Metodología para la Gestión de Riesgos

VERSIÓN 1
Enero 2025

inai

Norma Mexicana en Igualdad Laboral y No Discriminación

DIRECTORIO

Adrián Alcalá Méndez
Comisionado Presidente

Norma Julieta Del Río Venegas
Comisionada

Blanca Lilia Ibarra Cadena
Comisionada

Josefina Román Vergara
Comisionada

Av. Insurgentes Sur 3211, Col. Insurgentes Cuicuilco, C.P. 04530, Alcaldía Coyoacán, Ciudad de México.

Edición Enero de 2025.

Tabla de contenido

Presentación

El presente documento muestra una metodología que puede ser adoptada para la gestión de los riesgos que parte de las directrices generales contenidas en el esquema de un proceso de gestión de riesgos conforme al estándar internacional ISO 31000:2018 Gestión de Riesgos-Directrices[1], para que cualquier tipo de organización, sin importar el sector al que pertenezca, o, el tamaño, pueda considerar el riesgo como elemento de trabajo en las dimensiones de confidencialidad, integridad y disponibilidad en los soportes en donde se almacenan los datos personales.

En ese orden de ideas, esta metodología identifica las definiciones relacionadas con la gestión de riesgos, que permitirán comprender cada uno de los aspectos que componen a la gestión de riesgos de manera integral.

Posteriormente, incluye la descripción de las actividades relacionadas con la gestión del riesgo a fin de definir una serie de pasos a seguir dentro de un ciclo de mejora continua que tiene compatibilidad con un sistema de gestión de seguridad de la información.

En suma, esta metodología proporciona una base común para el personal con y sin experiencia, técnicos y no técnicos que usan el proceso de gestión de riesgos en sus sistemas de tratamiento de datos personales y se encuentran realizando su documento de seguridad.

[1] Disponible en: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es consultado el 04 de noviembre de 2024.

I. La evolución del concepto de Riesgo

El concepto de riesgo parte en sus orígenes de manera incierta, sin embargo, desde el punto de vista etimológico, es posible identificarlo desde el siglo XI, derivado de la palabra en latín *risicare*[2] que alude a peligro, así como la palabra francesa *risque* y la palabra italiana *rischio,* palabras que retoman el termino árabe *rizq*[3] que significa lo que depara la providencia, alineándolo con los términos de prudencia, seguridad y con la posibilidad que tiene el hombre de elegir su destino.

En esa evolución, el concepto de riesgo, en el siglo XI identifica su origen empírico, siendo hasta el siglo XVII con las matemáticas asociadas y con los juegos de azar, que se hace referencia particularmente a la combinación de la probabilidad y la magnitud de pérdidas y ganancias potenciales, con ello, se encuentra una definición más formal.

Asimismo, con el paso de los años es posible identificar la adaptación de este término, en el siglo XVIII, el riesgo, fue visto como un concepto neutral, considerando las pérdidas y ganancias, y fue empleado en la marina. En el siglo XIX, el riesgo surgió en el estudio de la economía y para el siglo XX se asoció a una connotación negativa al referirse a los peligros en la ciencia y tecnología.

Es así como, el diccionario de la Real Academia Española de 1992 definió el riesgo como la contingencia o proximidad de un daño; en donde contingencia se define como la posibilidad de que algo suceda o no suceda, especialmente un problema que se plantea de manera no prevista.

Por lo tanto, es posible identificar que el concepto de riesgo, alude muchas áreas y abarca otros términos, siendo una necesidad generar parámetros que permitan asignar un valor al riesgo, estandarizando su definición y alinearla a acciones donde el concepto tenga un mayor significado, nos referimos específicamente al tema de seguridad de la información; el cual, conforme a la Organización Internacional de Normalización (ISO)[4], estandariza el concepto de riesgo como la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos, por lo tanto se causa daño a la organización, siendo este el concepto que será nuestro marco de referencia en esta metodología.

[2] Disponible en: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_risicare.html, consultado el 04 de noviembre de 2024.
[3] Disponible en: https://rua.ua.es/dspace/bitstream/10045/17898/1/Sharq%20Al-Andalus_06_14.pdf, consultado el 04 de noviembre de 2024.
[4] Disponible en: https://www.iso27000.es/glosario.html, consultado el 04 de noviembre de 2024.

II. Tópicos entorno al concepto de riesgo

Ahora bien, conociendo el origen de la definición de riesgos, se partirá de varios tópicos que son necesarios para comprender el riesgo, debido a que este concepto no puede definirse sin otros conceptos tales como activo, amenaza, vulnerabilidad, posibilidad y daño.

Imagen 1 – *conceptos clave para definir el riesgo (elaboración propia)*

Es posible definir un riesgo a partir de la interacción de amenazas que atacan una o diversas vulnerabilidades de un activo o grupo de activos en perjuicio de la organización

A partir del esquema anterior, se define cada tópico involucrado en el concepto de riesgo:

- Activo

Se define al activo como cualquier elemento que representa un valor para una organización. Según la Real Academia Española, «valor» se define como: a) grado de utilidad o aptitud de las cosas para satisfacer las necesidades o proporcionar bienestar o deleite, y b) cualidad de las cosas, en virtud de la cual se da por poseerlas cierta suma de dinero o equivalente.

- Amenaza

Es la circunstancia o evento con la capacidad de causar daño a una organización.

- Vulnerabilidad

Se define como, la falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

- Impacto

Es una medida del grado de daño a los activos o cambio adverso en el nivel de objetivos alcanzados por una organización.

- Posibilidad o probabilidad

Es la circunstancia u ocasión de que una cosa exista, ocurra o pueda realizarse.

Ahora bien, estos tópicos que se encuentran entorno al concepto de riesgo se interrelacionan como se señala en el siguiente esquema:

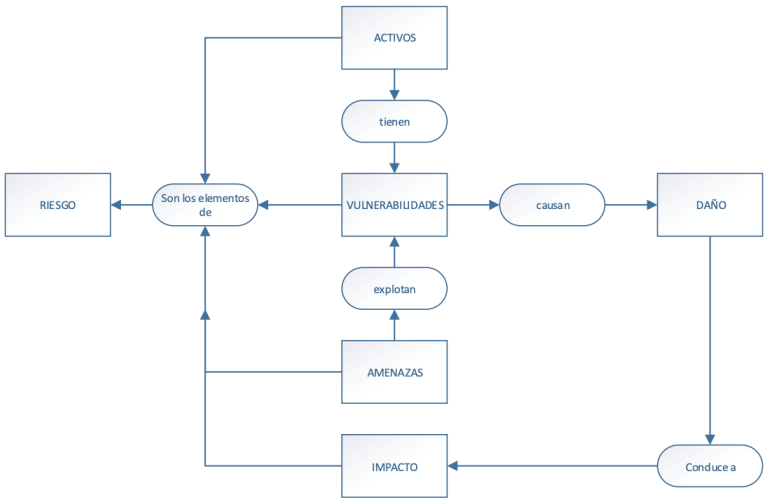


Imagen 2 – conceptos de riesgo relacionados (elaboración propia)

Este diagrama se explica de la siguiente manera: para que un riesgo exista, es necesario que se dé una interacción de diversos elementos, primero, se deben conocer los elementos físicos y/o digitales en que se tratan datos personales y que conforman un sistema de tratamiento, los cuales tienen información diversa y pueden encontrarse de manera física y/o digital, estos activos siempre están expuestos a amenazas, las cuales aprovechan una o varias vulnerabilidades propias de los activos causando un daño o cambio en el activo.

De esta manera se puede establecer que los activos, las amenazas y las vulnerabilidades se combinan para generar riesgos. Cuando un riesgo se materializa, ocurre un incidente de seguridad, el cual se traduce en una violación a las medidas de seguridad.

III. El concepto de riesgo vinculado con la seguridad de la información

Ahora que tenemos el entorno de los elementos que comprenden el riesgo, es necesario darles un enfoque para darles un uso, es decir, darle sentido a como se va a utilizar el concepto de riesgo, destacando que dicho concepto es un elemento inmerso en lo que se denomina seguridad de la información.

Seguridad de la información

La seguridad de la información establece que se debe **proteger la información y los sistemas de información ante un acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizados** a través de la **implementación de medidas de seguridad técnicas, organizativas y físicas** que permitan a la organización asegurar la **Confidencialidad, Integridad y Disponibilidad** de la información.

En ese sentido, la seguridad de la información se enfoca en preservar en todo momento tres propiedades de la información:

- **Disponibilidad:** propiedad de que la información pueda ser utilizada cuando se necesite en cualquier instante de tiempo.
- **Integridad:** propiedad que busca mantener las características de completitud y corrección de los datos, es decir, que la información no sea manipulada, corrompida o incompleta.
- **Confidencialidad:** propiedad de que la información que asegura que solo los usuarios con acceso autorizado puedan acceder a la información.

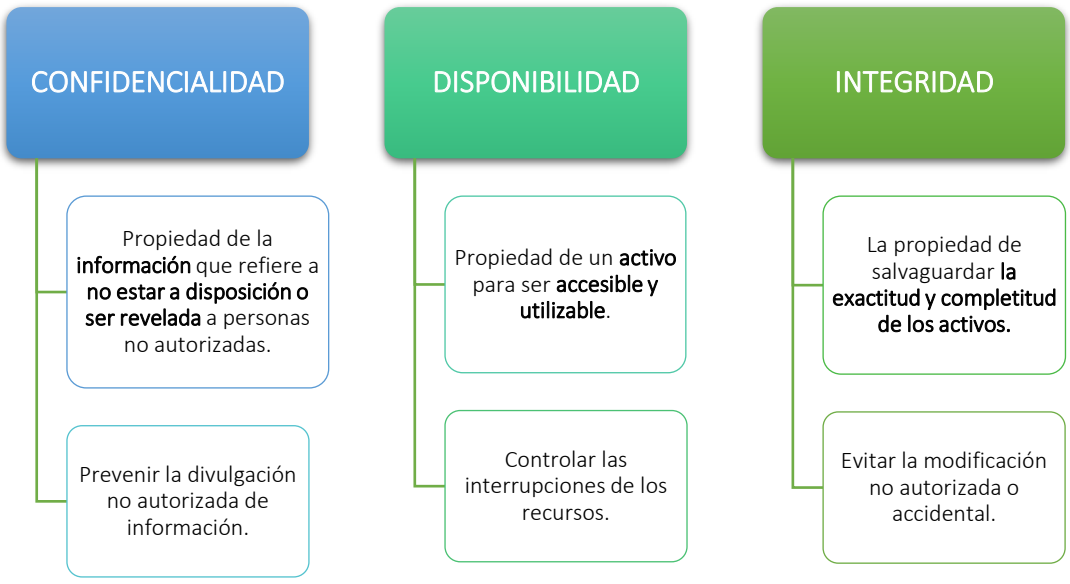


Imagen 3 – *definiciones de las propiedades de la información (elaboración propia)*

Es importante señalar que la propiedad de la información relativa a la propiedad de confidencialidad, no debe ser confundida con el deber de confidencialidad que habla sobre la secrecía que deben guardar todos aquellos que intervienen en el tratamiento de la información, sino que, la confidencialidad o secreto para el análisis como propiedad de la información, está enfocado en proteger los datos personales para evitar filtraciones, daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado que expongan éstos a ser conocidos o revelados a personas no autorizadas.

Para asegurar las propiedades de confidencialidad, integridad y disponibilidad de los datos personales, se deben establecer y mantener a partir de la integración de medidas de seguridad, es decir, del conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger la información, particularmente, datos personales.

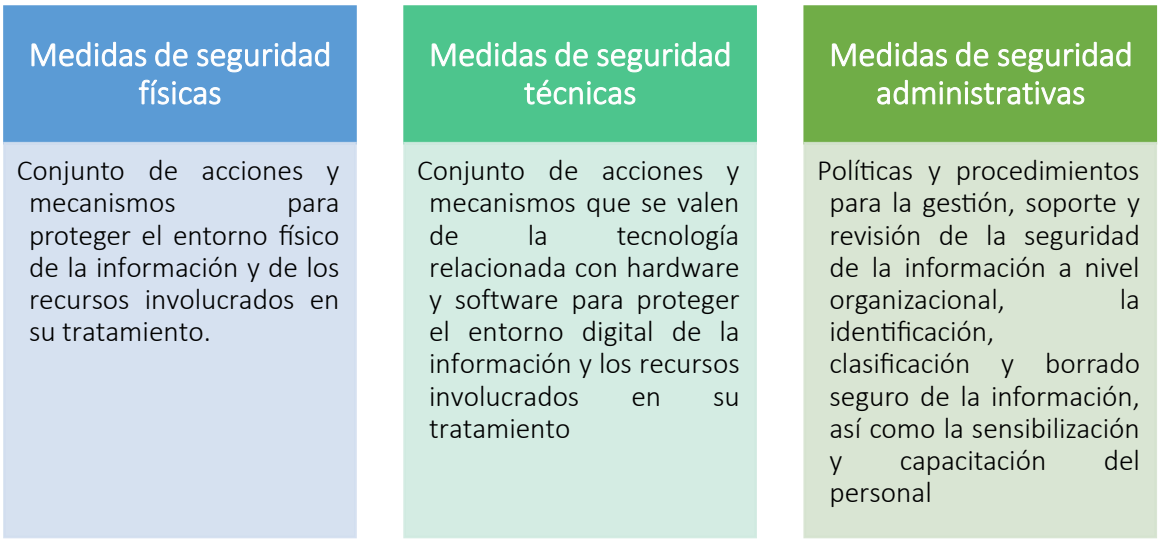


Imagen 4 – *definiciones de medidas de seguridad (elaboración propia)*

En ese sentido, una vez que se tienen la identificación de los conceptos de seguridad de la información y el concepto de riesgo, se puede establecer la conexión que existe entre estos, debido a que, se puede identificar al riesgo como un parámetro que permitirá conocer el entorno de seguridad, es decir, el foco de análisis se centrará en conocer, analizar, calificar y tratar los riesgos a fin de contar con métricas que permitan establecer controles para evitar situaciones en las que la información pueda ser comprometida.

Aunado a ello, realizado el análisis correspondiente, la persona que realice este, contará con elementos para la toma de decisiones en función de los resultados a los que puede someter la efectividad de las medidas de seguridad.

Es así que, para poder realizar esta tarea de integrar el riesgo a la seguridad, es necesario establecer actividades sistemáticas a manera de pasos o etapas enfocadas en conocer y describir el riesgo y su asociación con la seguridad de la información, por lo que, una vez que sabemos lo que queremos hacer, ahora resulta necesario definir acciones replicables que sean fáciles de entender y de repetir dentro de un ciclo que se pueda hacer las veces que se consideren necesarias con el objetivo de preservar la seguridad de la información.

IV. Metodología

La palabra, como tal, proviene del griego μέθοδος (méthodos)[5], que significa *método*, y el sufijo -logía, que deriva de λόγος (lógos)[6] y traduce *ciencia, estudio, tratado*. De allí que también sea definida como la ciencia del método.

La metodología es una serie de métodos y técnicas de rigor científico que se aplican sistemáticamente durante un proceso de investigación para alcanzar un resultado teóricamente válido. La metodología funciona como el soporte conceptual que rige la manera en que aplicamos los procedimientos en una investigación.

Podemos encontrar metodología en distintas áreas de estudio las cuales buscan ser una solución de problemas aplicando una serie de pasos definidos.

V. Gestión

La palabra gestión proviene del latín *gestĭo*[7], y hace la referencia a la administración de recursos, sea dentro de una institución pública o privada, para alcanzar los objetivos propuestos por la misma. Dicho de otra manera, la gestión se refiere a todas aquellas actividades realizadas con la finalidad de resolver una situación o materializar un proyecto.

Es por lo que, la gestión debe ser una actividad que se puede sistematizar, es decir, organizarlo a partir de procedimientos repetibles, en ese sentido, estaríamos hablando de un sistema de gestión que, para el caso que nos ocupa estaría centrado en la gestión del riesgo.

En las normas ISO, el sistema de gestión se define como "un conjunto de elementos y actividades relacionados y coordinados que interactúan entre sí, y que, a partir de Políticas y Objetivos establecidos, dirigen y controlan la organización con el fin de lograr dichas metas.

De igual manera, establece que es posible parametrizar la gestión del riesgo dentro de un sistema enfocado en mantener una mejora constante en todo momento, es posible adoptar la metodología clásica que consiste en el ciclo Planear, Hacer, Verificar y Actuar (PHVA), conocida como ciclo Deming[8] (Deming, 1982) o ciclo Shewhart de mejora continua (Laurett

[5] Disponible en: https://dle.rae.es/método#:~:text=μέθοδος%20méthodos.,decir%20o%20hacer%20con%20orden, , consultado el 04 de noviembre de 2024.
[6] Disponible en: https://www.filosofia.org/enc/ros/logos.htm#:~:text=(del%20griego%20λόγος%3A%20palabra%2C,es%20eterno%2C%20universal%20y%20necesario, consultado el 04 de noviembre de 2024.
[7] Disponible en: https://dle.rae.es/gestión, consultado el 04 de noviembre de 2024.
[8] Disponible en: https://qualitasbiblo.wordpress.com/wp-content/uploads/2013/01/sistemas-de-gestic3b3n-integrados-lrqa.pdf, pagina 2, consultado el 04 de noviembre de 2024.

y Mendes, 2019), que provee un medio para la implementación sistemática de un sistema de garantía de calidad, a partir de un sistema de planificación inicial.

En ese orden de ideas, al partir de un esquema sistematizado para desarrollar la gestión de riesgos no financieros que adoptan diversas metodologías de gestión, se puede encontrar una solución efectiva a la identificación del riesgo, en específico, la adaptación a partir de un enfoque de riesgo que se centra en proteger los datos personales, donde se pueden definir actividades específicas a realizar para cada fase que permitan al interesado replicarla basándose en cuatro fases definidas:

- Planear: Fase inicial que sienta las bases para las acciones posteriores, siempre orientadas a verificar la adecuación, idoneidad y promover la mejora continua.
- Hacer: Fase en la que se interpretan los resultados obtenidos de la planificación a fin de describir acciones para tratar el riesgo tomando en cuenta factores humanos, tecnológicos, administrativos y financieros.
- Verificar: Fase de monitoreo en donde se pretende obtener valores que definan si las decisiones de la fase de tratamiento tienen una afectación en los resultados obtenidos de la planeación.
- Actuar: Fase en la que se reinterpretan los resultados del monitoreo y se mejoran condiciones de tratamiento de riesgos.

Imagen 5 – esquema general ciclo de Deming (imagen libre)

VI. Metodología de gestión del riesgo

Los estudios de riesgo son vistos como una evaluación compleja que debe ser abordada mediante el análisis transversal para poder obtener una visión integral de la problemática de una actividad bajo estudio.

La gestión de riesgos permitirá mantener un entorno controlado, minimizando los riesgos hasta niveles aceptables. Es decir, el enfoque es la reducción de niveles mediante el despliegue de medidas de seguridad, esto es, se mantienen en niveles con los que se puede convivir, más nunca se erradican los riesgos con estos procesos.

El objetivo se alinea con la gestión de la información al orientarlo a proteger la información de la organización, siempre que se consideren las propiedades de la seguridad de la información, es decir, la confidencialidad, la disponibilidad y la integridad.

Es así como, una vez que hemos identificado conceptos clave del concepto de riesgo y que hemos alineado esta actividad con la gestión de la seguridad de la información, es necesario comenzar a definir las actividades que se deben realizar para conocer, calificar y tratar el riesgo, para este caso en particular, el enfoque se centrara en describir como activo principal a los datos personales.

En suma, antes de desarrollar cada contenido, es necesario aclarar que muchos de los elementos contenidos en este documento son retomados de la bibliografía publicada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) en el tema de seguridad de la información orientado a datos personales, la cual incluye documentos como la Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales para el sector público[9], la Guía de apoyo para la elaboración del documento de seguridad[10] y las Recomendaciones para reconocer las principales amenazas a los datos personales a partir de la valoración del riesgo[11], documentos que tienen elementos encaminados en describir puntos clave para realizar un análisis de riesgos, actividades que toman como marco de referencia el estándar internacional ISO 31000:2018: Gestión de riesgos[12], estándar internacional que proporciona principios y directrices para una gestión eficaz de riesgos.

Por lo que, en armonía con dichos documentos, el presente documento desglosa y detalla actividades para el análisis de riesgos abonando y otorgando elementos para mejorar esta actividad, de esta manera, si ha realizado trabajos tomando como apoyo alguno de los documentos referidos, este documento fortalece el contenido de los documentos

[9] Para su consulta en: https://home.inai.org.mx//wp-content/documentos/DocumentosSectorPublico/GuiaSGSDP_sectorpublico.pdf
[10] Para su consulta en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/Guia-apoyo-DS.pdf
[11] Para su consulta en: https://home.inai.org.mx/wp-content/uploads/AmenazasDP.pdf
[12] Para su consulta en: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

mencionados y servirá de complemento para sustentar actividades para realizar la gestión del riesgo.

Gestión de riesgos

Los estándares establecen directrices que homologan la ejecución de tareas, por la naturaleza y las particularidades de cada sistema de tratamiento, no es posible definir actividad por actividad, pues cada sistema es diferente entre sí, esta es la razón por la que surge la necesidad de contar con un documento que a partir de dichas directrices establezca un camino sobre cómo se puede realizar cada actividad definida en cada fase que comprende la gestión de riesgos, otorgando al lector elementos que le permitan tomar una decisión respecto a la ejecución de tareas para gestionar el riesgo.

Partiendo de lo anterior, la directriz general utilizada para desarrollar esta metodología es el esquema general de la gestión de riesgos del estándar ISO 31000:2018: Gestión de riesgos, el cual define en un ciclo de mejora continua la gestión de riesgos en 6 etapas interrelacionadas:

- Establecer alcance, contexto y criterios de riesgos
- Evaluación de riesgos:
    - Identificación de riesgo
    - Análisis de riesgo
    - Valoración de riesgo
- Tratamiento de riesgos
- Registro e informe
- Comunicación y consulta
- Seguimiento y revisión

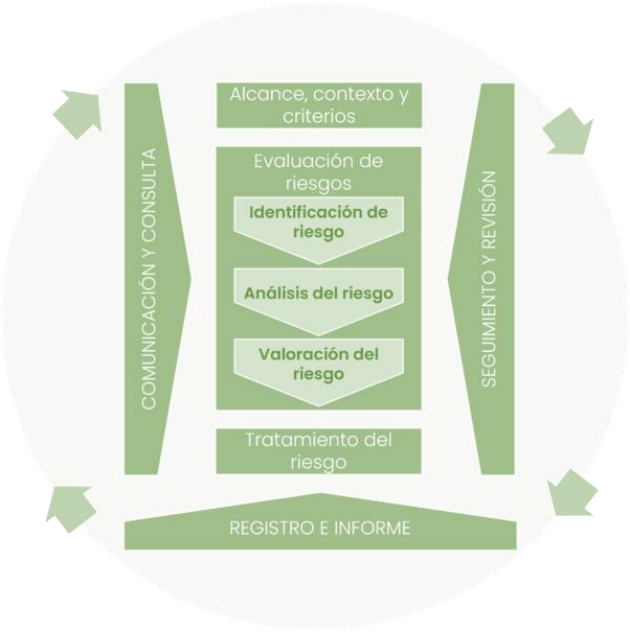


Imagen 6 – Esquema general gestión de riesgos (imagen dl estándar ISO 31000)

Si vemos estas actividades dentro de un ciclo de mejor continua, estaríamos describiendo un sistema de gestión formalizado en cuatro etapas cíclicas, donde todo gira alrededor del riesgo, es decir, alrededor de identificar, describir, conocer y finalmente gestionar el riesgo a partir de actividades definidas y descritas de la siguiente manera:

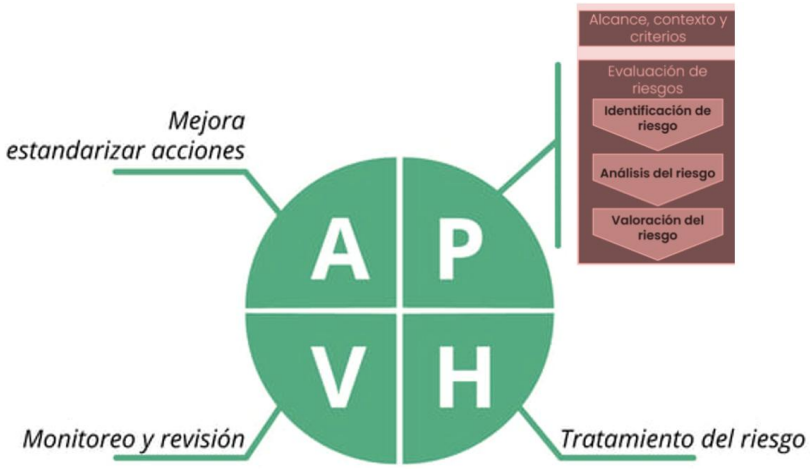


Imagen 6 – Descripción de la gestión de riesgos dentro del ciclo de Deming (elaboración propia)

La adopción de la presente metodología no elimina el riesgo ya que su objetivo principal es gestionar el riesgo, es decir, llevar el riesgo a un nivel aceptable para la organización.

Esquema general de la metodología

Esta metodología para la gestión de riesgos retoma la estructura que presenta el estándar ISO 31000:2018: Gestión de riesgos, realizando adecuaciones que permitirán identificar qué deberá realizar en cada fase, esta metodología se puede resumir en el siguiente gráfico:

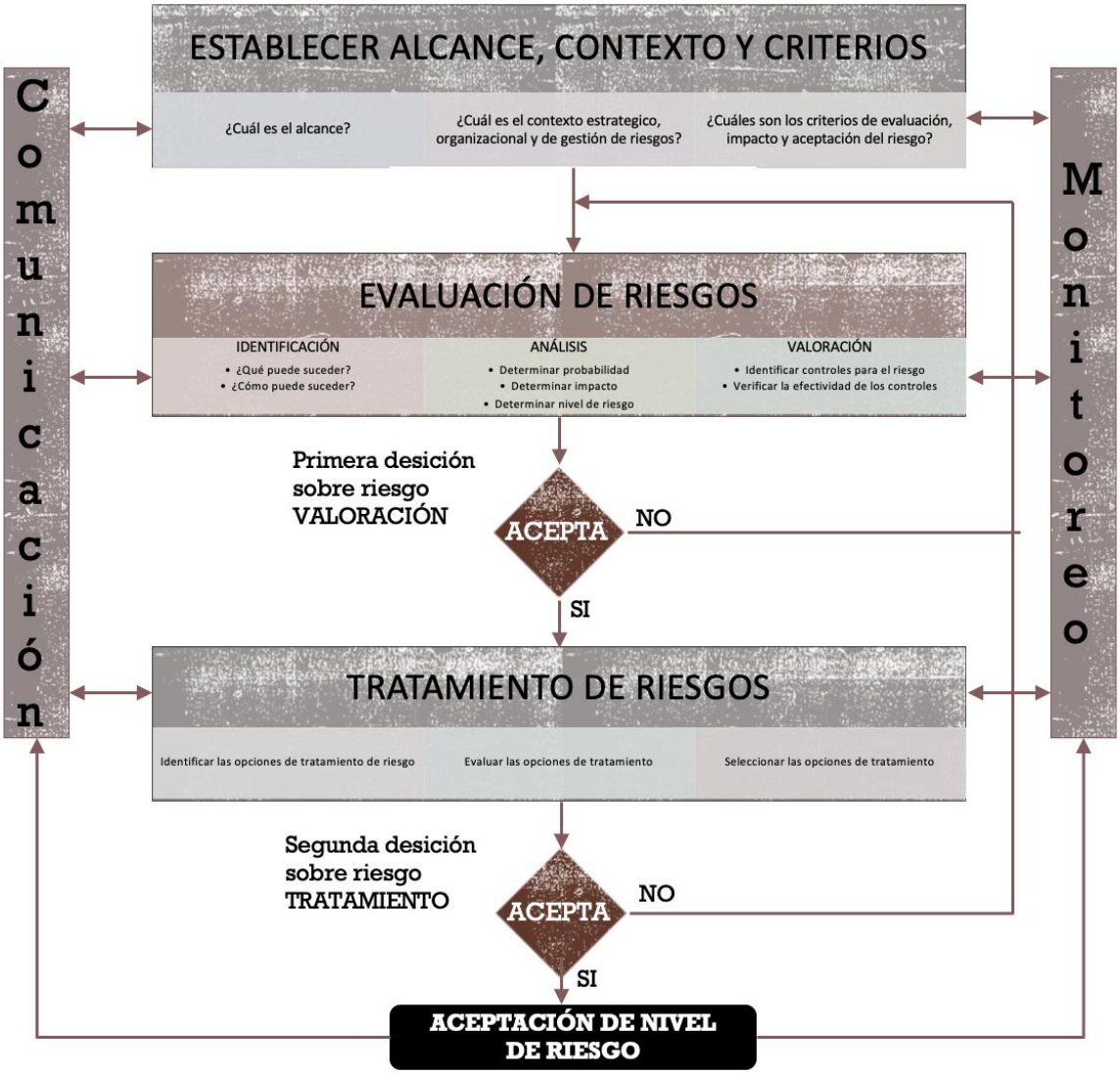


Imagen 8 – Diagrama General de la metodología para la gestión del riesgo

Si bien ya se ha definido una directriz general, antes de desarrollar cada una de las actividades contempladas en el esquema del ciclo de gestión, es necesario realizar una actividad previa.

Actividad previa Definición de la valoración y escala por tipo de datos

Para darle valor a algo es necesario definir una escala de medida, a veces se puede reflejar en valores numéricos, por ejemplo, el consumo de gasolina, la temperatura de un refrigerador, el nivel de un tanque estacionario; y a veces de manera no numérica, por ejemplo, el nivel de cumplimiento, la percepción de seguridad, la actitud de los trabajadores, elementos que se describen a manera de frases, expresiones positivas o expresiones negativas.

En esta actividad se debe definir cómo se va a realizar la valoración e interpretación de resultados, partiendo de las dos valoraciones mencionadas, las cuales reciben el nombre de valoración de datos cuantitativa y valoración cualitativa, por lo que, deberá decidir cuál es la que más le conviene en función del análisis de la siguiente información:

- Valoración de datos cualitativos

Los datos cualitativos se expresan en forma de palabras o textos que ayudan a comprender ciertas acciones que no son cuantificables, es decir, pueden expresar características, cualidades o atributos, por lo que este tipo de datos tienen como principal característica que no se pueden medir, ni expresarse con número, deben ser interpretados.

Esta presentación de datos suele utilizar la Escala de Likert[13], para medir algo cualitativo, por ejemplo: acuerdo, frecuencia, importancia y probabilidad.

Los datos cualitativos son utilizados principalmente como el primer acercamiento ya que aporta información acerca de la existencia de una realidad en la que están involucrados los elementos que se van a analizar.

En ese sentido, usted será libre de definir una escala de valoración tan detallada como lo requiera, recuerde que entre mayor detalle tenga su escala de valoración, tendrá datos más específicos sobre lo que requiere conocer, a continuación, se presentan de manera enunciativa más no limitativa ejemplos de escalas que puede utilizar:

Probabilidad	Importancia	Frecuencia	Acuerdo
Poco probable	Baja	Poco frecuente	En desacuerdo

[13] Disponible para su consulta en: https://www.insst.es/documents/94886/195574/NTP+15+Construcción+de+una+escala+de+actitudes+tipo+Likert.pdf/f5eee915-e80d-4c50-8f9f-5783e64f4449, consultado el 04 de noviembre de 2024

Probable	Media	Regularmente	Conforme
Bastante probable	Alta	Frecuentemente	De acuerdo

Ejemplo de escalas cualitativas (elaboración propia)

- **Valoración de datos cuantitativos**

Los datos cuantitativos consisten en cualquier información cuantificable que pueda utilizarse para realizar cálculos matemáticos y análisis estadísticos, de forma que puedan tomarse decisiones en la vida real basadas en estas derivaciones matemáticas.

Todo lo que se puede medir y contar, decimos que se puede cuantificar. El concepto datos cuantitativos hace referencia precisamente a eso, a la información tangible, la que es obtenida mediante algún método de investigación que sustenta el valor matemático presentado.

La manera de cuantificar los datos obtenidos da la pauta de hacia qué rumbo dirigirse, de ahí la importancia de su correcto análisis para poder demostrar si se está realizando una acción correcta o no.

Como se mencionó anteriormente, usted será libre de definir una escala de valoración tan detallada como lo requiera, recuerde que para este tipo de escala le permite presentar un mayor detalle y precisión de datos pues su escala puede incluir resultados de análisis numéricos, por lo que, podrá obtener resultados más específicos, a continuación, se presentan de manera enunciativa más no limitativa ejemplos de escalas que puede utilizar:

Números fijos	Escalas	Rangos
1	1/10	1-3
2	5/10	4-6
3	10/10	7-9

Ejemplo de escalas cuantitativas (elaboración propia)

- **Valoración de datos combinados**

Ahora bien, además de hacer valoraciones de datos cualitativas y cuantitativas, se puede realizar valoraciones de datos, de forma combinada, que se refieren a la combinación entre la cuantitativa y la cualitativa, que asocia resultados del análisis de la información y se puede ejemplificar de la siguiente manera:

Combinación 1	Combinación 2
1 – bajo	1-3 – bajo
2 – moderado	4-6 – medio
3 - serio	7-9 - alto

Ejemplo de escalas combinadas (elaboración propia)

Una vez definido que tipo de valoración y escala será la que utilizará para los elementos que requieran una valoración durante la ejecución de las actividades relacionados con la gestión del riesgo, se encuentra en condiciones para dar pie a las siguientes fases:

FASE 1 - PLANEAR

Actividad 1. Establecer alcance, contexto y criterios de riesgo

Desde el punto de vista de la seguridad de la información, se deben establecer los objetivos de seguridad, como pueden ser de manera enunciativa, más no limitativa asegurar la continuidad de los negocios, minimizar el daño comercial, maximizar el reembolso de las inversiones y oportunidades comerciales y; en este caso en particular cumplir con el deber de seguridad para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

Por lo que, al definir el objetivo de la gestión de riesgos, es necesario determinar cómo establecer el alcance y contexto.

Alcance

El alcance se refiere a la forma en que se describen los límites del proyecto, su cobertura, sus resultados y sus entregables. En esta etapa se debe responder a la pregunta *¿hasta dónde se quiere llegar con la gestión de riesgos?,* por lo que, para contestarla se debe determinar el propósito de la gestión del riesgo, identificando los limites dentro de la gestión del riesgo, su cobertura, sus resultados y sus entregables. Al definir el alcance, se debe ser claro en su importancia, para ser comprendido por el equipo y la dependencia o entidad.

Al definir el alcance debería considerar al menos la siguiente información:

- Recursos financieros disponibles
- Recursos humanos disponibles
- Recursos tecnológicos disponibles
- Cumplimiento normativo

Se debe hacer énfasis en el cumplimiento normativo al identificar que la gestión del riesgo debe considerar que lo que se está integrando a la valoración es el cumplimiento normativo en materia de protección de datos personales, por lo que, los riesgos que se están trabajando son riesgos que afectan un derecho humano, que la materialización de dicho riesgo puede afectar a las personas titulares de datos

Con el alcance deberá garantizar que todos los activos relevantes se toman en consideración y que se tiene un conocimiento respecto a los elementos que intervendrán al momento de tomar decisiones sobre el riesgo, identificando el enfoque que deberá tomar para cada actividad a realizar en función de los resultados obtenidos.

Contexto

Es esencial que la gestión de riesgos sea congruente con el alcance definido, es decir, que el contexto de aplicación parta del objetivo que se quiere cumplir, lo que permitirá integrar armónicamente los elementos alrededor de su aplicación.

El contexto debe contemplar a las Unidades Administrativas, su relación con el entorno. Por ello hay que definir el marco de trabajo, teniendo en cuenta a nivel interno la cultura, los recursos económicos y humanos, así como los procesos y los objetivos sustantivos y valores de la entidad.

En esta etapa se debe responder a la pregunta *¿cuál es el contexto estratégico, organizacional y de gestión de riesgos?,* por lo que, para contestarla, siendo necesario tener claridad del entorno de la gestión del riesgo, precisando como se desenvolverá, qué procesos involucrará, cual es el flujo de los elementos que intervienen y cualquier otra información que permita identificar el objetivo de la ejecución de la gestión del riesgo, destacando los parámetros y condicionantes tanto externos como internos que permitirán tener un encuadre respecto a los pasos a seguir para gestionar los riesgos.

Criterios de impacto, evaluación y aceptación de riesgo

Es en esta etapa se deben considerar diversos aspectos tales como el valor estratégico del tratamiento de la información, la criticidad de los activos involucrados en el tratamiento de la información, cumplimiento legal y los elementos de confidencialidad, disponibilidad e integridad, para esta metodología en específico, respecto a la evaluación, la prioridad del tratamiento de riesgo se centra en definir a los datos personales como activo de información o activo principal, destacando el derecho a la protección de datos personales como un derecho fundamental, es así que, debe analizarse el impacto en términos del daño que genera una vulneración en los activos y operación de la entidad, el cual se traslada a las personas titulares de los datos personales afectándolas.

Respecto al impacto, es recomendable especificar pautas centradas en identificar las consecuencias que resultarían si los riesgos identificados llegan a materializarse, en un análisis general se analizaría la afectación a la organización o al sujeto obligado, en sus recursos y su reputación, que si bien importa y afecta, no es el fin último y propósito de esta metodología de gestión de riesgos, por lo que, al valorarse el impacto a los datos personales, tomando en consideración a las personas titulares, deben considerarse, por ejemplo, sin ser este limitativo:

I. Daños o riesgos físicos en su persona e integridad;
II. Daños a su salud física o mental;
III. Discriminación o alguna vulneración de sus derechos fundamentales;
IV. Daño moral;
V. Daño patrimonial.

Es así como, para esta metodología el impacto se centra a analizar los riesgos a los que se enfrentan los datos personales vistos como el activo de información, por lo que, el impacto deberá valorar las potenciales consecuencias a las que se enfrentarían los titulares en caso de que sus datos personales sufran daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado.

En este punto deberá fijarse el criterio sobre el Nivel de Riesgo Aceptable (NRA). El cual se refiere al nivel en una escala cuantitativa y cualitativa que será el nivel máximo de riesgo para aceptar dentro de la entidad de acuerdo con los objetivos definidos, es decir, cuál será el valor máximo de tolerancia al riesgo con el que se puede trabajar.

Por lo que, llegamos al punto en el que surge la necesidad de definir una escala para que a partir de esta se identifique plenamente lo que será el nivel de riesgo aceptable, éste se refiere al nivel en una escala cuantitativa y cualitativa que será el nivel máximo de riesgo para aceptar dentro de la entidad. Si lo que se busca es salvaguardar los datos personales para a su vez proteger la vida, integridad, derechos y libertades de las personas titulares, se recomienda que el nivel de riesgo aceptable sea bajo o muy bajo (depende de la escala cuantitativa y cualitativa establecida). Sin embargo, en caso de que la entidad considerara aceptar un riesgo mayor —por cuestiones del contexto de la entidad, de los recursos humanos, administrativos y económicos—, es decir medio o alto (no se recomienda en ningún caso aceptar uno muy alto), deberá ser acordado y aceptado.

NIVEL DE RIESGO	ACCIÓN REQUERIDA
ALTO	Inaceptable: acciones deben tomarse inmediatamente
MEDIO	Razonablemente aceptable: acciones requeridas y que deben tomarse en plazo razonable
BAJO	Aceptable: no se requieren acciones de inmediato

Imagen 9 – *Ejemplo de escala de nivel de riesgo (elaboración propia)*

FASE 1- PLANEAR

Actividad 2 – Identificación de activos

Primero es importante definir el concepto de activo, el cual, de acuerdo con la norma ISO/IEC 27000:2013[14] se puede definir como todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección.

Partiendo de dicha definición, se puede entender a un activo como cualquier elemento que tiene un valor para la organización o entidad, para sus operaciones y para la continuidad de actividades o negocios, distinguiéndolo en dos clases de activos:

Activos de información o primarios	Activos de apoyo o secundarios
Corresponden a la esencia de la entidad o sujeto obligado: • Información relativa a los datos personales; • Información de procesos del negocio, en los que interviene el flujo de datos personales, actividades involucradas en el tratamiento de éstos;	Corresponden a los elementos en los cuales residen los activos de información, los cuales pueden ser de manera enunciativa más no limitativa: • Hardware (elementos tangibles, como lo son equipos de procesamiento de datos, periféricos y medios de comunicación • Software (elementos intangibles, como lo son el sistema operativo, servicio, software de aplicación) • Redes y telecomunicaciones • Estructura organizacional; • Infraestructura adicional.
Entendiendo a los datos personales como un activo de información, estos tienen valor para la organización y, en consecuencia, necesitan ser protegidos de manera adecuada.	Para esta metodología el análisis de los riesgos a los que se expondrán los activos primarios se centrará en describir los escenarios en los que los activos secundarios pueden comprometerse, identificando dos tipos de formato de activos: • Activos en formato físico • Activos en formato digital

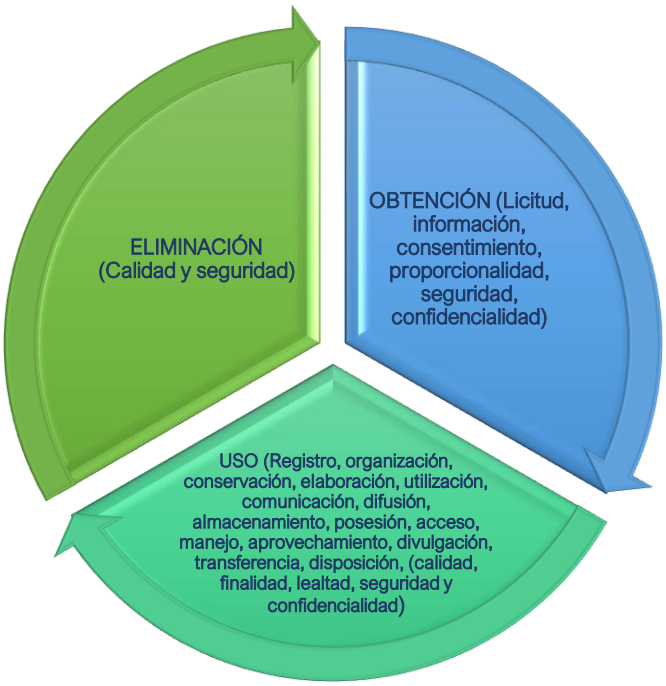
Tabla de elaboración propia

Al realizar el análisis de riesgos, resulta complicado desarrollar dicho análisis en los activos primarios o de información, pues, en este caso en particular, los datos personales como activo de información pueden existir en muchas formas; puede ser de forma escrita, impresa, electrónica, pueden ser comunicadas por correo o usando medios electrónicos o incluso hablado en una conversación, razón por la que la metodología se centra en analizar los

[14] Disponible en: https://www.iso27000.es/glosario.html, consultado el 04 de noviembre de 2024.

activos de apoyo, ya que, al enfocar los esfuerzos de proteger los elementos en donde se aloja la información, las medidas de seguridad alrededor de dichos activos se traslada a los activos de información (datos personales).

Partiendo de anterior, resulta relevante enfocarse en la descripción del tratamiento, es decir, todo el proceso de obtención, uso y eliminación de la información a fin de conocer todos los activos que en algún momento alojan información y que serán analizados para determinar el riesgo al que se enfrentan durante su tratamiento, esto permitirá revisar como intervienen los activos con el ciclo de vida de la información.



Esquema del ciclo de vida de los datos (elaboración propia)

Para obtener la información de los activos para cada fase es necesario responderse al menos las siguientes preguntas:

1. OBTENCIÓN

• ¿Cómo se recolectan los datos?	Se debe definir si los datos se obtienen directamente del titular o con algún mecanismo que defina si el repositorio que origina el sistema de tratamiento se encuentra de manera física o digital

2. USO

• ¿Cómo se procesan los datos?	Una vez identificado el formato en el que se van a trabajar los datos personales es

	necesario identificar el proceso de uso a fin de identificar en que equipos se está trabajando la información, como puede ser: • Equipos de cómputo de escritorio • Equipos de cómputo portátiles • Dispositivos móviles • Manejadores de base de datos • Dispositivos de almacenamiento extraíbles • Servicio de almacenamiento en la nube Adicionalmente, es necesario conocer si los dispositivos en los que se procesa la información son propiedad de los Responsables o Encargados a fin de tener descritos los contratos que faculten a un externo a realizar un tratamiento a nombre y cuenta del Responsable.
• ¿Cuántos respaldos de datos se tienen?	Un proceso adicional a la obtención de los datos es la generación de bases de respaldo o la generación de bases controlados para tratamientos parciales o totales del grueso de información que se está procesando, es importante identificar el formato de estos respaldos y a quienes son responsables de su realización.
• ¿Qué comunicaciones de datos se realizan?	El proceso de comunicación de información, particularmente por lo que hace a datos personales se puede definir con lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de la siguiente manera: • Transferencia - Se denomina transferencia de datos personales a la comunicación de datos que realiza el responsable del tratamiento a un tercero, distinto del titular, del mismo responsable (por ejemplo, las comunicaciones al interior de la

	comunicación del responsable, como las que se realizan entre el personal) o del encargado. • Remisión – Al igual que en el caso de la transferencia, la remisión supone una comunicación de datos personales. La diferencia entre ambos conceptos consiste en que, en este caso, dicha comunicación se produce entre un responsable y un encargado del tratamiento. Las remisiones también pueden ser nacionales o internacionales. Sin embargo, ambas están reguladas de la misma forma, como se verá más adelante, pues sin importar que el responsable del tratamiento remita los datos personales a un encargado dentro o fuera del territorio nacional, el primero sigue siendo quien responde por el debido tratamiento de la información personal que comunicó.

3. ELIMINACIÓN

• ¿Cómo se eliminan los datos personales?	Un proceso importante previo a la eliminación de datos es el bloqueo, es decir, impedir el tratamiento de los datos para cualquier finalidad, con excepción de su almacenamiento, hasta el plazo de prescripción correspondiente. La eliminación implica el borrado seguro de la información aplicando algún algoritmo o metodología según el formato en el que se tiene almacenada la información.

La descripción de activos considerando el ciclo de vida de la información permitirá contar con un panorama más amplio de escenarios de vulneración que, en caso de un incidente a la seguridad de la información proporcionará detalles específicos sobre los elementos que resulten comprometidos.

Actividad 3 – Evaluación de los riesgos

Como se ha mencionado, la combinación de la probabilidad de que suceda algo que cause un daño es lo que se conoce como riesgo, algo que se puede calcular con una fórmula matemática. R (riesgo) = P (probabilidad) x I (Impacto).

Sin embargo, podemos encontrar diferentes tipos de riesgos:

- **Riesgo inherente:** Se calcula sin tomar en consideración las medidas de seguridad.
- **Riesgo residual:** Se calcula tomando en cuenta las medidas de seguridad implementadas para gestionar el riesgo identificado.
- **Riesgo aceptable:** Es un concepto que identifica una conformidad por los involucrados sobre el nivel de riesgo obtenido, es decir, cuando se asume formalmente que es posible coexistir con dicho valor de riesgo calculado.

Una vez definido el riesgo y conocidos los tipos de riesgos, es posible plantear la etapa de evaluación de riesgos mediante un proceso que busca determinar lo que podría causar una pérdida potencial y comprender cómo, dónde y por qué puede ocurrir dicha pérdida; identificando activos, amenazas, vulnerabilidades, probabilidad e impacto de la perdida de la confidencialidad, integridad y disponibilidad de la información.

Este proceso se puede dividir en tres subprocesos: a) identificación de riesgos, b) análisis de riesgo y c) valoración de riesgos.

A) Identificación del riesgo

La identificación del riesgo busca una relación de los posibles puntos de peligro. Lo que se identifique será analizado en la siguiente etapa. Lo que no se identifique quedará como riesgo oculto o ignorado.

En ese sentido, en esta etapa se construye un escenario que describe los riesgos a los que se enfrentan los activos que se definieron en el punto anterior, pudiendo partir esta actividad puede dividirse en las siguientes etapas:

Identificación de amenazas

Una amenaza tiene el potencial de dañar un activo y causar una vulneración a la seguridad. Las amenazas pueden ser de origen natural o humano, y pueden ser accidentales o deliberadas y además provenir de adentro o desde afuera del sujeto obligado. Las amenazas deben ser identificadas considerando que algunas pueden afectar a más de un activo al mismo tiempo.

Los propietarios, custodios y usuarios de los activos pueden proporcionar asesoría para identificar y estimar las amenazas relacionadas, por ejemplo, del área de recursos humanos, de los administradores de tecnologías y seguridad, profesionales en seguridad física, del departamento legal, externos como compañías de seguros, gobiernos y autoridades nacionales entre otras fuentes informativas de investigación. Los aspectos culturales también deben ser considerados dentro de las amenazas.

Las amenazas son acciones que ocurren y que pueden causarles daño a nuestros activos, son muy variadas y van cambiando con el tiempo. El desarrollo tecnológico, las comunicaciones y la información van asociadas, al tiempo van unidas al surgimiento de nuevas formas de vulneración de los datos personales, al honor, la intimidad personal y familiar e incluso a la propia imagen.

Por ello, es importante mencionar que, no todas las amenazas afectan a todos los activos, sino que hay cierta relación entre el tipo de activo y lo que le podría ocurrir.
En este paso se recomienda realizar las siguientes actividades:

a) Identificar todas las amenazas relacionadas con cada activo. Las amenazas se pueden identificar utilizando los catálogos definidos para tal fin en las metodologías de gestión de riesgos.
b) Se debe tomar en cuenta que cada activo puede estar relacionado con varias amenazas, y cada amenaza puede estar vinculada con varias vulnerabilidades.
c) La identificación de amenazas será realizada con la ayuda de los propietarios y custodios de los activos.

Las amenazas de acuerdo con las diversas metodologías de gestión de se pueden dividir en diversos grupos, al respecto, de acuerdo con el documento Recomendaciones para reconocer las principales amenazas a los datos personales a partir de la valoración respecto al riesgo[15] publicado por el INAI, se ejemplifican tres grandes grupos con algunos ejemplos de los tipos de amenazas, los cuales son:

- Deliberadas
- Ambientales
- Accidentales

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego accidental	Deliberada, Ambiental
	Daños por agua	Accidental, Deliberada, Ambiental
	Contaminación accidental	Deliberada, Ambiental
	Accidente grave	Accidental, Deliberada, Ambiental

[15] Disponible en: https://home.inai.org.mx/wp-content/uploads/AmenazasDP.pdf, consultado el 04 de noviembre de 2024.

TIPO	AMENAZA	ORIGEN
	Destrucción de equipos o medios	Accidental, Deliberada, Ambiental
	Polvo, corrosión, congelación	Accidental, Deliberada, Ambiental
Eventos naturales	Fenómeno climático	Ambiental
	Fenómeno sísmico	Ambiental
	Fenómeno volcánico	Ambiental
	Fenómeno meteorológico	Ambiental
	Inundación por fuerza natural	Ambiental
Pérdida de servicios esenciales	Fallo del sistema de suministro de agua o aire acondicionado	Deliberada, Ambiental
	Pérdida de suministro de energía	Accidental, Deliberada, Ambiental
	Fallo del equipo de telecomunicaciones	Deliberada, Ambiental
Perturbación debido a radiación	Radiación electromagnética	Accidental, Deliberada, Ambiental
	Radiación termal	Accidental, Deliberada, Ambiental
	Pulsos electromagnéticos	Accidental, Deliberada, Ambiental
Información comprometida	Intercepción de señales de interferencia comprometedoras	Deliberada
	Espionaje remoto	Deliberada
	Escuchar deliberadamente a escondidas	Deliberada
	Robo de soportes o documentos	Deliberada
	Robo de equipo	Deliberada
	Recuperación de medios reciclados o desechados	Deliberada
	Divulgación	Deliberada
	Datos de fuentes no confiables	Deliberada, Ambiental
	Manipulación de hardware	Deliberada
	Manipulación de software	Deliberada, Ambiental
	Detección de posición	Deliberada
Fallas técnicas	Falla en el equipo	Ambiental
	Mal funcionamiento del equipo	Ambiental
	Saturación del sistema de información	Deliberada, Ambiental
	Mal funcionamiento del software	Ambiental
	Incumplimiento del mantenimiento del sistema de información	Deliberada, Ambiental
Acciones no autorizadas	Uso no autorizado de equipos	Deliberada
	Copia fraudulenta de software	Deliberada

TIPO	AMENAZA	ORIGEN
	Uso de software falsificado o copiado	Deliberada, Ambiental
	Corrupción de datos	Deliberada
	Tratamiento ilegal de datos	Deliberada
Compromiso de funciones	Error en uso	Ambiental
	Abuso de derechos	Deliberada, Ambiental
	Forja de derechos	Deliberada
	Negación de acciones	Deliberada
	Incumplimiento de disponibilidad de personal	Accidental, Deliberada, Ambiental

Adicionalmente, puede consultar el árbol de amenazas de la Agencia de la Unión Europea para la Ciberseguridad, ENISA[16], la cual divide las amenazas en cinco tipos:

- Fenómenos naturales y sociales
- Fallas de sistemas
- Errores humanos
- Fallos de terceros
- Acciones maliciosas

Asimismo, en caso de requerir mayores elementos sobre las amenazas en materia de tecnología de la información y comunicaciones, el catálogo de amenazas de la metodología MAGERIT[17], facilita el trabajo de identificación de los activos que puede vulnerar cada amenaza, así como las propiedades o dimensiones que se ven afectadas por la amenaza.

Específicamente cuando hablamos de datos personales, es importante, recordar que el objetivo de la gestión de los riesgos que plantea esta metodología es garantizar la confidencialidad, integridad y disponibilidad de los datos ante cualquier incidente que pueda afectar en estas dimensiones al titular de los datos personales, por lo que, los escenarios de vulneración que al menos deben considerarse son:

- La pérdida total o parcial
- La destrucción
- El robo total o parcial.
- El extravío total o parcial
- La generación de copias no autorizadas
- El uso no autorizado
- El acceso no autorizado

[16] Para su consulta: https://www.enisa.europa.eu/publications/smart-airports/wp2016-1-1-3-threat-taxonomy.pdf
[17] Para su consulta: *https://pilar.ccn-cert.cni.es/index.php/docman/documentos/2-magerit-v3-libro-ii-catalogo-de-elementos/file*

- El tratamiento no autorizado
- El daño a los datos
- La alteración o modificación no autorizada.
- La falsificación
- La divulgación no autorizada

Esto no deja de lado ni quita del análisis a una gran cantidad de amenazas que pueden presentarse y afectar el funcionamiento, operación, continuidad o trabajo cotidiano del sistema de información, lo que ocurre es que estas amenazas en caso de materializarse, pueden llegar a contenerse sin afectar la seguridad de los titulares, por ejemplo, la perdida de suministro eléctrico de un equipo de cómputo que realiza el procesamiento de información, dejaría fuera de funcionamiento un sistema sin perjudicar al titular, afectando directamente la operación del sistema.

Caso contrario, a la ocurrencia de un uso no autorizado, el cual afecta al menos la confidencialidad de los datos, exponiendo la información y pudiendo afectar al titular sin comprometer la continuidad de la operación.

Por eso resulta importante describir las amenazas que afectarían a los titulares, considerando al menos las que se enlistan en este documento y, adicionalmente, incluir el resto de amenazas que no afectan directamente al titular pero que si permiten identificar áreas de oportunidad para mejorar y gestionar riesgos de operación del sistema que se está analizando.

Identificación de las vulnerabilidades a partir de las amenazas identificadas anteriormente

Las vulnerabilidades son debilidades en la seguridad de los activos. Pueden ser identificadas en los siguientes ámbitos:

- Organizacionales;
- De procesos y procedimientos;
- De personal;
- Del ambiente físico;
- De la configuración de sistemas de información;
- Del hardware, software o equipo de comunicación;
- De la relación con prestadores de servicios;
- De la relación con terceros.

Dada la asociación entre conceptos que definen el riesgo que ya se ha establecido, puede decirse que, la presencia de vulnerabilidades no causa daño por sí misma, se requiere de una amenaza que la explote.

Una vulnerabilidad que no se encuentre expuesta a una amenaza identificada, posiblemente no requiera la implementación de un control, pero debe ser reconocida y monitoreada constantemente, o bien cuando surja algún cambio. Por ejemplo, un equipo de cómputo o un archivero con información personal es vulnerable a inundaciones si se encuentra instalado en un sótano por el que pasan las tuberías del servicio de suministro de agua. De modo inverso, la amenaza de inundación se descarta si el equipo de cómputo o el archivero con datos se localiza en la parte más alta del edificio, lejos de tuberías de agua y de amenazas ambientales relacionadas.

Los controles usados incorrectamente o con una mala implementación son causa de vulnerabilidades. Un control puede ser entonces efectivo o no efectivo, dependiendo del contexto en el cual opera. Las vulnerabilidades pueden estar relacionadas con propiedades de los activos, que pueden ser usadas para otros propósitos distintos a los que se habían destinado originalmente. Deben considerarse vulnerabilidades y amenazas provenientes de diferentes fuentes. Por ejemplo, la posibilidad de que un correo electrónico sea interceptado por un atacante, o de que un empleado envié información confidencial a su cuenta personal.

En resumen, para realizar una correcta identificación de vulnerabilidades es necesario asociarla con la lista de amenazas que hemos identificado anteriormente para una correcta descripción del escenario de vulneración, por lo que, el tipo de activo y la identificación de las amenazas a las que se enfrenta el activo son determinantes para realizar la siguiente relación:

- Un activo puede tener al menos una amenaza
- Una amenaza puede tener al menos una vulnerabilidad

Estableciendo que un activo se enfrenta a diversas amenazas y cada una de ellas puede ser explotada por una o diversas vulnerabilidades, por lo que, es necesario realizar una relación de la siguiente manera:

Identificación del tipo de activo	Identificación de la o las amenazas a la que se enfrenta el activo	Identificación de la o las vulnerabilidades del activo que exploten las amenazas
ACTIVO 1	AMENAZA 1	VULNERABILIDAD 1 VULNERABILIDAD 2 . . . VULNERABILIDAD N

Por ejemplo:

TIPO DE ACTIVO	AMENAZA	VULNERABILIDAD
Repositorio de datos en formato digital	• Pérdida total de información	• Mal funcionamiento del software por falta de actualización. • Falla en la configuración de uso por el administrador. • Transferencia tecnológica de programas que operan elementos del sistema. • Error en el uso.
	• Acceso no autorizado a la base de datos	• Pérdida de credenciales de acceso a sistema. • Robo de credenciales de acceso a sistema. • Falta de configuración de perfiles de usuario.
Repositorio de datos en formato físico	• Acceso no autorizado a la base de datos	• Falta de controles de supervisión a la consulta de documentación. • Error en el manejo de archivos. • Falta de capacitación de los usuarios para el acceso al sistema.
	• Perdida parcial de información	• Falta de controles de supervisión a la consulta de documentación. • Error en el almacenamiento de los archivos.

Tabla de elaboración propia

B) Análisis de riesgo

La Estimación del riesgo es vista en los escenarios de vulneración, para ello es necesario identificar que cuando un activo es víctima de una amenaza, puede no verse afectado en su totalidad, por lo que, una vez que se ha identificado la amenaza que puede perjudicar al activo, se debe valorar la influencia en el valor del activo en dos sentidos:

- **Impacto:** Que tan perjudicado resultaría el valor del activo, visto en las dimensiones de confidencialidad, integridad y disponibilidad.
- **Probabilidad:** Que probable o improbable es que se materialice la amenaza.

Como se ha visto, la presente metodología hace una asociación directa entre tipos de activos, las amenazas a las que se enfrenta el activo y las vulnerabilidades en función del tipo de activo identificado, esta base permite definir los elementos a analizar para conocer el escenario de vulneración, en donde se debe calcular la probabilidad de ocurrencia de que la amenaza explote la vulnerabilidad señalada y se convierta en un incidente de seguridad, así como el impacto que va a tener en la información, en las dimensiones de confidencialidad, integridad y disponibilidad, recordando que, para esta metodología se contempla el daño a los titulares de los datos, estos elementos permitirán conocer el valor del riesgo.

En pasos anteriores se definió la valoración de datos, por lo que, deberá retomar el formato de presentación de datos de manera cuantitativa o cualitativa para definir el cálculo del riesgo.

Es así como, en este punto deberá contemplar el siguiente esquema para proceder a realizar el análisis de riesgo correspondiente:

ETAPA DE IDENTIFICACIÓN DEL RIESGO			ETAPA DE ANÁLISIS DE RIESGO		
Activos	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Riesgo

Cálculo de la probabilidad

El cálculo de la probabilidad se define como la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o de factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque este no se haya materializado.

En este paso, se debe asignar un valor a la posibilidad de que un evento ocurra, en dos dimensiones, cuando se tienen registros (valor de frecuencia) y cuando no se tienen registros (valor de factibilidad).

Por lo que, en este paso se debe identificar que valoración se está realizando, con información que sustente el valor asignado o con datos que no sustentan el valor asignado.

- Probabilidad por frecuencia

Es la valoración más recomendable ya que incluye una evidencia que sustenta el cálculo realizado, es decir, se cuenta con un elemento que sustenta al valor asignado garantizando el grado de confianza de los cálculos de los niveles de riesgo.

Por ejemplo, el registro de sucesos, revisión de la bitácora de vulneraciones, análisis del entorno en que se tratan los datos personales, interpretación de fallas en reportes de resultados de pruebas, entre cualquier evidencia documental o no que permita establecer un valor.

Es más común utilizar este cálculo de probabilidad por frecuencia en la segunda iteración del cálculo del riesgo, es decir, en el cálculo del riesgo residual, debido a que se identifica el escenario de vulneración y se cuentan con elementos que ayudan a describir de mejor manera con antecedentes la probabilidad de ocurrencia describiendo el número de eventos ocurridos en un lapso.

Por poner un ejemplo, durante 365 días de operación de un centro de datos, se tiene el registro de que 4 ocasiones se ha perdido el suministro de energía eléctrica y 100 ocasiones se ha perdido la conexión a internet, estos valores comienzan a describir de mejor manera la probabilidad a partir del análisis del entorno.

Ejemplo:

Frecuencia definida	Valor asignado
Ha ocurrido entre una y tres veces en un periodo de un mes	Poco probable
Ha ocurrido entre cuatro y seis veces en un periodo de un mes	Medianamente probable
Ha ocurrido más de seis veces en un periodo de un mes	Bastante probable

- Probabilidad por factibilidad:

Es la evaluación de la magnitud de las consecuencias de un evento, si ocurriera, y la posibilidad del evento y sus consecuencias asociadas, como alternativa, cuando no hay a disposición datos del pasado, se pueden hacer estimaciones subjetivas que reflejen el grado de creencia de un individuo o grupo con respecto a la probabilidad de ocurrencia de un evento o resultado particular.

A fin de evitar los sesgos subjetivos, al analizar las consecuencias y la posibilidad, se recomienda emplear los mejores recursos y técnicas de información disponibles. Entre las fuentes de información se pueden incluir:

a) registros de eventos de seguridad;
b) experiencia en el manejo de los activos del sistema;
c) ensayos y resultados de experimentos y prototipos;
d) modelos económicos, de ingeniería y otros;
e) juicios de especialistas y expertos.
f) entrevistas estructuradas con expertos en el área de interés;
g) empleo de grupos de expertos multidisciplinarios;
h) uso de árboles de falla y arboles de eventos.

Este tipo de cálculo de probabilidad se utiliza más en la valoración del riesgo inherente, pues, en ese análisis aún no se analiza el entorno real de la vulneración, son apreciaciones que se realizan sin integrar la descripción de medidas de seguridad y que aún no reflejan un valor de riesgo real.

Por ejemplo:

Factibilidad definida	Valor asignado
Hay pocos elementos que permitan determinar una posibilidad real	Poco probable
Hay elementos que permiten determinar una posibilidad media	Medianamente probable
Hay muchos elementos que permiten determinar una posibilidad alta	Bastante probable

Cálculo del impacto

El impacto, es la medida del grado de daño a los activos o cambio adverso en el nivel de objetivos alcanzados por una organización. Esta metodología considerara que el impacto debe analizarse por cuanto, a los daños o afectaciones a las personas titulares de datos personales, y no así la afectación a la organización, particularmente a su reputación, que, si bien importa y afecta, no es el fin último y propósito del Documento de Seguridad, en tanto que se trata de la protección de un derecho fundamental.

La estimación del grado de impacto o consecuencias debe ser determinado mediante la aplicación de criterios en función de los tres principios básicos de seguridad de la información:

- Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados;
- Integridad: Propiedad de la información de completitud y exactitud;

- **Disponibilidad:** Propiedad de la información de ser y estar accesible y utilizable, a petición de una entidad autorizada.

Será importante que la valoración por cada dimensión de seguridad sea en el mismo rango que el impacto, en sí a partir de una valoración individualizada que permita conocer cómo se puede perder cada una de las propiedades de la información, o bien, en caso de que así lo determine, podrá realizar un promedio de las propiedades a partir de la siguiente valoración matemática:

$$\text{impacto total} = \frac{\text{confidencialidad} + \text{integridad} + \text{disponibilidad}}{3}$$

Para realizar esta determinación, es más recomendable realizar una valoración individualizada para asignar medidas específicas para los escenarios en los que se ve afectada una, dos o las tres propiedades de la información.

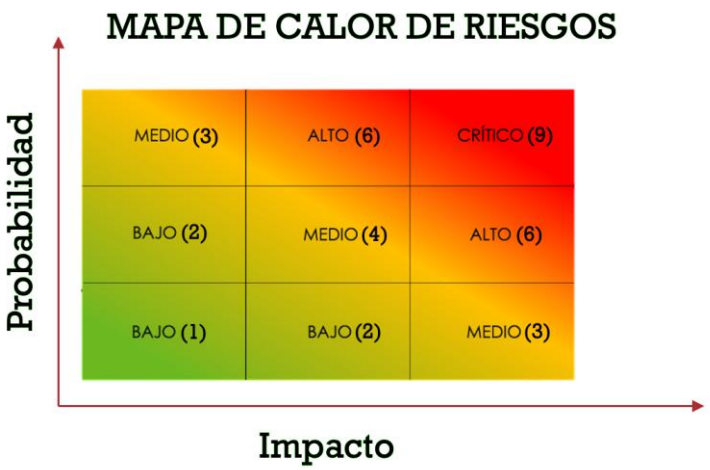
Determinación del nivel del riesgo

El valor del riesgo se interpreta con la fórmula universal del riesgo, donde y ase conocen los valores de probabilidad e impacto, en donde se debe aplicar la siguiente operación:

$$\text{Riesgo= probabilidad x impacto}$$

La determinación del riesgo se da en dos instancias, la primera antes de la identificación de los controles de seguridad, llamada riesgo inherente y es la que se realiza en esta etapa.

Por lo que, recordando una de las actividades de la primera fase, la que se refiere a la definición de la escala para describir el riesgo ya sea con una escala cuantitativa, cualitativa o combinada, deberá tener un mapa de calor de riesgos que le ayude a identificar el valor del riesgo que ha calculado, esta representación es gráfica y ayuda a tener un fácil acceso a la identificación de los valores de riesgos definidos, por ejemplo, en una escala básica se podría presentar el siguiente mapa de calor:



Mapa de elaboración propia

En complemento del mapa de calor, el sujeto obligado deberá identificar el valor para el impacto y la probabilidad de ocurrencia del incidente para obtener un valor que sea la base de la creación de escenarios de vulneración, la escala básica que puede seguir es la siguiente:

Impacto		Probabilidad		Nivel de riesgo	
Cuantitativo	Cualitativo	Cuantitativo	Cualitativo	Cuantitativo	Cualitativo
1	Bajo	1	Bajo	1	Bajo
1	Bajo	2	Medio	2	Bajo
2	Medio	1	Bajo	2	Bajo
1	Bajo	3	Alto	3	Medio
3	Alto	1	Bajo	3	Medio
2	Medio	2	Medio	4	Medio
2	Medio	3	Alto	6	Alto
3	Alto	2	Medio	6	Alto
3	Alto	3	Alto	9	Critico

Tabla de elaboración propia

Esta es la escala básica de ejemplo con 3 valores para probabilidad y 3 valores para impacto, por lo que, se hace la precisión de que el sujeto obligado podrá añadir más valores en caso de que requiera detallar de mejor manera el nivel de riesgo. Se recomienda usar esta escala como punto de partida para realizar los cálculos para el nivel de riesgo y también, si es de las primeras veces que realiza esta actividad.

C) Valoración de riesgo

Este es el paso final de la evaluación de los riesgos, ya que parte del cálculo del riesgo inherente, tomando este valor y realizando una re interpretación del valor del riesgo a partir de un análisis que identifica el contexto en el que la organización tiene al riesgo, describiendo elementos que permitan reasignar valores de impacto y/o asignar valores de probabilidad de ocurrrencia a partir de registros, haciendo una nueva valoración del valor del riesgo pero ahora incluyendo y analizando la efectividad de las medidas de seguridad que se tienen implementadas.

Identificación de las medidas de seguridad

Es importante mencionar que para poder llevar a cabo una valoración de manera efectiva, es necesario contar con una base de comparación que describa los objetivos de seguridad que deben satisfacerse con al menos una medida de seguridade, con ello, establecer un punto de análisis respecto a la eficiencia de la o las medidas de seguridad que se tienen implementadas al momento de la realización de la valoración.

Es así que, se desarrolla una tabla que enlista y clasifica diversos controles de seguridad, la cual es opcional en su uso ya que, puede ser usada como referencia para esta actividad, en caso de contar con alguna base comparativa que quisiera aplicar en este paso.

Sin embargo, las organizaciones deberán asegurarse de que no pasaron por alto la implementación de medidas que permitan atender riesgos que posiblemente no identificaron durante el análisis de riesgos.

Esta tabla parte del análisis y re interpretación del Anexo D. Ejemplos de Controles de Seguridad de la Guía para implementar un Sistema de Gestión de Seguridad de Datos Pesonales[18] y del Anexo A Controles de la seguridad de la información de referencia del estandar UNE-ISO/IEC 27001:2023[19]

ID	OBJETIVO	DESCRIPCIÓN
CONTROLES ORGANIZACIONALES		
1	Políticas para la seguridad de la información	La politica de seguridad de la información y las políticas temáticas especificas debe ser definidas y aprobadas por la por la Alta Dirección, publicadas, comunicadas y conocidas por el personal y las partes interesadas. Asimismo deberan ser exigibles en su cumplimiento para todo el personal que aplique la seguridad de la información, además de ser revisadas a intervalos planificados y en caso de producirse cambios significativos.

[18] https://home.inai.org.mx/wp-content/uploads/Gu%C3%ADa_Implementación_SGSDP(Junio2015).pdf
[19] https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0071320

2	Roles y responsabilidades en seguridad de la información	Todos los roles y responsabilidades de seguridad de la información deben ser definidos y asignarse de acuerdo al nivel de responsabilidad que tienen aquellos que intervienen en el tratamiento de datos.
3	Cumplimiento de requisitos legales, reglamentarios y contractuales	Se deden observar los requisitos legales, estatuarios, reglamentarios y contractuales pertinentes para la seguridad de la información, la privacidad y la protección de datos personales a nivel nacional e internacional, alineandolo al enfoque de la organización para cumplir con estos requisitos, manteniendose siempre actualizados, considerando la regulación específica de un sector o rama industrial, industrial.
4	Cumplimiento de derechos de propiedad intelectual	La organización debe implementar procedimientos apropiados para proteger la propiedad intelectual.
5	Seguridad de la información en la gestión de proyectos	La seguridad de la información debe integrarse en la gestión de proyectos que involucren el procesamiento de datos.
6	Segregación de tareas	Se trata de evitar usos o accesos indebidos a la información o a las aplicaciones o sistemas que la gestionan (activos de información) mediante la separación de las funciones asignando distintos perfiles o áreas de responsabilidad
7	Comunicación de compromisos en materia a la seguridad de la información	Quienes toman decisiones dentro del sujeto obligado, deben exigir a todo el personal que aplique la seguridad de la información de acuerdo con la politica de seguridad de la información, las políticas temáticas y sus procedimientos especificos establecidos en la organización.
CLASIFICACIÓN Y ACCESO A LOS ACTIVOS		
8	Elaboración de inventario de activos de información	Debe elaborarse y mantenerse un inventario de los activos en los que se tiene información a partir del ciclo de vida de los datos, identificando a los propietarios de cada elemento enlistado.
9	Uso aceptable de la información y activos asociados	Se deben identificar, documentar e implementar reglas para el uso aceptable y procedimientos para el manejo de información y los activos asociados al sistema de tratamiento.
10	Devolución de activos	Todos los involucrados en el tratamiento de datos, empleados y externos, según procedan, deben devolver todos los activos de la organización en su poder tras el cambio o la terminación de su trabajo, contrato o acuerdo de ejercicio de funciones.

11	Clasificación y etiquetado de la información	La información debe clasificarse de acuerdo con las necesidades de la seguridad de la información, en este caso en particular, se deberá tomar en cuenta el tipo de datos que se estan resguardando en los activos.
12	Comunicaciones de información	Debe desarrollarse e implantarse un conjunto adecuado de procedimientos, reglas o acuerdos para las comunicaciones de información, es decir para todos los tipos de medios de transferencia y/o remisión de datos dentre de la organicación y entre la organización y otras partes.
CONTROLES DE ACCESO		
13	Controles de acceso	Se deben establecer e implementar reglas de control de acceso fisico y/o logico a la información basadas en el tipo de activo descrito en el sistema de tratamiento.
14	Gestión de identidad	Se deben establecer e implementar controles que garanticen que solamente las personas autorizadas, y nadie más, tengan acceso a los activos que contienen datos y que son necesarios para realizar su trabajo
15	Derechos de acceso	Los derechos de acceso a los activos que contienen la información deben aprovisionarse, revisarse, modificarse y eliminarse tomando en cuenta una politica especifica para la gestión de identidad.
TERCERIZACIÓN DE SERVICIOS		
16	Seguridad de la información en las relaciones con los proveedores mediante un acuerdo	Se deben identificar e implementar procesos y procedimientos para gestionar los riesgos a la seguridad de la información asociados con la tercerización de servicios por proveedores externos. Estas actividades deben establecerse y acordarse con cada proveedor buscando garantizar la seguridad de la información en función del tipo de relación y la o las actividades en las que interviene este.
17	Seguimiento, revisión y gestión del cambio de los servicios de proveedores	Se deben contar con mecanismos que permitan a la organización supervisar, revisar, evaluar y gestionar de manera regular los cambios que pudieran presentarse en las prácticas de seguridad de la información y prestación de servicios de proveedores..
18	Seguridad de la información para el uso de servicios en la nube	Los procesos de adquisición, uso, gestión y finalización de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad definidos por la organización a fin de ser formalizados en un contrato de adhesión de servicios que tome en cuenta el ciclo de vida de la información.

19	Gestión de la seguridad de la información en la cadena de suministro de las TIC	Se deben definir e implementar procesos y procedimientos para hacer frente a los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios asociados al suministro de Tecnologías de la Información y de las Comunicaciones (TICs).
INCIDENTES A LA SEGURIDAD DE LA INFORMACIÓN		
20	Planificación y preparación de la gestión de incidentes de seguridad de la información	La organización debe planificar y estar preparada para gestionar incidentes a la seguridad de la información mediante la definición, establecimiento y comunicación de acciones especificas, estas acciones deben contemplar los procesos, roles y responsabilidades de los que intervienen en el tratamiento considerando el nivel de responsabilidad para la ejecución de medidas de seguridad correctivas.
21	Evaluación y decisión sobre los eventos de seguridad de la información	La orgranización debe evlauar los eventos de seguridad de la información y decidir si deben ser catalogados o no como incidentes, en este caso en particular, se debe recordar que hay eventos que afectan a los titulares de los datos y que deben pasar por un proceso de comunicación conforme a la norma en la materia y que hay otros incidentes que despues de un análisis derivan en la perdida de servicio o diponibilidad para el trabajador de manera temporal sin afectar ni comprometer la información resguardada, incidentes que no comprometen la seguridad de la información pero que si dan datos sobre fallas u omisiones en la funcionalidad de sistemas.
22	Respuesta a incidentes de seguridad de la información	Los incidentes de seguridad de la información deben ser repondidos de acuerdo con procedimientos documentados en un manual de respuesta a incidentes que tome en cuenta al menos los escenarios mapeados en el analisis de riesgos.
23	Aprender de los incidentes de seguridad de la información	La organización debe establecer e implementar procedimientos para la identificación, captura, adquisición y preservación de evidencias relacionadas con eventos de seguridad de la información a fin de mejorar los manuales de respuesta a incidentes y mejorar los planes de respuesta a partir de la experiencia previa.
24	Seguridad de la información durante la interrupción	La organización debe preveer como va a mantener la seguridad de la información a un nivel adecuado durante la interrupción de servicios derivada de la materialización de un incidente a la seguridad.
GENERACIÓN DE REGISTROS		
25	Inteligencia de amenazas	La información relativa a las amenazas a la seguridad de la información debe recopilarse y analizarse para generar

		información de soporte sobre los elementos de la gestión de riesgos, dicho analisis no corresponde directamente a la materialización de un incidente a la seguridad de la información.
26	Documentación de procedimientos operacionales	Deben documentarse los procedimientos operacionales de los medios de tratamiento de la información y ponerse a disposición de todos los usuarios que los necesiten.
27	Protección de registros	Los registros que se vayan generando con la implementación de la gestión del riesgo y su mejor continua deberán estar protegidos contra la pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.
GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
28	Revisión independiente de la seguridad de la información	El enfoque de la organización para gestionar la seguridad de la informaicón y su implementación, incluidos los procesos, tecnología y las personas, debe revisarse de forma independiente a intervalos planificados o siempre que se produzcan cambios significativos.
29	Cumplimiento de las políticas y normas de seguridad de la información	Debe comprobarse periodicamente el cumplimiento de la política de seguridad de la información, las políticas temáticas específicas, las reglas y las normas de la organización.
SEGURIDAD DE LA INFORMACIÓN ENFOCADA A DATOS PERSONALES		
30	Privacidad y protección de datos de carácter personal	La organización debe identificar y cumplir con los requisitos relativos a la preservación de la privacidad y la protección de datos de carácter personal de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.
SEGURIDAD AL PERSONAL		
31	Comprobación de antecedentes	La comprobación de antecedentes del personal que será contratado por la organización debe realizarse sin excepciones y de acuerdo con las leyes, reglamentos y éticas aplicables, y debe ser proporcional a los requisitos de contratación.
32	Terminos y condiciones de contratacion	Se deben establecer acuerdos contractuales especificos sobre la responsabilidad del personal en materia de seguridad de la información a partir de los roles y responsabilidades del empleado.
33	Concienciación, educación y formación en seguridad de la información	El personal de la organización y las partes interesadas pertinentes deben recibir una adecuada capacitación a partir del nivel determinado por su grado de responsabilidad, esta puede ser informativa, de consientización, educación o de formación en materia de

		seguridad de la información, programando actualizaciones periodicas.
34	Proceso disciplinario	Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados y partes interesadas pertienentes, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad, destacando acciones en caso de que esta sea intencional.
35	Responsabilidad ante la finalización o cambio	Las responsabilidades y obligaciones en materia de seguridad de la información deberan ser vigentes despues del cese o cambio de empleo.
36	Acuerdos de confidencialidad o no divulgación	Se debe firmar un acuerdo de confidencialidad o no divulgación de información que es trabajada por los empleados y que tenga que ver con tratamiento de datos personales.
37	Teletrabajo	Se deben implementar medidas de seguridad cuando el personal trabaje de forma remota para proteger la información a la que se acceda, procese o almacene fuera de las instalaciones de la organización.
38	Notificación de los eventos de seguridad de la información	La organización debe proporcionar un mecanismo para que el personal notifique a tiempo eventos de seguridad de la información observados o incluso manifestar sospechas de fallas de activos que pudieran derivar en un incidente a la seguridad a través de canales apropiados.
SEGURIDAD FISICA Y AMBIENTAL		
39	Perimetro de seguridad fisica	Identificar o en su caso, implementar mecanismos de seguridad en el perímetro de la organización, así como en areas que contengan información y otros activos asociados.
40	Controles físicos de entrada	Se deben implementar mecanismos que sólo permitan el acceso a personal autorizado, por ejemplo a través de dispositivos biométricos, tarjetas inteligentes, personal de seguridad, etc.
41	Seguridad de oficinas, despachos y recursos	Implementar mecanismos para mantener las áreas de resguardo o servicios de procesamiento de datos, aisladas de amenazas causadas por el hombre. Por ejemplo, puertas con cerradura, gabinetes o cajas de seguridad. Además deben existir mecanismos para proteger a los activos de fenómenos como el agua, fuego, químicos, vibraciones, radiación, etc. Por ejemplo, extintores, detectores de humo, etc.
42	Monitorización de la seguridad física	Las instalaciones deben ser monitorizadas continuamente para detectar accesos fisicos con autorizados.

43	Protección contra las amenazas físicas y ambientales	Se debe diseñar e implementar una protección a las infraestructuras contra las amenazas físicas y ambientales como lo son desastres naturales y amenazas fisicas intencionadas y no intencionadas.
44	Trabajo en áreas restringidas	Los activos de información sólo deben ser accesibles por personal que los requiera en sus deberes en la organización o bien por un tercero autorizado. Por lo tanto, debe existir acceso controlado para personal trabajando en un área restringida.
45	Puesto de trabajo despejado y pantalla limpia	Deben definirse y hacerse cumplir reglas de puesto de trabajo despejado de papeles y de medios de almacenamiento removibles, así como reglas de pantalla limpia para los recursos de tratamiento de la información.
46	Emplazamiento y protección de equipos	Los activos deben situarse en lugares seguros y mantenerse protegidos.
47	Seguridad de los equipos fuera de las instalaciones	Se deben establecer mecanismos autorizados por la Alta Dirección, para controlar la salida fuera de las instalaciones de cualquier activo que contenga datos personales, considerando que su seguridad sea equivalente al menos a la establecida dentro de la organización
48	Soportes de almacenamiento	Los soportes de almacenamiento deben gestionarse durante todo su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con las necesidades que originaron su uso.
49	Instalaciones de suministro	Las instalaciones de procesamiento de información deben estar protegidas contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.
50	Seguridad del cableado	Verificar el buen estado de las conexiones electricas y de telecomunicaciones o de transmisión de información, para evitar intercepciones, interferencias, fallas o daños en el servicio.
51	Mantenimiento de los equipos	Asegurarse de que los activos secundarios reciban mantenimiento periódicamente, (por ejemplo, según indicaciones del fabricante), además de realizarse por personal autorizado.
52	Eliminación o reutilización segura de equipos	Todos los soportes de almacenamiento deben ser comprobados para confirmar que ejecutado un borrado seguro de la información, o bien, de destrucción adecuado. Cualquier eliminación de activos debe registrarse con fines de auditoría.

CONTROLES DE ACCESO		
53	Gestión de privilegios de acceso	En un ambiente multiusuario se deben conceder privilegios en función de los roles y responsabilidades de cada usuario o grupo de usuarios para el cumplimiento de sus deberes, sin que se exponga a acceso, eliminación copia o alteración no autorizados a otros activos de información.
54	Restricción del acceso a la información	Se debe restringir el acceso a la información y otros activos relacionados, de acuerdo con politicas especificas para el control de acceso.
55	Autenticación segura	Las tecnologías y procedimientos de autenticación segura deben implementarse en función de las restricciones de acceso a la información y la política especifica sobre control de acceso.
USO DE TECNOLOGÍA		
56	Dispositivos finales de usuario	La información almacenada, procesada o accesible a través de dispositivos finales de usuario, sin importar la propiedad del dispositivo deben protegerse para garantizar la seguridad de la información.
57	Acceso al código fuente	Se debe gestionar adeacuadamente el acceso de lectura y escritura al código fuente, a las herramientas de desarrollo y a las bibliotecas de software.
58	Gestión de capacidades	Se debe supervisar y ajustar la utilización de los recursos en consonancia con los requisitos de capacidad actuales y esperados.
59	Controles contra el código malicioso	Se debe implementar una protección contra el código malicioso, respaldada por una concienciación adecuada para los usuarios.
60	Gestión de vulnerabilidades técnicas	Se de be obtener información acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas.
61	Gestión de la configuración	Se debe establecer, documentar, implementar, monitorizar y revisar las configuraciones de hardware, software, servicios y redes, incluyendo sus configuraciones de seguridad.
62	Eliminación de la información	La información almacenada en los sistemas de información, en los dispositivos y en cualquier otro medio de almacenamiento debe ser eliminada de manera segura cuando ya no sea necesaria.
63	Enmascaramiento de datos	Debido a los requisitos normativos y de privacidad, las organizaciones deben proteger los datos que recopilan. El enmascaramiento de datos crea versiones falsas de los

		datos al cambiar la información a través de diversas técnicas para crear cambios realistas y estructuralmente similares.
64	Prevención de fugas de datos	Se deben aplicar medidas de prevención de fugas de datos a sistemas, redes y cualquier activo que procese, almacene o transmita información.
65	Copias de seguridad de la información	Las copias de seguridad de la información, del software y de los sistemas deben mantenerse y probarse de manera periodica, lo cual debe estar alineado con una politica de copias de seguridad especifica.
66	Redundancia de recursos de tratamiento de la información	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer requisitos de disponibilidad.
67	Registros de eventos	Se deben generar, proteger, almacenar y analizar los registros de las actividades, excepciones, fallos y otros eventos relevantes.
68	Seguimiento de actividades	Las redes, sistemas y aplicaciones deben monitorizarse en busca de comportamientos anómalos y se deben tomar medidas de seguridad adecuadas para evaluar posibles incidentes de seguridad de la información.
69	Sincronización del reloj	Los relojes de los sistemas de procesamiento de información utilizados por la organización deben sincronizarse con fuentes de tiempo aprobadas.
70	Uso de los programas de utilidad con privilegios	Se debe restringir y controlar rigurosamente el uso de programas de utilidad que puedan ser capaces de invalidar los controles del sistema y de la aplicación.
71	Instalación del software en sistemas de producción	Deben implementarse procedimientos y medidas para gestionar de forma segura la instalación de sofware en los sistemas en producción.
72	Seguridad de redes	Las redes y los dispositivos de red deben estar protegidos, gestionados y controlados para proteger la información en los sistemas y aplicaciones.
73	Seguridad de los servicios de red	Se deben identificar, implementar y monitorzar los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de todos los servicios de red.
74	Segregación en redes	La red debe segregar a los usuarios a través de mecanismos como VPN o firewalls, por ejemplo, la red externa para usuarios de visita debe encontrarse en un segmento de red distinto de la red donde se encuentran los sistemas de datos personales.
75	Filtrado de webs	El acceso a sitios web externos debe gestionarse para reducir la exposición a contenido malicioso.

76	Uso de la criptografía	Deben definirse e implementarse reglas para el uso eficaz de la criptografía en la información que se encuentra en transito y en reposo, incluyendo reglas para la gestión de claves criptográficas.
77	Requisitos de seguridad de las aplicaciones	Los requisitos de seguridad de la informacion deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.
78	Gestión de cambios	Los cambios en los elementos que intervienen en el tratamiento de información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.
79	Datos de prueba	Los datos de prueba deben ser previamente seleccionados a partir del impacto significativo que pueden llegar a tener al ser analizados, asdemas de estar protegidos y controlados.
80	Protección de los sistemas de información durante las pruebas de auditoría	Las pruebas de auditoria y otras actividades de aseguramiento en la evaluación de los sistemas en producción deben ser cuidadosamente planificadas y acordadas entre el evaluador y los gestores adecuados.
DESARROLLO DE APLICACIONES O PROGRAMAS		
81	Seguridad en el ciclo de vida del desarrollo	Se deben establecer y aplicar reglas para el desarrollo seguro de aplicaciones y sistemas priorizando la protección de datos personales.
82	Arquitectura segura de sistemas y principios de ingenieria	Los principios de ingenieria de sistemas seguros se deben establecer, documentar, mantener y aplicar a todas las actividades de desarrollo de sistemas de información.
83	Codificación segura	Para el desarrollo de software deben definirse principios de codificación segura.
84	Pruebas de seguridad en desarrollo y aceptación	Deben definirse e implementarse procesos de pruebas de seguridad en el ciclo de vida del desarrollo.
85	Externalización del desarrollo	La organización debe controlar, monitorizar y rvisar las actividades relativas al desarrollo externalizado de sistemas.
86	Separación de los entornos de desarrollo, prueba y producción	Deben separarse y protegerse los entornos de desarrollo, prueba y producción.

De esta manera, al revisar los controles de seguridad que por su implementación conciernen a su sistema de tratamiento, tendrá un elemento que le ayude a asociar y describir los controles de seguridad que requiere implementar para mantener la seguridad de la información en sus sistema.

A partir de la interpetación de las medidas de seguridad, podrá comenzar a identificar la afectación de las medidas de seguridad sobre el valor del riesgo, determinando la eventual degradación del valor del riesgo gracias a las medidas de seguridad, por lo que, en esta etapa conocerá el valor del riesgo residual o el riesgo calculado despues del análisis de la afectación de las medidas de seguridad en el escenario de vulneración analizado.

Es así que deberá realizar el cálculo del riesgo nuevamente tal y como lo hizo en el cálculo del riesgo inherente, solo que ahora identificando elementos que sustenten el valor asignado al riesgo a partir de las evidencias que pueda llegar a tener.

ETAPA DE IDENTIFICACIÓN DEL RIESGO			ETAPA DE ANÁLISIS DE RIESGO			ETAPA DE VALORACIÓN DE RIESGO		
Activos	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Riesgo Inherente	Probabilidad	Impacto	Riesgo Residual

FASE 3 - VERIFICAR

Actividad 4. Monitoreo

Se debe monitorear y revisar el riesgo con sus factores relacionados, es decir, el valor de los activos, las amenazas, vulnerabilidades, el impacto, y la probabilidad de ocurrencia, para identificar en una etapa temprana cualquier cambio en el contexto del alcance y objetivos del SGSDP de la organización y así mantener una visión general de la imagen del riesgo.

El riesgo no es estadístico: las amenazas, vulnerabilidades, probabilidad y consecuencias pueden cambiar abruptamente sin previo aviso. Esta situación exige la revisión de cada riesgo por separado, así como la suma de ellos, para conocer el impacto potencial acumulado de las amenazas.

Por ello se requiere de constante monitoreo para detectar esos cambios. Por ejemplo, es posible apoyarse en servicios externos que provean información respecto a las amenazas o vulnerabilidades. Los sujetos obligados deben asegurar que los siguientes puntos estén continuamente monitoreados:

- Nuevos activos que se incluyan en los alcances de la gestión de riesgo;
- Modificaciones necesarias a los activos; por ejemplo, cambio o migración tecnológica;
- Nuevas amenazas que podrían estar activas dentro y fuera del sujeto obligado y que no han sido valoradas;
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
- Vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelven a surgir;
- Cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo;
- El histórico de incidentes y vulneraciones de seguridad.

Los factores que determinan la probabilidad de ocurrencia y consecuencias podrían cambiar, lo que afectaría la conveniencia y costos de las opciones de tratamiento. Los cambios mayores que afectan a la entidad deben ser revisados de modo específico, no obstante que las actividades de monitoreo requieren de regularidad y periodicidad.

El resultado del monitoreo de riesgo puede afectar su tratamiento y aceptación, y en consecuencia el contexto que se establezca en un ciclo de mejora continua.

Por lo anterior, en esta etapa se deben evaluar y medir los resultados de la implementación de las medidas de seguridad. Es decir, se debe verificar que las medidas realmente se estén aplicando dentro del sujeto obligado y que éstas funcionen para la correcta gestión del riesgo. Para ello es indispensable monitorear con debida anterioridad si existen nuevos

tratamientos de datos personales, nuevas amenazas, vulnerabilidades, y si las medidas de seguridad son acordes y suficientes para el nivel de riesgo asociado.

Para el monitoreo podemos identificar dos momentos en que se realiza el monitoreo, el primero se refiere al monitoreo continuo de la operación de la medida de seguridad, el cual parte de la idea general de que cada medida de seguridad que ponga en operación deberá contar con un mecanismo que genere una evidencia de su aplicación, con controles que aprovechen la tecnología en miras de ser automatizados o con controles de inspección manual programados. Este monitoreo ayudará a contar con evidencia continua que dará soporte a la determinación del nivel de madurez de esta.

Determinación del nivel de madurez de la medida de seguridad

Una vez que ha identificado las medidas de seguridad a partir de los objetivos de seguridad podrá determinar que medidas le hacen falta y que medidas tiene implementadas, ahora es importante que conozca cuáles son las medidas que ya están funcionando de manera efectiva, esto lo va a saber al conocer su nivel de madurez, con lo cual podrá tener mayores elementos para determinar el nuevo valor del riesgo en el análisis del escenario de vulneración completo. Identificando la medida de seguridad en algún nivel de seguridad, por ejemplo, se podrían considerar niveles en función de los registros documentados por el monitoreo y revisión de las medidas:

- Inexistente. No se tiene la medida de seguridad.
- Documentado. Se ha plasmado en un documento las características y objetivos del control, así como las medidas que soportan su cumplimiento.
- Implementado. El control ya se encuentra puesto en marcha a través de una o más medidas de seguridad.
- Con registros generados. Se generan registros de la operación del control y de sus medidas de seguridad.
- Monitoreado. Se han establecido métricas que permiten dar seguimiento a la eficacia del control.
- Mejora continua. Se toman las acciones necesarias para incrementar la eficacia de los controles con respecto al monitoreo realizado.
- Automatizado. El control requiere poca o nula interacción de una persona, en su operación, monitoreo o ajustes.

Mecanismos para el monitoreo y revisión

La gestión de riesgos incluye una etapa de monitoreo y revisión para garantizar la obtención de métricas que permitan hacer una valoración de cómo interactúan las medidas de seguridad con los riesgos por los que fueron implementados, es así como, se puede definir monitoreo y revisión de la siguiente manera:

- Monitoreo: Obtención de métricas de las medidas de seguridad a través de la obtención de registros de alertas y anomalías en el funcionamiento ordinario de las medidas de seguridad.
- Revisión: Una interpretación de los resultados obtenidos del monitoreo a través de una revisión general del funcionamiento de todas las medidas de seguridad en conjunto
- Pruebas de valor: Obtención de valores a través de la simulación de la materialización de los escenarios de vulneración descritos en la fase de análisis de riesgos o bien con una revisión externa de los resultados de la evaluación de los riesgos.

El obtener métricas a partir del monitoreo y revisión permitirá interpretar valores y realizar revisiones sobre los cálculos que se han realizado con el fin de obtener más elementos que aporten al análisis del funcionamiento de la seguridad de la información en el sistema de tratamiento. En este caso podemos identificar los siguientes:

Sistema de monitoreo

El objetivo de este tipo de sistemas es la alerta temprana frente a la concreción de incidentes de seguridad de la información y la recolección de métricas que son fundamentales para la gestión de seguridad de la información.

Las métricas provenientes del monitoreo deberán complementar la evaluación de los procesos y políticas de seguridad, brindando información relevante para realizar la gestión de riesgos.

Para implementar cualquier tipo de sistemas de monitoreo, puede incluso utilizar herramientas o software especializado siempre y cuando este le permita:

- Implementar y operar un sistema de medición y evaluación
- Realizar recolección de datos para su análisis
- Interpretar resultados de manera gráfica
- Contar con la posibilidad de implementar controles reactivos de seguridad

Auditoría

Se debe contar con un programa de auditoría interna y externa para monitorear y revisar la eficacia y eficiencia de la seguridad de la información. Este programa debe planearse, establecerse y mantenerse tomando en cuenta la política de gestión de datos personales. En su caso, se deben considerar auditorías a través de externos para procesos y circunstancias especiales, por ejemplo, cuando la organización desea unirse a un esquema de certificación.

En el ámbito de cumplimiento de protección de datos personales, podemos encontrar la figura de la auditoría voluntaria, una actividad que sólo puede desarrollarse a solicitud de un

responsable de tratamiento, en términos del marco normativo en materia de protección de datos personales del sector público.

Se deben establecer previamente los objetivos del programa de auditoría, el cual debe incluir el alcance e indicar explícitamente cualquier tratamiento de datos personales interno y externo a la organización, responsables, recursos, criterios a utilizar durante la auditoría, así como los procesos y/o áreas que serán auditadas.

La objetividad e imparcialidad del programa de auditoría debe ser asegurado por la apropiada selección de auditores y la conducción de la auditoría.

Las auditorías deben llevarse a cabo en intervalos de tiempo planeados para determinar si:

- Se está operando de acuerdo con la política de gestión de datos y con los procedimientos establecidos, y
- La seguridad de la información ha sido implementado y mantenido de acuerdo con los requerimientos tecnológicos en función de los resultados proporcionados en la gestión de riesgos.

La auditoría debe ofrecer al responsable información detallada respecto a cambios ocurridos en la seguridad, además se debe realizar una auditoría inmediatamente después de la implementación de modificaciones mayores en los procesos críticos de la organización respecto a los sistemas de tratamiento de información.

Como resultado de una auditoría se deben obtener observaciones sobre riesgos existentes para aplicar medidas preventivas, es decir, controles para que no ocurra una vulneración, así como observaciones sobre puntos que requieren medidas correctivas inmediatas.

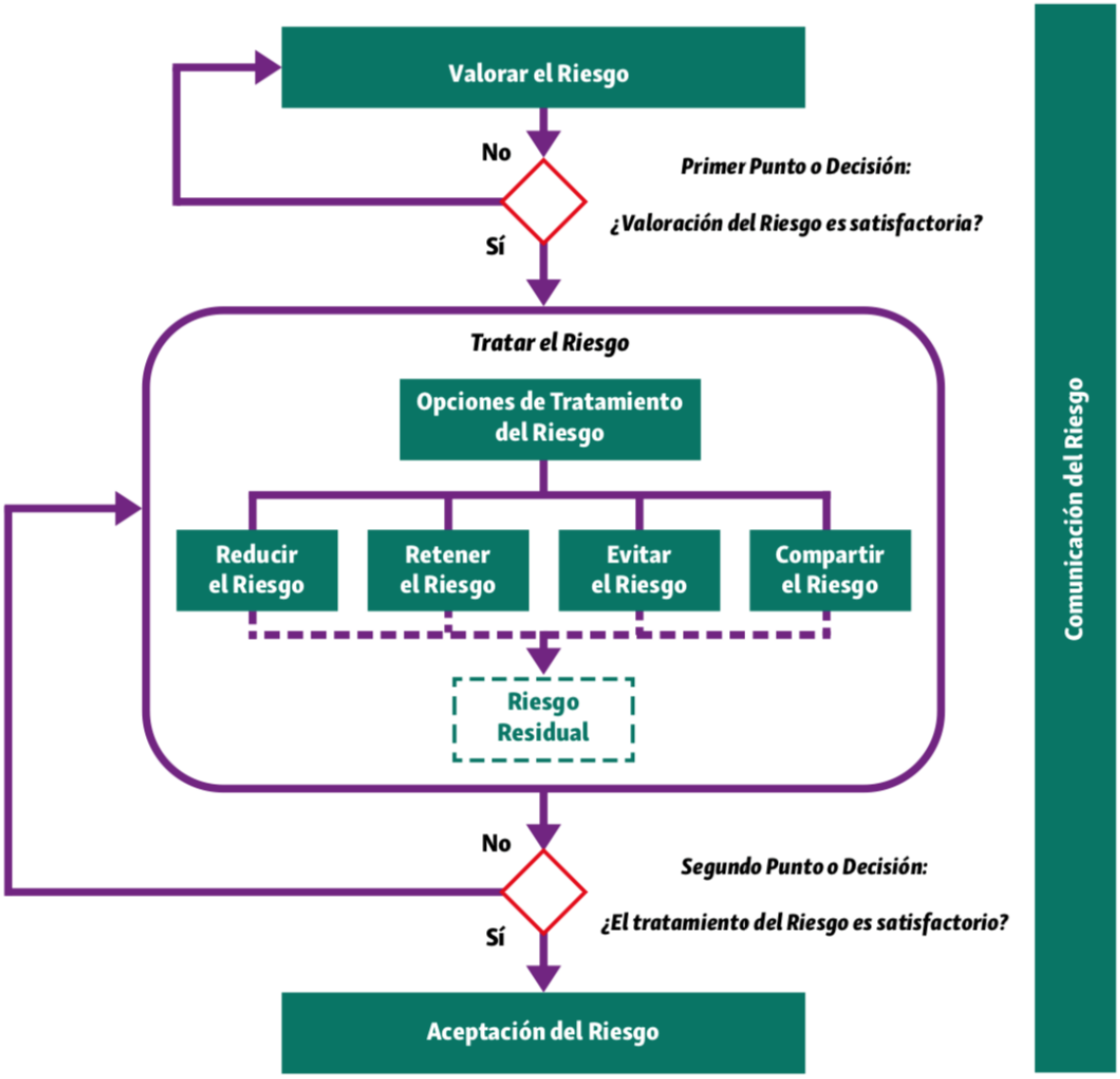
Se recomienda revisar el documento especifico de monitoreo y revisión publicado por este Instituto que se encuentra disponible en el apartado de Documentos y Guías para el sector público para identificar más mecanismos para considerar el monitoreo y revisión para las medidas de seguridad.

FASE 4 - ACTUAR

Actividad 5. Aceptación de nivel de riesgo

En este paso se toma el valor obtenido del riesgo residual a fin de interpretarlo y tomar una decisión sobre las actividades a realizar, para tratar los riesgos identificados en la etapa de valoración, esta actividad implica identificar el rango de opciones con miras a ocuparse de los riesgos, evaluar esas opciones y preparar planes para dicho tratamiento e implementarlos.

En ese sentido, los controles pueden proporcionar diversas opciones de tratamiento de riesgo:



Opciones del tratamiento del riesgo

Reducir el riesgo

Reducir el riesgo implica seleccionar y aplicar los controles, medidas de seguridad o salvaguardias apropiadas para reducir las probabilidades de una ocurrencia, o sus consecuencias, o ambas. Durante la selección de controles o medidas, es importante ponderar el costo de adqui- sición, implementación, administración, operación, monitoreo y mantenimiento de los controles contra el valor del activo a proteger. Adicionalmente, debe tenerse en conside- ración el conocimiento y habilidades especiales necesarias para definir e implementar nuevos controles o modificar los existentes.

Existen factores que pueden afectar la selección de controles. Límites técnicos, como requerimientos de rendimiento, capacidad de gestión (soporte operacional necesario) y los asuntos de compatibilidad pueden obstaculizar el uso de ciertos controles o inducir a errores humanos nulificando el control, dando un falso sentido de seguridad o incre- mentando el riesgo más allá del control. Por ejemplo, exigir contraseñas complejas sin entrenamiento establecido con la debida anterioridad, llevando a los usuarios a escribir las contraseñas en papel. Los responsables deben identificar las soluciones que satisfagan sus requerimientos y garanticen suficiente seguridad de los datos personales.

Retener el riesgo

Significa retener la responsabilidad por las pérdidas de los activos debido a la materialización del riesgo. En este caso, supone asumir la responsabilidad del impacto que puede generar lo anterior en la operación del sujeto obligado y probablemente en los derechos y libertades de los titulares de los datos personales, en tanto se busca implementar otra opción de tratamiento del riesgo.

Puede decidirse retener el riesgo sin considerar medidas adicionales, si a través de la evaluación del riesgo se determina que no hay posibilidad inmediata de implementar controles adicionales o que estos controles pueden implementarse posteriormente. Por ejemplo, el equipo de cómputo actual falla, pero al final del día se genera un respaldo de esa información; por lo que se decide retener ese riesgo durante un mes y esperar para cambiar el equipo de cómputo por uno nuevo.

Evitar el riesgo

Se refiere a la decisión de no verse involucrado en una situación de riesgo. Cuando el riesgo identificado es muy alto o los costos de tratamiento exceden a los beneficios, es recomendable evitar el riesgo, retirándose de las actividades actuales o cambiando las condiciones bajo las cuales operan dichas actividades. Por ejemplo, para un riesgo causado por la naturaleza podría ser más eficiente en costo mover físicamente el site de datos a una ubicación donde no exista el mismo riesgo, o que pueda mantenerse bajo control.

Una vez que ha calculado el valor del riesgo inherente, es decir, el valor del riego antes del análisis de las medidas de seguridad implementadas en el sistema de tratamiento, es necesario contar con una base comparativa que describa objetivos de seguridad, lo anterior permitira conocer si las medidas de seguridad que tiene implementadas cumplen con un objetivo o si bien estan implementadas de manera arbitraria,

Compartir el riesgo

Implica tomar la decisión de compartir el riesgo con un prestador de servicio que pueda gestionarlo. Es decir, un tercero interviene para mitigar los posibles efectos de un riesgo. Por ejemplo, al contratar un seguro o un proveedor que administre la seguridad del sujeto obligado.

En algunas ocasiones, las organizaciones deciden contratar seguros contra riesgos. De este modo, el riesgo se traslada a la entidad asegurada. Cabe mencionar que, cuando un sujeto obligado comparte un riesgo, no se comparte la responsabilidad. Es decir, la entidad no deja de ser responsable del tratamiento de los datos personales y, de darse un incidente de seguridad que afecte a los datos personales, será el sujeto obligado quien debe responder.
Además, es importante que se considere que involucrar a un nuevo actor en los procesos del responsable siempre representa un riesgo que debe ser analizado.

Aceptar el riesgo

Aceptar el riesgo quiere decir que se decide aceptar las consecuencias y probabilidad de un riesgo en particular.

Esta opción se toma cuando los costos de implementación de una medida de seguridad sobrepasan el valor del activo que se desea proteger, o cuando el nivel del riesgo es muy bajo. En ambos casos, la organización asume los daños provocados por la materialización del riesgo. En materia de seguridad enfocado a datos personales, debemos recordar que no sólo debe considerarse el valor del activo, sino también el impacto que puede causar su daño o pérdida a los titulares de los datos personales.

Dentro del tratamiento del riesgo, la entidad deberá ceñirse a lo establecido en dicho criterio. Aunque es posible que, por causas como la falta de recursos económicos, administrativos o humanos, deba aceptarse un riesgo de mayor nivel, lo cual se recomienda sea excepcional. En ese caso, será importante que se documente y sea aprobado por la o las personas propietarias del tratamiento, por el Comité de Transparencia y de ser posible por los Órganos Directivos de la entidad, a efecto de que el responsable del tratamiento esté aceptando un riesgo distinto al establecido en los criterios para la gestión del riesgo.

Aunado a lo anterior, y para efectos de la comprensión del riesgo, es importante aclarar que el riesgo cero no existe, por lo que se buscará mitigarlo a un nivel aceptable (bajo o muy

bajo) y dentro del plan de monitoreo y revisión deberán constar las acciones para supervisar dichos riesgos.

Lo que se busca en el tratamiento de los riesgos es que las consecuencias adversas de los riesgos se reduzcan lo más razonablemente posible, con independencia de cualquier criterio absoluto. Por ejemplo, deben considerarse los riesgos que es casi imposible que ocurran pero que serían catastróficos de suceder, en cuyo caso también deben implementarse controles de monitoreo y vigilancia

Ahora bien, los cuatro tipos de tratamiento de riesgo no son mutuamente excluyentes. A veces, los sujetos obligados pueden beneficiarse sustancialmente de la combinación de opciones, como reducir la probabilidad de un riesgo, reducir sus consecuencias, compartir o retener el riesgo residual.

Es así que, al encontrarse en un ciclo de mejora continua, deberá ir re calculando el riesgo tantas veces sea necesario a fin de conseguir el valor de riesgo aceptable que busca, analizando en todo momento la degradación a la que se esta enfrentando el valor calculado.

Comunicación

En suma, resulta relevante la comunicación del riesgo, que se refiere a la actividad que resulta de alcanzar los acuerdos sobre cómo administrar los riesgos, considerando su naturaleza, forma, probabilidad, severidad, tratamiento y aceptación.

La comunicación del riesgo debe realizarse para alcanzar los siguientes objetivos:

- Ofrecer garantías sobre la gestión del riesgo en el sujeto obligado;
- Recolectar información sobre el riesgo;
- Compartir los resultados de la valoración y el plan de tratamiento del riesgo;
- Evitar o reducir las vulneraciones de seguridad por desconocimiento entre los involucrados:
- Dar soporte a la toma de decisiones;
- Obtener nuevo conocimiento sobre la seguridad de la información;
- Que los responsables se tenga una comunicación con los proveedores de servicios;
- Incrementar la conciencia del riesgo en la organización.

La coordinación entre las personas principales que toman las decisiones y las partes involucradas es indispensable para la toma de decisiones. El sujeto obligado puede desarrollar planes o protocolos de comunicación del riesgo que involucren a personas que desempeñen roles fundamentales en la seguridad, donde pueda tener lugar el debate acerca de los riesgos, su prioridad, el tratamiento adecuado y la aceptación. Esto en momentos donde la operación del riesgo sea normal, pero también en casos de emergencia para responder, por ejemplo, a los incidentes de seguridad o vulneraciones y las obligaciones legales que éstas conllevan, como la notificación a los titulares y, en su caso, al Instituto y los Organismos garantes.

Es así como con esta actividad, se cierra el ciclo de gestión de riesgos, permitiendo tener una mejora continua con la reinterpretación de los resultados en función del valor del riesgo, por lo que, podemos establecer que la seguridad de la información toma al valor del riesgo como el elemento de análisis para identificar de qué manera se establecerán medidas de seguridad para mantener la información a salvo en sus dimensiones de confidencialidad, integridad y disponibilidad.

Conclusiones

Esta metodología no es obligatoria, solo es una base para que los interesados puedan identificar qué es el riesgo y como se puede trabajar, funciona como una llave de entrada para identificar al riesgo como parámetro de referencia para toma de decisiones alrededor de la preservación de la seguridad de la información, buscando en todo momento de un tratamiento de datos preservar las propiedades de confidencialidad, disponibilidad e integridad de los activos de apoyo en donde se resguardan los activos de información que son los datos personales.

Es así que, esta metodología establece pasos y actividades específicas a realizar para poder integrar todos los elementos que se involucran en la definición del riesgo, siendo un material de facilitación que permite definir acciones concretas para describir al riesgo y las acciones que se deben realizar a su alrededor dentro de un ciclo de mejora continua.