

Gestión del riesgo en las organizaciones

**Breve descripción:**

La innovación digital obliga a enfrentar nuevos retos relacionados con la gestión segura de la información; el crecimiento del mercado, y la globalización de las comunicaciones, hacen mucho más arriesgada la distribución y manejo de los datos, por lo que la gestión del riesgo es fundamental para la seguridad, requiriendo del conocimiento idóneo para tratar los incidentes, que, dentro de este contexto, pueda enfrentar una organización.

**Diciembre 2023**

Tabla de contenido

[Introducción 1](#_Toc152228227)

[1. Fundamentos de gestión del riesgo 3](#_Toc152228228)

[1.1. Caracterización de amenazas 4](#_Toc152228229)

[1.2. Tipos de riesgo 5](#_Toc152228230)

[1.3. Normatividad 6](#_Toc152228231)

[2. Metodologías para la gestión del riesgo 11](#_Toc152228232)

[2.1. Herramientas de apoyo para la gestión del riesgo 13](#_Toc152228233)

[2.2. Métricas e indicadores 15](#_Toc152228234)

[3. Identificación de riesgos 20](#_Toc152228235)

[3.1. Técnicas de recolección de información 22](#_Toc152228236)

[3.2. Valoración de activos 23](#_Toc152228237)

[3.3. Identificación de amenazas 26](#_Toc152228238)

[3.4. Estimación del riesgo 29](#_Toc152228239)

[4. Plan de tratamiento del riesgo 32](#_Toc152228240)

[4.1. Reconocimiento del impacto del riesgo 32](#_Toc152228241)

[4.2. Establecimiento de controles 34](#_Toc152228242)

[4.3. Estrategia de implementación de controles 46](#_Toc152228243)

[5. Evaluación del plan de tratamiento de riesgos 48](#_Toc152228244)

[5.1. Reconocimiento de controles 49](#_Toc152228245)

[5.2. Técnicas de auditoria 49](#_Toc152228246)

[5.3. Plan de auditoria 51](#_Toc152228247)

[5.4. Informe de auditoría 53](#_Toc152228248)

[5.5. Plan de mejoramiento 55](#_Toc152228249)

[Síntesis 57](#_Toc152228250)

[Material complementario 59](#_Toc152228251)

[Glosario 60](#_Toc152228252)

[Referencias bibliográficas 61](#_Toc152228253)

[Créditos 63](#_Toc152228254)

Introducción

Bienvenido a este componente formativo, para comenzar el recorrido por el mismo, revise la información que se presenta a continuación:

1. Gestión del riesgo en las organizaciones



[**Enlace de reproducción del video**](https://youtu.be/9ahtOzNyOVU)

|  |
| --- |
| Síntesis del video: Gestión del riesgo en las organizaciones |
| ¿Sabe por qué es importante la gestión de riesgos?  Pues bien, actualmente las organizaciones tienen como activo principal su información la cual es compartida por diversos canales, por ende, deben garantizar que sus datos estén protegidos y pueda realizar sus operaciones con la mayor tranquilidad posible.  Es innegable que en los últimos años los incidentes de ciberseguridad se han incrementado, causando daños significativos a las organizaciones lo que ha afectado, en muchos casos, la reputación y credibilidad hacia el cliente, pero también ha causado daños en el desarrollo de los procesos necesarios para la prestación de los servicios brindados.  Este panorama que no es únicamente local, ni regional, si no global y debe afrontarse con iniciativas desde los gobiernos, sectores y las mismas organizaciones a partir de una postura preventiva y ofensiva con el fin de salvaguardar los activos de información y evitar este tipo de incidentes.  Desde esta perspectiva, es fundamental tomar acciones que permita gestionar el riesgo en las organizaciones mucho antes de que este llegue a materializarse y generar daños irremediables.  En este orden de ideas, conocer las estrategias, normas y estándares que permitan gestionar de manera adecuada el riesgo es el objetivo del presente espacio de formación. |

# Fundamentos de gestión del riesgo

La gestión del riesgo se consolida como la combinación de actividades encaminadas a reducir una vulnerabilidad, que puede convertirse más adelante en una amenaza que afecte el desarrollo normal de una organización.

La gestión del riesgo se compone de dos actividades principales: el análisis y el tratamiento, las cuales, se revisan a continuación:

* **Análisis del riesgo**

En esta etapa la organización es evaluada, el análisis abarca el estudio de las posibles amenazas, y eventos no deseados, y el impacto, daños, o consecuencias que estos podrían producir a la organización.

* **Tratamiento del riesgo**

Esta etapa, permite establecer los controles y acciones necesarias para hacer frente a todos los riesgos que fueron identificados, de esta forma, evitar que se genere un impacto negativo en la organización.

* **Gestión del riesgo**

Es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza a través de una secuencia de actividades que incluyen la identificación, el análisis y la evaluación de riesgo, para luego establecer las estrategias de su tratamiento, utilizando diferentes recursos.

A continuación, se darán a conocer algunos conceptos importantes para el desarrollo de estas actividades, y como estas pueden ser útiles para hacer frente a los riesgos que pueden afectar a la organización:

## Caracterización de amenazas

Antes de hablar de amenazas es importante comprender el concepto de vulnerabilidad, la cual de acuerdo a INCIBE (2017), se define de la siguiente manera:

* **Vulnerabilidad:** una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información, pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma.

Teniendo en cuenta la anterior definición es más fácil definir lo que se considera una amenaza:

* **Amenaza:** cualquier acción que se aprovecha de una vulnerabilidad, para ocasionar un incidente que puede poner en riesgo la seguridad de la información.

Así mismo, algunas metodologías para la gestión de riesgo, sugiere tener presente las categorías de amenazas, entre las que se pueden resaltar:

* **De origen natural**

Comprende todas las amenazas que son causadas a partir de eventos generados por la naturaleza, y causados de forma natural, por ejemplo: sismos, huracanes, inundaciones, tormentas, entre otros.

* **Del entorno**

Son amenazas generadas a partir de desastres industriales, como por ejemplo sobrecarga eléctrica, infección, contaminación.

* **Defectos de aplicaciones**

Son aquellas amenazas generadas a partir de la debilidad o errores en programas, por ejemplo: “bugs”, desactualización, malas prácticas, entre otros.

* **Causadas por personas de forma accidental**

Como su nombre lo indica, son causadas por las personas, pero que no tenían la intención de generar daño, y se entiende que fue causada por desconocimiento o error.

* **Causadas por personas de forma deliberada**

A diferencia de la vista anteriormente, estas amenazas son causadas con intención o para obtener un beneficio, bien sea causando daños o no.

## Tipos de riesgo

Una vez, identificados y reconocidos los términos de vulnerabilidad y amenaza, es momento de hablar del riesgo, además, resulta fundamental reconocer la relación de dichos conceptos.

El riesgo es entendido como la probabilidad de que se genere un incidente de seguridad, mediante la materialización de una amenaza que aprovechó una vulnerabilidad para materializarse.

Ahora bien, el riesgo siempre existe, y generalmente prevalecen en el tiempo, por ende, es necesario conocer los aspectos fundamentales para su tratamiento, lo que permitirá reducir la probabilidad de ocurrencia o reducir el impacto que puede tener para una organización, de acuerdo a lo anterior, se puede decir que existe un riesgo antes de la gestión y uno diferente después de la gestión realizada, lo que permite categorizar el riesgo de la siguiente manera:

* **Riesgo inherente**

Este tipo de riesgo, es aquel que se identifica sobre un activo de información y sobre el cual, no se ha realizado ninguna acción ni aplicado control alguno.

* **Riesgo residual**

Este tipo de riesgo, corresponde al riesgo que prevalece después de haber aplicado acciones o controles para la mitigación del riesgo.

Se espera que una vez se realiza una gestión del riesgo, el residual sea muy diferente al inherente, ya que se debieron de haber aplicado los controles y/o correctivos para evitar que estos afecten la organización.

## Normatividad

La gestión del riesgo se ha convertido en uno de los insumos principales para la gestión de la ciberseguridad y la seguridad de la información, y esto, se ve reflejado en diferentes propuestas de normatividad tanto técnica como legal. Para las organizaciones salvaguardar la disponibilidad, confidencialidad y la integridad de la información a partir de la aplicación de controles, tanto lógicos como técnicos, se ha convertido en una obligación imperante.

A continuación, se pueden identificar una serie de normas técnicas que orientan la aplicación de este proceso:

**Normas y técnicas para la gestión de riesgo**

ISO:31000 Gestión del riesgo – Directrices: Esta norma comparte las directrices para la gestión de los riesgos en las organizaciones (ICONTEC, 2018).

Dicha norma se fundamenta en 3 elementos claves:

* **Los principios para la gestión de riesgos**

Se aplican para mayor eficacia en una organización.

* **La estructura de soporte o marco de trabajo**

El objetivo de este elemento es integrar el proceso de gestión de riesgos con la dirección, para que esta adquiera un fuerte compromiso con la implantación de la Gestión del Riesgo.

* **El proceso de gestión de riesgos**

Este proceso consta de tres etapas:

* Establecimiento del contexto,
* Valoración de riesgos y,
* Tratamiento de los mismos.

Además, la norma establece los siguientes principios:

* **Crear y proteger el valor**

Contribuye a la consecución de objetivos, así como la mejora de ciertos aspectos tales como la seguridad y salud laboral, cumplimiento de los requisitos legales y protección ambiental, etc.

* **Estar integrada en los procesos de una organización**

No debe ser entendida como una actividad aislada, sino como parte de las actividades y procesos principales de una organización.

* **Formar parte de la toma de decisiones**

La gestión del riesgo ayuda a la toma de decisiones evaluando la información sobre las distintas alternativas.

* **Tratar explícitamente la incertidumbre**

La gestión del riesgo trata aquellos aspectos de la toma de decisiones que son inciertos, la naturaleza de esa incertidumbre y como puede tratarse.

* **Ser sistemática, estructurada y adecuada**

Contribuye a la eficiencia y, consecuentemente, a la obtención de resultados fiables.

* **Basarse en la mejor información disponible**

Los “inputs” del proceso de gestión del riesgo están basados en fuentes de información como la propia experiencia, la observación y la opinión de expertos.

* **Estar hecha a la medida**

La gestión del riesgo está alineada con el contexto externo e interno de la organización, y con su perfil de riesgo.

* **Tener en cuenta factores humanos y culturales**

Reconoce la capacidad y percepción de los empleados y personas interesadas, esto puede facilitar o dificultar la consecución de los objetivos de la organización.

* **Ser transparente e inclusiva**

La apropiada y oportuna participación de los grupos de interés (“stakeholders”) y, en particular, de los responsables a todos los niveles, asegura que la gestión del riesgo permanece relevante y actualizada.

* **Ser dinámica, iterativa y sensible al cambio**

La organización debe velar para que la gestión del riesgo detecte y responda a los cambios de la empresa y de su entorno.

* **Facilitar la mejora continua de la organización**

Las organizaciones deberían desarrollar e implementar estrategias para mejorar continuamente, tanto en la gestión del riesgo como en cualquier otro aspecto de la organización.

Esta norma considera que la aplicación y relación de políticas, procedimientos y prácticas, conforman el proceso general de la gestión de riesgos.

Como es común en todas las normas ISO, esta norma incorpora el ciclo PHVA para el proceso de mejora continua y para garantizar que sea permanente en las organizaciones, generando una cultura de la seguridad basada en la gestión del riesgo.

* **ISO:27001 Tecnología de la información**

Técnicas de seguridad, sistemas de gestión de la seguridad de la información.

**Requisitos:** esta norma brinda los lineamientos para el establecimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI) en una organización.

Un sistema de gestión de la seguridad de la información se entiende como un sistema compuesto por una serie de procesos para implementar, mantener y mejorar de forma continua la seguridad de la información tomando como base los riesgos que afectan la seguridad en una organización (ICONTEC, 2018).

* **ISO:9001 Sistemas de gestión de la calidad**

**Requisitos:** esta norma brinda las orientaciones para el establecimiento de los sistemas de gestión de la calidad en las organizaciones.

En su última versión, adopta un enfoque basado en procesos para los sistemas de gestión de la calidad, buscando siempre un mejoramiento de los procesos, procedimientos y productos de las organizaciones (ICONTEC, 2015).

Además, adopta un pensamiento basado en riesgos en la aceptación de su sistema, con el cual se busca mantener un adecuado control de los activos de información de las organizaciones.

* **ISO:55002 Gestión de activos, Sistemas de gestión**

Esta norma da continuidad con la norma ISO 55000 con la cual se contempla el concepto, terminología y entorno de cuidado de los activos, con la norma ISO 55001 que indica los requerimientos para el Sistema de Gestión de Activos- SGA, La ISO 55002 comparte la interpretación y guía de implementación de las normas en las organizaciones (“UpKeep”, 2023).

La norma ISO 55002, resalta como establecer un programa de gestión de riesgos aplicado a los activos, agregándole un plus al programa integrado de gestión de activos, dando a la alta dirección una mejor comprensión de la relación entre la gestión de activos y la gestión de riesgos.

* **ISO:19011 Directrices auditoría de los sistemas de gestión**

Esta norma brinda los lineamientos para la auditoria de cualquier sistema de gestión.

Puede aplicarse a cualquier tipo de organización, independiente si mantiene un sistema de gestión o no, pero su apropiación es de vital importancia para validar el cumplimiento del sistema dentro de la organización (ICONTEC, 2018).

# Metodologías para la gestión del riesgo

Las metodologías, permiten articular y orientar las actividades y acciones para desarrollar y alcanzar una meta, en este caso será la de realizar una adecuada gestión del riesgo a la que pueda estar expuesta la información en las organizaciones, estas metodologías suelen estar enmarcadas en una serie de actividades relacionadas con los activos de la información con las que cuenta la organización.

Las cuales se encuentran enmarcadas en los siguientes objetivos:

* Reconocer los tipos de riesgo que llegan a afectar las organizaciones.
* Realizar la evaluación y proponer salvaguardar la información, para controlar y mitigar dichos riesgos.

La aplicación de estas metodologías para la gestión del riesgo en las organizaciones permitirá obtener entre otros, las siguientes características:

* Que la gestión del riesgo se convierta en un proceso continuo, lo que permitirá que este se mejore a través del tiempo y de las lecciones aprendidas.
* La aplicación de métodos, permitirá identificar y establecer controles para la gestión de riesgos basados en buenas prácticas.
* La gestión del riesgo deberá ser adoptada como parte de la cultura organizacional, con el fin de que esté presente en todas las actividades de la organización.

Todo esto permitirá obtener beneficios que a mediano y largo plazo pudiendo llevar a las organizaciones, más adelante y evitar problemas relacionados con la seguridad de la información, algunos de los beneficios que se esperan son:

* Mejorar los procesos de toma de decisiones en la organización.
* Mejorar la visión del negocio de la organización.
* Aprovechar los recursos para el desarrollo del negocio.
* Prevenir incidentes que pueden afectar las operaciones de la organización.
* Fortalecer los sistemas de gestión y de control de la organización.

Dinámicas que deberán estar apoyadas por normas y estándares, entre las primeras se resalta la ISO 31000 y la metodología “MAGERIT”, aunque hay otras metodologías que pueden ser útiles, estas son las más reconocidas y recomendadas en la actualidad, las cuales generalmente nos sugieren etapas o fases para la aplicación y el desarrollo de las mismas.

Las etapas para la gestión de riesgo permitirán adelantar las actividades y acciones de manera organizada y sistemática, a continuación, se describen las 4 principales:

1. **Etapa 1. Identificar Riesgos**

Etapa donde las organizaciones reconocen cada uno de sus activos importantes para el ejercicio de sus operaciones, lo que permitirá identificar vulnerabilidades y amenazas que pueden llegar a afectarla.

1. **Etapa 2. Evaluar Riesgos**

A partir de las vulnerabilidades y amenazas identificadas, se posibilita realizar la correspondiente evaluación del riesgo, medir la probabilidad y la criticidad que tendría en caso de llegar a materializarse.

1. **Etapa 3. Reaccionar ante Riesgos**

Es donde se establecen las acciones y actividades que realizará la organización para prevenir que una vulnerabilidad o amenaza afecte la organización.

1. **Etapa 4. Controlar Riesgos**

Un seguimiento y evaluación de la adecuada aplicación y pertinencia de las acciones adelantadas para gestión del riesgo, permitirá aplicar mejoras y nuevas acciones con el fin de fortalecer el sistema, o hacer frente a nuevas amenazas.

## Herramientas de apoyo para la gestión del riesgo

Una de las características que hace que la gestión de riesgos sea interesante es su capacidad de albergar y analizar información proveniente de varios sistemas, son las herramientas e instrumentos de las cuales hace uso, y que son necesarios para su análisis y el establecimiento de controles de acuerdo a las necesidades establecidas.

Las herramientas necesarias para la gestión de riesgos pueden variar dependiente de la organización, entre ellas se pueden resaltar:

1. **Lista de chequeo**

Son instrumentos para la recopilación de información en la auditoría interna, los cuales permiten reconocer puntos críticos y verificar los controles de prevención y mitigación se estén cumpliendo.

1. **Matriz de riesgo**

Este instrumento es útil para identificar, evaluar y clasificar en orden prioritario las amenazas o posibles eventos negativos, para abordarlas en función de su importancia, este instrumento se desarrolla en una tabla en la que se califica con números la probabilidad de que un riesgo se concrete. Permitiendo identificar las posibles causas, para poder establecer medidas de prevención.

1. **Matriz de impacto**

Similar a la anterior. Permite categorizar y priorizar riesgos en función del daño que puede generar a la organización. Suele unificarse con la matriz de riesgo, para permitir presentar la información y facilitar su análisis.

1. **Registro de riesgos**

Instrumento que permite el registro de amenazas, con el fin de planificar los esfuerzos y los recursos a emplear para su tratamiento.

1. **Diagrama de “Ishikawa”**

Aborda todos los factores involucrados en un proceso productivo: material, método, maquinaria, medio ambiente y recursos humanos.

La idea es, mediante una lluvia de ideas o sesiones de creatividad, comprender las causas que originan los problemas y así eliminarlos.

1. **Planillas de datos como hojas de cálculo**

Este tipo de recursos permite consolidar la mayor parte de las herramientas antes descritas. Una debilidad, es que el ingreso de información se realiza de forma manual, lo que facilita el registro errado de datos, generando inconsistencias en la información.

## Métricas e indicadores

Como todo proceso de evaluación, es necesario contar con un referente que facilite comparar el rendimiento o mejora de una acción, un control o alguna salvaguarda que permita identificar el nivel de tolerancia ante una amenaza en un activo de información.

Es así como, para el procedimiento de gestión de riesgos es necesario el establecimiento de las métricas o indicadores que permitan visualizar que tan seguro es un determinado activo. Las métricas admiten establecer un nivel de medición cuantitativo en relación al cumplimiento de un requisito de un control que implemente la organización para alcanzar un objetivo.

Estas métricas están organizadas en 2 categorías, como son:

* **Métrica indirecta:** esta se enfoca en la calidad, complejidad, fiabilidad, eficiencia, funcionalidad, facilidad de mantenimiento, entre otros.
* **Métrica directa:** se enfoca en velocidad de ejecución, defectos encontrados en una cantidad de tiempo, costo, tamaño de memoria usada, número de líneas de código, entre otros.

Para el caso de las métricas enfocadas en seguridad, estas permiten evaluar los controles implementados, el cumplimiento de los objetivos de seguridad establecidos y el grado de afectación que puede recibir un activo de información por la materialización de alguna amenaza.

Las métricas de seguridad son usadas en las auditorias para:

1. Gestionar la seguridad de la información en una organización.
2. Brindar la información necesaria para la generación de informes.
3. Cumplir con legislación, reglamentación y normas que rigen una organización.
4. Apoyar la gestión de riesgos.

Además, estas métricas deben de conservar las siguientes características:

1. Deben ser alcanzables.
2. Debe ser expresadas en escalas de porcentaje o escalas numéricas.
3. Deben explicar los componentes evaluados.
4. Deben permitir identificar puntos débiles.
5. Debe permitir conocer los riesgos a los que se enfrenta la organización.

**Como se mide la seguridad en una organización:**

Uno de los objetivos de las estrategias de seguridad es garantizar los pilares de la seguridad de la información a partir de la implementación estrategias, acciones y controles, pero como se indicó anteriormente, estos deben poder medirse para conocer el grado de eficiencia, es aquí donde es necesario hacer uso de las métricas las cuales permiten medir el cumplimiento de los controles propuestos e implementados, estas métricas permitirán identificar el nivel de apropiación en los 3 niveles de decisión de una organización como son: Operativo, Táctico y Estratégico como se puede observar a continuación:

* **Operativo:** 
  + Integridad.
  + Disponibilidad.
  + Confidencialidad.
* **Táctico:**
  + Servicios.
  + Aplicaciones.
  + Perímetro.
* **Estratégico:**
  + Administración de riesgos.
  + Objetivos de negocio.
  + Cumplimiento.

Los objetivos de seguridad de la organización deben de alinearse con los objetivos de negocio de la organización, de tal manera que se identifiquen los procesos que se deben de cubrir, y a partir de allí establecer los controles necesarios.

A continuación, se van a revisar de manera detallada algunos ejemplos de métricas de seguridad que pueden ser utilizados para cada uno de los niveles:

* **Métricas de nivel estratégico:** 
  + Conocer el % (tanto por ciento) de las cuentas inactivas de usuario deshabilitadas respecto al total de cuentas inactivas.
  + Conocer el valor total de los incidentes de seguridad informática respecto al presupuesto total de seguridad informática.
  + Conocer el % (tanto por ciento) de los nuevos funcionarios que completaron su entrenamiento de seguridad respecto al total de los nuevos funcionarios que ingresaron.
  + Propósito de esta métrica: desempeño de personas y procesos.
* **Métricas del nivel táctico:**
  + Conocer el número de mensajes salientes con spyware o virus.
  + Número de mensajes de spam detectado respecto al número total de mensajes ignorados.
  + Número de estaciones de trabajo en funcionamiento configuradas correctamente respecto total de las estaciones de trabajo.
  + Número de spyware o virus detectados en estaciones de trabajo o servidores.
  + Propósito de estas métricas: desempeño de las tecnologías de seguridad informática.
* **Métricas del nivel operativo:**
  + Número de incidentes asociados con la disponibilidad respecto al total de incidentes.
  + Número de incidentes asociados con la confidencialidad respecto al total de incidentes.
  + Propósito de estas métricas: desempeño de la administración de incidentes.

Ahora bien, a continuación, se van a reconocer algunos de los indicadores más comunes que se realizan y que permiten medir las capacidades de las organizaciones frente a la protección de sus activos de información:

**Indicadores para la protección de los activos de información**

* **Número de riesgos identificados**

Este ejemplo de indicador, permite mantener un registro de los riesgos que han sido identificados en una organización, un proceso o procedimiento especifico, su valor estará relacionado con lo realmente identificado.

* **Número de riesgos que se convirtieron en problema**

Permite identificar, los riesgos que fueron materializados, a partir del indicador anteriormente descrito, este indicador puede ser expresado de manera numérica o de manera porcentual, y representará la cantidad de riesgos identificados que causaron algún daño a la organización.

* **Número de riesgos que ocurrieron más de una vez**

Este indicador es muy importante, ya que permite reconocer de los riesgos presentes, cuales se materializaron incluso después de haber realizado acciones correctivas o preventivas.

* **El impacto previsto contra el real**

Este permitirá conocer si la estimación del impacto que se había calculado es acorde con lo que realmente impactó después de un incidente, en determinado caso que no sean equivalentes se podrá determinar una subestimación o sobreestimación.

* **Número de riesgos que no fueron identificados**

Permitirá reconocer los riesgos frente a los cuales no estaba preparada la organización.

* **Costo de la gestión de riesgos**

Posibilita mantener un control del costo estimado para gestionar el riesgo, frente a lo que realmente está requiriendo.

* **Número de riesgos cerrados**

Este indicador, permite identificar las capacidades que tiene determinada organización para gestionar un riesgo, a partir de allí se pueden establecer acciones de mejora que se gestionen de manera más rápida y efectiva.

# Identificación de riesgos

Para el ejercicio de identificar y reconocer los riesgos que pueden afectar a una organización, es necesario aplicar las metodologías que han sido puestas a disposición para este fin, es aquí, donde se trae como referente a “MAGERIT”, la cual es una metodología para la gestión del riesgo, que está basada en la norma ISO 31000, precisamente en su apartado 4.4 denominado “Implementar la gestión del riesgo”, consolida el marco para la gestión (ICONTEC, 2018), como se observa en la siguiente figura.

1. Marco de trabajo para la gestión de riesgos de acuerdo a ISO 31000

Figura 1 Marco de trabajo para la gestión de riesgos de acuerdo a ISO 31000.
En la figura se representa los siguientes pasos en el mismo orden:
3. Principios.
4.2 Mandato y compromiso
4.3 Diseño del marco de trabajo
4.4 Implementación de la gestión de riesgos, acá interactúa con Magerit
4.5 Seguimiento y revisión del marco
4.6 Mejora continua del marco, y regresa al punto 4.3

**Nota**: adaptado de “MAGERIT”– versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Marco de trabajo para la gestión de riesgos de acuerdo a ISO 31000

3 Principios

* 1. Mandato y compromiso.
  2. Diseño del marco de trabajo.
  3. Implementación de la gestión de riesgos.
  4. Seguimiento y revisión del marco.
  5. Mejora continua del marco.

MAGERIT.

A continuación, se van a reconocer los principales pasos para realizar una identificación de los riesgos en la organización.

## Técnicas de recolección de información

La aplicación de la metodología requiere de un insumo fundamental que es la información, y en esta ocasión el primer paso a realizar es la recopilación de la información tanto de la organización, como de los activos de la misma, lo cual serán objeto de la evaluación.

Un insumo principal para realizar una evaluación de riesgos, es en primer lugar, conocer la organización en la cual se va a trabajar, funciones, procesos, áreas, así como todos y cada uno de los activos de información importantes para el desarrollo de las operaciones, en este orden de ideas, se puede hacer uso de las siguientes técnicas:

* **Seguimiento en medios**

Realizar el seguimiento a través de medios como las redes sociales y páginas web, permite reconocer la importancia en el medio de la organización.

* **Entrevista**

Se debe realizar con personas preseleccionadas, a las cuales se les realizarán preguntas para conocer más de la organización, procesos, activos de información, y todos aquellos detalles importantes y que pueden ser útiles para analizar.

* **Lectura de documentos**

Esta técnica se basa en la revisión de otros recursos, como libros, documentos, registros, que hayan sido entregados a los funcionarios y que no están siendo objeto de revisión.

* **Encuesta**

Esta técnica se realiza a partir de una interrogación a terceros, mediante instrumentos que permiten documentar aspectos generales, y que sea útil para conocer las respuestas de cada uno de los actores. Estas encuestas pueden realizarse a partir de cuestionarios tanto impresos, como en línea.

* **Observación**

Esta técnica permite identificar comportamientos, hechos, reconocimiento de lugares y actividades, y que pueden ser útiles para tomar decisiones.

## Valoración de activos

En esta etapa es necesario que se identifiquen todos los activos relacionados con los procesos de negocio que se deben proteger, teniendo en cuenta los siguientes elementos en un sistema de información:

* Información propia.
* Información de terceros.

Entre los activos de información que se deben de identificar, se encuentran:

* Datos.
* Servicios.
* Aplicaciones Informáticas.
* Equipos informáticos.
* Soportes de información.
* Equipamiento auxiliar.
* Redes de comunicaciones.
* Instalaciones.
* Personas.

Otro aspecto importante por identificar será la dependencia entre los activos, lo cual es fundamental para determinar la relación y la correspondiente necesidad de un activo para con todo el sistema, estas dependencias se deben de estructurar a manera de árbol, lo que va a permitir establecer las ramas de relaciones, entre las más comunes se pueden encontrar:

**Dependencia de activos**

* **Activos Esenciales**
  + Información que se maneja.
  + Servicios prestados.
* **Servicios Internos**
  + Que estructuran ordenadamente el sistema de información.
* **Instalaciones físicas, personal**
  + Usuarios.
  + Operadores y administradores.
  + Desarrolladores.
* **Equipamiento Informático**
  + Aplicaciones (“software”).
  + Equipos informáticos (“hardware”).
  + Comunicaciones.
  + Soportes.
  + De información: discos, cintas, etc.
* **Del entorno**
  + Activos que se precisan para garantizar las siguientes capas:
  + Equipamiento y suministros: energía, climatización, etc.
  + Mobiliario.
  + Servicios subcontratados a terceros.

Otro aspecto muy importante a tener presente, será la valoración del activo, aquí, se debe dar respuesta a las siguientes preguntas, teniendo en cuenta las diferentes dimensiones:

**Valoración de un activo**

1. **Confidencialidad**

¿Cómo afectaría que la información la conociera un tercero que no debe?

1. **Integridad:**

¿Cómo afectaría a la organización, si la información es dañada?

1. **Disponibilidad**

¿Cómo afectaría que una organización no pueda consultar o acceder a la información?

1. **Autenticidad**

¿Cómo afectaría no conocer las acciones desarrolladas sobre la información?

1. **Trazabilidad**

¿Cómo afectaría no tener un registro detallado de las transacciones sobre la información?

Una vez se cuente con la información anterior, se podrá continuar con las valoraciones tanto cualitativa como cuantitativa, estas permiten realizar la valoración sistemática de los activos, a partir del establecimiento de escalas de medición:

* **Valoración cualitativa**

Permite evaluar rápidamente un activo, identificando el peso de cada activo en comparación con los demás.

* **Valoración cuantitativa**

Estas valoraciones, se presentan en escalas numéricas absolutas las cuales son algo complejas de establecer; pero permiten operaciones matemáticas para sus evaluaciones.

Un último elemento a tener presente en la caracterización de los activos es valorar la interrupción del servicio, ya que esta apreciación se diferencia de las anteriores porque afecta directamente la disponibilidad, por ende, se requiere determinar el costo de tener por fuera el servicio por un determinado tiempo, esta valoración se debe establecer en una línea de tiempo que permita identificar claramente las consecuencias de no contar con un sistema de información disponible y su impacto para la organización.

Los anteriores criterios son necesarios para identificar y caracterizar cada uno de los activos de la organización, y así poder continuar con la identificación de amenazas para cada uno de ellos.

## Identificación de amenazas

De acuerdo a la metodología “MAGERIT”, y como ya se mencionó anteriormente, existen una serie de amenazas “típicas”, entre las que se encuentran:

* Naturales.
* Industriales.
* Por errores de aplicación.
* Causadas por las personas de forma accidental.
* Causadas por las personas de forma deliberada.

Las amenazas sugeridas no necesariamente deben aplicarse a todos los activos, pero se debe determinar cuál es la relación entre el activo y la existencia de la amenaza, para identificar como esta pueda afectarlo en un determinado momento.

Una vez se haya realizado la identificación de las amenazas, se procede a realizar la valoración de las mismas, y así reconocer cual sería el efecto de influencia sobre el activo en los siguientes sentidos:

* **Degradación**

Cómo afectaría a un activo, mide el daño causado por un incidente en el supuesto de que ocurriera, y esta se suele caracterizar como una fracción del valor del activo y da origen a expresiones como “activo totalmente degradado” o “degradado” en una pequeña fracción.

* **Probabilidad**

Que tan probable es que una amenaza sea aprovechada y llegue a materializarse en un riesgo.

La complejidad de ocurrencia es difícil de determinar y expresar, y se puede apoyar en escalas de tipo nominal, como la que se muestra a continuación:

1. Ejemplo de escala de degradación del valor por probabilidad de ocurrencia

| MA | Muy alta | Casi seguro | Fácil |
| --- | --- | --- | --- |
| A | Alta | Muy alto | Medio |
| M | Media | Posible | Difícil |
| B | Baja | Poco probable | Muy difícil |
| MB | Muy baja | Muy raro | Extremadamente difícil |

**Nota*:*** con base en “MAGERIT”– versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Ahora bien, en términos de tiempo, lo más recomendado es realizarlo en 1 año para establecer una frecuencia, de tal manera es posible reconocer una escala de probabilidad de ocurrencia de la siguiente manera:

1. Escala de probabilidad de ocurrencia

| MA | 100 | Muy frecuente | A diario |
| --- | --- | --- | --- |
| A | 10 | Frecuente | Mensualmente |
| M | 1 | Normal | Una vez al año |
| B | 1/10 | Poco frecuente | Cada varios años |
| MB | 1/100 | Muy poco frecuente | siglos |

**Nota:** con base en “MAGERIT”– versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

## Estimación del riesgo

Riesgo potencial, se le llama a la medida del daño probable sobre un sistema, teniendo en cuenta el impacto de las amenazas de cada uno de los activos, este riesgo crece con el impacto y la probabilidad, estableciendo las zonas de riesgo como se determinan a continuación:

**El riesgo en función del impacto y la probabilidad**

* **Zona 1**

**Franja roja:** zona de riesgo muy probable, así como de alto impacto.

* **Zona 2**

**Franja amarilla**: abarca un amplio espectro que representa desde las diferentes situaciones improbables y de impacto medio, hasta situaciones muy probables, pero de impacto reducido.

* **Zona 3**

**Franja verde:** riesgos poco probables y de bajo impacto.

* **Zona 4**

**Franja naranja:** riesgos improbables, de muy alto impacto.

Es importante revisar con atención otros tipos de riesgos que se pueden presentar en una organización:

* **Riesgo acumulado**

Este es el riesgo que es calculado sobre un activo de información a partir de:

* + Impacto acumulado.
  + Probabilidad de ocurrencia de la amenaza.

Este riesgo se debe calcular en cada activo, amenaza y dimensión de seguridad, convirtiéndose en una función del valor acumulado, la degradación causada y la probabilidad de la amenaza.

Cuando se calcula sobre los activos base de la información, permite identificar las salvaguardas necesarias para aplicar en los entornos de trabajo: endurecimiento de equipos, “backup”, etc.

* **Riesgo repercutido**

Es el calculado sobre un activo teniendo en cuenta:

* + Impacto repercutido.
  + Probabilidad de ocurrencia de la amenaza.

Este riesgo repercutido se obtiene para activo, amenaza y dimensión de valoración, convirtiéndose en una función del valor propio, la degradación causada y la probabilidad de la amenaza.

Este riesgo, permite determinar las consecuencias de las incidencias técnicas sobre la finalidad del sistema de información. Ya que se consolida como un recurso gerencial que permite la toma de decisiones críticas de un análisis de riesgos.

* **Riesgos de agrupación**

Bajo las siguientes condiciones, se permite la agregación de los riesgos:

* + Se puede agregar el riesgo repercutido a diferentes activos.
  + Se puede agregar el impacto acumulado sobre activos que no sean dependientes entre sí, y no hereden valor de un activo superior común.
  + No debe agregarse el riesgo acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el riesgo al incluir varias veces el valor acumulado de activos superiores.
  + Puede agregarse el riesgo de diferentes amenazas sobre un mismo activo, aunque conviene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes.
  + Se puede agregar el riesgo de una amenaza en diferentes dimensiones.
* **Riesgo residual**

Este riesgo es calculado a partir del conjunto de salvaguardas implementadas y que conllevan a que un activo no esté sujeto a una potencial alteración en su calidad por ende no ha sido degradado.

Su cálculo se determina de la siguiente manera. Tomando como referente que los activos no han cambiado, ni sus dependencias, sino solamente la magnitud de la degradación y la probabilidad de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la probabilidad residual de ocurrencia.

La magnitud de la degradación se toma en consideración en el cálculo del impacto residual.

La magnitud de la probabilidad residual tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

# Plan de tratamiento del riesgo

Como parte integral en el ejercicio de la gestión de riesgo, se encuentra el establecimiento de los planes para el tratamiento del riesgo, para el establecimiento de estos planes es importante apoyarse en normas técnicas como la ISO 19011 (ICONTEC, 2018), la cual brinda las directrices para la auditoria de sistemas de gestión y que puede adoptarse para la conformación de auditorías no únicamente de estos sistemas, si no de cualquier auditoria.

Es importante tener presente que los planes de tratamiento contemplan la identificación y evaluación realizada a la organización y a sus procesos o procedimientos, y de acuerdo a los hallazgos identificados deberá establecerse un conjunto de acciones que unidas, permitirán hacer frente a todas las debilidades de la organización.

## Reconocimiento del impacto del riesgo

El impacto potencial, es reconocido como la medida del daño sobre un activo en particular, a partir de la materialización de una amenaza, este impacto se puede determinar una vez se haya establecido el valor de los activos y su degradación, causando dicha amenaza.

El impacto potencial, se puede clasificar de la siguiente manera:

* **Impacto acumulado**

Es el impacto sobre un activo, teniendo como referencia:

* + El valor acumulado.
  + Las amenazas a las que se puede enfrentar un activo.
* **Impacto repercutido**

Es el impacto que se determina sobre un activo partir de:

* + La importancia para la organización.
  + Las amenazas a las que están expuestas los activos. Este se calcula para cada activo, por cada amenaza y en cada dimensión de valoración.

El impacto se incrementa, cuando mayor es el valor propio de un activo y mayor se degrade el activo de información, así como cuando el activo depende de otros sistemas o viceversa.

El impacto es mayor de acuerdo a su dependencia sobre sí mismo, dicho impacto, permitirá identificar las consecuencias que tendría una afectación para la organización.

**Agregación de valores de impacto**

A continuación, se revisarán algunas condiciones que permiten agrupar algunos criterios y así determinar el impacto:

* El impacto repercutido puede aplicarse sobre activos de diferente tipo.
* El impacto acumulado puede acumularse sobre activos que no sean dependientes entre sí, y no hereden valor de un activo superior.
* No se recomienda agregar el impacto acumulado sobre activos que no sean independientes, dado que esto supondría sobre ponderar el impacto al incluir varias veces el valor acumulado de activos superiores.
* Pueden concluir el impacto de otras amenazas sobre un mismo activo, aunque se recomienda considerar en qué medida las otras amenazas son independientes y pueden ser concurrentes.
* El impacto de una amenaza se puede agregar en diferentes dimensiones.

**Impacto residual**

De acuerdo al conjunto de salvaguardas determinadas y desplegadas, así como también medir la madurez de su proceso de gestión, posibilita que el sistema quede en una situación de posible impacto, el cual debe ser mínimo, a esto se le denomina residual. Y se consolida una vez se haya modificado el impacto, desde un valor potencial a un valor residual.

Su cálculo es determinado a partir de la premisa de que un activo no ha sufrido cambio ni degradación, y que las salvaguardas implementadas han actuado de manera positiva evitando la consolidación de algún tipo de incidente.

El impacto residual puede calcularse a partir de los activos inferiores, o repercutido sobre los activos superiores.

## Establecimiento de controles

En esta etapa, se procede a determinar los controles que serán necesarios para reducir el riesgo, algunas amenazas pueden ser controladas a partir de cambios y acciones de gestión sobre algún activo, pero en otras ocasiones, estas deberán de intervenirse a partir de controles técnicos tecnológicos o procedimentales.

* **Selección de salvaguardas**

Es un ejercicio donde se revisan las posibles acciones necesarias para reducir el riesgo sobre un activo, para lo cual, es necesario tener presente lo siguiente:

1. Tipo de activos a proteger.
2. Dimensión que requiere mejorar la protección.
3. Amenazas sobre las que se actuara.
4. Posibles salvaguardas complementarias.

Además, es necesario determinar un principio de proporcionalidad para este ejercicio.

1. El mayor o menor valor propio o acumulado sobre un activo, tomando como referente lo más valioso y obviando lo irrelevante.
2. La mayor o menor probabilidad de que una amenaza se materialice, tomando como referencia los riesgos más importantes.
3. La cobertura que proporciona cada salvaguarda sobre los riesgos.

Lo anterior permite establecer dos tipos de excepciones sobre las cuales no se ejercerá un control:

* **No aplica**

Cuando una salvaguarda no es adecuada o no se ajusta técnicamente al activo, o no se considera eficiente.

* **No se justifica**

Cuando la salvaguarda es adecuada, pero desproporcionada al riesgo que se desea proteger.

El resultado de estas consideraciones se reflejará en un documento denominado “**declaración de aplicabilidad**” que corresponde a la determinación de las salvaguardas que serán implementadas, como se aplicarán, y cuales, no justificando la decisión.

* **Efecto de las salvaguardas**

Una vez determinadas las salvaguardas, estas deberán ser evaluadas de acuerdo a su impacto sobre el riesgo, así:

1. **Reduciendo la probabilidad de las amenazas**

También denominadas salvaguardas preventivas. Las cuales deben de impedir que una amenaza se materialice.

1. **Limitando el daño causado**

Salvaguardas que reducen la posible degradación del activo, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance.

La lógica de su aplicación, se puede apreciar en la siguiente figura, en donde se integran las salvaguardas al procedimiento de gestión del riesgo.

1. Elementos de análisis del riesgo residual

Figura 2 Elementos de análisis del riesgo residual.
En la figura se representan los activos expuestos a amenazas, que causan degradación residual, con probabilidad residual, igualmente los activos con su valor tienen impacto residual y riesgo residual. Salvaguardar degradación y probabilidad.

**Nota**: con base en “MAGERIT”– versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Elementos de análisis del riesgo residual. Están expuestos a:

**Amenazas**

causan una cierta

Degradación residual, lo que conlleva un impacto residual.

con una cierta

Probabilidad residual produciendo un riesgo residual.

Lo que implica el Salvaguardas para

Tipo de activo.

Dimensión.

Amenaza.

Nivel de riesgo.

**Activos**

Interesan por su valor

Impacto residual.

Riesgo residual.

**Tipo de protección**

La determinación del tipo de protección es fundamental a continuación, se reconocen los tipos sugeridos por la metodología “MAGERIT”:

* **[PR] Prevención**

Salvaguardas preventivas que reducen las oportunidades de que un incidente ocurra. Si la salvaguarda falla y el incidente llega a ocurrir, los daños son los mismos.

**Ejemplos:** autorización previa de los usuarios, gestión de privilegios, planificación de capacidades, metodología segura de desarrollo de software, pruebas en preproducción, segregación de tareas.

* **[DR] Disuasión**

Salvaguarda disuasoria, tiene efecto sobre los atacantes, reduciendo la intención de que estos se atrevan a atacar un activo.

Ejemplos: vallas elevadas, guardias de seguridad, avisos sobre la persecución del delito o persecución del delincuente.

* **[EL] Eliminación**

Son salvaguardas que eliminan un incidente, impidiendo que éste tenga lugar. Actúan antes de que el incidente se haya producido. No reducen los daños en caso de que la salvaguarda no sea perfecta y el incidente llegue a ocurrir.

Ejemplos: eliminación de cuentas estándar, de cuentas sin contraseña, en general, todo lo que tenga que ver con la fortificación o bastionado, cifrado de la información.

* **[IM] Minimización del impacto / limitación del impacto**

Salvaguarda que minimiza o limita el impacto acotando las consecuencias de un incidente.

Ejemplos: desconexión de redes o equipos en caso de ataque, detención de servicios en caso de ataque, seguros de cobertura, cumplimiento de la legislación vigente.

* **[CR] Corrección**

Salvaguarda que actúa después de un incidente, ejerciendo una reparación al activo.

Ejemplos: gestión de incidentes, líneas de comunicación alternativas, fuentes de alimentación redundantes, entre otros.

* **[RC] Recuperación**

Salvaguarda que ofrece la recuperación de un activo que ha sufrido una alteración, regresándolo al estado útil y viable.

Ejemplos: copias de seguridad (“back-up”).

* **[MN] Monitorización**

Salvaguardas enfocadas en la vigilancia y monitoreo de activos para identificar posibles cambios o alteraciones en el normal comportamiento de un activo de información.

Ejemplos: registros de actividad, registro de descargas de “web”.

* **[DC] Detección**

Salvaguarda que detecta un ataque, determinando lo que está sucediendo. No necesariamente debe detener la acción, pero si permite establecer las medidas mínimas necesarias para su protección.

Ejemplos: antivirus, IDS, detectores de incendio, etc.

* **[AW] Concienciación**

Actividades relacionadas con la transferencia del conocimiento para la seguridad de todos los actores involucrados en la organización y que dependan de los activos de información.

Ejemplos: cursos de concienciación, cursos de formación.

* **[AD] Administración**

Salvaguardas relacionadas con los componentes de seguridad del sistema.

Ejemplos: inventario de activos, análisis de riesgos, plan de continuidad.

De acuerdo al modelo anterior, se puede determinar y agrupar las salvaguardas de acuerdo a su efecto sobre una amenaza, como se puede identificar en la siguiente tabla:

1. Tipos de salvaguardas sugeridos por “MAGERIT”

| Efecto | Tipo |
| --- | --- |
| Preventivas: reducen la probabilidad. | [PR] Preventivas. |
| Preventivas: reducen la probabilidad. | [DR] Disuasorias. |
| Preventivas: reducen la probabilidad. | [EL] Eliminatorias. |
| Acotan la degradación. | [IM] Minimizadoras. |
| Acotan la degradación. | [CR] Correctivas. |
| Acotan la degradación. | [RC] Recuperativas. |
| Consolidan el efecto de las demás. | [MN] De monitorización. |
| Consolidan el efecto de las demás. | [DC] De detección. |
| Consolidan el efecto de las demás. | [AW] De concienciación. |
| Consolidan el efecto de las demás. | [AD] Administrativas. |

**Nota**: con base en “MAGERIT”– versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

**Eficacia de la Protección**

Las salvaguardas también por la eficacia en el momento de actuar frente al riesgo para el cual fueron consideradas, una salvaguarda adecuada en 100 % eficaz si combina los siguientes factores:

Desde el punto de vista técnico:

1. Técnicamente adecuada para enfrentarse al riesgo que protege.
2. Aplicación permanente.

Desde el punto de vista de operación de la salvaguarda:

1. Perfectamente desplegada, configurada y mantenida.
2. Existen procedimientos claros de uso normal y en caso de incidencias.
3. Los usuarios están formados y concienciados.
4. Existen controles que avisan de posibles fallos.

Entre una eficacia del 0 % para aquellas que faltan y el 100 % para aquellas que son idóneas y que están perfectamente implantadas, se estimará un grado de eficacia real en cada caso concreto. Para medir los aspectos organizativos, se puede emplear una escala de madurez que recoja en forma de factor corrector, la confianza que merece el proceso de gestión de la salvaguarda:

1. Eficacia y madurez de las salvaguardas

|  |  |  |
| --- | --- | --- |
| Factor | Nivel | Significado |
| 0 % | L0 | Inexistente. |
| 0 % | L1 | Inicial / ad hoc. |
| 0 % | L2 | Reproducible, pero intuitivo. |
| 0 % | L3 | Proceso definido. |
| 0 % | L4 | Gestionado y medible. |
| 100 % | L5 | Optimizado. |

**Nota**: con base en “MAGERIT”– versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Desde la norma ISO/IEC 27001:2013, como norma fundamental para la implementación de sistemas de gestión de la seguridad de la información, se propone una serie de medidas que a partir de su implementación, permite controlar las posibles vulnerabilidades que se presentan en las organizaciones, estas recomendaciones se muestran de manera general y sin sugerir marcas, acciones específicas, ni referencias a productos, su interpretación obedece a las capacidades y la decisión de cada organización para realizar su implementación.

Los controles de seguridad se recomiendan que sean implementados a partir del análisis de riesgos, esto permitirá hacer frente de manera asertiva a las necesidades identificadas en cada uno de los activos de información.

La norma **ISO/IEC 27001:2013** en su anexo A, que equivale a la norma **ISO/IEC 27002:2013**, presenta una propuesta de controles bajo un esquema basada en dominios, los cuales tienen enfoque desde lo operativo, lógico, físico y legal.

Los controles que se proponen en dicha norma, corresponden a las categorías y/o aspectos que deben ser abordados desde la estrategia de seguridad propuesta para contar con un nivel mínimo de resistencia ante cualquier riesgo.

1. Dominios de seguridad de la norma ISO/IEC 27001:2013

*Figura 3 Dominios de seguridad de la norma ISO/IEC 27001:2013
En la figura se representan lo operativo y estratégico, para seguridad operativa, lógica, física, legal.*

**Nota:** ISO/IEC 27001:2013 – Anexo A

De lo Estratégico a lo Operativo

A.5 Políticas de la seguridad de la información. \_\_ A.15 Relaciones con los proveedores.

A.6 Organización de la seguridad de la información.

A.8 Gestión de activos. \_\_\_ A.9 Control de acceso.

A.18 Cumplimiento.

A.11 Seguridad física del entorno. \_\_\_\_ A.7 Seguridad de los recursos humanos.

A.16 Gestión de incidentes de seguridad de la información. \_\_\_ A.17 Aspectos de la seguridad de la información de la gestión continuidad del negocio \_\_\_ A.12 Seguridad de las operaciones. \_\_\_ A.13 Seguridad de las comunicaciones. \_\_\_ A.14 Adquisición, desarrollo y mantenimiento de sistemas.

Estas categorías se enumeran desde la A5 hasta la A18, que corresponden a 14 dominios que representan los niveles de seguridad como son: operativos, lógicos, físicos y legales, y que estos también se pueden identificar desde el ámbito estratégico como operativo, como se puede observar en la siguiente figura:

1. Ejemplo de dominio de la norma ISO/IEC 27001:2013

Figura 4 Ejemplo de dominio de la norma ISO/IEC 27001:2013
La figura 4 indica un ejemplo de dominio de la norma ISO/IEC 27001:2013, mediante el dominio, los objetivos de control y los controles aplicados en dicha norma.

**Nota:** ISO/IEC 27001:2013 – Anexo A

Estos dominios permiten reconocer cada uno de los ámbitos de aplicación y administración, los cuales necesariamente deben ser tenidos en cuenta, estos 3 ámbitos son abordados desde la óptica de la organización y de acuerdo a sus necesidades, activos de información, relación con terceros y desde el análisis de riesgo que se debe realizar.

**Objetivos de control**

Cada uno de los dominios de seguridad que nos presenta la norma ISO/IEC 27001:2013, se encuentra dividido en categorías denominadas objetivos de control. Estos objetivos como su nombre lo indica, representa aquello que se busca obtener con la aplicación de los controles de seguridad, de tal manera que, en un ejercicio de aplicación, su adopción corresponde a las necesidades y problemas que la organización quiere abordar. Se presentan como las propuestas y directrices para la implementación de una estrategia de seguridad, que puede ir desde el endurecimiento de la infraestructura, hasta la consolidación de un sistema de gestión de la seguridad SGSI, y con los cuales se busca garantizar los objetivos de seguridad de la organización.

En este orden de ideas, la estructura de los objetivos de control se presenta en la figura 4, plasmando una idea principal de manera general, acompañada de una descripción de la utilidad del mismo.

## Estrategia de implementación de controles

Una vez se haya realizado la evaluación de los riesgos en los activos de la organización, y se hayan determinado las salvaguardas necesarias para gestionar el riesgo, es recomendable establecer un documento que consolide los controles o salvaguardas necesarios para implementar, este documento se denomina: **Declaración de Aplicabilidad** o también conocido como (“Statement of Aplicability SoA”), se profundiza un poco más en que consiste dicho documento a continuación:

* **Control o las salvaguardas para mitigar riesgos**

¿Has escuchado hablar del documento SoA?. Pues bien, este documento permite a una organización establecer control o las salvaguardas necesarias para mitigar los riesgos.

* **Norma ISO/IEC 27001:2013**

Este se apoya en normas técnicas como la Norma ISO/IEC 27001:2013, la cual sugiere algunas recomendaciones generales para la gestión segura de los activos de información.

* **Análisis y evaluación del riesgo**

Dicho documento debe ser construido a partir del ejercicio de análisis y evaluación del riesgo realizado por los miembros encargados

* **Ajustado las necesidades**

y deberá ser ajustado a las necesidades, sin sobredimensionar o subvalorar el riesgo, así se determinará las acciones necesarias.

* **Ejemplo de documento SoA**

A continuación, se presente un ejemplo de documento SoA, el cual muestra un ejercicio de establecimiento de controles, aplicación, justificación, responsable, así como el plan de acción para implementarlo. En el siguiente enlace puede visualizar en el [**Ejemplo de documento SOA**](https://www.minsalud.gov.co/Ministerio/Institucional/Procesos%20y%20procedimientos/ASIS02.pdf)

* **Diligenciada en su totalidad**

La declaración de aplicabilidad debe ser diligenciada en su totalidad, realizando el registro de todos y cada uno de los controles establecidos por la norma.

* **Aplicables y no aplicables**

Indicando cuales serán aplicables en la organización y cuáles no, y su razón de no aplicabilidad.

* **Aplicable hacia los activos de información**

Así como la forma en que será aplicable hacia los activos de información, de esta manera permitirá a las partes interesadas identificar los controles que se deben realizar y establecer el plan de acción para ejecutarlos.

# Evaluación del plan de tratamiento de riesgos

Como toda estrategia de implementación, es importante evaluar la efectividad de su aplicación, en este caso, corresponde a la evaluación del plan de tratamiento de riesgos que se ha propuesto para gestionar los riesgos en la organización.

La evaluación del plan de tratamiento de riesgos se realiza a partir de:

* **Riesgos identificados**: partiendo de los riesgos que se identificaron en la organización antes de aplicar los controles.
* **Controles implementados**: salvaguardas establecidas e implementadas para la gestión del riesgo.
* **Métricas e indicadores**: registros, métricas e indicadores para la gestión del riesgo establecidas, lo cual nos dará una orientación para conocer su efectividad.

A continuación, se realiza una descripción detallada de cada una de las actividades que una organización determinada debe desarrollar para trabajar en la mitigación y el control de los riesgos:

## Reconocimiento de controles

Es fundamental reconocer los controles existentes desde la última revisión del plan de tratamiento de riesgos, uno de los insumos primordiales es el documento de **Declaración de Aplicabilidad** (SOA), este brindara un punto de partida sobre los controles que se deben de evaluar.

Aquí cobra importancia la documentación de la gestión de incidentes, que permitirá contar con insumos para determinar si las acciones adelantadas fueron eficientes.

## Técnicas de auditoria

La auditoría para la seguridad de la información puede realizarse desde diferentes puntos de vista, y esto permitirá reconocer alguna debilidad o vulnerabilidad presente en la organización.

Las técnicas pueden variar dependiendo del objetivo y el tipo de auditoría que se desea realizar, desde la óptica de la ciberseguridad se pueden apreciar los siguientes tipos de auditoria:

* **Auditoria de vulnerabilidades**

Este tipo de auditorías permite reconocer las fallas de seguridad a la que se enfrentan las aplicaciones con las cuales opera la organización, estaría incluido también la seguridad que se puede desplegar hacia su uso y las debilidades de manejo de las aplicaciones.

* **Auditoria de código fuente**

Permite reconocer la calidad y la seguridad de las aplicaciones desde su código fuente y busca identificar algunas malas prácticas o agujeros existentes que pueden poner en riesgo la seguridad de la información.

* **Auditoria de redes**

Como su nombre lo indica, permite evaluar la seguridad en las infraestructuras de redes conectadas como inalámbricas, incluye la evaluación de dispositivos de gestión y aplicaciones de red (Firewall*,* Router, Switch, Utm, Acces point, etc).

* **Auditoria “web”**

Busca identificar el nivel de seguridad de sitios y portales web de la organización.

* **Auditoria forense**

Se realiza posterior a un incidente sucedido en la organización y busca en primer lugar identificar el origen del incidente, vulnerabilidades explotadas e impacto generado, para tomar decisión y establecer controles necesarios para que no vuelva a suceder.

* **“Hacking” ético**

Se desarrollan a partir de pruebas de penetración o también conocido como “pentesting”*,* con el cual se indagan vulnerabilidades a partir de la búsqueda y posible explotación de sistemas de información, aplicaciones, servicios o infraestructura de red, para determinar el grado de explicación de la organización.

## Plan de auditoria

El ejercicio de la auditoria debe estar enmarcado en un plan que permita establecer su alcance, objetivos, técnicas entre otros aspectos claves para su desarrollo.

La norma ISO 19011, sugiere un ciclo de vida, que permite estructurar los pasos necesarios para el desarrollo de estos ejercicios (ICONTEC, 2018), como lo presenta en la siguiente figura:

1. Flujograma de la gestión de un programa de auditoría

Figura 5 Flujograma de la gestión de un programa de auditoría
En la figura se representan el flujo de planear, hacer, verificar y actuar.
Planear tiene los puntos:
5.2 Establecer los objetivos del programa.
5.2 Determinar y evaluar los riesgos y oportunidades del programa de auditoría.
5.4 Establecer el programa de auditoría.
Pasa el flujo a Hacer con el punto:
5.5 Implementar el programa de auditoría.
Pasa el flujo a verificar con el punto:
5.6 Monitorear el programa de auditoría.
Pasa el flujo a Actuar con el punto:
5.7 Revisar y mejorar el programa de auditoría
Pasa el flujo a Planear con el punto:
6.2 Iniciar auditoría.
6.3 Preparar actividades de auditoría.
Pasa el flujo a Hacer con el punto:
6.4 Realizar actividades de auditoría.
6.5 Preparar y distribuir informe de auditoría.
Pasa el flujo a Verificar con el punto:
6.6 Completar la auditoría.
Pasa el flujo a Actuar con el punto 
6.7 Realizar auditoría de seguimien

**Nota**: tomado de Norma ISO 19011:2018

Flujograma de la gestión de un programa de auditoría.

**Planear.**

* 1. Establecer los objetivos del programa.
  2. Determinar y evaluar los riesgos y oportunidades del programa de auditoría.
  3. Establecer el programa de auditoría.
  4. Iniciar auditoría.
  5. Preparar actividades de auditoría.

**Hacer.**

* 1. Implementar el programa de auditoría.
  2. Realizar actividades de auditoría.
  3. Preparar y distribuir el informe de auditoría.

**Verificar.**

* 1. Monitorear el programa de auditoría.
  2. Completar la auditoría.

**Actuar.**

* 1. Revisar y mejorar el programa de auditoría.
  2. Realizar auditoría de seguimiento.

En material complementario se puede consultar más información sobre el desarrollo una auditoria en la norma ISO 19011.

## Informe de auditoría

Una vez desarrollada la auditoria, en donde se realizaron las verificaciones y validaciones, se podrá dar cierre al ejercicio y proceder a conformar un informe donde se consolidan las conclusiones de la misma; de acuerdo a la norma ISO 19011, este informe deberá de reforzar aspectos como:

* Objetivos de la auditoría.
* Alcance de la auditoría, particularmente la identificación de la organización (el auditado) y las funciones o procedimientos auditados.
* Identificación del cliente auditado.
* Identificación del equipo auditor y de los participantes del auditado que han sido participantes.
* Fechas y locaciones donde las actividades de auditoría fueron llevadas a cabo.
* Los criterios de auditoría.
* Hallazgos de auditoría y evidencia relacionada.
* Conclusiones de auditoría.
* Una declaración del grado en el cual los criterios de auditoría han sido cumplidos.
* Alguna opinión divergente sin resolver entre el equipo auditor y el auditado.
* Las auditorías son por naturaleza un ejercicio de muestreo; como tal hay un riesgo de que la evidencia de auditoría examinada no sea representativa.

Además, se deberá de especificar claramente:

* Plan de auditoría, incluido el cronograma.
* Resumen del proceso de auditoría, presentando cualquier obstáculo encontrado que pudiera disminuir la confiablidad en las conclusiones de auditoría.
* Confirmación del alcance de los objetivos del plan de auditoría.
* Aclaración, si alguna área no puso ser incluida, especificando la causa y justificación.
* Resumen incluyendo conclusiones de la auditoría y los hallazgos principales.
* Buenas prácticas identificadas.
* Plan de acción de seguimiento acordado, si aplica.
* Declaración de la naturaleza confidencial de los contenidos.
* Cualquier implicación para el programa de auditoría o auditorías posteriores.

Este informe deberá ser presentado y entregado a las partes interesadas, líderes de sistemas de gestión o la alta gerencia cuando sea el caso.

## Plan de mejoramiento

Tomando como referencia el informe de la auditoria, en donde se consignaron los hallazgos tanto negativos como positivos de la evaluación realizada, la organización, deberá establecer un plan de tratamiento que permita mejorar las condiciones para hacer frente a los riesgos que pueden presentarse en la organización.

Así mismo se deberá de establecer planes de atención a cada una de los hallazgos, informando de aspectos como son:

* Causas que llevaron a la identificación del problema raíz.
* Responsable de la acción de mejoramiento.
* Actividades destinadas a la remediación del problema o falla.
* Estas deben ser realistas.
* Alcanzables.
* Permitir registro de su aplicación y validez.
* Las actividades no deberán depender de entidades externas.
* Las actividades deben ser establecidas para eliminar la causa detectada.
* Tiempo estimado para aplicar acciones de mejora.

Los planes de mejoramiento deberán contar con revisiones periódicas para validar sus avances y una vez se realicen completamente o se cumpla el tiempo establecido, deberán ser comunicadas al auditor quien verificará su aplicación y dará por cerrado el plan de mejoramiento.

Para la construcción de estos planes de mejoramiento, se pueden apoyar en instrumentos como hojas de cálculo que permiten mantener un registro de las acciones implementadas.

Es así que se puede concluir que el ejercicio de la evaluación del riesgo en las organizaciones es un factor fundamental para mantener la seguridad de los activos de información, este ejercicio debe ser continuo y permanente a partir de su ciclo PHVA, el cual permite el mejoramiento continuo.

Síntesis

Una adecuada gestión del riesgo de manera proactiva y temprana, permitirá hacer frente a cualquier amenaza que se pueda presentar, por ende, resulta fundamental que las organizaciones consideren dentro de sus planes de acción inclusión de políticas y estrategias para el manejo de incidente de seguridad dentro de cada una de sus áreas de trabajo.

Realizar los ejercicios de identificación de vulnerabilidades, así como el establecimiento de las salvaguardas apropiadas permitirá establecer planes de acción en pro del beneficio de la organización, este componente formativo brinda las bases sobre la cuales cualquier tipo de empresa pueda identificar y gestionar los riesgos evitando de esta forma el acceso a diferentes incidentes de seguridad.

Una breve revisión de los temas vistos, se encuentran en el siguiente esquema.

Síntesis
La gestión del riesgo en las organizaciones, parte de la conceptualización relacionada con el riesgo y las posibles amenazas que se encuentran a su alrededor, se basa en la normatividad regulada mediante las normas ISO, y las principales metodologías para su tratamiento, a la vez que tiene en cuenta el establecimiento de controles para su aplicación y tratamiento

Material complementario

|  |  |  |  |
| --- | --- | --- | --- |
| Tema | Referencia | Tipo de material | Enlace del recurso |
| Normatividad | ICONTEC (2018). Norma GTC-ISO- 19011:2018 directrices para la auditoría de los sistemas de gestión. | Libros digitales | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1j5choe/sena_aleph000109369> |
| Normatividad | ICONTEC (2018). NTC-ISO 31000:2018 - Gestión del Riesgo. Directrices. | Libros digitales | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/q6j6k0/sena_aleph000098205> |
| Normatividad | ICONTEC (2018). NTC-ISO-IEC 27001:2013 – Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. | Libros digitales | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1j5choe/sena_aleph000074860> |
| Normatividad | Fernández P., Gómez, L. (2018). Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad. AENOR - Asociación Española de Normalización y Certificación. (pp 36-57). | Libros digitales | <https://elibro-net.bdigital.sena.edu.co/es/ereader/senavirtual/53624?page=36> |
| Estrategia de implementación de controles | Ministerio de Salud y Protección Social. (2022). Declaración de aplicabilidad - ISO/IEC 27001:2013. 3. Anexo A – objetivos de control y controles de referencia, página 4. | Documento | <https://www.minsalud.gov.co/Ministerio/Institucional/Procesos%20y%20procedimientos/ASIS02.pdf> |

Glosario

**Activo de información:** componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos (MAGERIT, 2012).

**Autenticidad:** propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

**Confidencialidad:** la información llegue solamente a las personas autorizadas.

**Disponibilidad:** disposición de los servicios a ser usados cuando sea necesario.

**Integridad:** mantenimiento de las características de completitud y corrección de los datos.

**PHVA:** ciclo determinado por Planear, Hacer, Verificar y Actuar.

Salvaguarda: procedimientos o mecanismos tecnológicos que reducen el riesgo.

**Trazabilidad:** aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.

**Vulnerabilidad:** toda debilidad que puede ser aprovechada por una amenaza.

Referencias bibliográficas

Escorial, Á. Escalera, J., Simón, S. (2019). Guía para la aplicación de UNE-ISO 31000:2018. AENOR - Asociación Española de Normalización y Certificación. <https://elibro-net.bdigital.sena.edu.co/es/ereader/senavirtual/118154>

ICONTEC (2015). ISO:9001 Sistemas de gestión de la calidad. <https://www.normas-iso.com/iso-9001/>

ICONTEC (2018). NORMA GTC-ISO- 19011:2018 Directrices para la auditoría de los sistemas de gestión. <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1j5choe/sena_aleph000109369>

ICONTEC (2018). NTC-ISO 31000:2018 - Gestión del Riesgo. Directrices. <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/q6j6k0/sena_aleph000098205>

INCIBE (2017). Gestión de riesgos - Una guía de aproximación para el empresario. <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf>

ISO/IEC 27001:2013 (2013). NORMA ISO 27001. <https://normaiso27001.es/>

MINTIC. (2016). Seguridad y Privacidad de la Información - Guía de gestión de riesgos. <https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf>

PAe, Portal Administración Electrónica. (2012). “MAGERIT” versión 3 (versión española): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

<https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html>

Tamayo Saborit, M. González e, D. (2020). La gestión de riesgos: herramienta estratégica de gestión empresarial. Editorial Universo Sur. <https://elibro-net.bdigital.sena.edu.co/es/ereader/senavirtual/131885>

Tithink. (2015). Gestión de Riesgos “MAGERIT”. <https://www.tithink.com/publicacion/MAGERIT.pdf>

“UpKeep”. (2020). ISO:55002 ¿Qué es la gestión de activos e ISO 55000? <https://upkeep.com/es/learning/asset-management-iso-55000/#%C2%BFcu%C3%A1les-son-algunos-est%C3%A1ndares-que-lo-definen>?

Créditos

| Nombre | Cargo | Regional y Centro de Formación |
| --- | --- | --- |
| Claudia Patricia Aristizábal | Responsable del Equipo | Dirección General |
| Norma Constanza Morales Cruz | Responsable de Línea de Producción | Regional Tolima - Centro de Comercio y Servicios |
| Hernando José Peña Hidalgo | Experto temático | Regional Norte de Santander –  Centro de la Industria, la Empresa y los Servicios - |
| Jeimy Lorena Romero Perilla | Diseñador Instruccional | Regional Norte de Santander –  Centro de la industria, la empresa y los servicios |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo de Desarrollo Curricular | Regional Santander –  Centro Industrial del Diseño y la Manufactura. |
| Juan Guillermo Zuluaga Saavedra | Experto temático | Regional Tolima –  Centro de Industria y Construcción |
| Humberto Arias Díaz | Diseñador instruccional | Regional Tolima –  Centro de Comercio y Servicios |
| María Inés Machado López | Evaluadora metodológica | Regional Tolima –  Centro de Comercio y Servicios |
| Luis Fernando Botero Mendoza | Diseñador Web | Regional Tolima – Centro de Comercio y Servicios |
| Sebastián Trujillo Afanador | Desarrollador Fullstack | Regional Tolima – Centro de Comercio y Servicios |
| Gilberto Junior Rodríguez Rodríguez | Storyboard e Ilustración | Regional Tolima – Centro de Comercio y Servicios |
| María Alejandra Vera Briceño | Productor y Animador Audiovisual |  |
| Nelson Iván Vera Briceño | Productor y Animador Audiovisual | Regional Tolima – Centro de Comercio y Servicios |
| Oleg Litvin | Productor y Animador Audiovisual | Regional Tolima – Centro de Comercio y Servicios |
| Sebastián Trujillo Afanador | Actividad Didáctica | Regional Tolima – Centro de Comercio y Servicios |
| Jorge Bustos Gómez | Validación y Vinculación en Plataforma LMS | Regional Tolima – Centro de Comercio y Servicios |
| Gilberto Naranjo Farfán | Validación de Contenidos Accesibles | Regional Tolima – Centro de Comercio y Servicios |