Recomendaciones para el Monitoreo y Revisiones de las Medidas de Seguridad

inai

Norma Mexicana en Igualdad Laboral y No Discriminación

DIRECTORIO

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Secretaría de Protección de Datos Personales

Dirección General de Prevención y Autorregulación

Dirección de Seguridad de Datos Personales del Sector Público
Av. Insurgentes 3211,
Colonia Insurgentes Cuicuilco, Alcaldía Coyoacán,
Ciudad de México, C. P. 04530.

Edición, Noviembre de 2024

NOTA

El presente documento desarrolla de manera técnica actividades que requieren un conocimiento previo de la gestión de seguridad de la información y gestión de riesgos, por lo que, es un material de apoyo para que sea utilizado como complemento para realizar las acciones para el monitoreo y revisión de las medidas de seguridad.

En ese sentido, el presente documento se encuentra relacionado con los materiales de facilitación, como son, la Guía de apoyo para la elaboración del Documento de Seguridad[1]y la Guía para implementar un sistema de gestión de seguridad de datos personales (sector público)[2].

[1] Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/Guia-apoyo-DS.pdf consultado el 04 de noviembre de 2024.
[2] Disponible en: https://home.inai.org.mx//wp-content/documentos/DocumentosSectorPublico/GuiaSGSDP_sectorpublico.pdf consultado el 04 de noviembre de 2024.

ÍNDICE

OBJETIVO GENERAL

Este documento tiene como objetivo proporcionar recomendaciones dirigidas a los Responsables del tratamiento de datos personales, para implementar, desarrollar y crear documentación para llevar a cabo las acciones de Monitoreo y Revisión, como parte de los procesos que se realizan en la gestión de riesgos, para que los servidores públicos que realizan estas actividades cuenten con referencias para su actuar.

DEFINICIONES Y ABREVIATURAS

Las definiciones de este documento son retomadas del Diccionario de Protección de Datos Personales, Conceptos fundamentales[3], Guía de apoyo para la elaboración del Documento de Seguridad[4]y Guía para implementar un sistema de gestión de seguridad de datos personales (sector público)[5].

Activo: En términos generales, un activo es cualquier elemento que representa un valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones.

Para efectos de este documento, los activos deben entenderse como los datos personales y sistemas de tratamiento que representan un derecho intrínseco de las personas titulares, y también como los elementos que representan un valor para el sujeto obligado, en tanto que, con ellos opera la propia entidad.

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

Comité de Transparencia: Instancia a la que hace referencia el artículo 43, de la Ley General de Transparencia y Acceso a la Información Pública.

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

ISO: Organización Internacional de Normalización

Ley General: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Encargado: La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

Riesgo: Potencial de que cierta amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos en perjuicio de la organización.

Sistema de Gestión de Seguridad de Datos Personales (SGSDP): Sistema de gestión general para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios básicos de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad previstos

[3] Disponible en: https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf consultado el 04 de noviembre de 2024.
[4] Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/Guia-apoyo-DS.pdf consultado el 04 de noviembre de 2024.
[5] Disponible en: https://home.inai.org.mx//wp-content/documentos/DocumentosSectorPublico/GuiaSGSDP_sectorpublico.pdf consultado el 04 de noviembre de 2024.

en la Ley General, los Lineamientos Generales, normatividad secundaria y cualquier otro principio que la buena práctica internacional estipule en la materia.

Unidad de Transparencia: Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.

Vulneración: Falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

Vulnerabilidad: Falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

MARCO NORMATIVO DE REFERENCIA

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[6] (Ley General); identifica la actividad de monitorear y revisar las medidas de seguridad, sin especificar un tiempo, en la fracción VII de su artículo 33, que menciona lo siguiente:

> ***Artículo 33.*** *Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
> *[…]*
> *VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y*
> *[…]*

De manera complementaria sobre el monitoreo y revisión de las medidas de seguridad, en la fracción II de su artículo 35, establece lo siguiente:

> ***Artículo 35.*** *De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:*
> *[…]*
> *VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y*
> *[…]*

Asimismo, respecto al tema de monitoreo y revisión a las medidas de seguridad, la Ley General menciona en la fracción II de su artículo 36 que:

> ***Articulo 36.*** *El responsable deberá actualizar el documento de seguridad cuando ocurran los siguientes eventos:*
> *[…]*
> *II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;*
> *[…]*

Por otro lado, en los Lineamientos Generales de Protección de Datos Personales para el Sector Público[7] (Lineamientos Generales), es posible identificar que el monitoreo y revisión de las medidas de seguridad es una actividad relacionada con el análisis de riesgos, conforme a lo dispuesto en la fracción V del articulo 56 que mencionar lo siguiente:

> ***Artículo 56.*** *Con relación a lo previsto en el artículo 33, fracción I de la Ley General, el responsable deberá incluir en el diseño e implementación de las políticas internas para la gestión y el tratamiento de los datos personales, al menos, lo siguiente:*
> *[…]*

[6] Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf consultado el 04 de noviembre de 2024.
[7] Disponible en: http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf consultado el 04 de noviembre de 2024.

V. El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales, y
[…]

Asimismo, en los Lineamientos Generales es posible identificar

Monitoreo y supervisión periódica de las medidas de seguridad implementadas
Articulo 63. *Con relación al artículo 33, fracción VII de la Ley General, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.*
Para cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente:

I. Los nuevos activos que se incluyan en la gestión de riesgos;
II. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;
III. Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;
IV. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
V. Las vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y
VII. Los incidentes y vulneraciones de seguridad ocurridas.

Aunado a lo previsto en las fracciones anteriores del presente artículo, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

A partir de lo anterior, es posible identificar que la normatividad en la materia indica que es deber de los sujetos obligados como responsables del tratamiento, integrar el monitoreo y revisión especifico a las medidas de seguridad como una actividad que da pauta a la mejora continua dentro de la implementación de un Sistema de Gestión orientado a la seguridad de la información, específicamente orientado a proteger los datos personales que son tratados, lo cual quedara como evidencia en el llamado Documento de Seguridad.

Es por lo que, resulta necesario ver al monitoreo y revisión como la actividad que analizará la interacción de las medidas de seguridad con los riesgos que identificaron su implementación dando un panorama general de mejora continua al ser el elemento que permite generar cambios para mejorar la seguridad de los datos personales.

En ese sentido, este documento orientará a los responsables y encargados del tratamiento, para comprender qué se tiene que observar al momento de planificar el monitoreo y revisión de las medidas de seguridad, lo anterior considerando lo que menciona el marco normativo señalado.

Por último, se debe aclarar que el seguimiento de este documento no exime a los sujetos obligados de su responsabilidad con relación a cualquier vulneración que pudiera ocurrir a sus bases de datos y los datos personales que se encuentren bajo su custodia.

MONITOREO Y REVISIÓN

Establecido el marco normativo de aplicación del monitoreo y revisión, se debe definir conceptualmente lo que se entiende por los conceptos de monitoreo y revisión con la finalidad de que, los responsables cuenten con elementos que les permitan identificar a que se refieren cada uno de ellos.

En suma a lo anterior, para que los responsables se encuentren en condiciones de dar cumplimiento de manera idónea al deber de seguridad en lo que respecta al sistema de gestión de seguridad de datos personales en específico en el monitoreo y revisión, relacionado con el principio de responsabilidad establecido en el artículo 30, fracciones V y VI de la Ley General, el cual impone obligaciones adicionales respecto al monitoreo y vigilancia o supervisión y vigilancia, en particular de las políticas y programas de gestión y tratamiento de datos personales y de seguridad, y que al ser estos medidas de seguridad administrativas que inciden en el SGSDP, resultan necesarias para el cumplimiento de la Ley.

En ese orden de ideas, es que resulta necesario identificar los conceptos de monitoreo y revisión y relacionarlos para poder establecer una directriz que permita generar una serie de pasos que puedan replicarse.

¿Qué es el monitoreo?

El monitoreo es un proceso sistemático en el que se recolecta analiza y utiliza información para el seguimiento al progreso de una actividad en la consecución del objetivo por el que fue implementada, cuyos resultados guiaran las decisiones de gestión.

Derivado de ello, el monitoreo generalmente es permanente, iniciando el monitoreo a la par del comienzo de la actividad que se va a estar revisando y continuara durante todo el período de implementación, dirigiéndolo a resolver el cómo, cuándo y dónde tienen lugar las actividades, quién las ejecuta y a cuántas personas o entidades beneficia.

En ese sentido, el monitoreo conlleva la vigilancia de los activos, las amenazas, las vulnerabilidades, el impacto de vulnerabilidades ocurridas y el nivel de riesgo conforme a los escenarios de vulneración que se plantean en el análisis de riesgos.

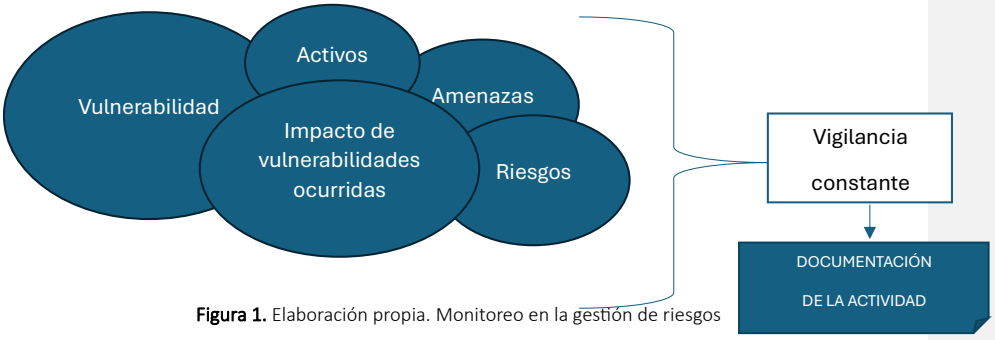


Figura 1. Elaboración propia. Monitoreo en la gestión de riesgos

En suma, la Ley General refiere al monitoreo de manera particular con las medidas de seguridad implementadas, así como a las amenazas y vulneraciones a las que están sujetas los datos personales; de igual manera, a los activos de información que contienen datos personales y los factores del riesgo y a la revisión de estos resultados para la toma de decisiones a futuro.

En ese orden de ideas, debe tenerse presente el hecho de que, el monitoreo, permite que los Responsables consideren lo que desean lograr al evaluar el desempeño de la seguridad de los datos personales y la efectividad de las medidas implementadas, para así, determinar sus necesidades.

Los Responsables deben decidir qué medidas se necesitan para respaldar cada necesidad de seguridad y qué datos se requieren para establecer las medidas de seguridad requeridas. Por lo tanto, el monitoreo siempre debe corresponder a las necesidades en materia de seguridad.

Aunado a ello, los Responsables deberán incorporar a la medición de los resultados las políticas, planes, procesos, y demás elementos que puedan ser medidos con el fin de verificar que estos estén siendo eficaces en el cumplimiento de los objetivos de seguridad.

Además, es necesario considerar que el monitoreo debe ayudar a conocer elementos tales como:

a. Adición, modificación o eliminación en los activos de apoyo en los que residen los datos personales
b. Actividades contenidas en la gestión de riesgos tales como nuevas amenazas y vulnerabilidades no estudiadas con antelación, nuevas amenazas que exploten viejas vulnerabilidades no analizadas, el cambio en el impacto o en alguno de los factores del riesgo, que cambien el nivel de riesgo.
c. Medición de la eficacia del propio sistema de gestión

¿Qué es la Revisión?

El otro de los conceptos que se debe definir es la revisión, la cual, es una apreciación sistemática de una actividad definida en un tiempo. La revisión se concentra en identificar lo que se espera obtener con una acción y conocer a partir de la evidencia obtenida lo que se logró.

Es por lo que, una revisión debe proporcionar información basada en evidencia que sea creíble, fidedigna y útil. Los datos de las conclusiones, recomendaciones y lecciones de una evaluación deben ser usados en los futuros procesos de toma de decisiones relacionados con las actividades en materia de seguridad.

En ese orden de ideas, es que, la revisión implica la evaluación de las medias de seguridad (físicas, técnicas y administrativas), siendo así, la evaluación de las políticas y controles de seguridad con relación a la aplicación que realiza el sujeto obligado respecto de si son necesarias o suficientes para el objetivo del riesgo planteado.[8]

Es importante señalar que la evaluación y revisión de los resultados de las medidas de seguridad, es necesario previamente haber monitoreado que dichas medidas realmente estén atendiendo los

[8]Recomendaciones para la elaboración de Políticas Internas de Gestión y Tratamiento de Datos Personales. p.p. 28 y 29, disponible en: RecomendacionesPolíticasPDP.pdf (inai.org.mx) consultado el 04 de noviembre de 2024.

riesgos analizados[9], es decir, la interpretación de los resultados obtenidos en el monitoreo de las actividades.

Por todo lo anteriormente señalado, los mecanismos de monitoreo y revisión a las medidas de seguridad deben observarse como una actividad permanente en todas las fases que corresponden a la gestión de riesgo, dicha actividad permitirá valorar las medidas de seguridad con la finalidad de darle tratamiento a este.

[9] Recomendaciones para la elaboración de Políticas Internas de Gestión y Tratamiento de Datos Personales. p. 30, disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/RecomendacionesPol%C3%ADticasPDP.pdf consultado el 04 de noviembre de 2024.

EL MONITOREO Y REVISIÓN COMO UN PROCESO REPETIBLE

Ahora bien, como se ha mencionado, el monitoreo y revisión son parte de la gestión de riesgos y la gestión de la seguridad de la información, por lo que, se pueden alinear al ciclo de mejora continua previsto en el sistema de gestión, identificando actividades a desarrollar considerando lo establecido en el estándar internacional ISO/IEC 27004:2016[10]

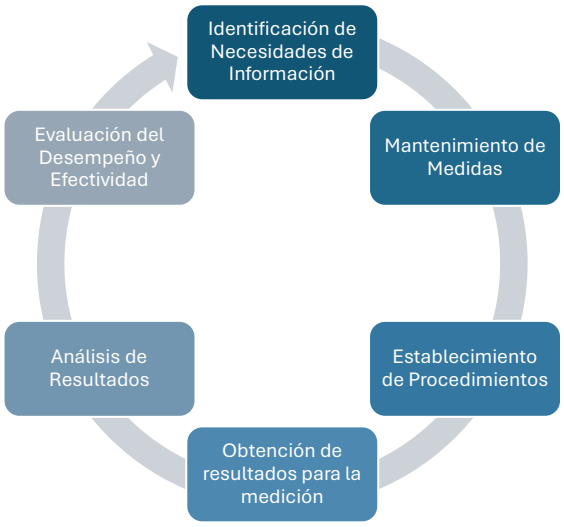


Figura 2. Elaboración Propia. Monitoreo y revisión dentro de la gestión

Partiendo de las actividades de gestión podemos establecer lo siguiente:

1. Identificar las necesidades de información

Este aspecto se refiere a la necesidad de identificar la información a partir del monitoreo de cada una de las necesidades que nos permitan integrar medidas de seguridad. Por lo que ya sea que existan, o bien, que no existan las medidas de seguridad, se debe determinar la necesidad de generar información de su aplicación, es decir, generar registros que permitan conocer las características operativas y o desempeño de cualquier aspecto referente a la gestión de los riesgos, para contemplar estos elementos se pueden identificar directrices de monitoreo tales como:

- Objetivos en materia de seguridad de la información
- Necesidades de la institución
- Generación de información que de sustento a la gestión del riesgo
- Valorar la información generada
- Documentar y comunicar las necesidades de información seleccionadas a todas las partes interesadas relevantes.

[10] Disponible en: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27004:ed-2:v1:en consultado el 04 de noviembre de 2024.

2. Implementar y mantener medidas

Esta actividad implica que las Instituciones se comprometan a revisar las medidas de seguridad y, en su caso, actualizarlas de manera sistemática a intervalos de tiempo planificados o cuando el entorno del sistema de gestión de seguridad de datos personales experimente cambios sustanciales.

3. Establecer procedimientos

Para implementar medidas de seguridad es necesario establecer procedimientos para el monitoreo y revisión, es decir, integrar a todos los involucrados en el proceso de medición de la seguridad a cooperar para entregar información de ayuda que permita realizar un juicio de valor sobre lo que se esta haciendo en materia de seguridad.

Estos procedimientos son diversos, aunque deben de considerar que su implementación genera información a partir de actividades tales como:

- Monitoreo de registros y escaneos.
- Obtención de estadísticas sobre capacitación y otras actividades de recursos humanos.
- Resultados de la aplicación de encuestas y/o cuestionarios realizados a personal que trabaja con los activos
- Registros de incidentes ocurridos
- Resultados de las auditorías realizadas (de cualquier índole)
- Resultados de los ejercicios diversos para conocer el funcionamiento de las medidas de seguridad
- Presentación de informes de revisiones

Lo anterior define diversas maneras en las que se pueden obtener datos de que es lo que esta ocurriendo con la medida de seguridad, a través de mecanismos que permitan realizar recopilación de datos, que incluyan los recursos humanos disponibles para recopilar y gestionar datos, así como la integración de herramientas tecnológicas que automaticen esta actividad, entregando información de soporte. Actividades que permitan generar datos para su posterior análisis

4. Obtención de resultados para la revisión

Como se ha mencionado, el objetivo del monitoreo y la revisión es obtener datos que permitan conocer la interacción de las medidas de seguridad con los escenarios de vulneración que dieron origen a su implementación, ver que las medidas están mitigando los riesgos que se describieron.

Por ello, las actividades de monitoreo son esenciales para la obtención de datos, que, conforme a lo que se ha establecido, deben ser útiles para respaldar las decisiones que se implementen a partir de la interpretación de estos datos de interacción.

Es así como, se puede resumir que las actividades de monitoreo y revisión se encuentran interrelacionados, ya que, son actividades complementarias al plantearse de la siguiente manera:

1- Un monitoreo continuo que recupere información de lo que esta sucediendo con las medidas de seguridad y su interacción con los riegos que puede ayudar a prevenir y
2- Una revisión de todos esos resultados que valore la efectividad de las medidas de seguridad que son instauradas por los análisis que se realizan.

Siendo así que bajo esa lógica podemos decir que el proceso de monitoreo y revisión debe dar respuesta a las preguntas:

- ¿Qué tengo que medir?
- ¿Cómo lo voy a medir?
- ¿Cómo voy a documentar lo que estoy midiendo?
- ¿Qué voy a hacer con los resultados obtenidos?
- ¿Cuándo vuelvo a revisar como parte del seguimiento?

En este punto, es posible establecer un ciclo con acciones especificas que busquen atender esa respuesta de la siguiente manera:

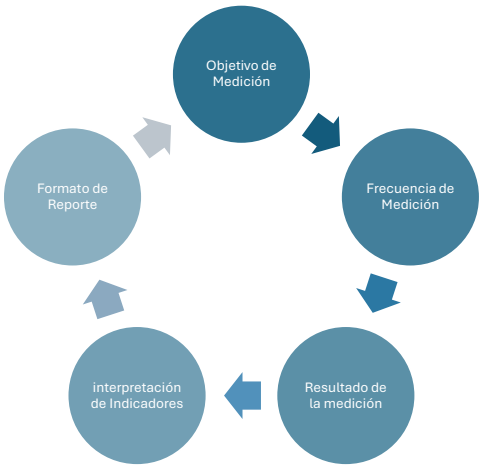


Figura 3. Elaboración propia. Ciclo de actividades para monitoreo y revisión dentro de la gestión

4.1 Objetivo de Medición

En esta actividad debe identificar ¿qué es lo que se quiere lograr con esta actividad?, por ejemplo, conocer la frecuencia de anomalías en el funcionamiento de un activo, cómo adquirir información sobre a la omisión de los usuarios, para aplicar las políticas administrativas, como puede ser el hacer el uso adecuado de las impresoras, el uso de adecuado del correo electrónico y la gestión de contraseñas, entre otros.

4.2 Frecuencia de Medición

Esta actividad se refiere a establecer el tiempo en el que se realizará la revisión de las medidas de seguridad, como, por ejemplo, se puede hacer una recopilación de información por día, por semana, por mes, por bimestre, trimestre, semestre o de manera anual.

Para definir dicha frecuencia, debe considerar el tipo de medida de seguridad que se va a revisar la medida, por ejemplo, las medidas de seguridad tecnológicas, por la cantidad de información que procesan, tienden a ser las revisiones en un periodo inmediato, a diferencia de las medidas de seguridad físicas y administrativas, que, por su mera condición, requieren una programación en periodos más largos.

4.3 Resultado de la Medición

En esta actividad, lo que se debe obtener es un valor de la medición que se realiza de la implementación de medidas de seguridad, es importante mencionar que, en ocasiones la ausencia de resultados no debe entenderse como una falla en la medida de seguridad, sino más bien, debe ser complementada con el nivel de madurez de la medida.

4.4 Interpretación de Indicadores

En este punto se debe considerar el realizar la evaluación analizando cada uno de los riegos, para identificar la efectividad del uso de los indicadores.

4.5 Formato de Reporte

Documento estructurado que sirve como evidencia de la ejecución de los apartados previamente señalados, en los que se da cumplimiento conforme al objetivo que se establece.

5. Analisis de resultados

Ahora bien, obtenidos los resultados, se debe tomar en cuenta que los datos recopilados deben analizarse y/o interpretarse en relación con el objetivo de cada medida individual.

El sujeto obligado que analiza los resultados deberá poder obtener algunas conclusiones iniciales basadas en los resultados. Sin embargo, dado que es posible que el comunicador no esté directamente involucrado en los procesos técnicos y de gestión, dichas conclusiones deben ser revisadas por otras áreas interesadas.

El análisis de datos debe identificar brechas entre los resultados de medición esperados y reales de un sistema de gestión, controles o grupos de controles implementados. Las brechas identificadas pueden indicar la necesidad de mejorar el sistema de gestión implementado, incluido su alcance, políticas, objetivos, controles, procesos y procedimientos.

6. Evaluación el desempeño y efectividad en torno a la seguridad

La evaluación es el proceso de interpretar datos para responder a las preguntas sobre el desempeño de la seguridad de la información de la organización y la efectividad del sistema de gestión por lo que en este punto se deberán:

1. Expresar las necesidades de información en términos de las preguntas de la organización sobre el desempeño de la seguridad de la información y la efectividad del sistema de gestión; y
2. Expresar sus medidas en términos de esas necesidades de información.

Por lo tanto, el análisis de los resultados del seguimiento y la medición proporcionará datos que pueden utilizarse para satisfacer las necesidades de información.

Los procesos de seguimiento, medición, análisis y evaluación deben mejorar continuamente con las necesidades del sistema de gestión. Las actividades de mejora continua pueden incluir, entre otras cosas:

a) Solicitar comentarios de las partes interesadas;
b) Revisar las técnicas de recopilación y análisis, basándose en las lecciones aprendidas y otros comentarios;
c) Revisar los procedimientos de implementación; y
d) Generar datos de evaluación comparativa de seguridad de la información.

Por lo tanto, las instituciones deben realizar con la información obtenida al menos lo siguiente:

a) Conservar la información documentada como evidencia del monitoreo y las mediciones de la organización.
b) Decidir qué es apropiado (pueden documentar el proceso y los métodos utilizados para analizar y evaluar los resultados).
c) Preparar informes en formatos adecuados que faciliten su análisis.
d) Comunicar a quienes toman decisiones los resultados de la medición de la seguridad de la información para buscar generar un cambio orientado a la mejora.

CONSIDERACIONES DEL MONITOREO Y REVISIÓN DE ACUERDO CON LO PREVISTO EN EL MARCO NORMATIVO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Como se ha establecido, se identifica un marco general de consideraciones para establecer una estrategia de monitoreo y revisión a partir de la siguiente primicia:

Monitoreo	Revisión
Obtención de datos útiles de la interacción de la medida de seguridad con el o los riesgos identificados	Interpretación de los resultados del monitoreo.

Establecimiento de tiempo para la de la revisión de los resultados del monitoreo

Como se ha mencionado el monitoreo parte de la recolección de información de la interacción de una o varias medidas de seguridad con el entorno en que los potenciales riesgos pueden dañar los activos físicos y/o digitales en los que se encuentran los datos personales, por lo que, para realizar una recopilación de información se debe establecer una pauta que determine dos acciones:

a) Cada cuanto tiempo se van a recabar los resultados del monitoreo
b) Como se van a presentar estos resultados para su análisis

De manera complementaria, es necesario determinar un calendario que identifique el tiempo en el que se llevaran a cabo las acciones de revisión que interpretaran los resultados la eficiencia y eficacia que tienen las medidas de seguridad, pudiendo establecerse en periodos de tiempo por meses o años, dependiendo de los recursos humanos, físicos, tecnológicos y financieros con los que cuenta el sujeto obligado.

Monitoreo individualizado de las medidas de seguridad

Para la revisión medida a medida de seguridad los sujetos obligados deben definir plazos específicos en función de las necesidades de información, las medidas requeridas y el ciclo de vida de los datos que respaldan las medidas individuales como, por ejemplo, si bien los datos sobre incidentes de seguridad se pueden recopilar continuamente, la comunicación de dichos datos a partes interesadas externas debe basarse en requisitos específicos, como la gravedad o valores agregados.

Los responsables deberán tener en cuenta que, para satisfacer ciertas necesidades de información, antes del análisis, es necesario conjuntar un volumen de información que represente obtener una base significativa para su evaluación y comparación.

Aunado a ello, los responsables deben determinar un límite a la duración de cualquier ajuste (para proceder con la medición del SGSDP) y durante cuánto tiempo deben continuar el seguimiento y la recopilación antes de que puedan comenzar el análisis y la evaluación.

Asimismo, los responsables pueden ajustar sus plazos de medición, a medida que actualizan sus actividades de medición.[11]

De igual manera, las Medidas de desempeño expresan los resultados planificados en términos de las características de la actividad planificada, como el recuento de personas, el logro de hitos o el grado en que se han implementado los controles de seguridad de la información; se pueden utilizar para demostrar el progreso en la implementación de procesos SGSDP, procedimientos asociados y controles de seguridad específicos.

Estas medidas de desempeño utilizan datos que se pueden obtener de actas, registros de asistencia, planes de proyectos, herramientas de escaneo automatizadas y otros medios comúnmente utilizados para documentar, registrar y monitorear las actividades del SGSDP.

La recopilación, el análisis y la presentación de informes de medidas deben automatizarse siempre que sea posible, a fin de reducir el costo y el esfuerzo requeridos y el potencial de error humano.

En cuanto a las medidas de eficacia nos referimos al grado en que se han realizado las actividades planificadas y se han logrado los resultados previstos.

Estas medidas deben usarse para describir la efectividad y el impacto que se realizan del plan de tratamiento de riesgos del SGSDP, así como los procesos y controles que tienen en los objetivos de seguridad de la información de la organización. Estas medidas deben usarse para determinar si los procesos del SGSDP y los controles de seguridad de la información están funcionando según lo previsto y logrando los resultados deseados. Pueden proporcionar la visión más directa sobre el valor de la seguridad de la información para la organización y pueden ser los que deberían ser de mayor interés para la alta dirección.

Tanto la eficacia como el desempeño ayudan a determinar si los procesos del SGSDP y los controles de seguridad de la información se han implementado según lo especificado.[12]

Se recomienda que el responsable revisé y monitoreé constantemente a partir de tres consideraciones:

Revisión de los Factores del Riesgo

Bajo la gestión de riesgos aplicada para identificar las necesidades de las medidas de seguridad que son necesarias para mitigar los riesgos, se puede establecer que la descripción de escenarios de vulneración en donde los activos, amenazas, vulnerabilidades, el impacto y la probabilidad de ocurrencia y el valor del riesgo establecen una directriz para considerar la eficacia y efectividad de la medida de seguridad, surge la particularidad de establecer que estos valores se encuentran en constante cambio, pues debido a su interacción contante con las amenazas en el tiempo se verán reflejados cambios en la valoración final del riesgo, por lo que, se recomienda que se considere esta

[11] ISO/IEC 27004:2016 (E) -Information Technology – Security Techniques- Monitoring, measuement, analysis and evaluation. Página 6- 15/05/2024
[12] ISO/IEC 27004:2016 (E) -Information Technology – Security Techniques- Monitoring, measuement, analysis and evaluation. Páginas 7 y 8 - 15/05/2024

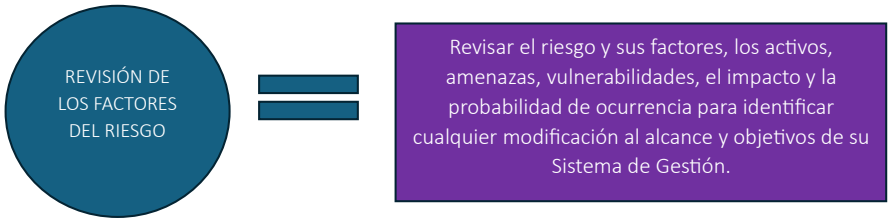
actividad cada que se realice una nueva valoración del riesgo, misma que puede asociarse a su vez con un siguiente catálogo de elementos que activan a la revisión del riesgo.

Catálogo de elementos que activan a la revisión del riesgo[13]	
Naturaleza	• Cambios en la identidad del responsable. • Cambios en la implementación del tratamiento. • Cambios o actualización de elementos tecnológicos. • Sustitución de elementos humanos por elementos técnicos. • Cambios sustanciales en los elementos organizativos. • Cambios sustanciales en los encargos de tratamiento. • Detección de falta de eficacia en las medidas y garantías incluidas en el tratamiento.
Ámbito	• Cambio en la extensión del tratamiento. • Modificación en las categorías de los datos recogidos. • Cambio en el volumen de los datos recogidos. • Cambio en la frecuencia de la recogida de datos. • Modificación del alcance (temporal o espacial)
Contexto	• Cambios importantes en los objetivos de la organización, sus modelos de gobernanza o su cultura. • Cambio en las situaciones que justificaron el tratamiento. • Ocurrencia de incidencias y brechas que se han producido en el tratamiento o tratamientos similares. • Evolución del modelo de amenazas, las incidencias, las brechas o las tecnologías aplicables. • Cambios en el volumen o tipología de solicitudes en el ejercicio de los derechos de los interesados. • Cambios en los marcos o garantías jurídicas. • Cambios en el marco normativo de aplicación. • Cambios sociales, políticos, económicos o estratégicos
Fines	• Cambio o ampliación de los fines principales o secundarios del tratamiento

Tabla 1.- Referenciada de la ISO

Comentado [KEC1]: Poner la ISO

Por lo que, el seguimiento de la valoración del riesgo puede permitir al Responsable determinar si un riesgo se ha materializado y, por lo tanto, indicar qué medidas puede tomar para tratar dicho riesgo.[14]



[13] Gestión del riesgo y evaluación de impacto en tratamientos de datos personales. p.128. Disponible en: https://www.aepd.es/documento/guia-analisis-de-riesgos-rgpd.pdf consultado el 04 de noviembre de 2024.
[14] ISO/IEC 27004:2016 (E) -Information Technology – Security Techniques- Monitoring, measuement, analysis and evaluation . p. 4.

Figura 3.- Elaboración Propia, con información obtenida de la Guía de apoyo para la elaboración del Documento de Seguridad.

Auditorías

Como se ha mencionado en este documento, dentro de los mecanismos para revisar la efectividad de las medidas de seguridad en torno a su interacción con los riesgos, es decir, dar sentido a los resultados del monitoreo conforme a un contexto definido, se encuentra la figura de la Auditoría.

La figura de auditoría se encuentra definida conforme a lo dispuesto en la fracción I del artículo 30 de la Ley General menciona que los sujetos obligados deben "Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales", especificando en el último párrafo del articulo 63 de la Ley General que "el responsable deberá de contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión."

En ese sentido, es necesario identificar los tipos de auditorías que existen y que pueden ser aplicadas por los sujetos obligados, para ello, en suma al concepto de la Ley General, se considera el concepto de auditoría, definido conforme a la ISO 19011:2018 Guidelines for auditing management systems[15], como un proceso sistemático, independiente y documentado para obtener evidencias objetivas y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría, es decir, el conjunto de requisitos usados como referencia frente a la cual se compara la evidencia objetiva.

Dicho dicumento identifica tres tipos distintos de auditoría:

Auditoría de primera parte	Auditoría de segunda parte	Auditoría de tercera parte
Auditoría interna	Auditoría externa de proveedor	Auditoría de certificación y/o acreditación
	Otra auditoría externa de parte interesada	Auditoría legal, reglamentaria o similar

Por lo que, una vez identificados los tipos de auditorías, es necesario conocer el alcance de cada una, destacando que de inicio las que ayudaran a revisar y darle orden a los resultados del monitoreo de las medidas de seguridad son las auditorías internas, mismas que generaran información valiosa que permitirá conocer a grandes rasgos el estado de la seguridad de la información en torno a datos personales bajo los objetivos determinados por el sujeto obligado.

En ese sentido, cada tipo de auditoría tiene un objetivo de cumplimiento especifico, mismo que esta determinado por lo que se quiere alcanzar, identificando que, para una revisión de las medidas de seguridad internas, una auditoría de primera parte es la base para establecer un camino para ir escalando en los tipos de auditorías fijando el alcance de ésta.

Por otra parte, ya que se conoce el tipo de auditoría a aplicar, es necesario conocer las siguientes directrices generales que aplican para una auditoría sin tomar en consideración el tipo de auditoría que se plantee realizar, las cuales conforme a lo dispuesto por la norma ISO 19011:2018 Guidelines for auditing management systems[16] son:

[15] Disponible para su consulta: https://www.iso.org/obp/ui#iso:std:iso:19011:ed-3:v1:es consultado el 04 de noviembre de 2024.
[16] Disponible para su consulta en: https://www.iso.org/obp/ui#iso:std:iso:19011:ed-3:v1:es consultado el 04 de noviembre de 2024.

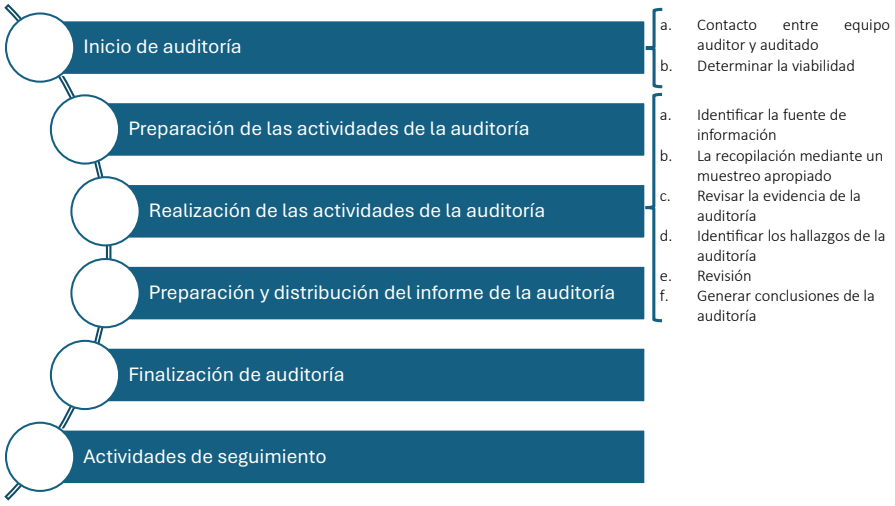


Figura 4. Directrices Generales de una auditoría

Comentado [KEC2]: De dónde se saco este esquema.

En conclusión, es necesario conocer los tipos de auditoría para identificar esta figura como como actividad que permitirá revisar los resultados del monitoreo desde su planteamiento, destacando que los alcances y la manera de ejecutar será determinante para seleccionar el tipo de auditoría a aplicar.

Auditoría voluntaria

Dada la complejidad que pudiera suponer la realización de una auditoría y en concordancia con lo dispuesto en el marco normativo en materia de protección de datos personales para el sector público, fuera del esquema general de los tipos de auditoría se encuentra la figura de la Auditoría voluntaria, misma que esta definida de acuerdo con la Guía de auditorías voluntarias en materia de protección de datos personales[17] como un proceso sistemático, independiente y documentado, iniciado por solicitud de un responsable al Instituto, enfocado a evaluar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados por los responsables para el tratamiento de datos personales, para la obtención de evidencia que permita determinar su conformidad con las disposiciones previstas en la Ley General, los Lineamientos Generales y demás normativa aplicable.

La figura de auditoría voluntaria queda asentada en el articulo 151 de la Ley General que menciona lo siguiente:

> Artículo 151. Los responsables podrán voluntariamente someterse a la realización de auditorías por parte del Instituto o los Organismos garantes, según corresponda, que tengan por objeto verificar la adaptación, adecuación y eficacia de los controles,

[17] Disponible para su consulta en: https://home.inai.org.mx//wp-content/documentos/DocumentosSectorPublico/GuiaAuVol.pdf consultado el 04 de noviembre de 2024.

medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la presente Ley y demás normativa que resulte aplicable.
El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles implementados por el responsable, identificar sus deficiencias, así como proponer acciones correctivas complementarias, o bien, recomendaciones que en su caso correspondan.

Todo lo dispuesto a las auditorías voluntarias puede ser consultado en el capitulo V Auditorías voluntarias de los Lineamientos Generales, el cual abarca del articulo 218 al 231.

De manera complementaria, conforme al artículo 218 de los Lineamientos Generales, los responsables podrán someterse a auditorías voluntarias cuyo objetivo es verificar:

- La adaptación de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en el marco normativo.
- La adecuación de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en el marco normativo.
- La Eficiencia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en el marco normativo.

La finalidad de las auditorías voluntarias es una evaluación preventiva de la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados por un sujeto obligado para el cumplimiento de las disposiciones previstas en la Ley, siendo una actividad que solo pueden realizar los sujetos obligados del marco normativo señalado.

Vulneraciones

La real academia española, define a la vulneración como transgresión, quebrantamiento, conculcación, contravención.[18] Un concepto que permite identificar que una vulneración habla de la materialización de un incidente, el cual dejara un registro de algo que ocurrió, lo cual puede ser analizado para repararse, para mejorarse y para prevenir que no vuelva a ocurrir.

Las vulneraciones se encuadran a lo dispuesto al artículo 38 de la Ley General el cual establece que se consideran vulneraciones de seguridad a la pérdida o destrucción no autorizada, el robo, extravío o copia no autorizada, el uso, acceso o tratamiento no autorizado o el daño, la alteración o modificación no autorizada.

Figura X.- Elaboración Propia. Realizada con información de la Guía de apoyo para la elaboración del Documento de Seguridad.

Comentado [KEC3]: Poner el número de figura.

[18] Disponible en https://dle.rae.es/vulneraci%C3%B3n consultado el 04 de noviembre de 2024.

Las vulneraciones pueden ocurrir en cualquier fase del tratamiento y pueden ser identificadas a través de las revisiones, auditorías, así como indicadores y alertas en el sistema de gestión.

En caso de haber sido afectados por una vulneración a la seguridad de la información, es necesario documentar lo que esta ocurriendo para en un inicio, contener el impacto del incidente y de manera complementaria, contar con registros que describen las fallas en la seguridad que se tenían.

Respecto a la remediación del incidente, conforme al artículo 37 de la Ley General se establece que:

> Articulo 37. En caso de que ocurra una vulneración a la seguridad, el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso, a efecto de evitar que la vulneración se repita.

Lo anterior, implica que una vez identificada la vulneración y después de haber hecho la notificación de esta, se recomienda analizar a fondo respecto de las causas del incidente para establecer medidas correctivas inmediatas que ayuden a reducir los efectos de la vulneración, así como las medidas a largo plazo.

RECOMENDACIONES

Como se ha mencionado, es necesario hacerse de información del monitoreo del funcionamiento particularizado o en conjunto de las medidas de seguridad, por lo cual, es posible integrar actividades diversas que dotaran a los interesados de información para su posterior análisis y la determinación de acciones para el tratamiento de riesgos.

Dentro de las actividades para el monitoreo se debe identificar el tipo de sistema en el que se encuentra el tratamiento a fin de identificar las acciones que permitirán generar datos de valor para su análisis, en el caso de contar con sistemas que en su mayoría incluyan medidas de seguridad físicas y administrativas se pueden realizar acciones tales como:

Recorridos de verificación de cumplimiento a medidas de seguridad

Esta actividad advierte la necesidad de integrar un equipo multidisciplinario que realizara un recorrido o barrido en donde se encuentren los activos que resguardan los datos personales para verificar el cumplimiento de medidas de seguridad físicas tales como cerrar con llave gavetas y cajoneras que resguardan expedientes físicos, ver al personal debidamente identificado, buscar si se tienen equipos de computo desatendidos, impresoras con documentos que pudieran tener datos personales, claves de usuario y contraseñas, entre otras.

Esta actividad permite generar información sobre como interactúan las medidas de seguridad con los riesgos, cómo es que las personas involucradas en los tratamientos cumplen con las políticas y cuidan estos activos que procesan datos personales.

Por otra parte, en el caso particular de los sistemas informáticos que incluyen en su mayoría medidas de seguridad de carácter tecnológico, se pueden realizar acciones tales como:

Pentesting

De acuerdo con el Instituto Nacional de Ciberseguridad de España, el pentesting[19], también conocido como prueba de penetración, consiste en la simulación de un ataque a un sistema software o hardware con el objetivo de encontrar vulnerabilidades para prevenir ataques externos.

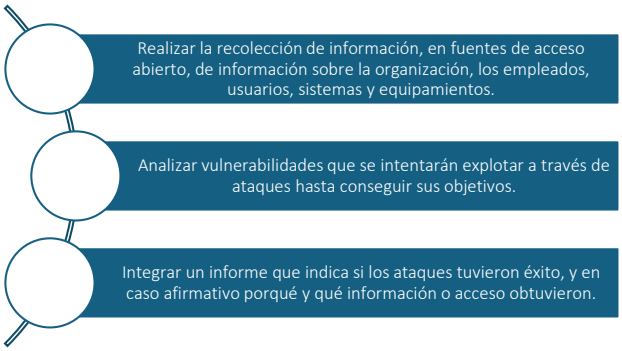
Esta actividad se efectúa mediante un conjunto de ataques simulados dirigidos a un sistema informático con la finalidad de detectar posibles debilidades o vulnerabilidades para que sean corregidas y no puedan ser explotadas.

Existen diferentes tipos de pruebas de penetración según la información inicial con la que cuenta el auditor, así, pueden ser:

- de caja blanca: si disponen de toda la información sobre los sistemas, aplicaciones e infraestructura, pudiendo simular que el ataque se realiza por alguien que conoce la empresa y sus sistemas;
- de caja gris: si dispone de algo de información, pero no de toda;
- de caja negra: si no dispone de información sobre nuestros sistemas; en este caso, se simula lo que haría un ciberdelincuente ajeno.

No obstante, cuando se llegue a contratar un servicio de pentesting además de acordar la finalidad del servicio, el objeto del análisis y qué tipo de prueba se va a realizar, se deben tomar en consideración diversas cuestiones legales.

El proceso para realizar esta actividad es:



El informe obtenido de esta actividad permitirá conocer:

- si el sistema informático es vulnerable o no,
- si las defensas con las que cuenta son suficientes y eficaces,
- la repercusión de los fallos de seguridad que se detecten.

[19] Disponible en: https://www.incibe.es/empresas/blog/el-pentesting-auditando-seguridad-tus-sistemas consultado el 04 de noviembre de 2024.

Comentado [KEC4]: Poner de donde sale este esquema

OWASP Testing Guide

OWASP (Open Web Application Security Project)[20] es una comunidad global de voluntarios y expertos en seguridad informática. Su misión es mejorar la seguridad de las aplicaciones web mediante la concienciación, la educación y la promoción de las mejores prácticas de seguridad. OWASP ofrece una amplia gama de recursos, herramientas y pautas para ayudar a las organizaciones a proteger sus aplicaciones web de amenazas y vulnerabilidades.

En ese marco, surge la herramienta *The OWASP Testing Guide*[21], que es una guía para realizar pruebas de seguridad de aplicaciones web, este es el principal recurso de pruebas de ciberseguridad para desarrolladores de aplicaciones web y profesionales de seguridad.

El WSTG es una guía completa para probar la seguridad de aplicaciones y servicios web. Creado gracias a los esfuerzos colaborativos de profesionales de la ciberseguridad y voluntarios dedicados, el WSTG proporciona un marco de mejores prácticas utilizado por evaluadores de penetración y organizaciones de todo el mundo.

[20] Disponible en: https://www.arsys.es/blog/owasp#tree-1 consultado el 04 de noviembre de 2024
[21] Disponible en: https://owasp.org/www-project-web-security-testing-guide/ consultado el 04 de noviembre de 2024

ANEXO UNICO FORMATO DE REPORTE DE DATOS OBTENIDOS POR EL MONITOREO

Ejemplo de cuadro para realizar el monitoreo y revisión de las medidas de seguridad conforme a las consideraciones que son necesarias para recolectar datos de utilidad y revisarlos para identificar si cumplen con el objetivo por el que fueron implementadas.

Tipo de Medida			Descripción de la Medida	Mecanismo de Monitoreo	Revisor	Periodo para la Revisión	Resultados	Anotaciones	Validador
Fisica	Técnica	Administrativa							

Tabla.- Elaboración Propia

Comentado [KEC5]: De dónde sacamos la información ?