la protección de derechos y libertades es de naturaleza epistemológica, lo cual implica que es fundamental conocer el entorno y calibrar bien los datos para reducir la incertidumbre en la toma de decisiones que mitiguen al máximo el riesgo de vulneración de derechos y libertades de los titulares de datos.

a) Métodos frecuentistas. Los métodos frecuentistas consisten en determinar la frecuencia de un incidente en un lapso determinado. Por ejemplo, para calibrar la frecuencia de ocurrencia de un ataque de *phishing* que haya involucrado datos personales, se puede hacer un análisis histórico estadístico acerca de cuantos ataques ha tenido el responsable del tratamiento en los últimos tres años, estimando el promedio histórico.

ATAQUES DE PHISHING EN 2022	8
ATAQUES DE PHISHING EN 2023	4
ATAQUES DE PHISHING EN 2024	3
PROMEDIO	5

Si las condiciones del responsable del tratamiento no han cambiado significativamente en cuanto al perfilamiento de amenazas, vulnerabilidades y medidas de tratamiento de riesgos existentes relacionadas al escenario de riesgo *phishing*, se puede estimar un intervalo de acierto entre 3 y 8 probables ataques de *phishing* en el 2025. Si las circunstancias actuales han cambiado significativamente, se recomienda estimar los valores de entrada calibrando el impacto de las circunstancias actuales.

b) Métodos Bayesianos. Los métodos Bayesianos son útiles para estimar la probabilidad de un evento que depende de otro evento. Por ejemplo, para calibrar la probabilidad de una vulneración de datos que depende de haber realizado una evaluación de impacto de tratamiento de datos (DPIA) efectiva:

db = Vulneración de datos personales
ext = Ataque externo
dpia = Evaluación de impacto del tratamiento de protección de datos

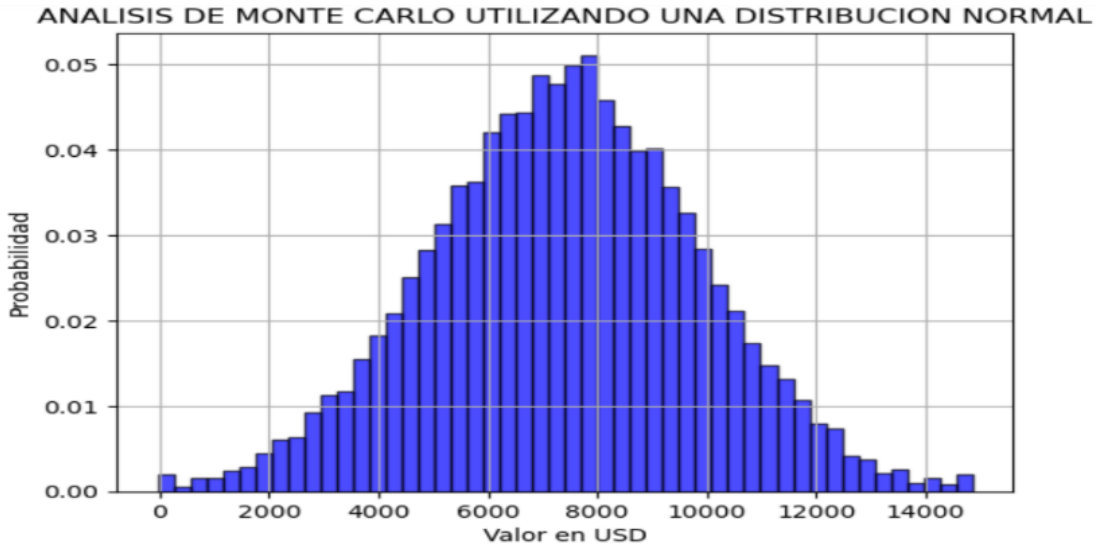
Valores calibrados
P(db|ext) = 0.80
P(db | ~ext) = 0.20
P(~db | ext) = 0.20
P(ext | dpia) = 0.10
P(ext|~dpia) = 0.90
P(dpia) = 0.70
P(~dpia) = 0.30
P(~ext) = 0.66
P(~db) = 0.59

Valores derivados
P(ext) = P(dpia) · P(ext | dpia) + P(~dpia) · P(ext | ~dpia) = 0.34
P(db) = P(ext) · P(db | ext) + P(~ext) · P(db | ~ ext) = 0.404
P(ext | db) = P(db | ext) · P(ext) / P(db) = 0.673
P(ext | ~db) = P(~db | ext) · P(ext) / P(~db) = 0.114

Resultados

P(db | dpia) = P(ext | dpia) · P(db | ext) + P(~ext | dpia) · P(db | ~ext) = 26% (Probabilidad de vulneración con DPIA)
P(db|~dpia) = P(db|ext) · P(ext|~dpia) + P(db|~ext) · P(~ext|~dpia) = 74% (Probabilidad de vulneración sin DPIA)

c) Análisis de Monte Carlo. Consiste en generar datos aleatorios dentro de intervalos establecidos para mejorar la toma de decisiones en escenarios de incertidumbre. Por ejemplo, el análisis de Monte Carlo puede utilizarse para estimar la magnitud del impacto de una vulneración de datos en los titulares considerando que el menor impacto ha sido de $120 y el máximo impacto de $15 000. De esta manera generamos 10 000 escenarios aleatorios:



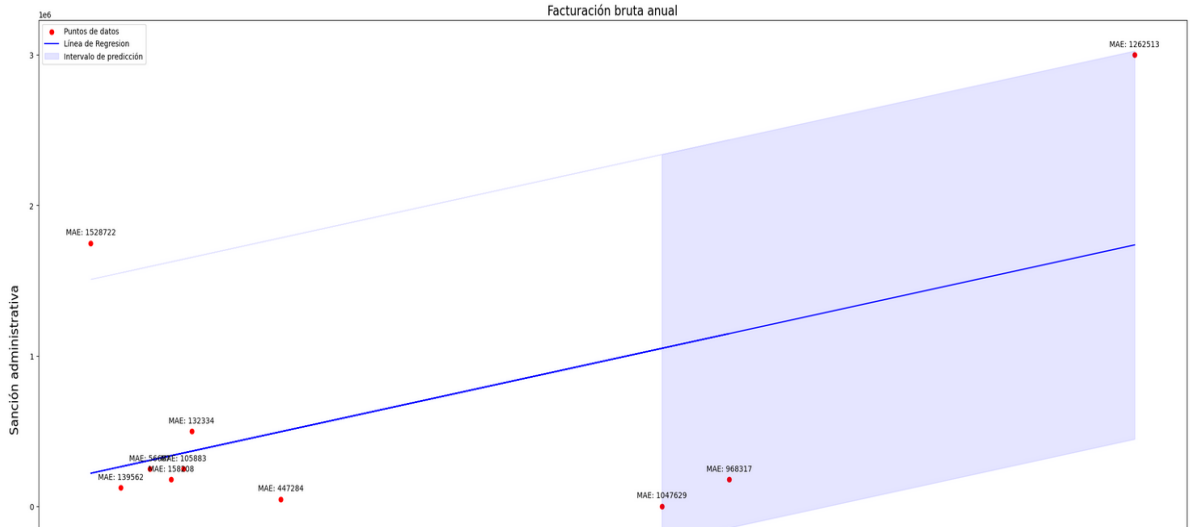
El resultado es un promedio (mean) de 7 542. Hay que tomar en cuenta que el resultado promedio será ligeramente diferente en cada intento.

d) Predicción conformal (Conformal prediction). La predicción conformal es un método no paramétrico muy efectivo que ayuda de gran manera a la calibración del riesgo, en particular, en la ciencia de datos y las metodologías de la inteligencia artificial. Ayuda a calibrar intervalos de acierto a un nivel de confianza determinado, a través del análisis histórico. Hay varios tipos de predicción conformal que bien pueden adaptarse a las necesidades de calibrar riesgos en muchos tipos de uso[15].

Desde una perspectiva de los titulares de los datos puede utilizarse para estimar los intervalos de confianza acerca del impacto de un riesgo en los derechos y libertades de los titulares de los datos. Desde una perspectiva de los responsables y encargados del tratamiento, será posible estimar la cuantía de una sanción administrativa de la SPDP con relación a vulneraciones de la seguridad de datos, tomando en cuenta la facturación bruta anual del responsable del tratamiento y el monto de cada sanción. Así se pueden comparar entre los datos históricos utilizados para el entrenamiento y la predicción. El siguiente ejemplo muestra una conformidad al 90% el que se utiliza un set de datos de 10, *un modelo de Linear*

[15] Para mejorar su conocimiento en *conformal prediction*, se recomienda la siguiente obra: Manokhin, V. (2023). *Practical Guide to Applied Conformal Prediction in Python*, Packt Publishing, Reino Unido, 1st Edition.

Regression, utilizando como métrica el *Mean Absolute Error* (MAE) entre los datos de entrenamiento y las predicciones:



e) Verificación del funcionamiento del modelo. Existen métricas cuantitativas que ayudan a verificar el nivel de acierto o desacierto de las predicciones; entre ellas: el *Log Loss* o el *Brier Score*. Por ejemplo, determinar la frecuencia de aciertos con respecto a la probabilidad de cinco incidentes que pudieron convertirse en vulneraciones de la confidencialidad de datos, utilizando el *Brier Score* como métrica:

Fórmula: Brier score = (1/N) ∑(forecasted_prob – outcome)2

Incidente	Estimación	Resultado positivo o negativo de las presuntas vulneraciones de confidencialidad (Positivo = '1'; Negativo = '0')
Acceso no consentido a bases de datos	90%	Positivo
Interceptación de datos en red de área local (LAN)	40%	Negativo
Aprovechamiento de vulnerabilidad (SQL injection)	30%	Negativo
Ataque de fuerza bruta	50%	Negativo
Robo de teléfono inteligente	50%	Positivo

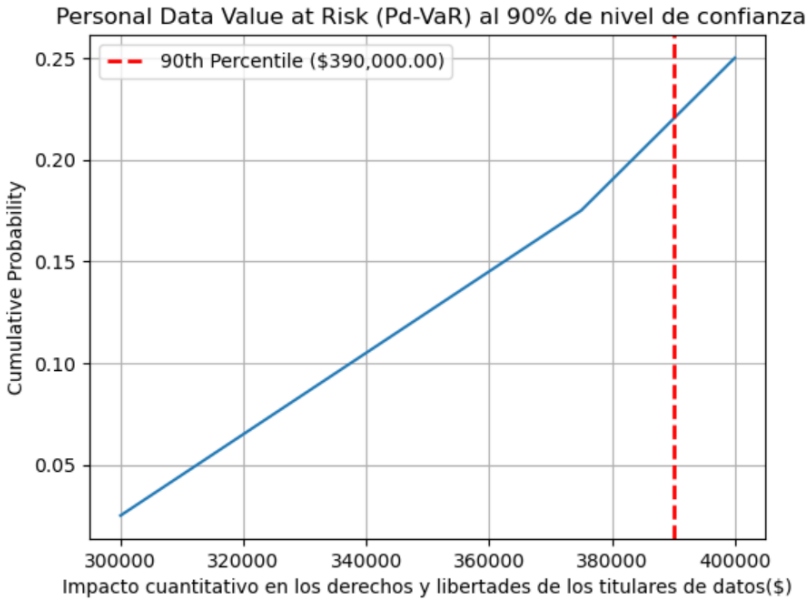
Resultado:

Brier score = (1/5) * (0.01 + 0.16 + 0.09 + 0.25 + 0.25)
Brier score = 0.152

El resultado muestra un aceptable grado de acierto en las estimaciones realizadas.

3.4. Modelos cuantitativos de riesgo. Modelar el riesgo de manera cuantitativa implica construir un método u ontología mediante el cual se puedan derivar un rango de acierto. Ejemplo de modelos cuantitativos son el Valor al Riesgo o el modelo FAIR.

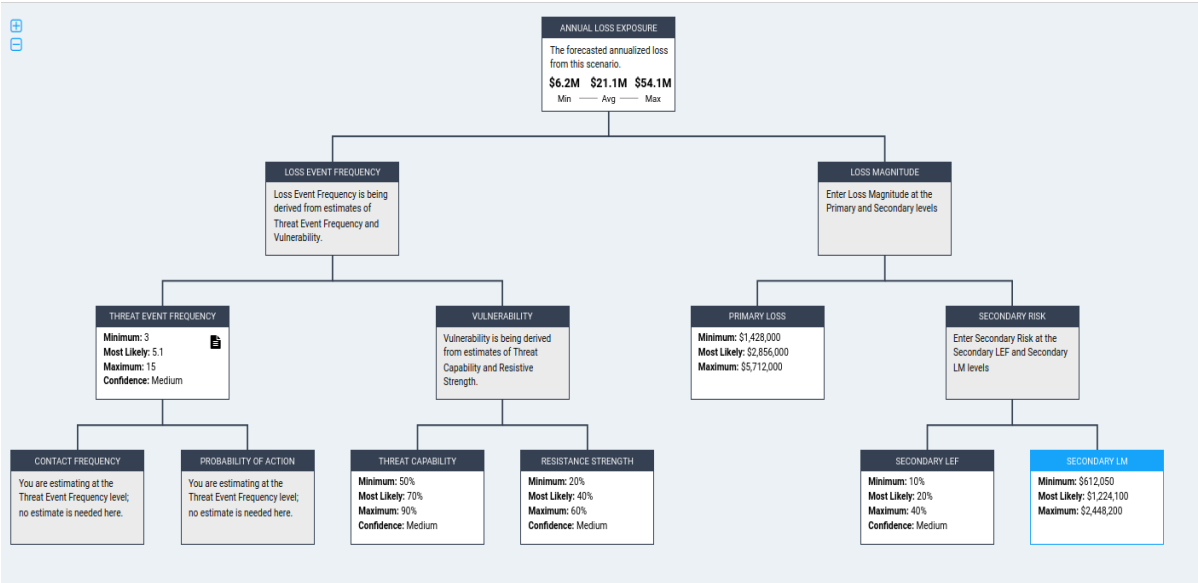
a) Valor al Riesgo VaR: Proveniente del mundo financiero, consiste en estimar la peor pérdida probable en un lapso determinado, de acuerdo con un nivel de confianza. Tiene sus variaciones en el Cy-VaR (ciberseguridad) y el Pd-VaR (privacidad/datos personales). Tiene tres métodos: VaR histórico (datos pasados), VaR *variance co-variance* (no datos) y VaR con análisis de Monte Carlo (datos futuros). El Valor al riesgo de datos personales (Pd-VaR) puede implementarse desde una perspectiva del impacto financiero en los titulares de los datos o desde una perspectiva de los impactos primarios y secundarios que los responsables y encargados del tratamiento pueden recibir por una sanción administrativa. Por ejemplo: "Estoy seguro a un 90% de nivel de confianza, de que el impacto total por una vulneración de la disponibilidad de datos y su consecuente sanción administrativa será menor a $500 000 USD el próximo año"[16].



Algo importante de tener en cuenta es que si el nivel de confianza (ej: 90%) es subjetivo, el cálculo del valor al riesgo resultará un placebo. Para convertir el nivel de confianza en objetivo, se sugiere utilizar métodos como la *predicción conformal* que permiten generar los *rationales* necesarios.

b) Modelo FAIR: Es un modelo de riesgos muy utilizado en el área de la ciberseguridad[17]. Su ontología permite estimar de manera eficiente la frecuencia de ocurrencia y la magnitud de un riesgo. Utiliza el análisis de *Monte Carlo* para obtener rangos de acierto de pérdida. Es representado en una distribución de probabilidades *PERT* con tres parámetros: mínimo, más probable y máximo. Por ejemplo, podemos realizar un análisis cuantitativo de riesgos de vulneraciones a la confidencialidad de datos en conformidad al artículo 37 de la LOPDP:

[16] Para revisar estrategias de Valor al Riesgo para la gestión de riesgos de protección de datos personales, se recomienda: Enríquez, L. (2024). *A personal data value at risk (Pd-VaR) approach*. *Journal of Research, Innovation and Technologies*, Volume III, 2(6), 141-158.
[17] Ver https://www.fairinstitute.org/what-is-fair.

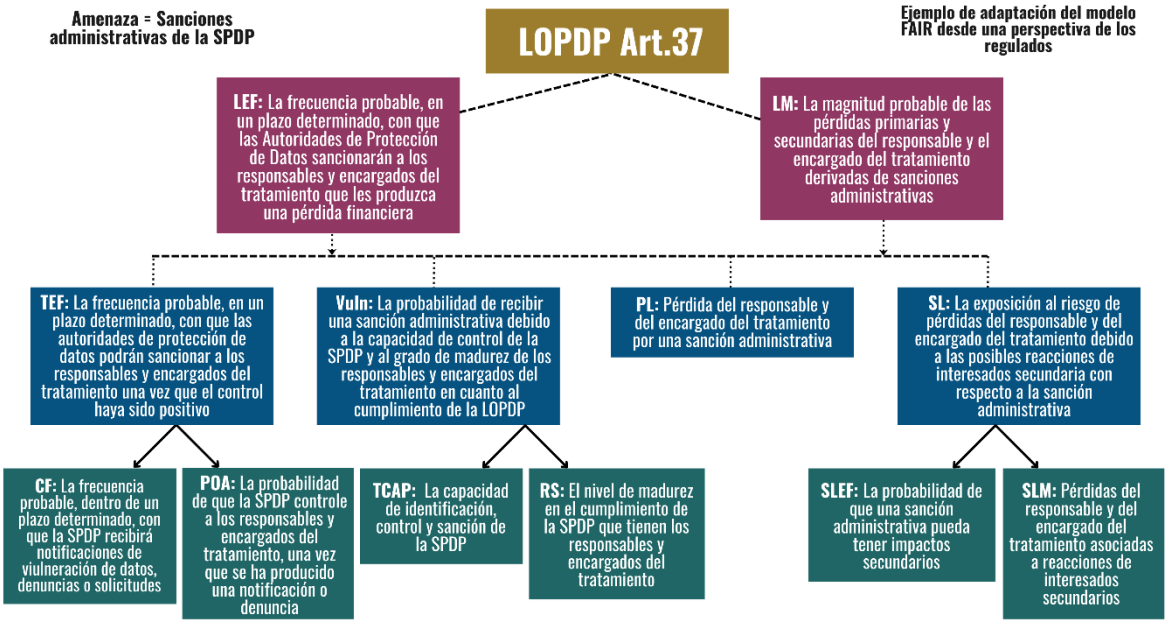


***Ejemplo realizado en la URL: https://app.fairu.net**

El modelo FAIR[18] es muy útil en el área de riesgos de seguridad de la información; por cuanto, permite calibrar la frecuencia de ocurrencia en un lapso determinado y a la vez permite comprender los diferentes tipos de pérdidas financieras que produce una vulneración de la seguridad de datos, en donde las sanciones administrativas son un tipo de pérdida secundaria, debido a la reacción de la SPDP para sancionar al responsable o encargado del tratamiento que haya vulnerado derechos de los titulares de datos. Sin embargo, el modelo FAIR también puede ser personalizado para fines de protección de datos personales. Desde una perspectiva del riesgo de conformidad con la LOPDP, los responsables y encargados del tratamiento pueden calibrar directamente cualquier riesgo jurídico de cumplimiento; y, luego exportar sus valores al riesgo a un análisis cuantitativo de seguridad de la información, como el presentado en el ejemplo anterior. Cabe considerar que esta estrategia de análisis cuantitativo sirve para estimar el probable monto de una sanción administrativa y pérdidas secundarias derivadas de ella. Este método funciona siempre y cuando existan precedentes de sanciones administrativas, considerando cómo la SPDP ha estimado el impacto contra los derechos y libertades de los titulares de datos en sus propios precedentes.

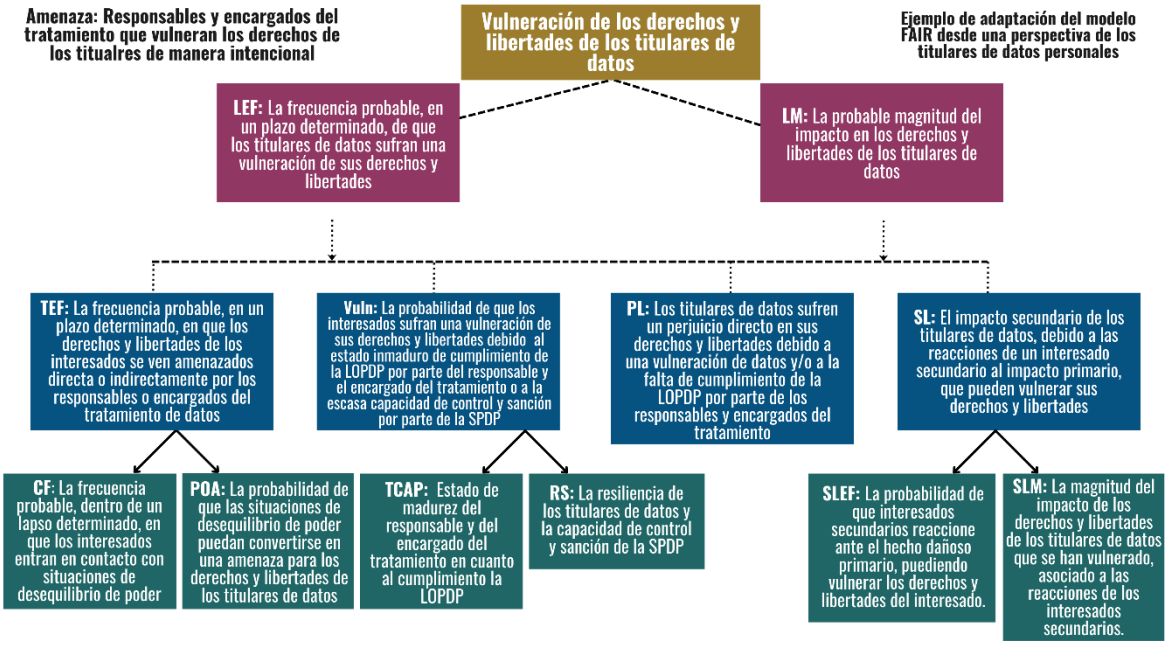
A continuación, se presenta un modelo personalizado para calibrar el riesgo material de una vulneración de datos personales, desde la perspectiva de cumplimiento a la LOPDP que tienen los responsables y encargados del tratamiento:

[18] Para aprender a utilizar el modelo FAIR, se recomienda leer el siguiente estándar: THE OPEN GROUP, (2021), *Risk Taxonomy (O-RT)*, Versión 3.01. Disponible en: https://pubs.opengroup.org/security/o-rt/.



En el caso de que no existan precedentes de sanciones administrativas o que haya habido un cambio de dirección importante en la visión sancionatoria de la SPDP, se recomienda modelar el impacto contra los derechos y libertades de los titulares tomando en cuenta la situación de cada escenario de riesgos.

El siguiente ejemplo muestra un modelo del impacto en los derechos y libertades de los titulares de los datos utilizando una ontología inspirada en el modelo FAIR:



En el ejemplo propuesto, se modelan la probabilidad o frecuencia de ocurrencia de una potencial vulneración de los derechos de los titulares de datos cuando estos sean cuantificables. También es posible hacer modelos paralelos para calibrar el grado de

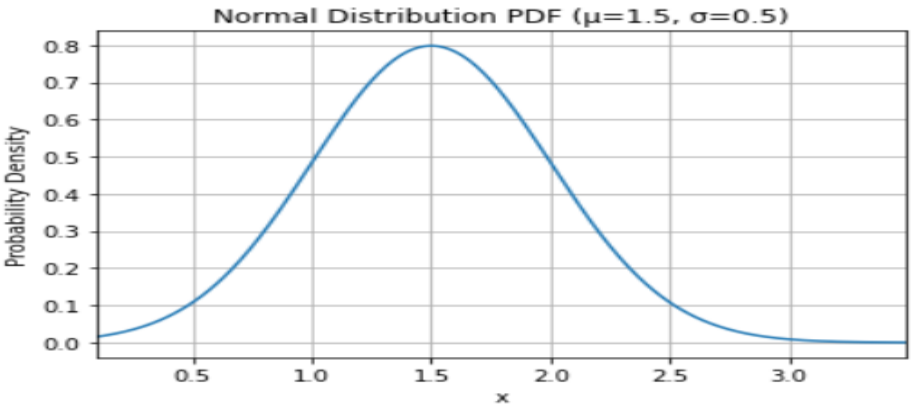
vulnerabilidad de grupos especialmente vulnerables, como se presenta en el ejemplo siguiente.

Primero, se estima el grado de vulnerabilidad en un grupo promedio de titulares de datos (50%), y después en el grupo vulnerable (80%):

Los resultados podrían informar acerca de la necesidad de implementar medidas de seguridad extras para los grupos más vulnerables. Por ejemplo, un hospital podría ver la necesidad de implementar medidas de seguridad especiales para grupos de titulares de datos con enfermedades graves.

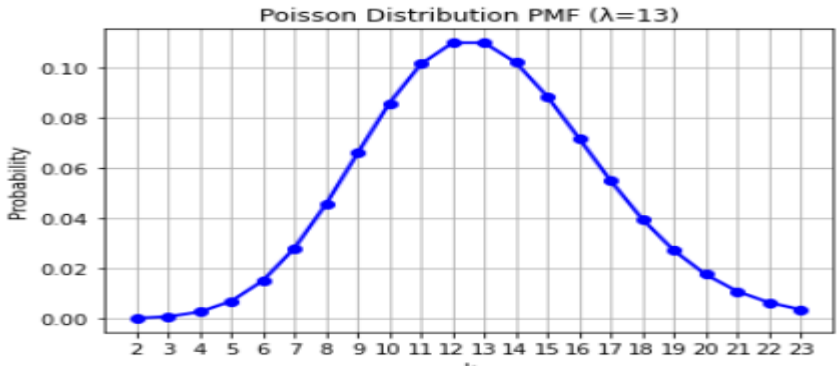
3.5. Representación cuantitativa del riesgo. Los resultados de un análisis cuantitativo son usualmente representados en distribuciones de probabilidades continuas, discretas, en curvas de excedencia de pérdidas (*Loss Exceedance Curves*) y en matrices de riesgo.

a) Distribuciones de probabilidades continuas. Representan la probabilidad de ocurrencia de un evento probable de manera continua en un rango determinado. Es continua por cuanto cualquier valor numérico es posible. Ejemplo de distribuciones de probabilidades continuas son: *Gaussian distribution, Beta distribution, Pert distribution, Exponential distribution*.

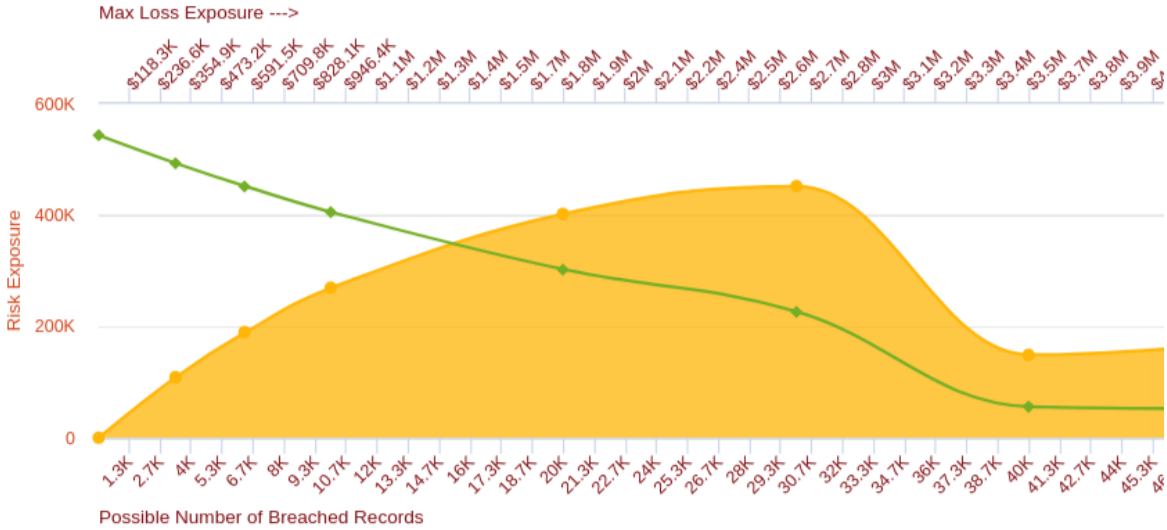


b) Distribuciones de probabilidades discretas. Representan la probabilidad de ocurrencia de un incidente en valores específicos, tales como números enteros. Ejemplo de

distribuciones de probabilidades discretas son la *Poisson binomial distribution, beta-binomial distribution*.



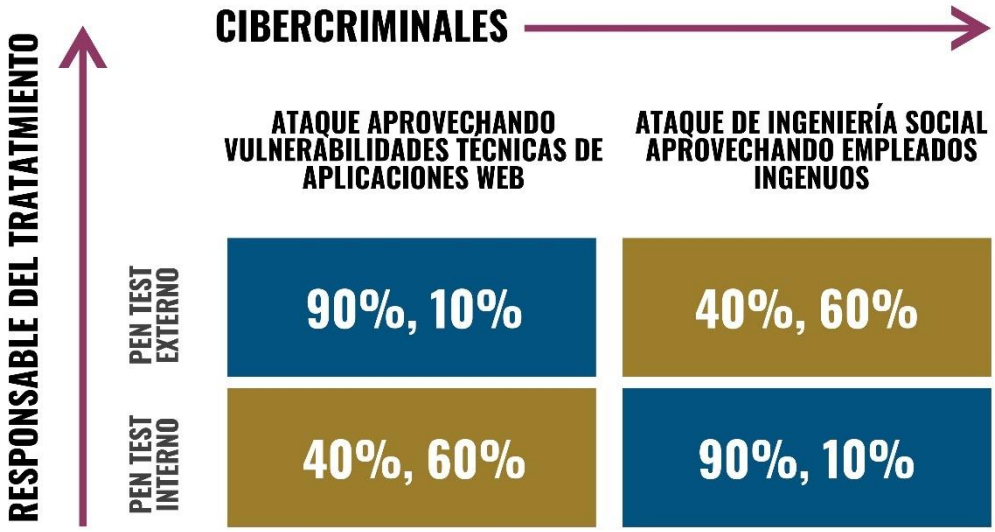
c) Curvas de excedencia de pérdidas. Ayudan a comunicar la probabilidad de que la pérdida financiera exceda una determinada cantidad en un lapso determinado. Es un excelente mecanismo para comunicar el riesgo, pues es visualmente fácil de comprender y representa el riesgo de manera no lineal.



***Ejemplo realizado en la URL: https://app.blackkitetech.com**

d) Matrices de riesgo. Las matrices de riesgo son muy utilizadas en áreas como la gestión de proyectos o la teoría de juegos. Pueden ser útiles cuando se comprende bien el escenario estratégico que se pretende representar. No obstante, todos los valores de entrada deben estar justificados a través de sus respectivos *rationales*; pues, la matriz, es un mecanismo para representar los riesgos, más no para calibrarlos. Por ejemplo, podemos analizar la estrategia por parte de un responsable del tratamiento para identificar vulnerabilidades en donde se debe escoger entre realizar prioritariamente un test de penetración (*pen test*) externo o interno. El alcance del test de penetración externo incluye conseguir acceso identificando y aprovechando una vulnerabilidad de las aplicaciones Web, pero no contempla ni ataques en el intranet, ni empleados ingenuos que puedan ser engañados por los cibercriminales. El test

de penetración interno incluye, en cambio, identificar las vulnerabilidades en el intranet y las vulnerabilidades de los empleados, pero no las vulnerabilidades de software de las aplicaciones Web externas. Dado que tenemos dos actores (responsable del tratamiento y cibercriminales) con dos opciones cada uno, una matriz puede representar su porcentaje de probabilidades en cuatro escenarios:



- **Escenario 1:** El responsable del tratamiento opta por el test de penetración externo y el cibercriminal escoge atacar aprovechando vulnerabilidades técnicas de las aplicaciones Web. En este escenario, el responsable tendría la resiliencia de un 90%, mientras la capacidad de la amenaza tendría el 10%.

- **Escenario 2:** El responsable del tratamiento opta por el test de penetración externo y el cibercriminal escoge atacar mediante ingeniería social, la ingenuidad de los empleados. En este escenario, el responsable tendría la resiliencia de un 40%, mientras la capacidad de la amenaza tendría el 60%.

- **Escenario 3:** El responsable del tratamiento opta por el test de penetración interno y el cibercriminal escoge atacar aprovechando vulnerabilidades técnicas de las aplicaciones Web. En este escenario, el responsable tendría la resiliencia de un 40%, mientras la capacidad de la amenaza tendría el 60%.

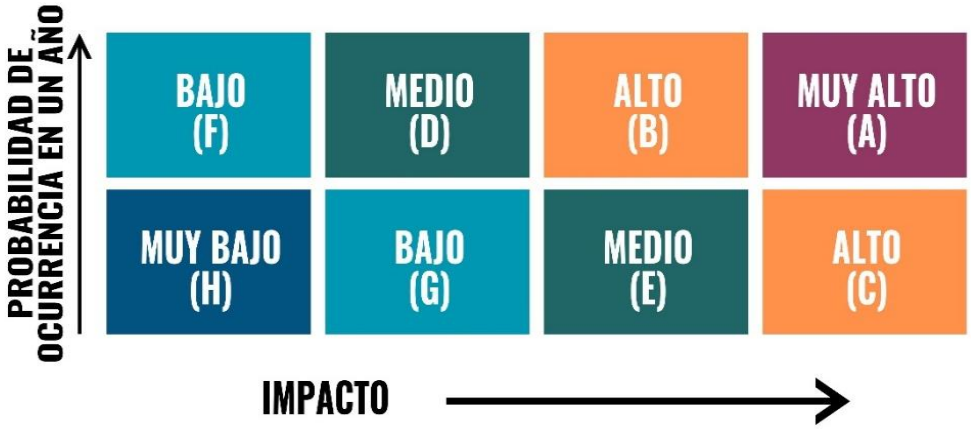
- **Escenario 4:** El responsable del tratamiento opta por el test de penetración interno y el cibercriminal escoge atacar mediante ingeniería social, la ingenuidad de los empleados. En este escenario, el responsable tendría la resiliencia de un 90%, mientras la capacidad de la amenaza tendría el 10%.

Es necesario comprender que el riesgo no es lineal; y, por ello, no siempre es conveniente multiplicar o combinar la probabilidad de ocurrencia por el impacto, ni alinear los riesgos de manera simétrica. En riesgos que pueden vulnerar derechos y libertades puede ser común tener riesgos de muy baja probabilidad de ocurrencia, pero muy alto impacto.

Por ejemplo, pensemos en los carros chocones (juegos) que pueden tener un 99% de probabilidad de ocurrencia para chocarse, pero el peor impacto es una lesión leve, cuyo tratamiento cuesta $100. Esto no es igual a tener un accidente de avión que tiene el 1% de probabilidad de ocurrencia, pero un impacto inaceptable, pues es casi seguro que los pasajeros pierdan la vida en caso de suceder un accidente. Lo mismo sucede en la protección de datos personales, pues no se trata de activos sino de derechos y el impacto en los derechos de las personas naturales puede tener mucho más peso que la probabilidad de ocurrencia.

El siguiente ejemplo muestra una matriz de riesgos con *rationales* cuantitativos que establecen la probabilidad de ocurrencia y el impacto mostrado con sus valores calibrados. Hay dos niveles de probabilidad de ocurrencia y cuatro de impacto. No obstante, la diferencia es que los niveles de riesgo bajo, medio, y alto tienen dos escenarios considerando un mejor balance para los riesgos de baja probabilidad y alto impacto:

Riesgo Muy Alto: A) Probabilidad (>0.3), Impacto (>$1 000 000)
Riesgo Alto: B) Probabilidad (>0.3), Impacto (>=$100 000; < $1 000 000). C) Probabilidad (<0.3), Impacto (>$1 000 000)
Riesgo Medio: D) Probabilidad (>0.3), Impacto (>=$10 000; <$100 000). E) Probabilidad (<0.3), Impacto (>=$100 000; <1 000 000)
Riesgo Bajo: F) Probabilidad (>0.3), Impacto (>=$1 000; <$10 000). G) Probabilidad (<0.3), Impacto (>=$10 000; <100 000)
Riesgo Muy Bajo: Impacto (<$1000)



En este caso, los resultados son relativamente simétricos, pero podrían no serlo. Todo depende del escenario de riesgos planteado y la calibración de los valores de entrada.

3.6. Análisis cualitativo. Son tipos de análisis que usualmente utilizan una escala de atributos o niveles de riesgo. Es esencialmente un análisis subjetivo; en el cual, se evalúan la probabilidad o frecuencia de ocurrencia y el impacto por una persona que obligatoriamente debe ser un experto. Al fundamentarse en opiniones subjetivas pueden ser considerados como superficiales y poco confiables debido a factores como el desconocimiento del contexto del riesgo, el exceso de confianza del experto, los problemas de sesgo y los problemas de ruido.

Sin embargo, hay circunstancias en las cuales no hay datos cuantitativos de entrada, los datos no son confiables, escenarios excepcionales en donde un análisis cualitativo puede ser más informativo o simplemente un análisis cualitativo está mejor alineado a los recursos financieros y *know how* de una institución. En los casos en que el análisis cualitativo sea la opción, es fundamental implementar métodos para mejorarlo. Estos métodos consisten en la

calibración de las opiniones de expertos con el fin de obtener mayor objetividad en sus estimaciones. En el área de la gestión de riesgos para la protección de derechos y libertades de los titulares de datos, pueden combinarse el análisis cuantitativo y el cualitativo. Es bastante común realizar un análisis cualitativo para analizar riesgos primordialmente de cumplimiento jurídico e implementar análisis cuantitativo para riesgos operacionales como los de seguridad de la información o de la analítica predictiva.

3.7. Métodos cualitativos de análisis. Ejemplos de métodos cualitativos de análisis son las entrevistas y cuestionarios o el análisis argumental.

a) Entrevistas y cuestionarios. Un cuestionario puede ser mejorado cuando el entrevistador utiliza técnicas para calibrar al entrevistado a través de una entrevista. En principio, el entrevistado puede dar opiniones generales, imprecisas o vagas, en donde el rol del auditor (como un Delegado de Protección de Datos) es ayudar al entrevistado a autocalibrarse. El siguiente ejemplo contempla la entrevista de un Delegado de Protección de Datos (DPD) que entrevista a un CISO acerca de la estimación de la probabilidad de ocurrencia de un incidente de denegación de servicio:

RIESGO: Vulneración de la disponibilidad de datos personales / Ransomware (Art. 37 LOPDP).

IMPACTO PARA EL RESPONSABLE DEL TRATAMIENTO: Entre USD 10 000 y USD 15 000 la hora (CUANTITATIVO).

IMPACTO EN LOS DERECHOS Y LIBERTADES DE LOS TITULARES: Se viola su derecho de acceso por un día (CUALITATIVO).

DPD: Si los sistemas de información son infectados con un ransomware que cifre las bases de datos, ¿Cuánto tiempo estarían los procesos *offline*?

CISO: No lo sabemos con certeza, a veces son horas, a veces son días. Lo importante es restaurar el sistema y no documentar.

DPD: Ok, busquemos un rango. ¿Cuál es el mayor tiempo que los sistemas estuvieron *offline* como consecuencia de un ataque?

CISO: No lo sé.

DPD: ¿Unos dos días?

CISO: Probablemente.

DPD: Necesitamos encontrar el 90% de intervalo de confianza. Considerando todos los incidentes cibernéticos que han ocurrido en el pasado, ¿son en promedio mayores a 1 día?

CISO: Usualmente el promedio sería de menos de un día.

DPD: ¿Entonces el máximo tiempo *offline* sería?

CISO: 24 horas.

DPD: OK. ¿Cuál sería el mínimo tiempo *offline* en tu opinión?

CISO: Algunos eventos se han podido resolver en 2 horas.

DPD: ¿Alguna vez pudieron restaurar los datos en menos de 1/2 hora? **CISO:** Una sola vez. **DPD:** Bien. Entonces tú estarías 90% seguro (nivel de confianza) de que los límites de tiempo para restaurar los datos son entre 30 minutos y 24 horas? **CISO:** Sí, pero una vez tuvimos los sistemas *offline* por 3 días. **DPD:** ¿Una vez entre cuántos ataques de ransomware? **CISO**: Entre 10 ataques sufridos el año pasado. **DPD:** OK. Entonces tenemos el 90% de nivel de confianza de que los incidentes de ransomware dejarán los sistemas *offline* entre ½ hora y 24 horas.

En el ejemplo anterior, el CISO es el experto en seguridad de la información; y, en el caso particular, en el escenario de riesgo de vulneración de la disponibilidad de datos personales por un ataque de ransomware. El DPD ayuda al experto a autocalibrarse con el fin de obtener datos que le sirvan para su evaluación de impacto del tratamiento de datos personales.

b) Análisis argumental. Consiste en analizar los argumentos de documentos, textos o precedentes jurídicos; y, con base en los argumentos analizados, dar una estimación cualitativa. Es un método común utilizado por profesores al calificar un examen o por jueces y autoridades administrativas al estimar el monto de una sanción. El siguiente ejemplo analiza el argumento jurídico sobre el factor tipo de datos personales y lo etiqueta de acuerdo con una escala dividida en porcentajes del 1% al 100%, siendo interpretado 1% como deficiente y 100% como eficiente:

FACTOR	TEXTO	EVALUACIÓN
Tipo de datos	En el presente caso, los datos sensibles son de la salud y pueden afectar gravemente los derechos de los titulares.	99%
Tipo de datos	Los datos de la salud son sensibles, pero no afectan mayormente los derechos.	1%
Grupos especialmente vulnerables	La causal de interés legítimo del responsable del tratamiento no puede justificar la divulgación de datos de la salud, pues impacta gravemente a las personas con enfermedades permanentes.	99%
Grupos especialmente vulnerables	La causal de interés legítimo del responsable del tratamiento justifica la divulgación de datos sensibles de la salud para impulsar la industria.	1%

En el ejemplo anterior, podemos encontrar calificaciones en los extremos, en donde la evaluación del 99% son argumentos jurídicos adecuados y la evaluación del 1% son argumentos jurídicos ilegales y deficientes. Se recomienda el análisis argumental para ir

formando los criterios adecuados de evaluación de impacto, a la luz de los argumentos y sanciones de la Superintendencia de Protección de Datos; y, también, del análisis y doctrina de expertos. Para utilizar este método basta contar con un experto. Cuando el responsable del tratamiento cuente con el *know how* necesario, es de gran ayuda implementar modelos de procesamiento de lenguaje natural (*Natural Language Processing*) en función de opiniones de expertos o de las mismas sanciones administrativas pasadas de la SPDP para evaluar los argumentos y etiquetarlos en función de su importancia. De esta manera es posible tener una referencia en el futuro acerca de los argumentos jurídicos de la autoridad para utilizarlos como entrada en el análisis de riesgos.

	LOPDP	Caso	año	impacto	argumento
0	Arts. 8, 24	Responsable del tratamiento 1	2024	5	El responsable del tratamiento implementó un s...
1	Arts. 8, 24	Responsable del tratamiento 2	2024	1	El responsable del tratamiento utilizó los dat...
2	Arts. 8, 24	Responsable del tratamiento 3	2025	3	El responsable del tratamiento no verifica la ...

```
In [36]: evaluations[evaluations.impacto==5]['argumento'][0]
Out[36]: 'El responsable del tratamiento implementó un sistema de identificación remota personalizado, mediante el cual los p
         adres, madres, o representantes adultos del menor, autorizan el tratamiento de sus datos.'

In [37]: evaluations[evaluations.impacto==1]['argumento'][1]
Out[37]: 'El responsable del tratamiento utilizó los datos personales de menores de edad sin legitimidad, vendiéndolos a vari
         as empresas.'

In [38]: evaluations[evaluations.impacto==3]['argumento'][2]
Out[38]: 'El responsable del tratamiento no verifica la edad de los titulares de datos, pero tiene un sistema de denuncias cl
         aramente visible en su aplicación web, y un aviso visible acerca de que el sitio es disponible únicamente para mayor
         es de edad.\xa0'
```

El ejemplo anterior analiza los argumentos jurídicos la autoridad de control acerca de tres responsables del tratamiento en el cumplimiento de los artículos 8 y 24 de la LOPDP. Puede ser de gran ayuda implementar modelos de *Natural Language Processing* (NLP), en función de opiniones de expertos o de las mismas sanciones administrativas pasadas de la Superintendencia de Protección de Datos Personales para evaluar los argumentos y etiquetarlos en función de su importancia. De esta manera, es posible tener una referencia en el futuro acerca de los argumentos jurídicos de la autoridad para utilizarlos como entrada en el análisis de riesgos.

3.8. Modelos calibración de opiniones. Existen modelos de calibración de opiniones enfocados a una toma de decisiones más objetiva, que eliminen el sesgo y el ruido. Entre los recomendados están los siguientes:

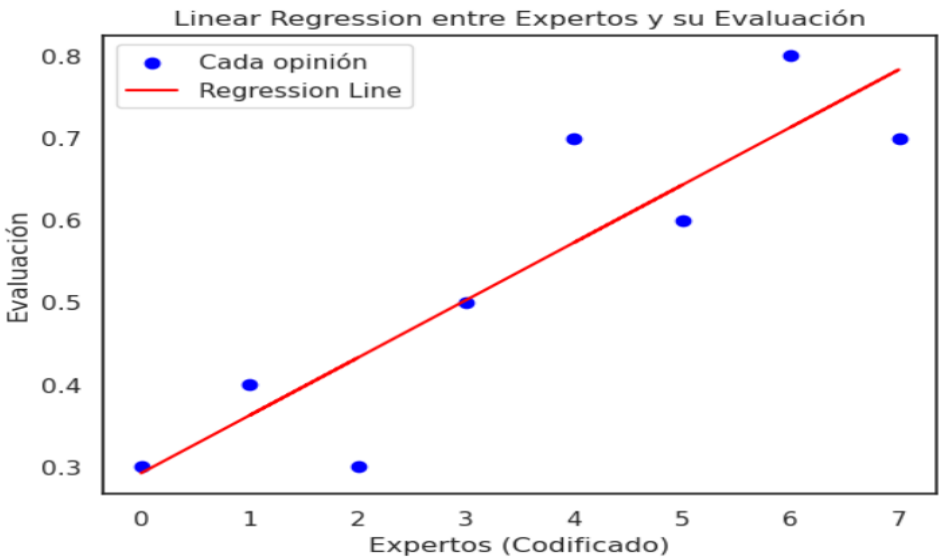
a) Método Delphi. Consiste en los siguientes cuatro pasos: (1) Consultar a varios expertos acerca de la estimación del nivel de un riesgo, pero de manera anónima. Esto permite eliminar el sesgo en las opiniones, dado que nadie sabrá la identidad del experto. (2) Consultar a expertos con diferentes puntos de vista y experticia, (3) Utilizar al menos 5 expertos, (4) Promediar las opiniones.

b) Modelo Lens. Tiene similitudes con el método Delphi. Consiste al menos en: (1) Invitar expertos en el tipo de riesgo, (2) Los expertos identifican los factores del riesgo, (3) Los expertos evalúan un escenario de riesgo, (4) Se promedian las opiniones de los expertos, (5) Con sus opiniones, se implementa un modelo de *Logistic Regression* con el objeto de representar resultados.

Todos estos métodos de calibración de expertos son altamente recomendados para reducir la subjetividad en un análisis cualitativo de riesgos. El siguiente ejemplo muestra como las opiniones de ocho expertos anónimos puede ayudar a calibrar los datos de entrada:

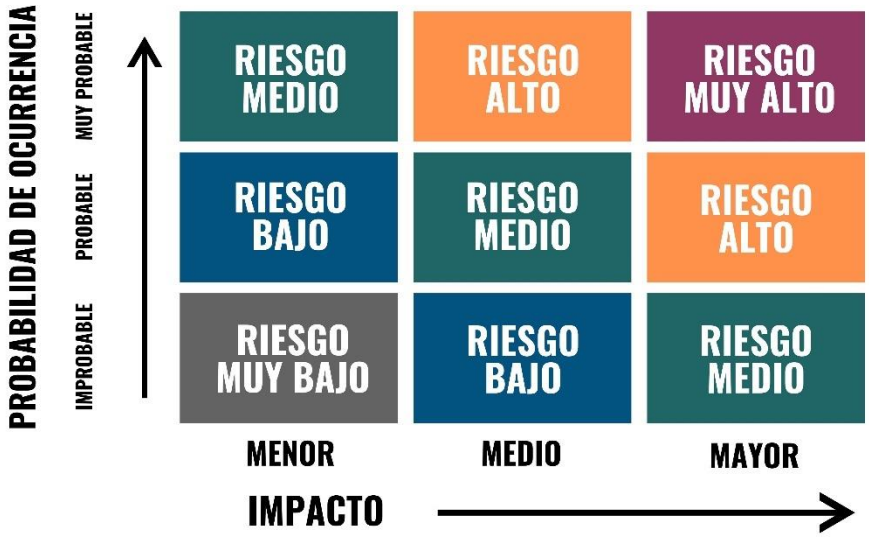
Experto A	0.3
Experto B	0.4
Experto C	0.3
Experto D	0.5
Experto E	0.7
Experto F	0.6
Experto G	0.8
Experto H	0.7

Cuando los responsables y encargados del tratamiento tengan los medios y el conocimiento; y, sobre todo, para el tratamiento a gran escala, los resultados de las opiniones de expertos pueden ser automatizados. Es posible implementar sistemas inteligentes entrenados con modelo de aprendizaje automático como *Logistic Regression, Linear Regression* y/o redes neuronales, con el objetivo de automatizarlos para futuras calibraciones en casos y circunstancias similares.



3.9. Representación cualitativa del riesgo. Usualmente, el análisis cualitativo utiliza matrices de riesgos con mapas de calor. Sin embargo, las matrices con *rationales* cualitativos tienen problemas considerables para la interpretación del riesgo. En el sector de la seguridad de la información son comunes matrices que combinan la probabilidad de ocurrencia con el

impacto, utilizando niveles de riesgo (como bajo, medio, y alto) y mapas de calor. Esta representación tiene varios problemas como: inconsistencia en la aceptación del riesgo, compresión de rangos, centralización de sesgos e ilusión de comunicación[19]. No obstante, pueden ser útiles ante audiencias no expertas cuando se las utiliza como instrumento de representación, mas no de calibración. En el análisis cualitativo de riesgos es común hacer una escala con niveles de riesgo y combinarlos, por ejemplo:



Sin embargo, los riesgos de protección de datos personales no son lineales y es necesario al menos contar con un *rationale* que explique los escenarios que se representan. El siguiente ejemplo muestra el ejemplo optimizado de utilizar una matriz para la probabilidad de ocurrencia y el impacto, pero utilizando insumos cualitativos:

Riesgo crítico :
A) Probabilidad (alta)
Impacto (Datos sensibles de personas más vulnerables)

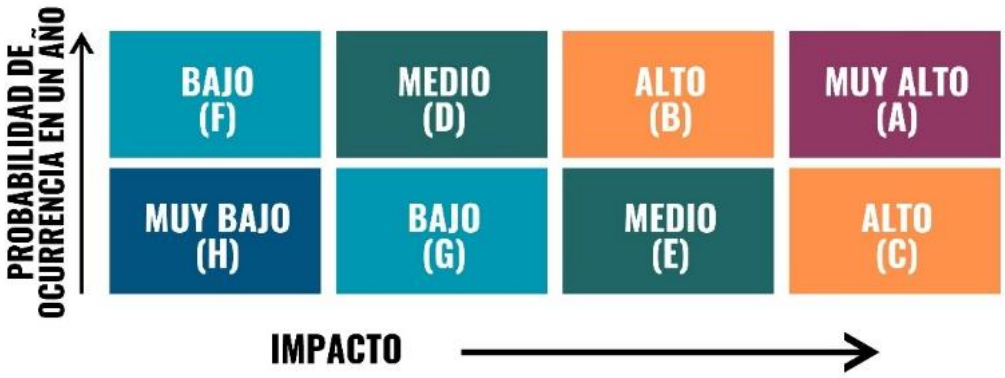
Riesgo Alto:
B)Probabilidad (Alta)
Impacto (Datos financieros de personas más vulnerables. datos sensibles de personas promedio)
c) Probabilidad (Baja)
Impacto (Datos sensibles de personas más vulnerables)

Riesgo Medio:
D) Probabilidad (Alta)
Impacto (Datos comportamentales de personas máas vulnerables. Datos financieros de personas promedio)
E) Probabilidad (Baja)
Impacto (Datos financieros de personas más vulnerables. Datos sensibles de personas promedio)

Riesgo Bajo:
F)Probabilidad (Baja)
Impacto (Datos comportamentales de personas más vulnerables. Datos financieros de personas promedio)
G) Probabilidad (Alta)
impacto (datos simples de personas más vulnerables. Datos comportamentales de personas promedio)

Riesgo Muy bajo:
H) Probabilidad (Baja)
Impacto (Datos simples de personas promedio)

[19] Para expandir su conocimiento acerca de las limitaciones de las matrices de riesgos, se recomienda la siguiente lectura: BRATVOLD (R.), BICKEL (J.), *The Risk of Using Risk Matrices*, SPE Economics & Managment 6, 2013, pp. 56-66.



En un análisis cualitativo se recomienda: un enfoque estricto de *rationales*, calibrar la probabilidad de ocurrencia en un lapso determinado; y, no combinar la probabilidad de ocurrencia y el impacto por defecto, sin un previo análisis del tipo de riesgo.

a) Un enfoque estricto de *rationales*. Es fundamental mejorar la efectividad de una matriz de riesgos a través de la justificación objetiva de los valores de entrada que sustentan los niveles de probabilidad de ocurrencia e impacto. No se trata de adivinar, sino de calibrar los valores de entrada para un modelo de riesgos.

b) Calibrar la probabilidad o frecuencia de ocurrencia en un lapso determinado. Es fundamental que la probabilidad de ocurrencia sea calibrada en un lapso determinado.

c) No combinar la probabilidad o frecuencia de ocurrencia y el impacto por defecto. Otro error concurrente en los mapas de calor es combinar la probabilidad de ocurrencia por el impacto en todo tipo de escenario de riesgo. Perder la visibilidad de los criterios de la probabilidad de ocurrencia y del impacto no ayuda a la toma de decisiones informadas.

Estos ejemplos muestran varias formas de analizar riesgos de manera cuantitativa o cualitativa. Es recomendable revisar guías o normas de mejores prácticas que aborden métodos de análisis de riesgos, tales como el Risk Taxonomy (O-RT), la norma ISO 31010, e incluso métodos y modelos cuantitativos provenientes de otras áreas como las ciencias actuariales, la econometría o métodos cualitativos provenientes de la psicología y de la gestión de proyectos.

4. Evaluación de riesgos de protección de datos personales

Esta etapa de la gestión de riesgos consiste en comparar los niveles obtenidos de cada riesgo, con los criterios de evaluación establecidos en la etapa de establecimiento del contexto. En un escenario ideal, todos los niveles de riesgo que superen la tolerancia o capacidad al riesgo establecida deberán ser mitigados en la etapa de tratamiento de riesgos.

4.1 Evaluación de impacto del tratamiento de datos. La LOPDP dispone que la evaluación de impacto del tratamiento de datos personales es obligatoria cuando el tratamiento conlleva un alto riesgo para los derechos y libertades de los titulares de los datos en el artículo 42. No obstante, para poder determinar el nivel de riesgo ALTO del tratamiento de datos personales, es necesario realizar una evaluación de impacto en el contexto de una gestión de riesgos, como lo establece el artículo 40. Por ello, se recomienda realizar la evaluación de impacto por defecto en cualquier tratamiento de datos personales. Además, hay que considerar que el estado del arte de los análisis de impacto de privacidad (*Privacy Impact Assessments*) es muy inmaduro. En la práctica, los análisis de impacto de privacidad se han convertido más en listas de chequeo, priorizando la descripción sobre el análisis de riesgos; y, con una estrecha visión del riesgo, en particular desconectada de riesgos operacionales como los de seguridad de la información[20].

Considerando la necesidad de actualizar los análisis de impacto del tratamiento de datos personales, esta guía propone ahondar en el análisis de riesgos del tratamiento de datos personales; y, en una visión holística y multidimensional del riesgo.

4.2. Etapas previas. La evaluación de impacto del tratamiento de datos personales debe ser el resultado del establecimiento del contexto, de la identificación y del análisis de riesgos de protección de datos personales. Es importante considerar que la principal finalidad es evaluar el impacto que pueden tener los titulares de datos en sus derechos y libertades, debido al tratamiento de sus datos personales. No obstante, no es posible evaluar de manera eficaz y eficiente el impacto, si no se han construido los criterios de evaluación de riesgos, si no se han identificado riesgos jurídicos, organizacionales y técnicos y si no se han analizado los riesgos en función de su probabilidad o frecuencia de ocurrencia e impacto. Esto ha generado confusiones, pues la palabra *"Assessment"*[21] en inglés incluye la identificación, análisis y evaluación de riesgos y no tiene una traducción exacta al español. Por otro lado, el impacto es solo una dimensión del riesgo. Si bien la idea es estimar el impacto en los derechos y libertades de los titulares de datos, no es realista prescindir de la dimensión de la probabilidad o frecuencia de ocurrencia, pues siempre está presente.

Es obligatorio que la evaluación de impacto del tratamiento de datos personales sea tratada como una gestión de riesgos para reducir la incertidumbre y tomar decisiones informadas para la protección de los derechos y libertades de los titulares de datos; y, no simplemente, una lista chequeo en la que se procede a evaluar riesgos sin ningún sustento. Esta deberá ser el resultado al menos los siguientes pasos:

---

[20] Para expandir su conocimiento en la necesidad de mejorar los PIA, se recomienda leer el siguiente artículo: Shapiro S. (2021), *Time to Modernize Privacy Impact Assessment*, en Issues in Science and Technology, Vol.38, No.1, pp. 19-22.

[21] Se recomienda revisar el estándar ISO/IEC 27005:2022, cláusula 5.1.

Contenidos: Evaluación de impacto del tratamiento de datos personales

- Establecer los criterios de evaluación de riesgos para la protección de los derechos y libertades de los titulares.
- Una descripción de los procesos que implican tratamiento de datos personales.
- La identificación de los tipos de datos personales tratados.
- Los activos de los cuales dependen los datos personales.
- Elaborar escenarios de riesgo.
- Los mecanismos para el ejercicio de los derechos por parte de los titulares de los datos.
- El perfilamiento de amenazas.
- La identificación de vulnerabilidades jurídicas, organizacionales y técnicas.
- El análisis de riesgos en función de su probabilidad o frecuencia de ocurrencia y de su impacto en cada escenario de riesgo.
- La calibración del impacto en función del impacto mayor que pueden sufrir ciertos grupos especialmente vulnerables de titulares de los datos.
- La evaluación de impacto de cada escenario de riesgo.
- Las medidas de tratamiento para reducir el nivel del riesgo evaluado.

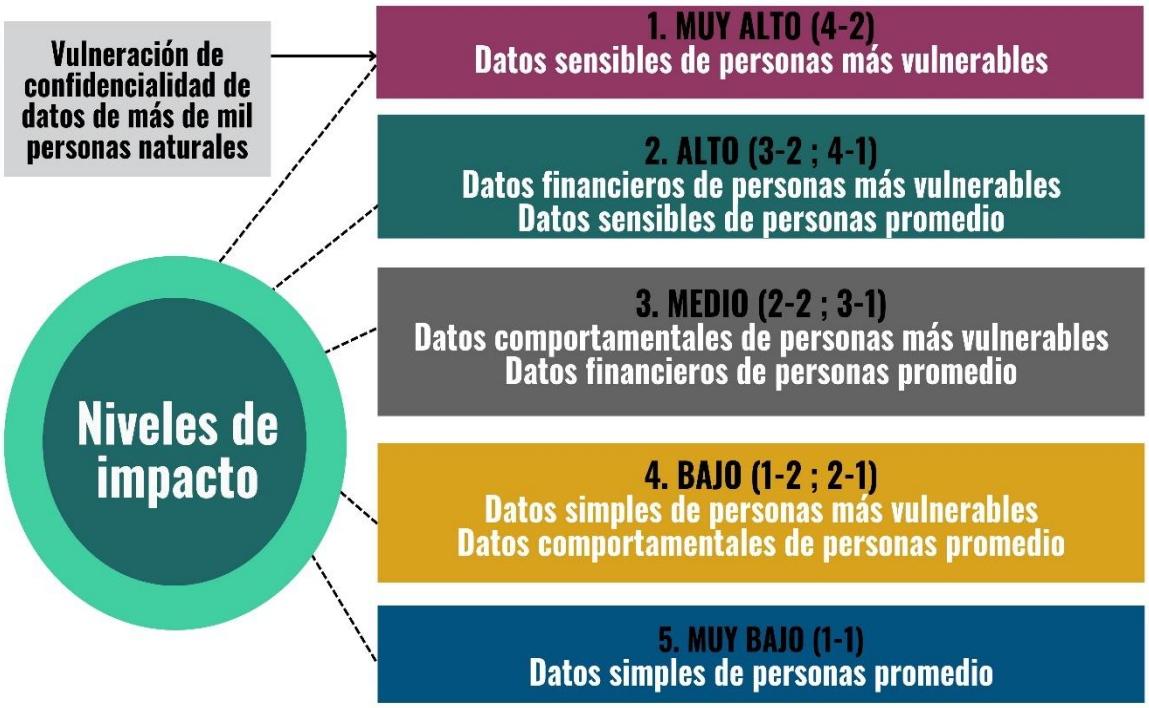
4.3. Contenidos. La evaluación de riesgos contendrá fundamentalmente los niveles de riesgo obtenidos, comparados a los criterios de evaluación del riesgo. No existe un estilo definido, pero hay que tener mucho cuidado en visualizar el nivel del riesgo como un producto, pues no es lo mismo una gestión de riesgos para la protección de activos, que una gestión de riesgos para la protección de derechos y libertades. Es común pensar en el valor del riesgo (R) como un producto de la probabilidad de ocurrencia (P) multiplicado por el impacto (I). Formula R= P*I. No obstante, esto puede ofuscar el valor real del impacto, considerando que estamos protegiendo derechos, no activos. Si bien se puede agregar el porcentaje de vulnerabilidad (V) que tienen grupos especialmente vulnerables de titulares de datos implementando la fórmula: R = (P) * (I * V), en ciertos escenarios de riesgo, multiplicar las dimensiones del riesgo puede ofuscar la claridad de la información obtenida en el análisis de riesgos, así como sus *rationales*. Sin embargo, otra opción es más bien utilizar registros de evaluación de riesgos que mantengan los resultados de ambas dimensiones del riesgo.

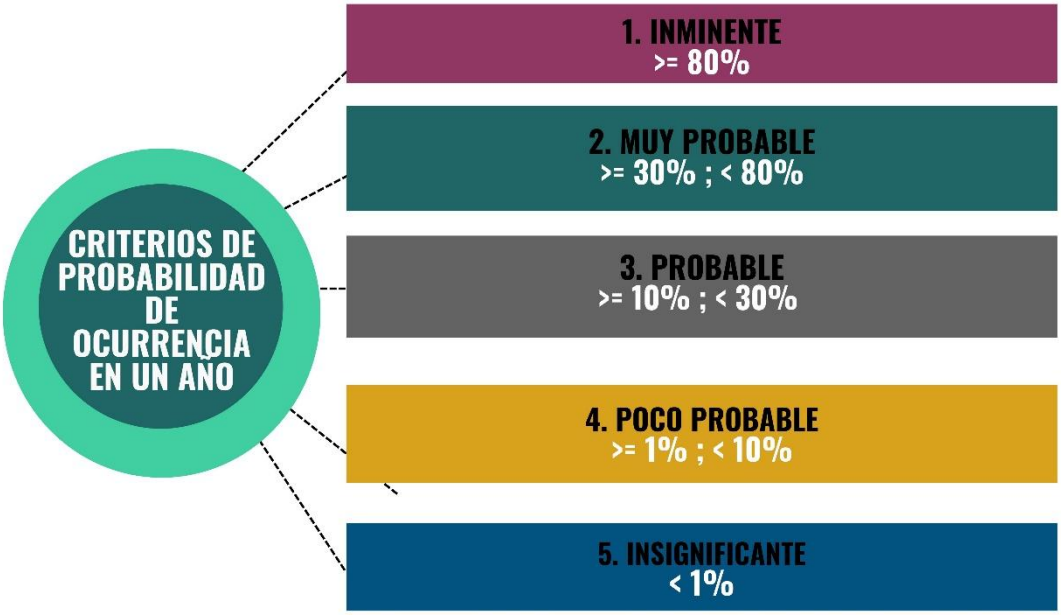
Se puede implementar una lista de los artículos de la LOPDP y sus niveles de riesgo, una modalidad de cuestionario en donde se incluyan preguntas ilustrativas relacionadas con las obligaciones establecidas en la LOPDP, curvas de exceso de pérdidas en caso de análisis cuantitativo, histogramas y cualquier otra que sea de utilidad para comunicar los niveles de riesgo. A partir de ello, es importante priorizar los riesgos, lo cual involucra un proceso de

toma de decisiones informadas, gracias a haber realizado una gestión de riesgos eficiente y eficaz.

El siguiente ejemplo muestra la evaluación de riesgos cualitativa, considerando los criterios de evaluación de riesgos previamente establecidos y los resultados del análisis de riesgos. Este ejemplo está enfocado en la evaluación del impacto en los derechos y libertades de los titulares de datos y utiliza varios de los artículos de la LOPDP. Consecuentemente, el criterio de aceptación de riesgo no aplica, pues el cumplimiento es al 100 %:

CRITERIOS DE EVALUACIÓN DEL IMPACTO Y DE LA PROBABILIDAD Y FRECUENCIA DE OCURRENCIA (CUALITATIVO):





EVALUACIÓN DE RIESGOS (CUALITATIVO)

Riesgos jurídicos por vulneración de derechos y libertades de los titulares de datos

ARTÍCULO	PROBABILIDAD DE OCURRENCIA	IMPACTO TITULARES PROMEDIO	IMPACTO GRUPOS MAS VULNERABLES
Art. 7. Tratamiento legítimo de datos personales	Poco probable	Medio	Alto
Art. 10 (c) Transparencia	Poco probable	Alto	Muy alto
Art. 10 (d) Finalidad	Poco probable	Bajo	Medio
Art. 10 (e) Pertinencia y minimización de datos personales	Probable	Medio	Alto
Art. 10 (i) Conservación	Muy probable	Medio	Alto
Art. 12. Derecho a la información	Poco probable	Alto	Muy alto
Art. 13. Derecho de acceso	Poco probable	Bajo	Medio
Art. 14. Derecho de rectificación y actualización	Insignificante	Muy Bajo	Bajo
Art. 15. Derecho de eliminación	Probable	Alto	Muy alto
Art. 16. Derecho de oposición	Poco probable	Medio	Alto
Art. 17. Derecho a la portabilidad	Insignificante	Bajo	Medio
Art. 20. Derecho a no ser objeto de una decisión basada única o	Poco probable	Alto	Muy alto

parcialmente en valoraciones automatizadas			
Art. 55. Transferencia o comunicación internacional de datos personales	Poco probable	Medio	Alto

Riesgos operacionales de seguridad de datos personales (confidencialidad)

ARTÍCULO	PROBABILIDAD DE OCURRENCIA	IMPACTO TITULARES PROMEDIO	IMPACTO GRUPOS MÁS VULNERABLES
Art. 37. Seguridad de datos personales	Probable	Alto	Muy alto

Riesgos operacionales de seguridad de datos personales (integridad)

ARTÍCULO	PROBABILIDAD DE OCURRENCIA	IMPACTO TITULARES PROMEDIO	IMPACTO GRUPOS MÁS VULNERABLES
Art. 37, art. 10 (j). Seguridad de datos personales	Poco probable	Medio	Alto

Riesgos operacionales de seguridad de datos personales (disponibilidad)

ARTÍCULO	PROBABILIDAD DE OCURRENCIA	IMPACTO TITULARES PROMEDIO	IMPACTO GRUPOS MÁS VULNERABLES
Art. 37, art. 10 (j). Seguridad de datos personales	Probable	Medio	Alto

Gracias a este registro de evaluación de riesgos es posible priorizar los riesgos que deben ser mitigados. Los criterios de evaluación del impacto han sido calibrados en el ejemplo de acuerdo con dos criterios: el tipo de datos personales y el nivel de vulnerabilidad de los titulares de los datos. Esto fue planteado así por cuanto el cumplimiento en derechos es al 100%. La única opción de mitigación sería dejar de tratar ciertos tipos de datos de mayor riesgo o no tratar datos de grupos especialmente vulnerables.

Sin embargo, los criterios de evaluación de probabilidad de ocurrencia sí tienen un criterio de aceptación al riesgo ubicado en el nivel "poco probable". Esto quiere decir, que se tendrán que mitigar los niveles que sobrepasen este criterio y priorizarlos de acuerdo con su nivel. Es recomendable incluir los *rationales* de cada riesgo en esta lista de riesgos a mitigar:

ARTÍCULO	PROBABILIDAD DE OCURRENCIA	IMPACTO TITULARES PROMEDIO	IMPACTO GRUPOS MÁS VULNERABLES
Art. 10(e). Pertinencia y minimización de datos personales	Probable	Medio	Alto
Art. 10(i). Conservación	Muy probable	Medio	Alto
Art. 15. Derecho de eliminación	Probable	Alto	Muy alto
Art. 37. Seguridad de datos personales (CONFIDENCIALIDAD)	Probable	Alto	Muy alto
Art. 37, art. 10 (j). Seguridad de datos personales (DISPONIBILIDAD)	Probable	Medio	Alto

Con esta información, los responsables y encargados del tratamiento pueden pasar a la fase de tratamiento de riesgos de manera informada, priorizando estos riesgos como resultado de las respectivas auditorias jurídicas, organizacionales y técnicas. No hay que olvidar que la gestión de riesgos es fundamental para poder tomar decisiones informadas. Pero la toma de decisiones podría considerarse como un arte; y, a la final, dependerá de los objetivos, de la voluntad y del presupuesto de cada responsable y encargado del tratamiento en particular.

Por un lado, una ventaja de la evaluación de riesgos cualitativa es que es relativamente más fácil de comprender para el usuario no entrenado. No obstante, una desventaja de la evaluación de riesgos cualitativa es que no está vinculada directamente el valor del riesgo en caso de materializarse. Si bien es aún poco usual el realizar un análisis y evaluación de riesgos cuantitativa en riesgos primordialmente de cumplimiento jurídico, es mucho más utilizada en los riesgos operacionales como los de la seguridad de la información. Hay opciones para implementarlo, algunas fundamentadas en una lógica del Valor al Riesgo de Datos Personales (Pd-VaR) que ya fueron presentadas anteriormente.

La primera consiste en evaluar el valor al riesgo fundamentado en el análisis jurimétrico de sanciones administrativas ya existentes; esto, bajo la lógica de que las autoridades de protección de datos y los jueces son quienes cuantifican el impacto en los derechos y libertades de los titulares de datos[22]. Esta alternativa es funcional, pero depende de la eficacia y eficiencia de la autoridad de protección de datos personales en la cuantificación de las sanciones.

La segunda consiste en estimar el impacto material utilizando métodos estadísticos y probabilísticos con el fin de calibrar el promedio del impacto que pueden sufrir los titulares de los datos ante una vulneración de sus derechos. Esta alternativa, bien implementada,

[22] Para expandir sus conocimientos en jurimetría y analítica predictiva legal, se recomiendan los siguientes trabajos: Aletras, N., Lampos, V. (2016). *Predicting judicial decisions of the European Court of Human Rights: A Natural Language Processing Perspective*, Pee J. Computer Science 2, e93, 1-19. Katz, D., *et al*. (2017). *A General Approach for Predicting the Behavior of the Supreme Court of the United States*, arXiv:1612.03473 [physics.soc-ph], pp.1-15. Enriquez, L. (2024). *Personal data Breaches: towards a deep integration between information security risks and GDPR compliance risks*, Université de Lille, Francia. Ashley K. (2017), *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age*, Cambridge University Press, Reino Unido.

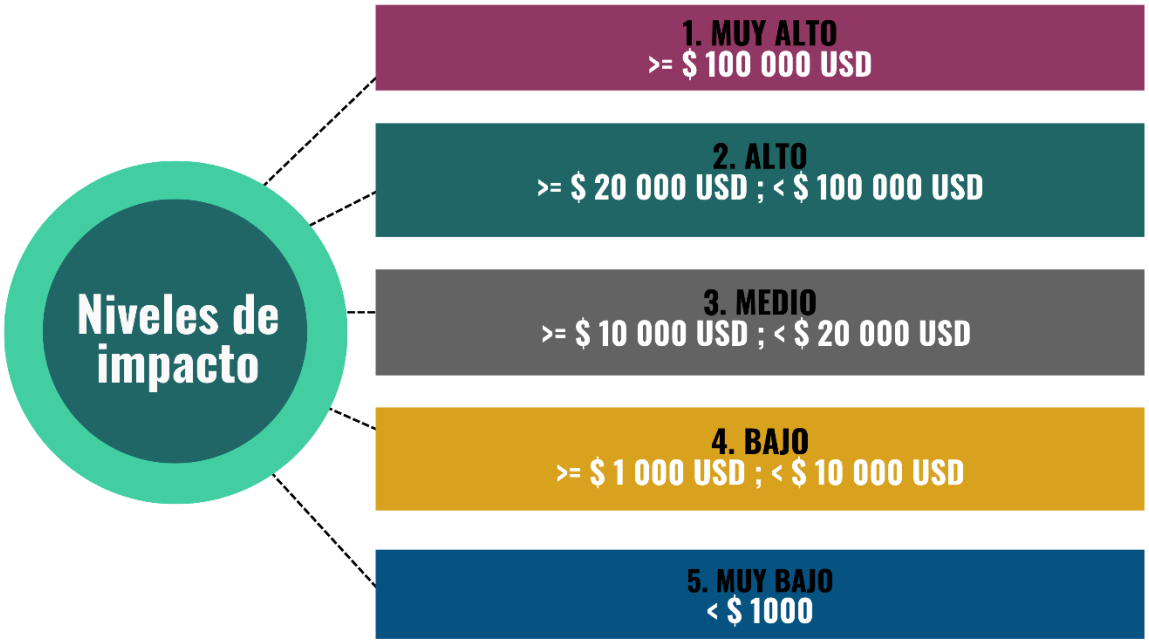
puede tener grados altos de acierto; sin embargo, corre el riesgo de que las autoridades de protección de datos y jueces cuantifiquen el impacto de las vulneraciones de derechos y libertades de otra manera.

En el ámbito de la probabilidad o frecuencia de ocurrencia en áreas de riesgos operacionales como la seguridad de la información, es mejor utilizar frecuencia de ocurrencia, por cuanto es más común que haya varios incidentes en un lapso determinado. Por ejemplo, una violación de consentimiento será reconocida como tal únicamente cuando la SPDP la sancione. En cambio, pueden existir varios incidentes de vulneración a la seguridad de datos, al margen de que sean sancionados o no por la SPDP.

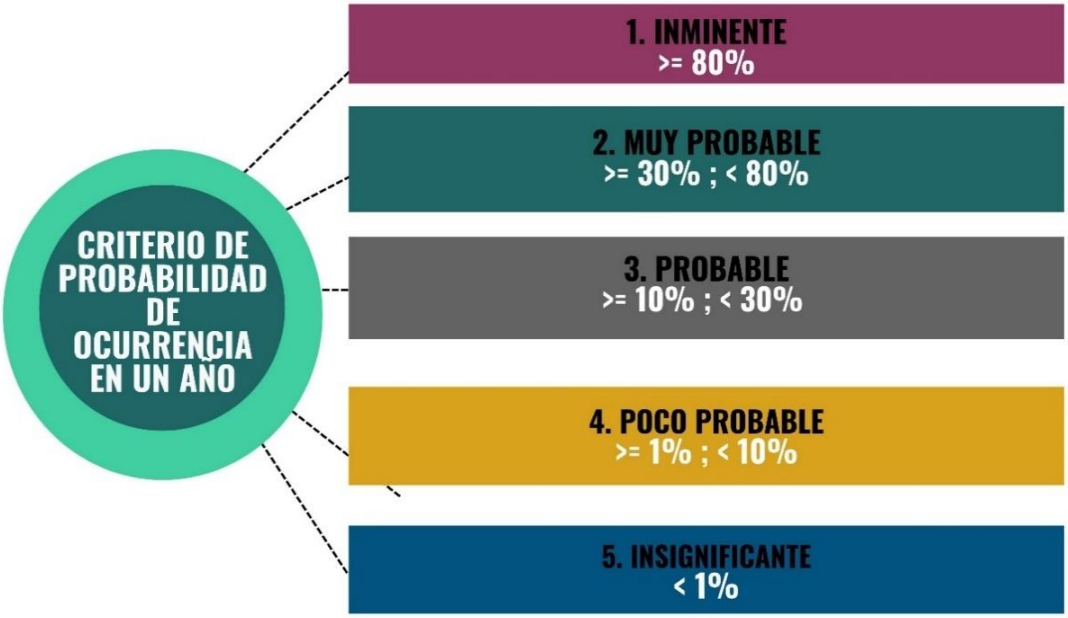
Por lo tanto, en una evaluación cuantitativa de riesgos, en ciertos casos puede resultar más adecuado emplear criterios basados en la frecuencia de ocurrencia.

El siguiente ejemplo muestra el ejemplo anterior, pero con criterios de evaluación cuantitativos en cuanto al impacto, a la probabilidad de ocurrencia para riesgos de cumplimiento primordialmente jurídicos; y, a la frecuencia de ocurrencia para riesgos operacionales de seguridad de datos:

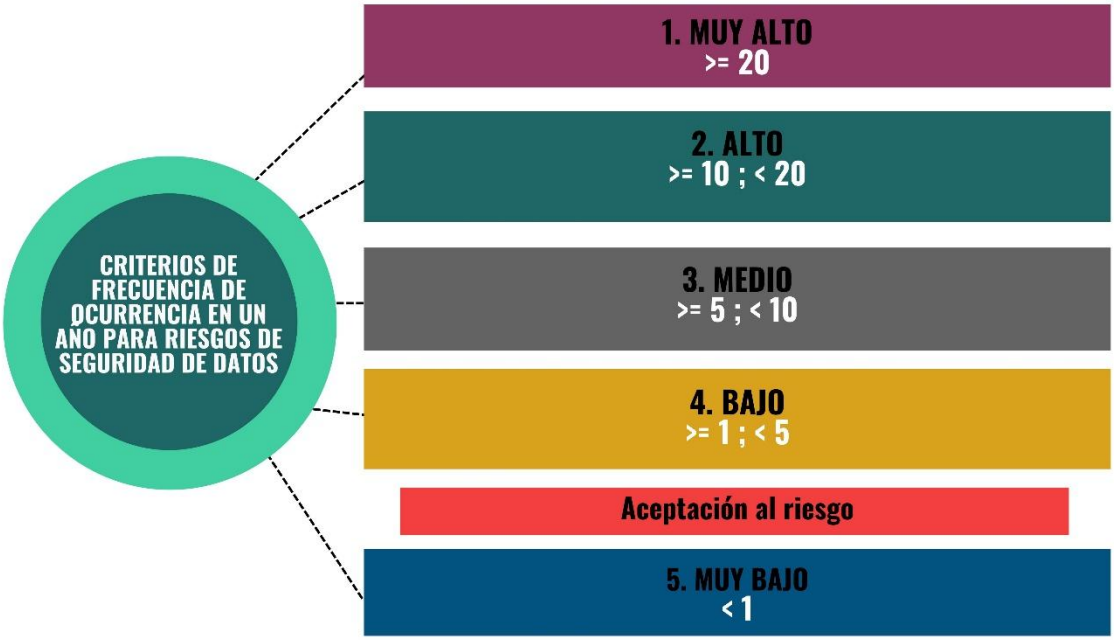
CRITERIOS DE EVALUACIÓN DE RIESGOS (IMPACTO)



CRITERIOS DE EVALUACIÓN DE RIESGOS (PROBABILIDAD DE OCURRENCIA EN RIESGOS PRIMORDIALMENTE DE CUMPLIMIENTO JURÍDICO)



CRITERIOS DE EVALUACIÓN DE RIESGOS (FRECUENCIA DE OCURRENCIA EN RIESGOS DE SEGURIDAD DE DATOS)



EVALUACIÓN CUANTITATIVA DE RIESGOS

Riesgos jurídicos por vulneración de derechos y libertades de los titulares de datos

ARTÍCULO	PROBABILIDAD DE OCURRENCIA	IMPACTO TITULARES PROMEDIO	IMPACTO GRUPOS MÁS VULNERABLES
Art. 7. Tratamiento legítimo de datos personales	Mínimo: 0.01 **Más probable: 0.04** Máximo: 0.09	Mínimo: $5 000 **Más probable: $14 000** Máximo: $22 000	Mínimo: $20 000 **Más probable: $30 000** Máximo: $50 000
Art. 10(c). Transparencia	Mínimo: 0.02 **Más probable: 0.06** Máximo: 0.2	Mínimo: $32 000 **Más probable: $60 000** Máximo: $90 000	Mínimo: $90 000 **Más probable: $110 000** Máximo: $180 000
Art. 10(d). Finalidad	Mínimo: 0.005 **Más probable: 0.03** Máximo: 0.08	Mínimo: $1 000 **Más probable: $7 000** Máximo: $12 000	Mínimo: $5 000 **Más probable: $12 000** Máximo: $19 000
Art. 10(e). Pertinencia y minimización de datos personales	Mínimo: 0.1 **Más probable: 0.22** Máximo: 0.3	Mínimo: $8 000 **Más probable: $13 000** Máximo: $18 000	Mínimo: $16 000 **Más probable: $34 000** Máximo: $60 000
Art. 10(i). Conservación	Mínimo: 0.35 **Más probable: 0.6** Máximo: 0.85	Mínimo: $8000 **Más probable: $15 000** Máximo: $22 000	Mínimo: $17 000 **Más probable: $34 000** Máximo: $42 000
Art. 12. Derecho a la información	Mínimo: 0.2 **Más probable: 0.7** Máximo: 1	Mínimo: $18 000 **Más probable: $40 000** Máximo: $80 000	Mínimo: $70 000 **Más probable: $105 000** Máximo: $150 000
Art. 13. Derecho de acceso	Mínimo: 0.02 **Más probable: 0.07** Máximo: 0.1	Mínimo: $4 000 **Más probable: $8 000** Máximo: $12 000	Mínimo: $7 000 **Más probable: $12 000** Máximo: $19 000
Art. 14. Derecho de rectificación y actualización	Mínimo: 0 **Más probable: 0.001** Máximo: 0.005	Mínimo: $100 **Más probable: $500** Máximo: $800	Mínimo: $1 000 **Más probable: $2 000** Máximo: $4 000
Art. 15. Derecho de eliminación	Mínimo: 0.05 **Más probable: 0.2** Máximo: 0.35	Mínimo: $25 000 **Más probable: $50 000** Máximo: $80 000	Mínimo: $80 000 **Más probable: $120 000** Máximo: $180 000
Art. 16. Derecho de oposición	Mínimo: 0.05 **Más probable: 0.08** Máximo: 1.2	Mínimo: $10 000 **Más probable: $15 000** Máximo: $25 000	Mínimo: $20 000 **Más probable: $30 000** Máximo: $50 000
Art. 17. Derecho a la portabilidad	Mínimo: 0 **Más probable: 0.005** Máximo: 0.008	Mínimo: $50 **Más probable: $200** Máximo: $400	Mínimo: $800 **Más probable: $2 000** Máximo: $4 000
Art. 20. Derecho a no ser	Mínimo: 0.001	Mínimo: $18 000	Mínimo: $80 000

objeto de una decisión basada única o parcialmente en valoraciones automatizadas	**Más probable: 0.004** Máximo: 0.1	**Más probable: $35 000** Máximo: $50 000	**Más probable: $180 000** Máximo: $300 000
Art. 55. Transferencia o comunicación internacional de datos personales	Mínimo: 0.01 **Más probable: 0.04** Máximo: 0.09	Mínimo: $12 000 **Más probable: $18 000** Máximo: $30 000	Mínimo: $25 000 **Más probable: $50 000** Máximo: $80 000

Riesgos operacionales de seguridad de datos personales (Confidencialidad)

ARTÍCULO	FRECUENCIA ANUAL	IMPACTO TITULARES PROMEDIO	IMPACTO GRUPOS MÁS VULNERABLES
Art. 37. Seguridad de datos personales	Mínimo: 1 **Más probable: 6** Máximo: 11	Mínimo: $50 000 **Más probable: $95 000** Máximo: $150 000	Mínimo: $120 000 **Más probable: $200 000** Máximo: $280 000

Riesgos operacionales de seguridad de datos personales (Integridad)

ARTÍCULO	FRECUENCIA ANUAL	IMPACTO TITULARES PROMEDIO	IMPACTO GRUPOS MÁS VULNERABLES
Art. 37, art. 10 (j). Seguridad de datos personales	Mínimo: 0 **Más probable: 2** Máximo: 5	Mínimo: $4 000 **Más probable: $10 000** Máximo: $16 000	Mínimo: $18 000 **Más probable: $40 000** Máximo: $70 000

Riesgos operacionales de seguridad de datos personales (Disponibilidad)

ARTÍCULO	FRECUENCIA ANUAL	IMPACTO TITULARES PROMEDIO	IMPACTO GRUPOS MÁS VULNERABLES
Art. 37, art. 10 (j). Seguridad de datos personales	Mínimo: 2 **Más probable: 8** Máximo: 13	Mínimo: $6 000 **Más probable: $15 000** Máximo: $30 000	Mínimo: $25 000 **Más probable: $60 000** Máximo: $100 000

De igual manera, se procede a priorizar los riesgos en donde el nivel informativo del impacto ayudará a una inversión más informada en medidas de seguridad que se consideren necesarias. En conclusión, se recomienda a los responsables y encargados del tratamiento escoger la metodología de evaluación de riesgos que consideren más adecuada, adaptable, implementable; y, que cuenten con el conocimiento necesario, siempre y cuando cumplan con los principios fundamentales establecidos en esta guía.

Es común que bancos, seguros y empresas de seguridad de la información estén mucho más familiarizados con el análisis y la evaluación cuantitativa de riesgos, dado que realizan tratamiento de datos personales a gran escala y estimar el retorno a la inversión es prioritario. En cambio, es común que PYMES o estudios jurídicos estén más familiarizados con el análisis y evaluación cualitativa de riesgos. El ANEXO contiene un tutorial práctico de evaluación de impacto del tratamiento de datos personales, con una metodología híbrida: cualitativa para riesgos de cumplimiento primordialmente jurídico y cuantitativa para riesgos operacionales como los de seguridad de la información.

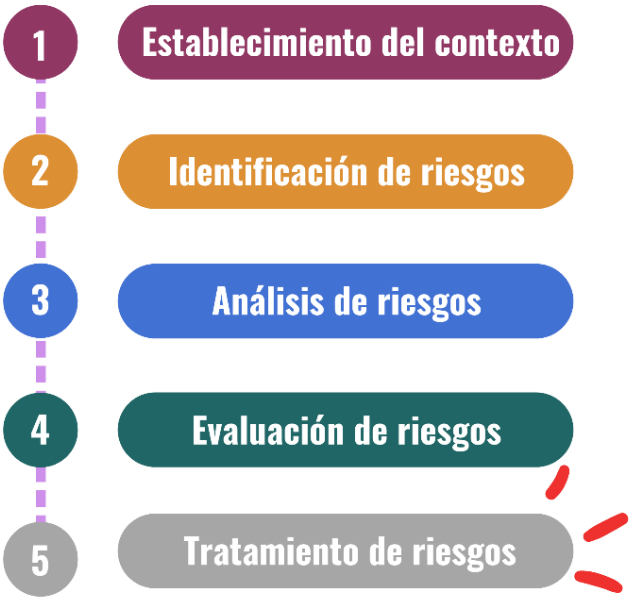
4.4. Integración de resultados. Se recomienda que los resultados de la evaluación de impacto sean integrados de manera omnipresente en la gestión de riesgos jurídicos, operacionales y financieros de los responsables y encargados del tratamiento. Esto con el fin de cumplir de manera efectiva con el principio de protección de datos desde el diseño y por defecto; y, la reducción de riesgos para la protección de derechos y libertades en todos los procesos organizacionales.

4.5. Integración en una evaluación holística de riesgos. Con el objeto de realizar una mejor inversión en medidas de seguridad de protección de datos personales, la evaluación de impacto realizada desde un enfoque de protección de los derechos y libertades de los titulares debe ser integrada en la práctica con la evaluación de riesgos de seguridad de la información. Esto por cuanto los riesgos de seguridad de la información y los riesgos jurídicos de conformidad a la LOPDP son interdependientes.

5. Tratamiento de riesgos de protección de datos personales

Esta quinta etapa consiste en seleccionar e implementar las medidas de seguridad jurídicas, organizacionales y técnicas, con el fin de mitigar los riesgos evaluados en la etapa de evaluación de riesgos. Las medidas de control de riesgos deben manejarse bajo una lógica de medidas de prevención, de identificación y de respuesta a los riesgos evaluados. La inversión en medidas de seguridad debe ser eficiente y eficaz, desde una lógica de conformidad en riesgos.

5.1. Etapas previas. El tratamiento de riesgos debe considerarse como la etapa en donde los responsables y encargados del tratamiento toman las decisiones para invertir en medidas de seguridad para la protección de los derechos y libertades de los titulares de los datos. Para tomar decisiones informadas es fundamental haber seguido las cuatro etapas anteriores de la gestión de riesgos. Esto permitirá que los responsables y encargados del tratamiento puedan destinar recursos de manera informada, priorizando los escenarios de alto riesgo contra los derechos y libertades de los titulares de los datos.



5.2. Taxonomías de controles de riesgos. Un buen comienzo es utilizar taxonomías de controles de riesgos (como los estándares ISO/IEC 27001-27002-27701, CIS Controls, etc.)[23], en donde las medidas de control se entregan en una declaración de aplicabilidad[24], que contiene el control de seguridad, su aplicabilidad, su descripción, su justificación, su documentación y la delegación del responsable del control. Es importante considerar que las guías de controles de riesgos son recomendaciones que deben ser adaptadas a las necesidades específicas de mitigación de riesgos surgidas en las etapas anteriores de la gestión de riesgos; y, no únicamente, como catálogos genéricos. Para la conformidad a la LOPDP se recomienda

[23] Por ejemplo, el anexo A del estándar ISO/IEC 27001:2022 contiene una lista exhaustiva de controles de riesgos de seguridad de la información.
[24] Ver ISO/IEC 27001:2022, cláusula 6.1.3(d).

utilizar la cláusula del estándar pertinente (por ejemplo: ISO/IEC 27701) y la norma jurídica de la LOPDP a la que se relaciona.

Declaración de aplicabilidad en conformidad con la norma ISO/IEC 27701:2025

CONTROL	APLICABILIDAD	DESCRIPCIÓN	JUSTIFICACIÓN	RESPONSABLE
B.1.2.4 Determinar cuándo y cómo se obtiene el consentimiento del titular. - (Art. 8 LOPDP)	Si	Consiste en utilizar el consentimiento como base legal para el tratamiento legítimo de datos personales conforme al artículo 8 de la LOPDP.	Es necesario definir las condiciones de obtención del consentimiento en la política de protección de datos.	Director jurídico
B.1.2.5 Mecanismo de obtención del consentimiento del titular. - (Art. 8 LOPDP)	Si	Consiste en los mecanismos para obtener el consentimiento de los titulares de los datos.	Es necesario implementar los mecanismos digitales para obtenerlo de manera remota vía aplicaciones web y vía aplicaciones de chat.	Director de Tecnologías de la Información
B.1.2.6 Evaluación de impacto del tratamiento de datos personales - (Art. 42 LOPDP)	Si	Consiste en la obligación de responsables del tratamiento de realizar evaluaciones de impacto del tratamiento de datos personales.	Sí es necesario por cuanto el responsable del tratamiento procesa datos personales a gran escala.	Responsable del tratamiento delega a las áreas concernidas. Revisión y retroalimentación obligatoria del Delegado de Protección de Datos Personales.
B.1.2.7 Uso de criptografía - (Art. 37 LOPDP)	Si	Consiste en implementar controles criptográficos para proteger datos personales.	Es necesario por cuanto la LOPDP establece la obligación de implementar medidas de seguridad a responsables y encargados del tratamiento.	Oficial de Seguridad de la Información.
		[…]		

En el ejemplo anterior se presenta un extracto de lo que sería una declaración de aplicabilidad de protección de datos personales. En el caso de que ya exista una declaración de

aplicabilidad de seguridad de la información en conformidad con otro estándar (como el ISO/IEC 27001), los controles pueden ser copiados a la declaración de aplicabilidad de datos personales y también se pueden agregar anexos o utilizar referencia con el objeto de no repetirlos. Algo importante a considerar es que no toda organización tendrá departamentos jurídicos, de seguridad de la información o de gobernanza de datos. En instituciones pequeñas es común que se presenten conflictos de roles; por ello, la recomendación general es que siempre debe ponderarse a favor de la protección de derechos y libertades de los titulares.

5.3. Retorno a la inversión en seguridad de datos personales. Las medidas de seguridad organizacionales y técnicas deben considerarse como inversión y no como gasto[25]. Es recomendable adoptar una lógica de Retorno a la Inversión en Seguridad de datos personales, para poder evaluar la eficiencia, eficacia y rentabilidad de las medidas de seguridad implementadas. Además, es útil evaluar cómo varios controles interactúan entre sí para mitigar un riesgo. El siguiente ejemplo muestra el Retorno a la inversión en seguridad de dos controles de riesgos:

Formula ROSI: (Reducción de pérdida – Costo de la solución) / (Costo de la solución)

Valor al Riesgo de Datos Personales (Pd-Var) = $260 000 Expectativa de eficacia = 50% Costo de la medida de seguridad = $100 000 ROSI (PdVar) = (Reducción de pérdida – Costo de la solución) / (Costo de la solución) ROSI (PdVar) = (130 000 – 100 000) / (100 000) ROSI (PdVar) = 0.3 = 30%

El resultado refleja un retorno a la inversión del 30%. Cabe agregar que es conveniente implementar modelos estadísticos y probabilísticos de aprendizaje automático (como *Linear Regression, Random Forest*, etc.) para tener una mejor visión del rendimiento de las medidas de seguridad en conjunto.

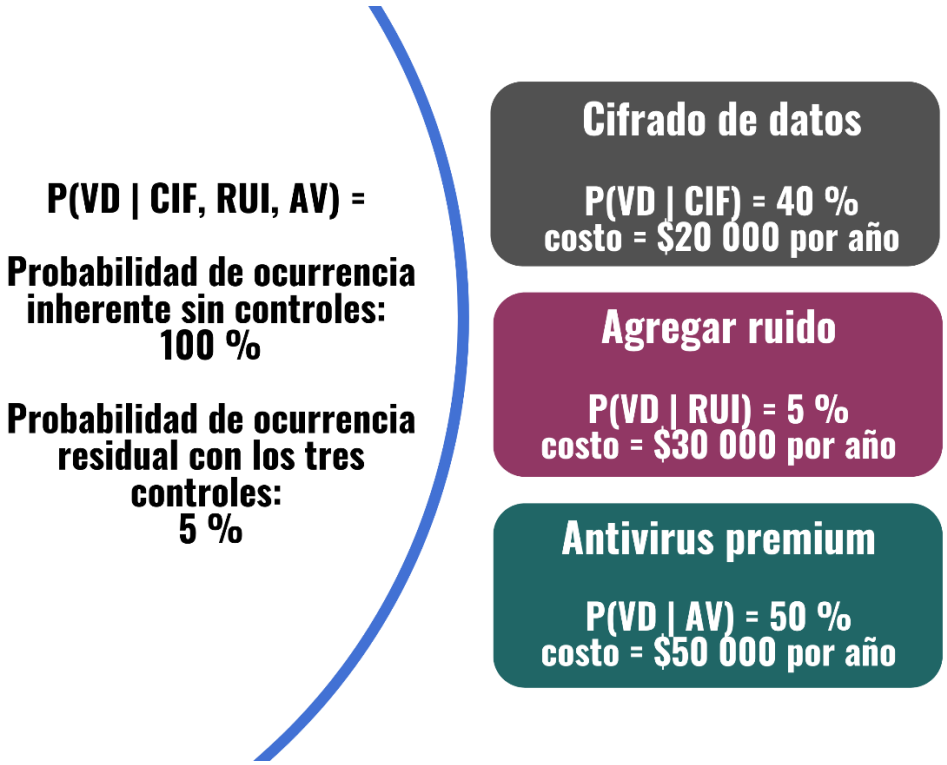
5.4. Interdependencias de controles. Las medidas de control de riesgos son interdependientes. Las medidas de seguridad jurídicas, organizacionales y técnicas no son un catálogo, pues dependen del contexto específico de cada escenario de riesgo. Estas medidas usualmente son interdependientes y es muy recomendable analizar el grado de protección que ofrece cada una de ellas. Gracias a estos análisis de interdependencias, es posible identificar los riesgos que requieren mayor inversión e identificar áreas de riesgos en las que se está invirtiendo un exceso de dinero.

Para escoger las medidas adecuadas se pueden utilizar diferentes estrategias. Una eminentemente cualitativa es confiar en los expertos (jurídicos o en seguridad de la información) para que seleccionen las mejores medidas de seguridad de acuerdo con su criterio y experiencia. Sin embargo, hay que considerar que, en la práctica, las medidas de seguridad deben ser eficaces, eficientes, pero también rentables. La justificación es simple, pues en un escenario real siempre habrá un presupuesto limitado. Por ello, se recomienda utilizar los métodos de calibración de expertos anteriormente explicados para el análisis de

[25] Ver https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment.

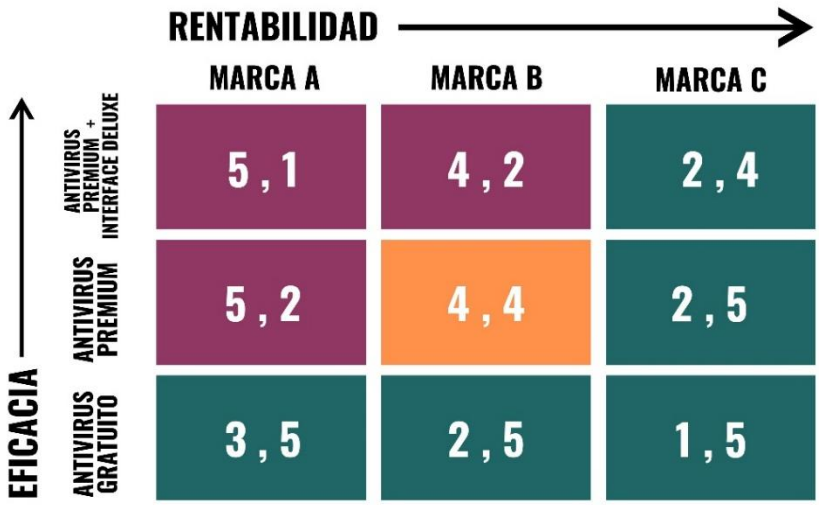
riesgos y también para el tratamiento de riesgos. No obstante, con el fin de analizar las interdependencias entre las medidas de seguridad, pueden utilizarse varios métodos cuantitativos y cualitativos para justificar los valores de entrada con los siguientes métodos. La finalidad es ayudar al experto en su toma de decisiones:

a) Utilizar el teorema de Bayes. Se puede utilizar probabilística condicional para plantear un escenario de riesgo protegido por varios controles de riesgos y calibrar el nivel de protección que cada una aporta.



En el ejemplo anterior, las medidas de seguridad más efectivas, eficaces y rentables son el Antivirus Premium y el Cifrado. Los valores de entrada pueden ser cuantitativos (como por ejemplo utilizando el ROSI) o cualitativos (utilizando las opiniones de uno o varios expertos).

b) Utilizar el equilibrio de Nash. Muy utilizado en teoría de juegos. Puede ser útil para encontrar el balance ideal entre dos principios adversarios. Se pueden construir matrices de riesgos para implementar de manera simple el equilibrio de Nash. Por ejemplo, consideremos un antivirus como control de riesgos, en el cual se pueden confrontar el principio de eficacia, con el principio de rentabilidad. Es necesario implementar un antivirus eficaz, pero con una limitación de presupuesto, pues hay muchas más medidas de seguridad de datos que implementar. Podemos utilizar una escala del 1 al 5 para calificar la eficacia y la rentabilidad de las tres marcas de antivirus ofrecidas por el proveedor. En el eje de la eficacia están tres opciones: antivirus gratuito, antivirus premium; y, el mismo antivirus premium con *interface de luxe*, en donde ambas opciones de antivirus premium ofrecen el nivel de eficacia requerido. En el eje de la rentabilidad, las opciones son: marca A, marca B, y marca C; en donde la marca más costosa es la marca A y la más barata, la marca C. La matriz nos ayudará a calificarlos en los dos criterios planteados para buscar la mejor opción:



5.5. Calificadores frágiles e inestables. Se recomienda evitar condiciones frágiles como cuando existe una sola medida de seguridad para un escenario de riesgo. También se recomienda evitar condiciones inestables en el caso de asumir que no se necesita una medida de seguridad para un escenario de riesgo, pero es probable que las situaciones cambien súbitamente. Se recomienda identificar condiciones frágiles y/o condiciones inestables para implementar en ellas al menos dos medidas de control de riesgos.

5.6. Modelos de tratamiento de riesgos[26]. Es recomendable utilizar modelos que permitan mapear las medidas de control de riesgos en cuanto a prevención, detección y respuesta. Los controles de prevención ayudarán a mitigar la probabilidad de ocurrencia del riesgo. Los controles de identificación contribuirán a monitorear e identificar los riesgos en tiempo real cuando un ataque está sucediendo; y, ayudarán a mitigar la probabilidad o frecuencia de ocurrencia y el nivel del impacto. Los controles responsivos, en cambio, servirán para mitigar el impacto una vez que se ha materializado el riesgo. Se recomienda utilizar el modelo FAIR-CAM para ello:

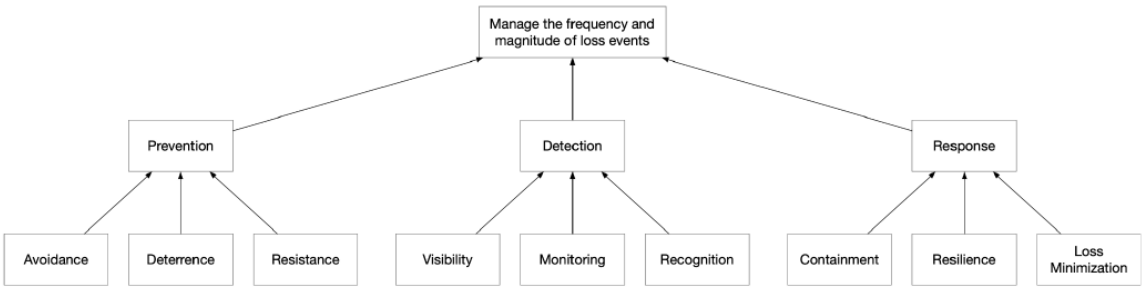


Gráfico tomado de: FAIR Institute (2025), An Overview of FAIR_CAM, Loss Event Control Functions, FAIR Institute, p.7.

La efectividad de las medidas de seguridad implementadas debe ser constantemente analizada y evaluada. Es pertinente restringir los cambios a un control de riesgos que está funcionando bien. También es importante identificar cuando estos ya no son efectivos. Una

[26] Para mayor información sobre el modelo FAIR-CAM, se recomienda la siguiente guía: Jones J. (2021), A Description of the FAIR Controls Analytics Model (FAIR-CAM) Standard, FAIR Institute.

medida de seguridad puede volverse ineficiente con el tiempo. Por ejemplo, un algoritmo de cifrado puede ser seguro hoy, pero volverse vulnerable en un año.

Siguiendo la lógica de la conformidad en riesgos a la LOPDP, no se trata de implementar medidas de seguridad como una lista de chequeo, sino que lo importante es evaluar su efectividad en los contextos específicos del tratamiento de datos personales. Un modelo recomendable es el FAIR-CAM en *Variance Management Domain*.

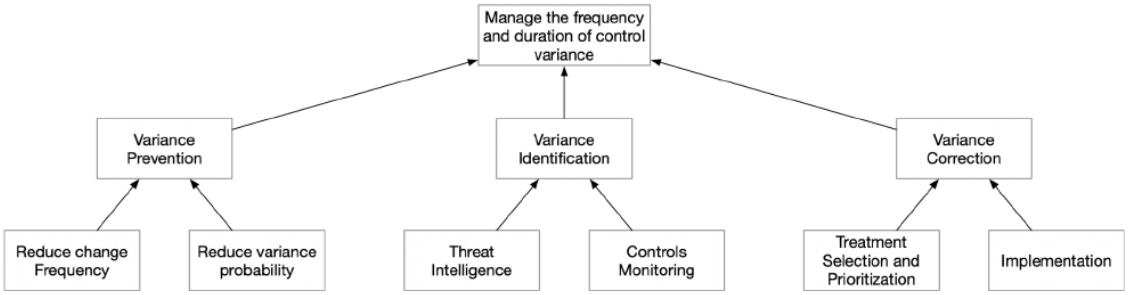


Gráfico tomado de: FAIR Institute (2025), An Overview of FAIR_CAM, Variance Management Control Functions, FAIR Institute, p.9.

5.8. Modelos de toma de decisiones. Es recomendable implementar también modelos de control de riesgos a nivel estratégico. Esto responde a que muchas veces las vulnerabilidades organizacionales y técnicas son el resultado de malas decisiones tomadas por la gerencia de una empresa o por los cargos superiores de una institución pública. Los responsables del tratamiento y encargados están obligados a alinear a la protección de datos personales como un objetivo principal de la institución. De esta manera, puede ser muy útil aplicar un método de identificación de decisiones no alineadas con el objetivo de protección de datos personales.

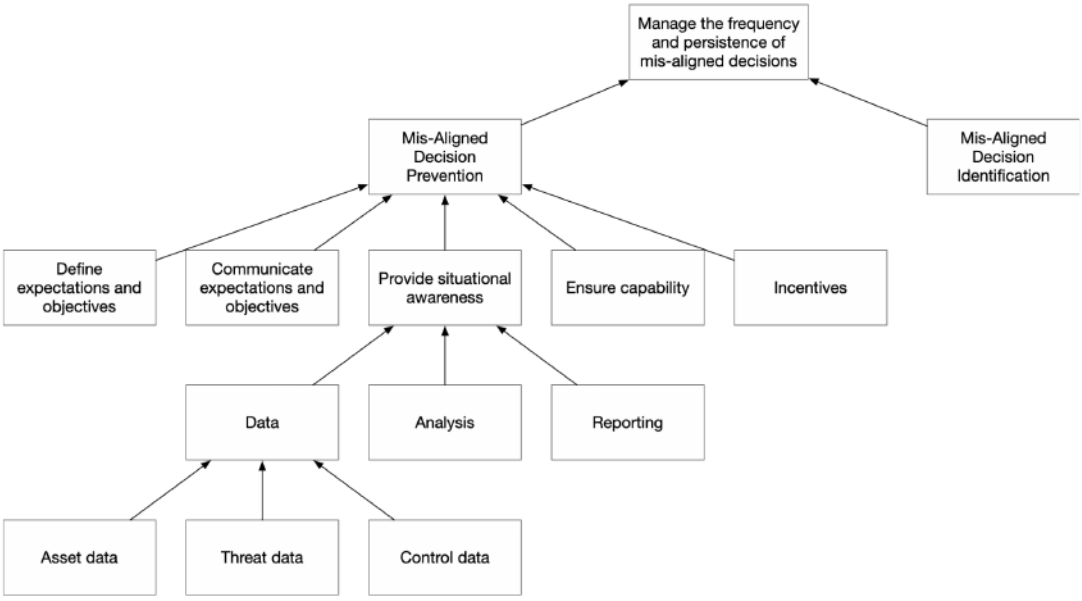


Gráfico tomado de: FAIR Institute (2025), An Overview of FAIR_CAM, Decision Support Control Functions, FAIR Institute, p.10.

5.9. Estrategias. Las cuatro estrategias generales para el tratamiento del riesgo son: aceptar el riesgo, modificar el riesgo, transferir el riesgo y evitar el riesgo. Por ejemplo, pensemos en un escenario de riesgo de vulneración a la confidencialidad de datos personales:

Escenario de riesgo: Vulneración de datos personales sensibles (confidencialidad) en un hospital, desde una perspectiva del impacto en los titulares de los datos.

Comunidad de amenaza: Cibercriminales

Perfil de la amenaza: Motivado para vender datos a empresas de recursos humanos y seguros.

Vector de ataque: Ingeniería social y ataque de Malware (troyano).

Vulnerabilidades organizacionales: Falta de capacitación a los empleados. La vulnerabilidad del responsable del tratamiento se convierte en una vulnerabilidad del titular de los datos.

Vulnerabilidad técnica: Ausencia de antivirus eficaz.

Impacto primario: La vulneración de la seguridad de datos personales viola el derecho de protección de datos personales del titular de los datos.

Impacto secundario: La violación de los datos personales del titular también afecta su derecho al trabajo, por cuanto su empleador se entera de que tiene una enfermedad grave.

En este contexto, la frecuencia de ocurrencia es igual a mínimo: 5, Más Probable: 10, Máximo: 20. El impacto es igual a Mínimo: $10 000, Más probable: $50 000, Máximo: $120 000. La aceptación de frecuencia de ocurrencia es 6 al año. La aceptación del impacto es $12 000.

A continuación, una descripción de como operarían las cuatro estrategias:

a) Aceptar el riesgo. Quiere decir que es un riesgo tolerable para el responsable del tratamiento, pues su criterio de aceptación de la frecuencia de ocurrencia podría ser de 6; y, su criterio de aceptación para el impacto podría ser de $12 000. Sin embargo, esto funciona

así desde la lógica del riesgo de conformidad con la LOPDP y desde una perspectiva del responsable del tratamiento. Hay que recordar que, desde la perspectiva de la protección de los derechos y libertades de los titulares de los datos, un derecho se cumple al cien por ciento.

b) Modificar el riesgo. Consiste en implementar medidas de seguridad jurídicas, organizacionales o técnicas con el fin de reducir el nivel del riesgo. Esta es la estrategia que debe ser prioritaria para la protección de derechos y libertades; es decir, intentar reducir todo riesgo al mínimo posible, para a la vez, reducir al máximo posible el riesgo de recibir una sanción administrativa. En el caso planteado, los criterios de evaluación de frecuencia de ocurrencia podrían estar en una frecuencia de 12 por año, con lo cual habría que reducir la frecuencia de 6 por año. Igualmente, el criterio de aceptación del riesgo podría estar establecido en $12 000, con lo cual habrá que reducir el impacto inherente de $50 000.

c) Transferir el riesgo. Consiste en reducir la frecuencia de ocurrencia o el impacto al delegar una responsabilidad a un tercero. En el ejemplo planteado, podría transferirse el riesgo de frecuencia de ocurrencia al utilizar interfaces de otras empresas para el proceso de autenticación de credenciales. Asimismo, podría transferirse el impacto al contratar una póliza de seguros que pueda cubrir la mayor parte del impacto.

d) Evitar el riesgo. Consiste en decidir no tomar el riesgo; y, por ende, no realizar el tratamiento de datos bajo determinadas circunstancias. En el ejemplo planteado, se podría evitar la materialización del riesgo, evitando recolectar ciertos datos personales; como, por ejemplo, datos biométricos. Por supuesto, esta no es una estrategia realista en muchos casos, pues se necesita utilizar datos personales para cumplir con los fines de la institución, sea pública o privada.

ANEXO

Ejemplo práctico de una evaluación de impacto del tratamiento de datos personales

El siguiente tutorial ficticio tiene la finalidad de mostrar una manera de realizar una evaluación de impacto del tratamiento de datos personales, cumpliendo los principios establecidos en el Capítulo I de esta guía. Para hacerlo simple, se ha elaborado un cuestionario, el cual a la vez está asociado a uno o varios artículos de la LOPDP.

Se mostrarán métricas cuantitativas y criterios cualitativos para sustentar los *rationales* de cada respuesta, de acuerdo con los escenarios de riesgo planteados. No obstante, no se incluye la documentación de sustento de cada *rationale* por cuestiones de espacio. Todo responsable del tratamiento tendrá que agregarlos de acuerdo con sus propios procedimientos de calibración del riesgo. Los *rationales* pueden provenir de herramientas automatizadas de manejo de riesgos de terceros, perfilamiento de amenazas, escaneos de vulnerabilidades y herramientas afines, en idioma español o en inglés. Los responsables del tratamiento pueden aplicar cualquier método mostrado en el capítulo II de esta guía u otros métodos, siempre y cuando se cumpla con los principios y conceptos fundamentales establecidos en el capítulo I. Además, los responsables del tratamiento pueden elaborar las preguntas que consideren necesarias para sus propios escenarios de riesgo; o no utilizar un cuestionario de referencia, sino simplemente poner los niveles de impacto y una explicación del *rationale* correspondiente.

En primer lugar, se muestran mecanismos para el establecimiento del contexto. En segundo lugar, se incluyen la identificación, análisis, evaluación y tratamiento de riesgos en cada escenario de riesgo planteado para facilitar su comprensión. La información de los *rationales* está resumida, pero puede estar referenciada a los anexos que el lector considere necesarios, adjuntos a la evaluación de impacto del tratamiento de datos personales. Cabe recordar que se incluyen las otras etapas de la gestión de riesgos a la etapa de la evaluación, por cuanto no es posible evaluar un riesgo sin haber establecido el contexto, sin haberlo identificado y sin haberlo analizado.

Esta evaluación de impacto es para la protección de derechos y libertades de los titulares, en donde la protección de derechos es al cien por ciento. Es por ello, que en la evaluación de impacto no necesariamente se incluye sólo el impacto inherente del riesgo en caso de materializarse, pues es muy informativo incluir la probabilidad o frecuencia de ocurrencia para poder estimar los niveles de riesgo inherente. No obstante, desde un punto de vista pragmático, los responsables del tratamiento pueden integrar los resultados del análisis y evaluación de impacto para la protección de derechos y libertades, con la gestión de riesgos de seguridad de la información o la gestión de riesgos financieros. Para el análisis y evaluación se puede utilizar el modelo FAIR u otro que les permita gestionar los riesgos de manera holística e interdisciplinaria. Será mostrado un ejemplo de esta integración en lo que concierne a los riesgos de seguridad, utilizando una lógica de valor al riesgo de datos personales.

Finalmente, hay que tomar en cuenta que la LOPDP dispone en su artículo 42, la evaluación de impacto para los responsables del tratamiento. No obstante, la LOPDP en su artículo 37

dispone la obligación de responsables y encargados del tratamiento para implementar medidas de seguridad en el tratamiento de datos; y, el artículo 40, la obligación de realizar análisis de riesgos, amenazas y vulnerabilidades. Si bien esta guía no aborda los criterios obligatorios para realizar una evaluación de impacto, los regulados deben considerar que el hecho de no hacer una evaluación de impacto no los exime de ser sancionados. Como hemos visto a lo largo de esta guía, no se deben saltar las etapas anteriores de una gestión de riesgos, tanto para la evaluación de impacto, como para el tratamiento de riesgos. Por ello, si bien el encargado del tratamiento no está obligado a realizar una evaluación de impacto del tratamiento de datos, se recomienda que lo haga a nivel interno de la organización para poder tomar decisiones informadas acerca de las medidas de seguridad jurídicas, organizacionales y técnicas a ser implementadas.

RESPONSABLE DEL TRATAMIENTO: MalaKompra S.A.

---

1. ESTABLECIMIENTO DEL CONTEXTO

Primero, establecemos la información sobre el tratamiento de datos personales y elaboramos los criterios de evaluación de riesgos. En el presente ejemplo, se utilizará una metodología de análisis y evaluación cualitativa para los riesgos primordialmente jurídicos de cumplimiento a la LOPDP; y, cuantitativa para el análisis y evaluación de riesgos de seguridad de datos.

1.1. Información sobre el responsable del tratamiento

¿Cuál (o cuáles) es el responsable del tratamiento?

- MalaKompra S.A.

¿Cuál (o cuáles) son los encargados del tratamiento?

- DataCuy Ltd. Servicios de marketing digital. Empresa Ecuatoriana.
- BestKloud: Servicios de nube Infrastructure as a Service (IaaS) en la nube. Empresa Estadounidense registrada en el Estado de California.

¿Cuál es el aproximado de titulares de datos personales (clientes)?

- Entre 5 000 y 8 000.
- Rationale: Promedio de clientes de los dos últimos años.

¿Cuál es el aproximado de empleados?

- Entre 300 y 400.
- Rationale: Promedio de empleados de los dos últimos años.

¿Cuáles son los límites territoriales del responsable del tratamiento?

El Ecuador. Matriz en Quito. Sucursales en Guayaquil y en Cuenca.

¿Cuáles son los límites organizacionales del responsable del tratamiento?
Gerencia, Dirección Jurídica, Dirección de Tecnologías de la Información, Dirección de Gobernanza de Datos, Dirección de Riesgos, Dirección de Recursos Humanos, Dirección Financiera, Dirección de Relaciones Públicas [...]

¿Cuáles son los límites de los sistemas de información del responsable del tratamiento?

- Intranet: 2 servidores, 60 computadoras de escritorio y treinta laptops con sistema Windows Server 2022.

- Externas: 8 Aplicaciones Web, 20 bases de datos y 2 servidor de correo electrónico en servicio IaaS (*Infrastructure as Service)* en BestKloud.

1.2. Información sobre el tratamiento de datos personales

¿Tiene un Delegado de Protección de Datos? En caso de respuesta afirmativa, ¿cuál es el nombre y apellido del DPD?

Sí lo tenemos. Ing. Juan Pérez.

¿Cuál (o cuáles) es el tratamiento (o los tratamientos) bajo consideración?

- Tratamiento de datos simples (biográficos y de contacto) para apertura de cuentas en nuestro portal web (nombre, apellido, edad, email, teléfono).

- Tratamiento de datos comportamentales para la autenticación y personalización de servicios (preferencias de cookies, preferencias de bienes y servicios, geolocalización).

- Tratamiento de datos financieros para realizar pagos (Números de tarjeta de crédito).

- Tratamiento de datos sensibles (relativos a la salud) a cambio de dinero y de descuentos en seguros de salud.

¿Cómo funciona el ciclo de vida de los datos personales?

- Recolección: A través de nuestro portal Web en la URL: https://malakompra.ec/signup; y, en persona en nuestros locales.

- Almacenamiento: Los datos están almacenados en la nube, en nuestra aplicación web hospedada en BestCloud (https://bestkloud.com); y, en nuestros *backups*, en discos duros externos.

- Eliminación: Los datos que genera el cliente son eliminados directamente al cerrar su cuenta. Los *backups* y datos/metadatos no generados por el cliente son eliminados tres meses después de haber cumplido con sus fines.

¿Qué estándares de mejores prácticas o modelos de riesgo son aplicables?

ISO/IEC 27701, DAMA-DMBOK, ISO/IEC 27001, ISO/IEC 27002, Modelo FAIR, Modelo FAIR-CAM, Modelo FAIR-TAM, OWASP ASVS, CoBiT 19, PCI-DSS, DoD 5220.22 [… los que sean útiles]

¿Qué tipos de datos personales son procesados?

- Datos simples: nombres, apellidos, correo electrónico, teléfono.
- Datos comportamentales: geolocalización, preferencias.
- Datos financieros: Números de tarjeta de crédito, cuentas de PayPal.
- Datos sensibles: Datos de la salud.

¿Existen grupos de titulares de datos especialmente vulnerables en el procesamiento de los datos?

Personas con discapacidad (5%), Tercera edad (20%).

¿Existen grupos de titulares de datos especialmente vulnerables como consecuencia del procesamiento de los datos?

Personas con enfermedades catastróficas (8%), Mujeres embarazadas (5%).

¿Cuáles son los activos de soporte de los datos?

Datos personales de clientes Bases de datos PostGreSQL Web Framework Ruby on Rails Servidor Web Nginx Sistema Operativo GNU/Linux distribución Ubuntu
Nodo en la nube en BestCloud

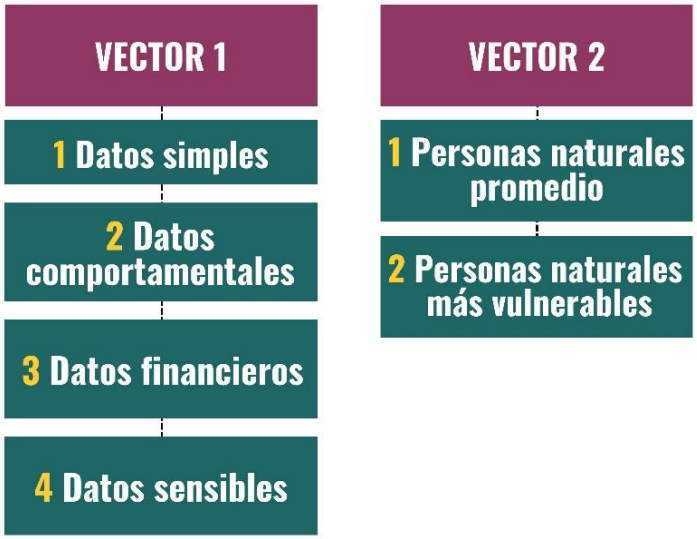
Datos personales de empleados Bases de datos Oracle Sistema Operativo Windows Server 2022 con .NET Framework (Intranet)
RAID 5

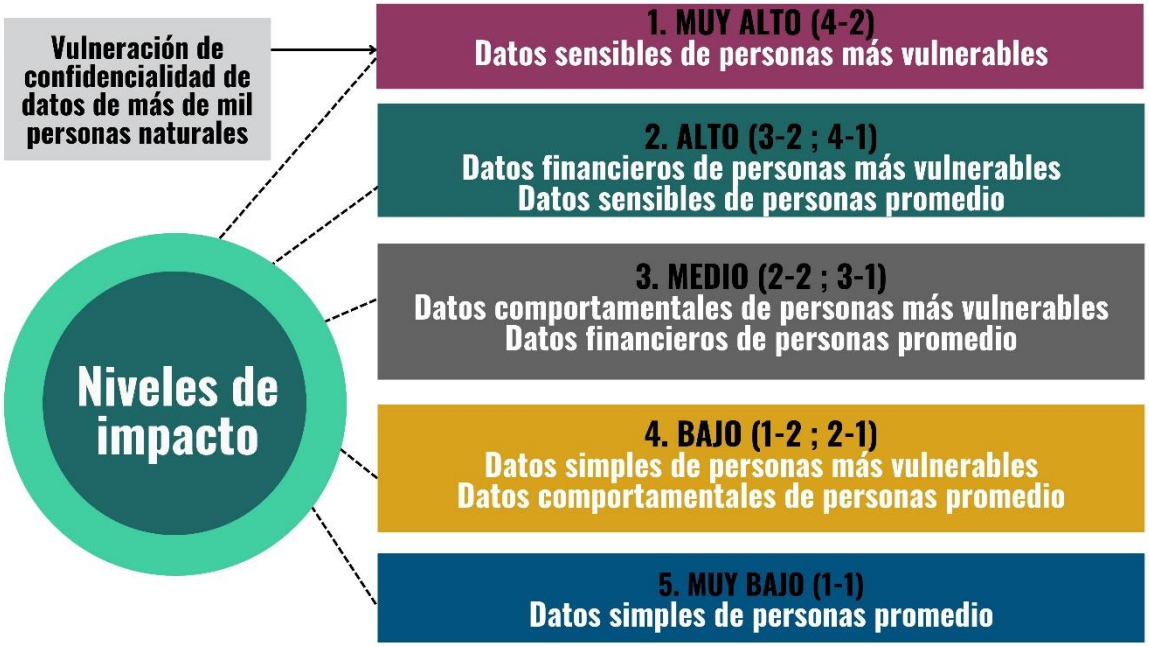
1.3. Criterios de evaluación de riesgos

¿Qué departamento o trabajador de la institución establece los criterios de evaluación de riesgos para la protección de derechos y libertades de los titulares?

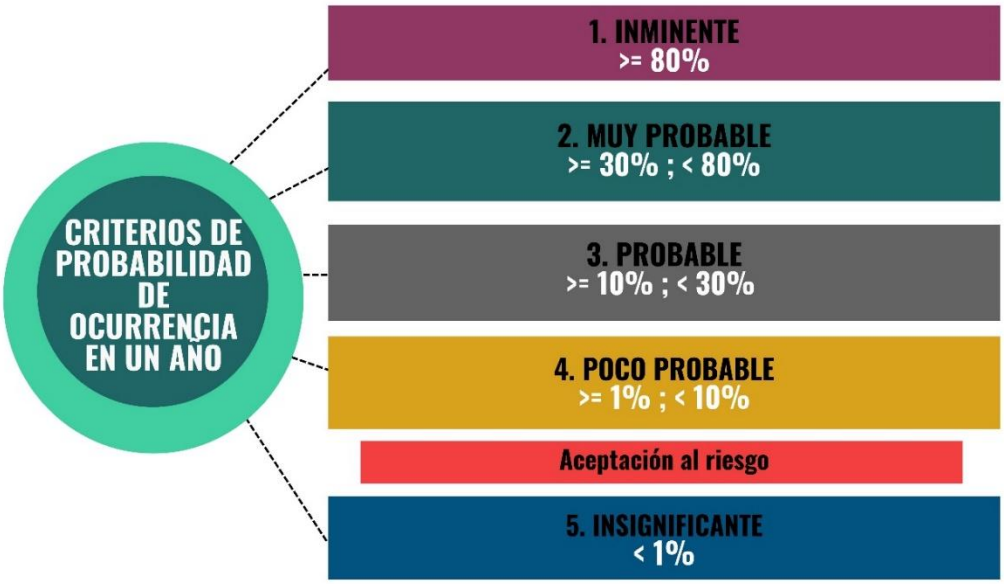
La Dirección de Gobernanza de datos y el rol responsable es el Delegado de Protección de Datos (DPD).

¿Cuáles son los criterios de evaluación del impacto para la protección de derechos y libertades de los titulares?





Opcional: Criterios de probabilidad de ocurrencia. (Hay que recordar que el cumplimiento de derechos se da al cien por ciento. Por ello, los criterios de evaluación de probabilidad de ocurrencia son únicamente informativos).

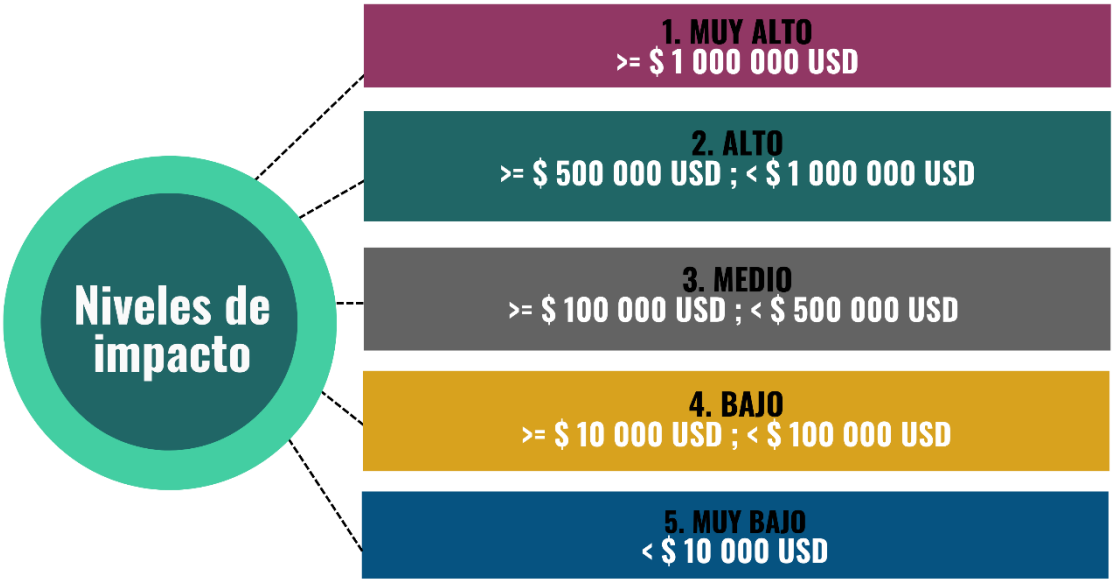


¿Qué departamento o trabajador de la institución establece los criterios de evaluación de riesgos de seguridad de la información?

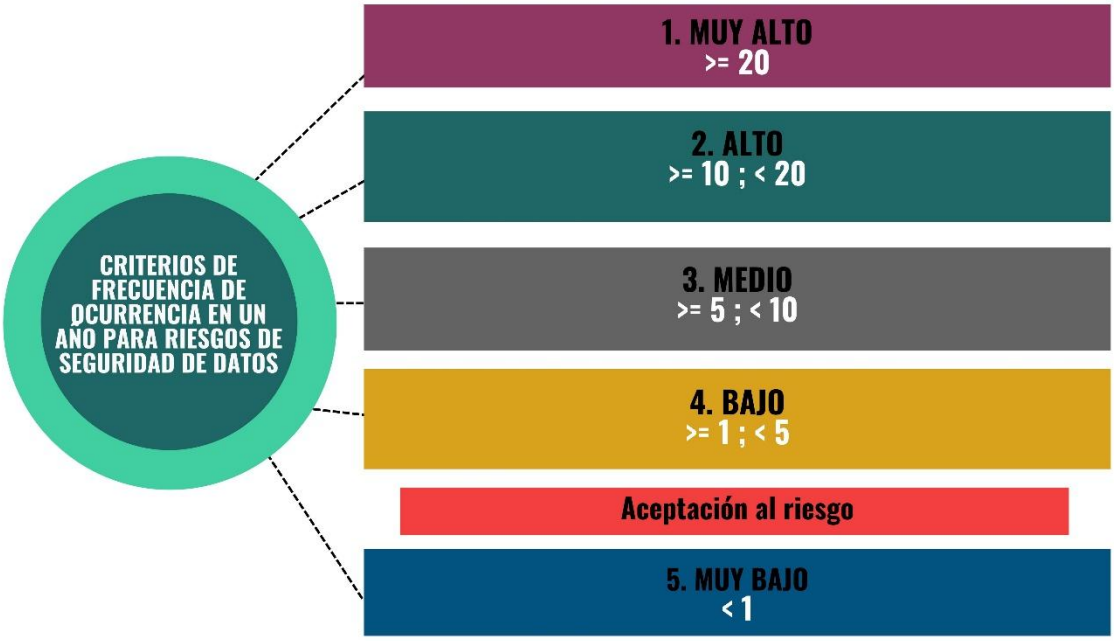
La Dirección de Seguridad de la Información y el rol responsable es el Director de Seguridad de la Información (CISO).

¿Cuáles son los criterios de evaluación de riesgos de seguridad de la información (incluye por cada incidente: pérdidas de productividad, pérdidas por respuesta a incidentes, pérdidas por reemplazo de activos, pérdidas de ventaja competitiva, pérdidas de reputación y pérdidas por sanciones administrativas / sentencias)?

Criterios de evaluación del impacto por todos los incidentes de seguridad:



Criterios de evaluación de frecuencia de ocurrencia:



2. ESCENARIOS DE RIESGOS JURÍDICOS DE CUMPLIMIENTO A LA LOPDP.

Para ejemplificar la gestión de riesgos de cumplimiento jurídico se han construido once escenarios vinculados a las obligaciones establecidas en la LOPDP. La finalidad es mostrar opciones acerca de cómo plantear los escenarios de riesgo jurídico en un formato. No obstante, los responsables del tratamiento deben incluir los escenarios de riesgo que

consideren necesarios de acuerdo con sus actividades de tratamiento de datos. No hay que olvidar que lo fundamental es sustentar cada estimación con su respectivo *rationale*, con el fin de evitar los análisis superficiales. La manera de lograrlo puede ser cuantitativa o cuantitativa, la que mejor se adapte de manera eficiente y eficaz a mitigar los riesgos contra los derechos y libertades de los titulares de los datos.

Es obligatorio incluir como anexos los documentos de respaldo en cuanto a las métricas y modelos de riesgo utilizados como *rationales* para justificar cualquier valor de entrada o criterio.

Los ejemplos de escenarios de riesgo no incluyen un registro general de evaluación del impacto o una declaración de aplicabilidad. Se recomienda agregar estos documentos siguiendo las directrices establecidas en esta guía. Es importante considerar que es necesario incluir un establecimiento del contexto, identificación de riesgos y análisis de riesgos como etapas previas para la evaluación de impacto. También es importante considerar que la evaluación de impacto está centrada únicamente en el impacto en los derechos y libertades de los titulares de los datos, por lo cual se recomienda mantener el valor del impacto por separado de la probabilidad o frecuencia de ocurrencia. En el caso de que se proceda a combinarlos o multiplicarlos por decisión del responsable del tratamiento, también es fundamental presentar los valores calibrados de probabilidad o frecuencia de ocurrencia y del impacto, por separado, en cada escenario de riesgo.

A continuación, se incluyen varios ejemplos de escenarios de riesgo en una evaluación de impacto que considera el impacto inherente y la probabilidad de ocurrencia inherente (riesgo inherente). Se recomienda agregar los niveles de impacto y probabilidad de ocurrencia residuales (riesgo residual), una vez que sean implementadas las medidas de seguridad jurídicas, organizacionales y técnicas recomendadas. Todos los escenarios de riesgo cuentan con una evaluación de impacto para titulares promedio y algunos de ellos con una evaluación de impacto para titulares de datos especialmente vulnerables.

2.1. Riesgo de que las finalidades del tratamiento no sean determinadas, explícitas, legítimas y comunicadas al titular

Concordancia: Art. 10 (d) LOPDP.

Identificación del riesgo

¿Son los propósitos del tratamiento especificados, explícitos y legítimos?

La mayoría de los propósitos son específicos, explícitos y legítimos. Sin embargo, la política de protección de datos no incluye la finalidad del tratamiento de utilizar los datos personales para campañas de marketing digital. Tampoco hace un análisis profundo del tratamiento de los datos de salud obtenidos a cambio de pagos en dinero y descuentos en seguros.

- Amenaza: Considerando que la amenaza es el responsable del tratamiento, la empresa MalaKompra S.A. puede vulnerar los derechos de los titulares de datos al no informarle sobre la finalidad del tratamiento de datos para campañas de marketing digital.

- Rationale: Se ha constatado en la auditoría jurídica que los datos personales son utilizados para esta finalidad (agregar respaldo en Anexo).

- Vulnerabilidad: El departamento jurídico de la empresa MalaKompra S.A no realiza los debidos controles de cada finalidad del tratamiento de manera periódica.

- Rationale: La política de protección de datos personales no incluye esta obligación (agregar respaldo en Anexo).

Análisis del riesgo

- Probabilidad de ocurrencia (informativo): Muy Probable (70%)

- Rationale: El equipo de auditoría utilizó el método Delphi para promediar las opiniones de cinco expertos jurídicos (agregar respaldo en Anexo).

- Impacto: El derecho a la información de los titulares de datos es vulnerado, pues ellos no conocen que sus datos serán utilizados en marketing digital. Esto puede producir vulneraciones de la confidencialidad de sus datos.

- Rationale: El equipo de auditoría determinó que los datos utilizados para campañas de marketing digital son datos simples, comportamentales y financieros de personas promedio. Sin embargo, vulnera los derechos de al menos 5 000 titulares de datos. (agregar respaldo en Anexo).

Evaluación del impacto

- Titulares promedio: Alto.

- Titulares especialmente vulnerables: Muy Alto.

Tratamiento del riesgo

Agregar esta finalidad del tratamiento a la política de protección de datos.

2.2. Riesgo de no cumplir con el tratamiento legítimo de datos personales

Concordancia: Art. 7 LOPDP.

Identificación del riesgo

¿Cuáles son las causales que hacen que el tratamiento sea legal?

La empresa MalaKompra S.A. justifica su base legal por el consentimiento obtenido de los titulares de datos y por su interés legítimo para utilizar los datos en campañas de marketing por cuanto es para el beneficio de sus clientes. No obstante, esta justificación no tiene proporcionalidad y por tanto puede vulnerar los derechos de los titulares de datos.

- Amenaza: Considerando que la amenaza es el responsable del tratamiento, la empresa MalaKompra S.A. puede vulnerar los derechos de los titulares de datos al adoptar una interpretación abusiva del interés legítimo.

- Rationale: El interés legítimo debe ser proporcional y de ninguna manera utilizarse como un mecanismo que sea manipulado para los intereses del responsable del tratamiento (agregar respaldo en Anexo).

- Vulnerabilidad: La empresa MalaKompra S.A. no cuenta con abogados especializados en protección de datos personales.

- Rationale: La auditoría informó que hay un bajo nivel de preparación del área jurídica del responsable del tratamiento en temas de protección de datos personales (agregar respaldo en Anexo).

Análisis del riesgo

- Probabilidad de ocurrencia (informativo): Inminente (90%).

- Rationale: El equipo de auditoría utilizó el modelo Delphi para promediar las opiniones de cinco expertos jurídicos (agregar respaldo en Anexo).

- Impacto: El derecho de confidencialidad de los titulares de datos es vulnerado, pues ellos no conocen que sus datos serán utilizados en marketing digital. Esto puede producir vulneraciones de la confidencialidad de sus datos.

- Rationale: El equipo de auditoría establece que no se puede realizar el tratamiento de datos personales sin una base legal que justifique el tratamiento. Utilizar sus datos para marketing digital equivale a vulnerar el derecho de protección de datos personales de todos los clientes (agregar respaldo en Anexo)

Evaluación del impacto

Muy Alto.

Tratamiento del riesgo

Eliminar el interés legítimo como base legal para realizar el tratamiento de datos con propósitos de marketing. En su lugar, incluir una forma específica en la aplicación web en la cual, inequívocamente, el titular de datos da el consentimiento para el tratamiento de sus datos con propósitos de marketing.

2.3. Riesgo no cumplir con las condiciones del consentimiento

Concordancia: Art. 8 LOPDP.

Identificación del riesgo

¿Cómo se obtiene el consentimiento de los interesados?

Se lo obtiene en la URL: https://malakompra.ec/signup y en persona en la matriz y sucursales de la empresa.

¿Es el consentimiento legítimo y lícito?

El consentimiento para el tratamiento de datos de la salud podría no cumplir con ser legítimo y lícito, por cuanto ofrecer dinero a cambio puede ser un mecanismo para aprovecharse de grupos vulnerables por condiciones de pobreza.

- Amenaza: Considerando que la amenaza es el responsable del tratamiento, la empresa MalaKompra S.A. puede vulnerar los derechos de los titulares de datos que entreguen sus datos de la salud.

- Rationale: La auditoría jurídica realizada ha concluido que el consentimiento para el tratamiento de datos de la salud a cambio de beneficios económicos no es transparente, por cuanto no se informa a los titulares de datos los fines del tratamiento de sus datos de la salud. Por ello, no se trata de un consentimiento informado (agregar respaldo en Anexo).

- Vulnerabilidad: La empresa no cuenta con abogados especializados en protección de datos personales.

- Rationale: La auditoría informó que hay un bajo nivel de preparación del área jurídica del responsable del tratamiento en temas de protección de datos personales (agregar respaldo en Anexo).

Análisis del riesgo

- Probabilidad de ocurrencia (informativo): Muy Probable (50%)

- Rationale: El equipo de auditoria realizó un análisis de la posición de la SPDP con respecto al impacto de grupos especialmente vulnerables y ha calibrado las opiniones de cinco expertos utilizando el modelo Lens (agregar respaldo en Anexo).

- Impacto: Los datos de la salud son datos sensibles, produciendo un elevado impacto en grupos especialmente vulnerables de titulares de datos. Su mal uso puede afectar sus derechos al trabajo, su derecho a la salud, entre otros.

- Rationale: Se utilizó un método estadístico para verificar la empleabilidad de personas con enfermedades en el mercado laboral ecuatoriano (agregar respaldo en Anexo).

Evaluación del impacto

Titulares promedio: Muy alto.

Titulares especialmente vulnerables: Muy alto.

Tratamiento del riesgo

Informar de manera adecuada y eficiente a los titulares de los datos acerca de los fines del tratamiento de sus datos de la salud, de las medidas de seguridad que estos tendrán; y, del impacto que puede tener la divulgación de estos datos en el mercado laboral, así como el impacto en el potencial costo de coberturas de seguros médicos, entre otros afines. Asimismo, informar con un lenguaje comprensible y darles el tiempo necesario para comprender los riesgos del tratamiento de sus datos de la salud.

2.4. Riesgo de guardar los datos personales de manera excesiva

Concordancia: Art. 10 (I) de la LOPDP.

¿Cuál es la duración de almacenamiento de los datos?

Los datos son conservados por dos meses posteriores a haber cumplido con las finalidades del tratamiento.

¿Qué método se utiliza para borrar los datos de manera segura?

Se utilizan sistema de sobre escritura de caracteres. Para el borrado de dispositivos de almacenamiento se utiliza el Estándar NIST SP 800-88.

Identificación del riesgo

- Amenaza: Considerando que la amenaza es el responsable del tratamiento, la empresa MalaKompra S.A. puede vulnerar los derechos de los titulares de datos al conservar los datos de manera indefinida y al no utilizar mecanismos de borrado seguro.

- Rationale: El Delegado de protección de datos identificó que la empresa conserva los datos y metadatos de manera indefinida en los *backups*. Por tanto, no cumple con lo establecido en su propia política de protección de datos personales (agregar respaldo en Anexo).

- Vulnerabilidad: Las políticas de seguridad de la información; y, en particular, el plan de Continuidad de actividades (*Business Continuity Plan*) no ha sido adaptado a las obligaciones de la LOPDP. La falta de comunicación entre el DPD y el CISO es una vulnerabilidad organizacional.

- Rationale: El equipo de auditoría de seguridad organizacional encontró esta vulnerabilidad en las políticas de seguridad de la información y solicitó revisar los *backups* constatando que los datos no eran borrados de los discos duros utilizados para tal finalidad (agregar respaldo en Anexo).

Análisis del riesgo

- Probabilidad de ocurrencia (informativo): Muy Probable (70%)

- Rationale: Los auditores de seguridad organizacional encontraron que alrededor del 60% de los datos personales tratados se conservan en los *backups* de manera indefinida y no están cifrados (agregar respaldo en Anexo).

- Impacto: La consecuencia para los titulares de datos es el aumento del riesgo de una vulneración de la confidencialidad de los datos personales. Con ello, se pueden vulnerar su derecho a la protección de datos personales y otros derechos como impacto secundario.

- Rationale: Los auditores constataron que los datos personales que constan en los *backups* son simples, comportamentales, financieros y sensibles (agregar respaldo en Anexo).

Evaluación del impacto

Muy Alto.

Tratamiento del riesgo

Mejorar el plan de continuidad de actividades incorporando un proceso para borrar datos personales de los *backups*. Implementar y cumplir con un borrado seguro en el que se sobreescriba cada sector. Se recomiendan seguir los procesos de los estándares DoD 5220.22, o el NIST 800-88.

2.4. Riesgo de no cumplir con el principio de pertinencia y minimización de datos

Concordancia: Art. 10 (e) LOPDP.

Identificación del riesgo

¿Los datos recopilados son adecuados, relevantes y limitados a lo que es necesario en relación con los fines para los que se procesan ('minimización de datos')?

Los datos recolectados son biográficos, de contacto, geolocalización, preferencias, financieros y datos sensibles de la salud en alrededor del 25% de titulares de datos.

- Amenaza: Considerando que la amenaza es el responsable del tratamiento, la empresa MalaKompra S.A. puede vulnerar los derechos de los titulares de datos al recopilar datos de manera excesiva y al no tener ninguna pertinencia para el tratamiento de datos necesario.

- Rationale: El equipo de auditores jurídicos procedió a abrir cuentas como potenciales clientes para auditar que datos personales eran requeridos al abrir una cuenta. Se identificó que se están recopilando datos biográficos (nombres, apellidos y edad) acerca de los hijos de los clientes al abrir cuentas, en la página web: https://malakompra.ec/signup. (agregar respaldo en Anexo).

- Vulnerabilidad: Los formularios los hace el *webmaster*, sin ningún control de la Dirección Jurídica.

- Rationale: El equipo de auditores jurídicos identificó que no hay procedimientos internos para auditar el desarrollo de formularios que desarrolla el *webmaster* (agregar respaldo en Anexo).

Análisis del riesgo

- Probabilidad de ocurrencia (informativo): Muy Probable (75%)

- Rationale: Tres de los cuatro expertos consideraron que los datos personales de los hijos no deben ser recopilados (agregar respaldo en Anexo).

- Impacto: Los datos personales de menores de edad son datos sensibles. El impacto primario es vulnerar el derecho a la confidencialidad de sus datos personales. El impacto secundario es exponerlos a riesgos de seguridad en un país con altos índices de delincuencia.

- Rationale: Estadísticas de extorsiones y secuestros en el Ecuador (agregar respaldo en Anexo).

Evaluación del impacto

Titulares promedio: Alto.
Titulares especialmente vulnerables: Muy alto.

Tratamiento del riesgo

Elaborar un proceso en el cual la dirección jurídica deba revisar y aprobar los formularios desarrollados por la dirección de tecnologías de la información; eliminar los datos de menores de edad de los formularios pertinentes y borrar todos los datos personales de edad que ya hayan sido recopilados y almacenados.

2.5. Riesgo de no cumplir con los derechos de acceso y portabilidad de datos

Concordancia: Art. 13 LOPDP.

Identificación del riesgo

¿Qué métodos se utilizan para garantizar el acceso de los titulares a sus datos personales?

Los titulares de datos tienen acceso directo y permisos de edición de todos los datos que generen en su espacio web. Para los datos y metadatos que estén fuera del control del titular de datos, se puede enviar un correo electrónico a derechos@malkompra.ec.

¿Qué métodos se utilizan para garantizar el derecho a la portabilidad de datos?

Los titulares de datos podrán ejercer su derecho de portabilidad de datos escribiendo a derechos@malakompra.ec. Los datos serán entregados en formato pdf y/o csv de acuerdo con el tipo de datos.

- Amenaza: Considerando que la amenaza es el responsable del tratamiento, la empresa MalaKompra S.A. puede vulnerar los derechos de los titulares de datos al no proporcionar mecanismos para ejercer el derecho de acceso y el derecho de portabilidad de datos a los titulares de datos.

- Rationale: El equipo de auditores jurídicos procedió a abrir cuentas como potenciales clientes para auditar los mecanismos implementados para el ejercicio de los derechos de acceso y portabilidad (agregar respaldo en Anexo).

- Vulnerabilidad: No fue encontrada vulnerabilidad para el ejercicio de ambos derechos.

- Rationale: Los mecanismos implementados funcionan de manera adecuada. El equipo jurídico abrió cuentas como clientes y verificó el control sobre toda su información propia generada en menos de diez días. Además, solicitó todos sus datos personales en un formato estandarizado, recibiendo respuesta también en un plazo razonable, con un enlace de descarga de un archivo en formato PDF (agregar respaldo en Anexo).

Análisis del riesgo

- Probabilidad de ocurrencia (informativo): Poco probable (5%)

- Rationale: El ejercicio de derechos fue solicitado de manera anónima por tres auditores. Dos solicitudes se cumplieron en cinco días. Una solicitud se cumplió en seis días. Los expertos concluyeron una eficiencia del 95% (agregar respaldo en Anexo).

- Impacto: El impacto puede generar una vulneración de disponibilidad de los datos personales de los titulares, ocasionando además la vulneración de su derecho a la protección de datos personales y pérdidas financieras debido a la falta de acceso.

- Rationale: El equipo de auditores estimó que el impacto es importante, pero influye que la empresa tiene mecanismos que funcionan (agregar respaldo en Anexo).

Evaluación del impacto

Bajo.

Tratamiento del riesgo

Vigilar que los controles de riesgo sigan siendo efectivos y eficaces.

2.6. Riesgo de no cumplir con el derecho de rectificación y actualización

Concordancia: Art. 14 LOPDP.

Identificación del riesgo

¿Cómo pueden los interesados ejercer sus derechos de rectificación y actualización?

Los titulares de datos tienen los privilegios correspondientes para rectificar y actualizar todos los datos que generen en su espacio web. Para rectificar y actualizar los datos y metadatos que estén fuera del control del titular de datos, se puede enviar un correo electrónico a derechos@malakompra.ec.

- Amenaza: Considerando que la amenaza es el responsable del tratamiento, la empresa MalaKompra S.A. puede vulnerar los derechos de rectificación y actualización los titulares de datos al no proporcionar mecanismos para su ejercicio.

- Rationale: El equipo de auditores jurídicos procedió a abrir cuentas como potenciales clientes, para auditar los mecanismos implementados para el ejercicio de los derechos de rectificación y actualización (agregar respaldo en Anexo).

- Vulnerabilidad: No fue encontrada vulnerabilidad para el ejercicio de ambos derechos.

- Rationale: Los mecanismos implementados funcionan de manera adecuada. El equipo jurídico abrió cuenta como clientes y verificó el control sobre toda su información propia generada. Además, pudo rectificar y actualizar otros datos personales sin permiso de edición, recibiendo respuesta también en un plazo razonable de tres días (agregar respaldo en Anexo).

Análisis del riesgo

- Probabilidad de ocurrencia (informativo): Poco probable (5%)

- Rationale: El ejercicio de derechos fue solicitado de manera anónima por tres auditores. Las solicitudes se cumplieron en tres días. Una solicitud se cumplió en seis días. Los expertos estimaron una eficiencia del 98% (agregar respaldo en Anexo).

- Impacto: El impacto puede generar una vulneración de integridad de los datos personales de los titulares, ocasionando además la vulneración de su derecho a la protección de datos personales; y, pueden vulnerarse otros derechos y libertades debido a no poder rectificar su información.

- Rationale: El equipo de tres auditores estimó que el impacto es importante, pero infiere que la empresa tiene mecanismos que funcionan (agregar respaldo en Anexo).

Evaluación del impacto

Bajo.

Tratamiento del riesgo

Vigilar que los controles de riesgo sigan siendo efectivos y eficaces.

2.7. Riesgo de no cumplir con el derecho de eliminación

Concordancia: Art. 15 LOPDP.

Identificación del riesgo

¿Cómo pueden los interesados ejercer su derecho de eliminación de datos?

Los titulares de datos pueden ejercer su derecho de eliminación de datos que ellos generen desde su propio espacio web. Sin embargo, los datos personales publicados en la sección "Prensa" no tienen un mecanismo para ser eliminados.

¿Qué método de borrado seguro es utilizado?

El responsable del tratamiento supuestamente utiliza herramientas basadas en el Estándar NIST 800-88.

- Amenaza: Considerando que la amenaza es el responsable del tratamiento, la empresa MalaKompra S.A. puede vulnerar los derechos de los titulares de datos al no proporcionarles mecanismos para ejercer el derecho de acceso de eliminación.

- Rationale: El equipo de auditores jurídicos procedió a abrir cuentas como potenciales clientes para auditar los mecanismos implementados para el ejercicio del derecho de eliminación de datos. El equipo de auditores técnicos procedió a implementar una estrategia de *file carving* para verificar si los datos son borrados de manera segura (agregar respaldo en Anexo).

- Vulnerabilidad: No hay mecanismos para ejercer el derecho de eliminación para los datos de la salud. La empresa no cumple con un sistema de borrado seguro en sus dispositivos de almacenamiento.

- Rationale: El equipo de auditores jurídicos identificó que la dirección jurídica no había considerado que dar beneficios financieros a sus clientes no presupone que la empresa se vuelva propietaria de esos datos de la salud, lo cual es ilegal a la luz de la LOPDP. Esto debido a la baja capacitación de la dirección jurídica en derecho de protección de datos personales. Además, el equipo de auditores técnicos procedió a extraer una copia de *bit a bit* de un disco duro de la empresa y utilizó la herramienta *Data Extractor*; con lo cual, identificó que los datos personales no son eliminados de manera segura. Por ello, la segunda vulnerabilidad identificada es la negligencia del departamento de seguridad de la información al no implementar los mecanismos adecuados de borrado seguro en todos los dispositivos de almacenamiento (agregar respaldo en Anexo).

<u>Análisis del riesgo</u>

- Probabilidad de ocurrencia (informativo): Muy Probable (85%)

- Rationale: Hubo tres auditores jurídicos que calibraron a partir del método Delphi, una probabilidad del 100%. Los dos auditores técnicos por su lado calibraron la probabilidad de ocurrencia en el 70%, con base en la aplicación del teorema de Bayes para calibrar la probabilidad condicional de tener una vulneración de seguridad de datos debido a no eliminarlos de manera segura (agregar respaldo en Anexo).

- Impacto: Los derechos y libertades de los titulares que entregan datos médicos están siendo sistemáticamente vulnerados por parte del responsable del tratamiento. La confidencialidad de los datos personales de todos los titulares presenta un alto riesgo debido a la negligencia de no implementar métodos de borrado seguro.

- Rationale: Los auditores jurídicos estimaron, utilizando el método Delphi, con un nivel de muy alto por tratarse de datos sensibles que afectan a más de 1 000 titulares, de acuerdo con lo establecido en los criterios de evaluación (agregar respaldo en Anexo).

Evaluación del impacto

Muy Alto.

Tratamiento del riesgo

En primer lugar, es necesario implementar un mecanismo para que los titulares de datos de la salud puedan eliminar sus datos. En segundo lugar, se debe capacitar a la dirección jurídica en las obligaciones de conformidad a la LOPDP. En tercer lugar, es necesario cumplir con la implementación de mecanismos de borrado seguro que sobreescriban en la práctica, los sectores de los discos duros con varias capas de caracteres.

2.8. Riesgo de no cumplir con los derechos de oposición y suspensión del tratamiento

Concordancia: Arts. 16, 19 LOPDP.

Identificación del riesgo

¿Cómo pueden los interesados ejercer sus derechos de oposición y de suspensión?

Los titulares de datos pueden ejercer sus derechos de oposición y suspensión escribiendo al correo electrónico: derechos@malakompra.ec.

- Amenaza: La empresa MalaKompra S.A. puede vulnerar los derechos de los titulares de datos al no proporcionarles mecanismos para ejercer los derechos de oposición y suspensión.

- Rationale: Considerando que la amenaza es el responsable del tratamiento, el equipo de auditores jurídicos abrió cuentas como potenciales clientes, para auditar los mecanismos implementados para el ejercicio de los derechos de oposición y suspensión (agregar respaldo en Anexo).

- Vulnerabilidad: No fue encontrada vulnerabilidad para el ejercicio de ambos derechos.

- Rationale: Los mecanismos implementados funcionan de manera adecuada. El equipo de auditores jurídicos verificó que tres clientes escriban al correo electrónico derechos@malakompra.ec y sus pedidos fueron realizados en un plazo razonable de 10 días (agregar respaldo en Anexo).

Análisis del riesgo

Probabilidad de ocurrencia (informativo): Poco probable (5%)

- Rationale: El ejercicio de derechos fue solicitado de manera anónima por tres auditores. Se cumplió con ellos en el plazo establecido (agregar respaldo en Anexo).

- Impacto: El impacto puede generar una vulneración de confidencialidad de los datos personales de los titulares, ocasionando además de la vulneración de su derecho a la protección de datos personales, probables vulneraciones a otros derechos y libertades.

- Rationale: Un equipo de cuatro auditores estimó que el impacto es importante, pero intuye que la empresa tiene mecanismos que funcionan (agregar respaldo en Anexo).

Evaluación del impacto

Bajo.

Tratamiento del riesgo

Vigilar que los controles de riesgo sigan siendo efectivos y eficaces.

2.9. Riesgo de que los encargados del tratamiento no cumplan con sus obligaciones

Concordancia: Arts. 34, 47 LOPDP.

Identificación del riesgo

¿Las obligaciones de los encargados del tratamiento están claramente identificadas y regidas por un contrato?

La empresa declara tener dos encargados del tratamiento: (1) DataKuy Ltd. Servicios de marketing digital. Empresa Ecuatoriana. (2) BestKloud: Servicios de nube Infrastructure as a Service (IaaS) en la nube. Empresa Estadounidense registrada en el Estado California. Ambos están regidos por contratos que contemplan la conformidad al reglamento General de Protección de Datos (UE) 2016/679. No obstante, hay la sospecha de si existe un tercer encargado del tratamiento no declarado en lo que concierne a los datos de la salud.

- Amenaza: La amenaza son los encargados del tratamiento que podrían incumplir con la protección de los derechos y libertades de los titulares de datos, conforme a la LOPDP. El equipo auditor identifica que los datos de la salud recopilados están siendo entregados a la empresa de seguros médicos Asegúrate S.A. sin ningún contrato de protección de datos personales.

- Rationale: El equipo de auditores técnicos auditó los flujos de datos personales y encontró un encargado del tratamiento no declarado, integrándolo a las comunidades de amenaza (agregar respaldo en Anexo).

- Vulnerabilidades: El equipo de auditores identificó dos vulnerabilidades. En primer lugar, el encargado del tratamiento DataKuy Ltd. no tiene políticas de seguridad de la información, poniendo en alto riesgo la seguridad de los datos personales encargados. La vulnerabilidad es la falta de debida diligencia de la dirección jurídica. En segundo lugar, la empresa AseguraTe S.A. no tiene un Convenio de protección de datos, y sin embargo está tratando los datos de la salud. La vulnerabilidad es la falta de capacitación de la dirección jurídica.

- Rationale: El equipo de auditores jurídicos procedió a auditar los convenios de procesamiento de datos personales (*Data protection Agreements*). Además, solicitó a los auditores técnicos, auditar el flujo de datos desde la aplicación web de la empresa (agregar respaldo en Anexo).

<u>Análisis del riesgo</u>

- Probabilidad de ocurrencia (informativo): Inminente (95%)

- Rationale: Los auditores utilizaron un modelo de predicción conformal inductiva (*inductive conformal prediction*), para establecer el nivel de confianza en el cumplimiento de obligaciones de encargados del tratamiento (agregar respaldo en Anexo).

- Impacto: Los derechos y libertades de los titulares están en muy alto riesgo, debido a la falta de medidas de seguridad organizacional y técnica por parte de la empresa DataKuy LTD; y, por la falta de un Convenio de protección de datos con la empresa AseguraTe S.A.

- Rationale: Los auditores utilizaron el modelo de aprendizaje automático supervisado *Decision Trees* para analizar el impacto de la falta de debida diligencia para contratar a los respectivos encargados del tratamiento como problema de clasificación (agregar respaldo en Anexo).

Evaluación del impacto

Muy Alto.

Tratamiento del riesgo

Se debe capacitar a la dirección jurídica en temas de convenios de protección de datos personales con los encargados de datos y para realizar la debida diligencia al escogerlos. También es necesario que el DPD asuma su rol de auditor de auditores, identificando a los encargados del tratamiento de manera adecuada y revisando el flujo de datos personales.

[SE HAN PRESENTADO VARIOS ESCENARIOS DE RIESGO, PERO SIEMPRE SERÁ NECESARIO AUMENTAR LOS ESCENARIOS QUE SEAN PERTINENTES PARA LA SITUACIÓN PARTICULAR DE LOS RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO]

3. ESCENARIOS DE RIESGOS DE SEGURIDAD DE DATOS PERSONALES

Para ejemplificar la gestión de los riesgos de seguridad de datos se han construido dos escenarios de riesgos por cada dimensión de la seguridad de datos (confidencialidad, integridad, disponibilidad). El responsable del tratamiento puede agregar los escenarios pertinentes. Los escenarios pueden ser promediados por motivos de presentación, lo importante es incluir *rationales* de cada uno de ellos y mantener por separado los resultados de la confidencialidad, de la integridad y de la disponibilidad. Puede incluirse el *rationale* en el documento de evaluación de impacto o adjuntar los *rationales* en anexos.

En el presente tutorial se ha optado por incluir una descripción corta, pero siempre referenciado al *rationale* correspondiente. Además, hay que considerar que los mismos riesgos de seguridad de datos personales que pueden vulnerar los derechos y libertades de los titulares son riesgos de seguridad de la información. Consecuentemente, se recomienda integrar los resultados de la evaluación de impacto del tratamiento de datos personales en la gestión de riesgos de seguridad de la información. En la presente evaluación ficticia se considera el impacto inherente y la frecuencia de ocurrencia inherente (riesgo inherente).

Se recomienda agregar los niveles de impacto y frecuencia de ocurrencia residuales (riesgo residual) una vez que sean implementadas las medidas de seguridad jurídicas, organizacionales y técnicas recomendadas. Todos los escenarios de riesgo cuentan con una evaluación de impacto para titulares promedio; y, a los relacionados a la confidencialidad, se les ha agregado una evaluación de impacto para titulares de datos especialmente vulnerables.

3.1. Escenarios de riesgo de confidencialidad

3.1.1. Vulneración de la seguridad de datos personales / Malware (Troyanos, spyware)

Concordancia: Arts. 10 (e), 37 LOPDP.

Identificación del riesgo

¿Qué comunidades de amenaza se pueden vincular al escenario de riesgo?

Cibercriminales, hackers mercenarios de otras empresas similares.

¿Qué mecanismos pueden utilizar las comunidades de amenaza?

Las comunidades de amenaza pueden utilizarla métodos de ingeniería social o aprovechando vulnerabilidades del software.

¿Qué vulnerabilidades organizacionales se han detectado con respecto a este escenario de riesgo?

Falta de capacitación de los empleados en seguridad de la información. Deficiente política de control de acceso.

¿Qué vulnerabilidades técnicas se han detectado con respecto a este escenario de riesgo?

La empresa utiliza software de antivirus gratuito que solo protege por reconocimiento de huellas digitales, pero no por anomalías. La empresa tiene un 30% de software no actualizado.

¿Qué consecuencias pueden sufrir los titulares de los datos si el riesgo se materializa?

La vulneración del derecho a la protección de datos personales de confidencialidad de sus datos como impacto primario y de otros derechos como impacto secundario.

- Amenazas: Cibercriminales, hackers, mercenarios contratados por otras empresas similares.

- Rationale: Se contrató a un especialista externo en inteligencia de amenazas (*threat intelligence*), quien realizó el análisis de adversarios utilizando matrices (agregar respaldo en Anexo).

- Vulnerabilidades: Falta de capacitación de los empleados en seguridad de la información. Deficiente política de control de acceso. La empresa utiliza software de antivirus gratuito que solo protege por reconocimiento de huellas digitales, pero no por anomalías. La empresa tiene un 30% de software no actualizado.

- Rationale: Se contrató a un equipo *red team* integrado por tres *ethical hackers* y *penetration testers* que consiguieron acceso con un *payload* para procesadores Intel 64, un troyano de conexión reversa y elevaron privilegios aprovechando la vulnerabilidad "ms14_058_track_popup_menu" en un sistema operativo obsoleto Windows 7 (agregar respaldo en Anexo).

Análisis del riesgo

- Frecuencia de ocurrencia: Media (Mínimo: 2; Más probable: 6; Máximo: 10)

- Rationale: Se realizó un análisis histórico. El CISO utilizó los reportes del SOC, en los que se registraron 80 tentativas de acceso en el año anterior, en donde el cortafuegos bloqueo 60 incidentes. De los 20 accesos no consentidos, 12 troyanos fueron neutralizados por el antivirus gratuito, pero 8 troyanos efectivamente pasaron el control de antivirus; y, 5 de ellos ocasionaron una vulneración de la seguridad de datos personales, con un promedio de 1 100 titulares afectados (agregar respaldo en Anexo).

- Impacto: Una vulneración de la seguridad de datos puede impactar de manera irreversible la confidencialidad de los datos. Para titulares de datos promedio, los valores obtenidos son: Mínimo: $100 000, Más probable: $600 000, Máximo: $1 200 000. Para los titulares de datos especialmente vulnerables, los valores obtenidos son: Mínimo: $150 000, Más probable: $900 000, Máximo: $1 600 000.

- Rationale: La dirección de gobernanza de datos contrató a un especialista en análisis de riesgos cuantitativos que realizó un análisis histórico del valor al Riesgo, considerando como espacio de sampleo, sanciones por vulneraciones de confidencialidad y el costo de una vulneración de confidencialidad de datos en los titulares de datos promedio, modelando el riesgo y calibrándolo a través de un análisis de Monte Carlo (agregar respaldo en Anexo).

Evaluación del impacto

- Titulares promedio: Alta. (Mínimo: $100 000, Más probable: $600 000, Máximo: $1 200 000).

- Titulares especialmente vulnerables: Alta. (Mínimo: $150 000, Más probable: $900 000, Máximo: $1 600 000).

Tratamiento del riesgo

- Implementar programas de capacitación para los empleados en seguridad de la información.

- Redactar e implementar una política de control de acceso eficiente. Implementar un software de antivirus premium que brinde reconocimiento por anomalías y entrenado con modelos de *machine learning*.
- Actualizar el software de la empresa y parchar las vulnerabilidades de manera periódica.

3.1.2. Vulneración de la seguridad de datos personales / Vulnerabilidades Web / SQL injection

Concordancia: Arts. 10 (e), 37 LOPDP.

Identificación del riesgo

¿Qué comunidades de amenaza se pueden vincular al escenario de riesgo?

Cibercriminales, hackers mercenarios.

¿Qué mecanismos pueden utilizar las comunidades de amenaza?

Escaneo de vulnerabilidades web, implementar métodos de *fuzzing* para la manipulación de caracteres.

¿Qué vulnerabilidades organizacionales se han detectado con respecto a este escenario de riesgo?

No hay plan de manejo de vulnerabilidades Web en la empresa.

¿Qué vulnerabilidades técnicas se han detectado con respecto a este escenario de riesgo?

Vulnerabilidad de *SQL injection* en las páginas web: https://clientes.malakompra.ec y https://seguro.malakompra.ec.

¿Qué consecuencias pueden sufrir los titulares de los datos si el riesgo se materializa?

La vulneración del derecho a la protección de datos personales de confidencialidad de sus datos como impacto primario; y, de otros derechos, como impacto secundario.

- Amenazas: Cibercriminales, hackers mercenarios.

- Rationale: Se contrató a un especialista externo en inteligencia de amenazas (*threat intelligence*), quien realizó el análisis de adversarios utilizando matrices utilizadas en la teoría de juegos (agregar respaldo en Anexo).

- Vulnerabilidades: *SQL injection* https://clientes.malakompra.ec y https://seguro.malakompra.ec.

- Rationale: La dirección de seguridad de la información realizó escaneos de vulnerabilidades y test de penetración a través de un método de *fuzzing*, con la herramienta Zed Attack Proxy (ZAP) (agregar respaldo en Anexo).

Análisis del riesgo

- Frecuencia de ocurrencia anual: Alta (Mínimo: 5; Más probable: 15; Máximo: 30)

- Rationale: En el último año se registraron 239 escaneos de vulnerabilidades provenientes mayormente del Ecuador, de Colombia y de Corea del Norte. La empresa sufrió 18 ataques de *SQL injection*. Sin embargo, la frecuencia disminuyó en un 50% hace dos meses, cuando se implementó un *firewall* de aplicación Web eficiente (WAF) y cifrado de curva elíptica, en el 80% de bases de datos (agregar respaldo en Anexo).

- Impacto: Una vulneración de la seguridad de datos puede impactar de manera irreversible la confidencialidad de los datos, considerando que se tratan datos sensibles y que existen grupos especialmente vulnerables. Para los titulares de datos promedio: Mínimo: $80 000, Más probable: $200 000, Máximo: $800 000. Para los titulares de datos especialmente vulnerables, los valores obtenidos son: Mínimo: $120 000, Más probable: $300 000, Máximo: $800 000.

- Rationale: La dirección de gobernanza de datos contrató a un especialista en análisis de riesgos cuantitativos que utilizó una variación personalizada del modelo FAIR, en donde los datos de entrada fueron calibrados en función de dos factores. En primer lugar, se realizaron encuestas a las víctimas de las anteriores vulneraciones de datos, con 50 titulares de datos promedio; y, 20 titulares de datos de grupos especialmente vulnerables. En segundo lugar, la calibración se hizo a partir del 0.3% de la facturación bruta anual de la empresa, anticipando una probable sanción (agregar respaldo en Anexo).

Evaluación del impacto

- Titulares promedio: Medio (Mínimo: $80 000, Más probable: $2 00 000)

- Titulares especialmente vulnerables: Medio (Mínimo: $120 000, Más probable: $300 000, Máximo: $800 000)

Tratamiento del riesgo

- Implementar una política de seguridad específica acerca de gestión de vulnerabilidades web, con base en el OWASP Top Ten y el estándar OWASP ASVS.
- Realizar escaneos de vulnerabilidades web de manera periódica.
- Corregir la vulnerabilidad de SQL injection, sanitizando los caracteres de entrada.
- En lo posible, adquirir una solución de software inteligente OSINT y TPRM que permita realizar un control permanente de vulnerabilidades de aplicaciones Web.

[AGREGAR LOS ESCENARIOS DE RIESGO DE CONFIDENCIALIDAD DE DATOS NECESARIOS ...]

3.2. Escenarios de riesgo de integridad

3.2.1. Vulneración de la integridad de datos personales / Ataques internos

Concordancia: Arts. 10 (e), 37 LOPDP.

Identificación del riesgo

¿Qué comunidades de amenaza se pueden vincular al escenario de riesgo?

Empleados con privilegios, empleados sin privilegios.

¿Qué mecanismos pueden utilizar las comunidades de amenaza?

Editar la información a la que tienen acceso, acceder a computadoras que son de recursos compartidos.

¿Qué vulnerabilidades organizacionales se han detectado con respecto a este escenario de riesgo?

La dirección de recursos humanos no realiza controles de antecedentes penales, ni exámenes psicológicos. No hay cámaras de seguridad en las instalaciones de la empresa en donde se guarda información confidencial. No se realizan test de penetración internos.

¿Qué vulnerabilidades técnicas se han detectado con respecto a este escenario de riesgo?

No se utilizan funciones de *hash* para controlar la integridad de los archivos.

¿Qué consecuencias pueden sufrir los titulares de los datos si el riesgo se materializa?

Como impacto primario, la vulneración de su derecho de protección de datos personales, por cuanto se vulnera la integridad de sus datos personales. A partir de ello, como impacto secundario, se pueden vulnerar otros derechos y libertades; como su derecho a la educación, su derecho al trabajo, entre otros.

- Amenazas: Empleados con privilegios, empleados sin privilegios.

- Rationale: Se contrató a un especialista externo en inteligencia de amenazas (threat intelligence), quien realizó el análisis de adversarios utilizando matrices (agregar respaldo en Anexo).

- Vulnerabilidades: La dirección de recursos humanos no realiza controles de antecedentes penales, ni exámenes psicológicos. No hay cámaras de seguridad en las instalaciones de la empresa en donde se guarda información confidencial. No se realizan test de penetración internos de manera periódica. No se utilizan funciones de *hash* para controlar la integridad de los archivos.

- Rationale: La dirección de seguridad de la información contrató a un *ethical hacker* externo, quien realizó un análisis de vulnerabilidades organizacionales y técnicas internas. El especialista concluyó que la principal raíz del problema es organizacional; y, que es necesario cambiar las prácticas de la dirección de recursos humanos. Además, verificó que no existe una cultura de trazabilidad eficiente en el manejo documental (agregar respaldo en Anexo).

<u>Análisis del riesgo</u>

- Frecuencia de ocurrencia: Muy alta (Mínimo: 14; Más probable: 22; Máximo: 38)

- Rationale: El análisis interno de vulnerabilidades comprobó que se han implementado funciones de *hash* para controlar un manejo documental íntegro, lo cual permite que empleados de la empresa puedan tomar ventaja y alterar archivos (agregar respaldo en Anexo).

- Impacto: Una vulneración de la seguridad de datos puede impactar la integridad de los datos, causando vulneraciones de los derechos y libertades de los titulares. Mínimo: $2 000, Más probable: $10 000, Máximo: $20 000.

- Rationale: La dirección de gobernanza de datos contrató a un especialista en análisis de riesgos cuantitativos que utilizó una variación personalizada del modelo FAIR, en donde los datos de entrada fueron calibrados en función de dos factores. En primer lugar, se realizaron encuestas a las víctimas de las vulneraciones de integridad de datos de la empresa, con 50 titulares de datos promedio; y, 20 titulares de datos de grupos especialmente vulnerables. En

segundo lugar, la calibración se hizo a partir del 0.3% de la facturación bruta anual de la empresa, anticipando una probable sanción (agregar respaldo en Anexo).

Evaluación del impacto

Bajo. (Mínimo: $2 000, Más probable: $10 000, Máximo: $20 000).

Tratamiento del riesgo

- Cambiar los procedimientos de contratación y auditoría de la dirección de recursos humanos, realizando chequeos de antecedentes de los empleados y evaluaciones psicológicas.
- Agregar en las políticas de seguridad de la información, políticas para el manejo y controles de empleados.
- Implementar un manejo documental en donde todos los archivos cuenten con al menos dos hashes (por ejemplo: MD5, SHA 1, SHA 256), que permitan verificar la integridad de datos.

3.2.2. Vulneración de la seguridad de datos personales / Ingeniería social - phishing

Concordancia: Arts. 10 (e), 37 LOPDP.

Identificación del riesgo

¿Qué comunidades de amenaza se pueden vincular al escenario de riesgo?

Cibercriminales, Hackers mercenarios auspiciados, empleados internos.

¿Qué mecanismos pueden utilizar las comunidades de amenaza?

Llamadas telefónicas falsas, *spear phishing*, *phishing* por correos electrónicos, *phishing* por mensajes de chat, *vishing* con mensaje de voz.

¿Qué vulnerabilidades organizacionales se han detectado con respecto a este escenario de riesgo?

Falta de capacitación de empleados. Falta de capacitación a los titulares de datos (clientes).

¿Qué vulnerabilidades técnicas se han detectado con respecto a este escenario de riesgo?

Falta de un detector eficiente de spam en el servidor de correo electrónico, https://mail.malakompra.ec.

¿Qué consecuencias pueden sufrir los titulares de los datos si el riesgo se materializa?

El impacto primario es la vulneración de su derecho de datos personales en cuanto a su integridad, disponibilidad y confidencialidad. Esto puede ocasionar como impacto secundario la vulneración de otros derechos y libertades.

- Amenazas: Cibercriminales, Hackers mercenarios auspiciados, empleados internos.

- Rationale: El especialista externo en inteligencia de amenazas (*threat intelligence)* combinó los datos de ataques de *phishing* de los reportes de IBM *security* y Verizon, con una calibración subjetiva con base en cinco incidentes internos en el último año (agregar respaldo en Anexo).

- Vulnerabilidades: Falta de capacitación de empleados. Falta de capacitación a los titulares de datos (clientes). Falta de un detector eficiente de spam en el servidor de correo electrónico https://mail.malakompra.ec.

- Rationale: La dirección de seguridad de la información contrató a un *ethical hacker* externo, quien realizó un análisis de vulnerabilidades organizacionales y técnicas. El hacker ético pudo aprovechar la ingenuidad de dos empleados para conseguir acceso a los sistemas de información (agregar respaldo en Anexo).

Análisis del riesgo

- Frecuencia de ocurrencia: Media (Mínimo: 4; Más probable: 8; Máximo: 15)

- Rationale: El CISO y el DPD utilizaron los datos de entrada de los especialistas externos y calibraron el valor (agregar respaldo en Anexo).

- Impacto: Una vulneración de la seguridad de datos puede impactar la integridad, confidencialidad y disponibilidad de los datos personales, causando vulneraciones de los derechos y libertades de los titulares. Mínimo: $100 000, Más probable: $160 000, Máximo: $220 000.

- Rationale: El CISO utilizó el modelo FAIR para calibrar de manera cuantitativa el impacto global de los ataques de *phishing* e ingeniería social, incluyendo el impacto en los derechos y libertades de los titulares. El DPD lo validó (agregar respaldo en Anexo).

Evaluación del impacto

ALTO (Mínimo: $100 000, Más probable: $160 000, Máximo: $220 000).

Tratamiento del riesgo

- Diseñar programas de capacitación eficaces para todos los empleados de la empresa. Diseñar campañas de concientización para los clientes (titulares de datos).
- Implementar una solución de detección de spam entrenada con modelos de aprendizaje automático eficientes que arrojen un nivel de falsos negativos menos al 1% en el servidor de email https://mail.malakompra.ec.

[AGREGAR LOS ESCENARIOS DE RIESGO DE INTEGRIDAD DE DATOS NECESARIOS ...]

3.3. Escenarios de riesgo de disponibilidad

3.3.1. Vulneración de la seguridad de datos personales / Ataques de Denegación Distribuida de Servicio (DDOS)

Concordancia: Arts. 10 (e), 37 LOPDP.

Identificación del riesgo

¿Qué comunidades de amenaza se pueden vincular al escenario de riesgo?

Hacktivistas, hackers mercenarios contratados, cibercriminales.

¿Qué mecanismos pueden utilizar las comunidades de amenaza?

Utilizar software como mecanismos para realizar ataques de denegación distribuida de servicio (DDOS), con el fin de ocasionar la interrupción temporal de servicios, incluyendo el acceso a la información por parte de los titulares de datos.

¿Qué vulnerabilidades organizacionales se han detectado con respecto a este escenario de riesgo?

No hay un plan de respuesta a incidentes en casos de ataques DOS, DDOS.

¿Qué vulnerabilidades técnicas se han detectado con respecto a este escenario de riesgo?

No hay protección *Cloudflare* que permita filtrar y mitigar ataques de DDOS.

¿Qué consecuencias pueden sufrir los titulares de los datos si el riesgo se materializa?

El impacto primario es la vulneración de la disponibilidad de sus datos personales. Esto puede ocasionar impactos secundarios como violación de otros derechos y libertades; y, pérdidas económicas.

- Amenazas: Hacktivistas, hackers mercenarios contratados, cibercriminales.

- Rationale: Había datos propios registrados sobre ataques de DDOS. Se contrató a un especialista externo en inteligencia de amenazas (*threat intelligence*), quien realizó el análisis de adversarios con los datos obtenidos de la plataforma Alien Vault OTX, y utilizando matrices (agregar respaldo en Anexo).

- Vulnerabilidades: No hay un plan de respuesta a incidentes en casos de ataques DOS, DDOS. No hay protección *Cloudflare* que permita filtrar y mitigar ataques de DDOS.

- Rationale: La dirección de seguridad de la información contrató a un *ethical hacker* externo y experto en respuesta a incidentes, quien realizó pruebas de *stress* para comprobar la resiliencia de los sistemas de información para calibrar el rango confiable de respuestas a solicitudes con el *Transfer Control Protocol* desde internet (agregar respaldo en Anexo).

<u>Análisis del riesgo</u>

- Frecuencia de ocurrencia: Alta (Mínimo: 8; Más probable: 16; Máximo: 30).

- Rationale: Se utilizó el modelo LENS con cinco expertos que calibren sus opiniones con base en la información de los reportes de violaciones de datos de *IBM Security y Protiviti*, enfocándolo en el tipo de industria y situaciones empresariales similares. Cabe destacar que este informe incluía pérdidas en productividad, respuesta a incidentes, reemplazo de activos, pérdidas de ventaja competitiva, pérdida de reputación y sanciones legales. El DPD procedió a interpretarlo solamente en el área de la protección de datos personales, utilizando una personalización del modelo FAIR (agregar respaldo en Anexo).

- Impacto: Vulneración temporal de la disponibilidad de los datos personales. El impacto primario es una vulneración del derecho de protección de datos personales; lo cual, puede ocasionar impactos secundarios vulnerando otros derechos y ocasionando pérdidas financieras a los titulares.

- Rationale: El impacto en los derechos y libertades de los titulares fue calibrado por la dirección de Gobernanza de datos de la empresa, con base en el informe recibido por parte de la del CISO de la empresa; en donde se aplicó el modelo LENS con cinco expertos para calibrar el impacto financiero de los potenciales ataques de DDOS. Los valores calibrados fueron: Mínimo: $10 000, Más probable: $40 000, Máximo: $120 000 (agregar respaldo en Anexo).

Evaluación del impacto

Medio (Mínimo: $10 000, Más probable: $40000, Máximo: $120 000).

Tratamiento del riesgo

No hay un plan de respuesta a incidentes en casos de ataques DOS, DDOS. No hay protección *Cloudflare* que permita filtrar y mitigar ataques de DDOS.

- Desarrollar un plan de respuesta a incidentes en casos de ataques DOS, DDOS.
- Implementar protección *Cloudflare* con *firewalls* de aplicaciones web (WAF), que permitan filtrar y mitigar ataques de DDOS.

3.3.2. Vulneración de la seguridad de datos personales / Malware (Ransomware)

Concordancia: Arts. 10 (e), 37 LOPDP.

Identificación del riesgo

¿Qué comunidades de amenaza se pueden vincular al escenario de riesgo?

Cibercriminales, crimen organizado, empleados internos, hackers mercenarios contratados.

¿Qué mecanismos pueden utilizar las comunidades de amenaza?

Utiliza ransomware existente con codificadores y *crypters* personalizadas o *ransomware zero day*. Para ello, pueden utilizar como medio el *phishing* para instalar un troyano que les permita acceder al sistema y elevar privilegios. También pueden aprovechar vulnerabilidades técnicas del software para conseguir acceso y se puede actuar en complicidad con empleados internos.

¿Qué vulnerabilidades organizacionales se han detectado con respecto a este escenario de riesgo?

Falta de capacitación de los empleados. Plan de continuidad de actividades deficiente (*Business Continuity Plan*).

¿Qué vulnerabilidades técnicas se han detectado con respecto a este escenario de riesgo?

Se verificó mediante auditoría que no hay *backups* en un aproximado del 50% de bases de datos personales de la empresa.

¿Qué consecuencias pueden sufrir los titulares de los datos si el riesgo se materializa?

Violación temporal o permanente de la disponibilidad de datos personales. Vulneración del derecho de datos personales y otros derechos y libertades.

- Amenazas: Cibercriminales, crimen organizado, empleados internos, hackers mercenarios contratados.

- Rationale: Se contrató a un especialista externo en inteligencia de amenazas (*threat intelligence*), quien realizó el análisis de adversarios utilizando matrices (agregar respaldo en Anexo).

- Vulnerabilidades: Falta de capacitación de los empleados. Plan de continuidad de actividad (*Business Continuity Plan*) que no incluye las métricas del *Recovery Time Objective* (RTO) y el *Recovery Point Objective* (RPO). Incumplimiento en alrededor del 50% de *backups*, los cuales deben estar en tres locaciones diferentes.

- Rationale: Se contrató a un equipo *red team* integrado por tres *ethical hackers* y *penetration testers* que consiguieron acceso primeramente con un troyano que incorporaba un *payload* para procesadores Intel 64, un troyano de conexión reversa. A partir de ello, elevaron privilegios aprovechando la vulnerabilidad "ms14_058_track_popup_menu" en un sistema operativo obsoleto Windows 7. Después utilizaron un ransomware personalizado programado en el lenguaje python, simulando un ataque real con una nota de ransomware que pedía 5 Bitcoins por el rescate, en un plazo de 5 días (agregar respaldo en Anexo).

<u>Análisis del riesgo</u>

- Frecuencia de ocurrencia: Baja. (Mínimo: 1; Más probable: 4; Máximo: 20).

- Rationale: Se realizó un análisis histórico. En el año anterior hubo 20 tentativas de ransomware, en donde un ataque pudo consumarse y se perdieron el 50% de datos, incluyendo datos personales de clientes. La empresa pagó el rescate de 2 BitCoin, pero los cibercriminales no devolvieron

la información secuestrada. El CISO calibró el resultado con base en una implementación del modelo FAIR respecto a las pérdidas financieras que ocasiona el ransomware en cuanto a: productividad, respuesta a incidentes, reemplazo de activos, pérdidas de ventaja competitiva, pérdida de reputación y potenciales sanciones legales. La dirección de gobernanza de datos interpretó el informe recibido del CISO, sólo para el ámbito de la protección de derechos y libertades de los titulares (agregar respaldo en Anexo).

- Impacto: Vulneración temporal o definitiva de la disponibilidad de los datos personales. El impacto primario es una vulneración del derecho de protección de datos personales, lo cual puede ocasionar impactos secundarios vulnerando otros derechos y ocasionando pérdidas financieras a los titulares.

- Rationale: Alto. El impacto en los derechos y libertades de los titulares fue calibrado por la dirección de Gobernanza de datos de la empresa, con base al informe recibido por parte de la del CISO de la empresa. Los valores de entrada calibrados fueron: Mínimo: $130 000, Más probable: $600 000, Máximo: $1 300 000 (agregar respaldo en Anexo).

Evaluación del impacto

Alto (Mínimo: $130 000, Más probable: $600 000, Máximo: $1 300 000).

Tratamiento del riesgo

- Realizar programas de capacitación a empleados.
- Mejorar el Plan de continuidad de actividades, incorporando las métricas de *Recovery Time Objective* y *Recovery Point Objective*, cuidando que los *backups* sean periódicos. Implementar un sistema de backups incremental que incluya todos los datos personales.
- Cifrar los archivos de *backup* que se guarden en dispositivos de almacenamiento externo o en la nube.
- Implementar un antivirus premium.

[AGREGAR LOS ESCENARIOS DE RIESGO DE DISPONIBILIDAD DE DATOS NECESARIOS ...]

www.spdp.gob.ec

Superintendencia de Protección de Datos Personales

Av. Amazonas y Unión Nacional de Periodistas.
Plataforma Gubernamental de Gestión Financiera.
Bloque Amarillo, piso 5 (externo).
Quito – Ecuador