



ISO 31000

Gestión del Riesgo

Copyright and Disclaimer

Copyright © T-CERT

Miami, Florida

2024

Todos los derechos reservados.

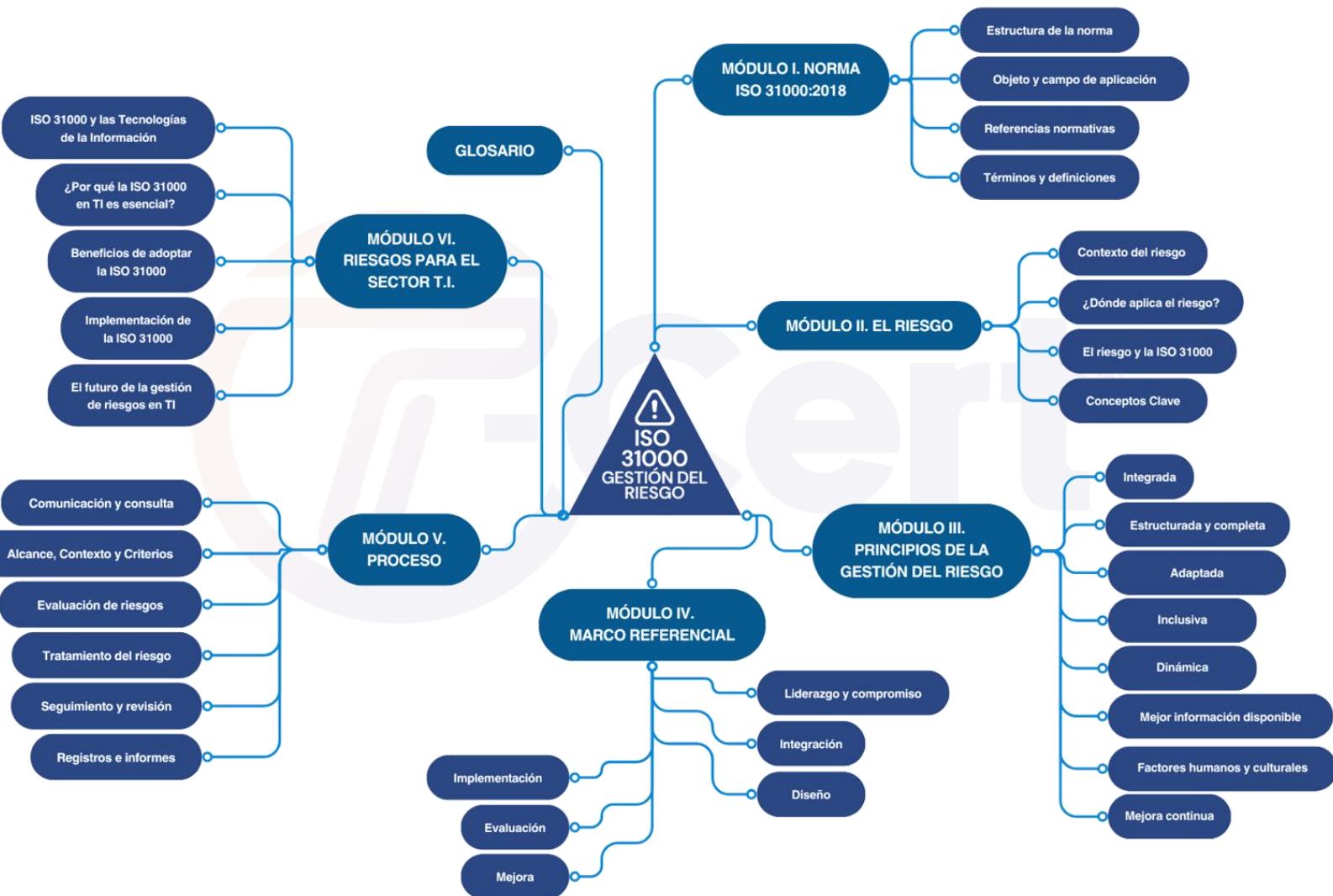
Ninguna parte de esta publicación puede reproducirse, de ninguna forma y por ningún medio, sin el permiso por escrito de T-CERT.

Esta es una publicación comercial confidencial. Todos los derechos reservados. Este documento no puede ser copiado, reproducido en parte, reproducido, traducido, fotocopiado o reducido a cualquier medio sin el consentimiento previo y expreso por escrito del editor. Este curso incluye trabajos sujetos a derechos de autor bajo licencia y está protegido por los derechos de autor

Disclaimer

La información proporcionada sobre el curso, los módulos, los temas y cualquier servicio para los cursos, incluyendo simulaciones o folletos, son sólo una expresión de intenciones y no deben tomarse como una oferta firme o compromiso.

Agenda



Contenido

	Pág.
Módulo I. Norma ISO 31000:2018	8
1.1. Estructura de la norma	9
1.2. Objeto y campo de aplicación	10
1.3. Referencias normativas	10
1.4. Términos y definiciones	11
Módulo II. El riesgo	15
2.1. Contexto del riesgo.....	17
2.2. ¿Dónde aplica el riesgo?	17
2.3. El riesgo y la ISO 31000	18
2.3.1. El ciclo PDCA	20
2.4. Conceptos Clave	21
2.4.1. Taxonomía Básica Del Riesgo.....	21
2.4.2. Elementos adicionales del Riesgo	23
2.4.3. Tipología de riesgos	24
2.4.4. Beneficios de Gestión De Riesgos	26
2.4.5. Planificación estratégica VS Riesgos	26
2.4.6. Medición de un programa de gestión de riesgos	28
Módulo III. Principios de la Gestión del Riesgo	32
3.1. Integrada	33
3.2. Estructurada y completa	33
3.3. Adaptada	33
3.4. Inclusiva	34
3.5. Dinámica	34
3.6. Mejor información disponible	34
3.7. Factores humanos y culturales	35
3.8. Mejora continua	35
Módulo IV. Marco Referencial.....	37
4.1. Liderazgo y compromiso	38
4.2. Integración.....	43
4.3. Diseño	44
4.3.1. Comprensión de la organización y de su contexto.....	44

4.3.2. Articulación del compromiso con la gestión del riesgo	45
4.3.3. Asignación de roles, autoridades, responsabilidades y obligación de rendir cuentas en la organización	48
4.3.4. Asignación de recursos	48
4.3.5. Establecimiento de la comunicación y la consulta	50
4.4. Implementación	52
4.4.1. Proceso de implementación de riesgos basado en decisiones	53
4.5. Evaluación	54
4.6. Mejora	55
4.6.1. Adaptación	55
4.6.2. Mejora continua	55
Módulo V. Proceso	61
5.1. Comunicación y consulta	62
5.2. Alcance, Contexto y Criterios	63
5.2.1. Definición del alcance	63
5.2.2. Contextos externo e interno	64
5.2.3. Definición de los criterios del riesgo	69
5.3. Evaluación de riesgos	72
5.3.1. Identificación del riesgo	72
5.3.2. Análisis del riesgo	74
5.3.3. Valoración del riesgo	77
5.4. Tratamiento del riesgo	82
5.4.1. Selección de las opciones para el tratamiento del riesgo	83
5.4.2. Preparación e implementación de los planes de tratamiento del riesgo	86
5.5. Seguimiento y revisión	88
5.6. Registros e informes	89
Módulo VI. Riesgos para el Sector TI.....	92
6.1. ISO 31000 y las Tecnologías de la Información	92
6.2. ¿Por qué la ISO 31000 en TI es esencial?	92
6.3. Beneficios de adoptar la ISO 31000	93
6.4. Implementación de la ISO 31000	94
6.5. El futuro de la gestión de riesgos en TI	94
6.5.1. Formación del personal	96
6.5.2. Riesgos asociados a la seguridad de la información	96
6.5.3. Riesgos de ciberseguridad	98
6.5.4. Riesgos de Infraestructura Tecnológica	99
6.5.5. Riesgos de acceso y autenticación	99
6.5.6. Riesgos de cumplimiento y regulatorios	100

6.5.7. Riesgos Humanos	100
6.5.8. Riesgos de terceros y asociados de negocio.....	100
Glosario.....	103

Módulo I.

Norma ISO

31000:2018

Módulo I. Norma ISO 31000:2018

La Organización Internacional de Normalización - ISO es una entidad no gubernamental, no dependiente con una membresía aproximada de 162 organismos nacionales de normalización. A través de sus miembros, ISO reúne a expertos para compartir conocimientos y desarrollar estándares internacionales voluntarios, basados en el consenso y asuntos relevantes para el mercado que apoyan la innovación y brindan soluciones a los desafíos globales.

La norma ISO 31000:2018 aceptada mundialmente proporciona las directrices sobre la Gestión del Riesgo. La primera edición de la norma ISO 31000 es del año 2009, y la segunda edición fue lanzada en el 2018, esta edición anula y sustituye a la primera edición (ISO 31000:2009) que ha sido revisada técnicamente. Se destacan las siguientes inclusiones:

- Se revisan los principios de la gestión del riesgo, que son los criterios clave para su éxito.
- Se destaca el liderazgo de la alta dirección y la integración de la gestión del riesgo, comenzando con la gobernanza de la organización; cabe destacar en otro sistema de gestión ISO también se incluyen este ítem.
- Mayor énfasis en la naturaleza iterativa de la gestión del riesgo, señalando que las nuevas experiencias, el conocimiento y el análisis pueden llevar a una revisión de los elementos del proceso, las acciones y los controles en cada etapa del proceso.

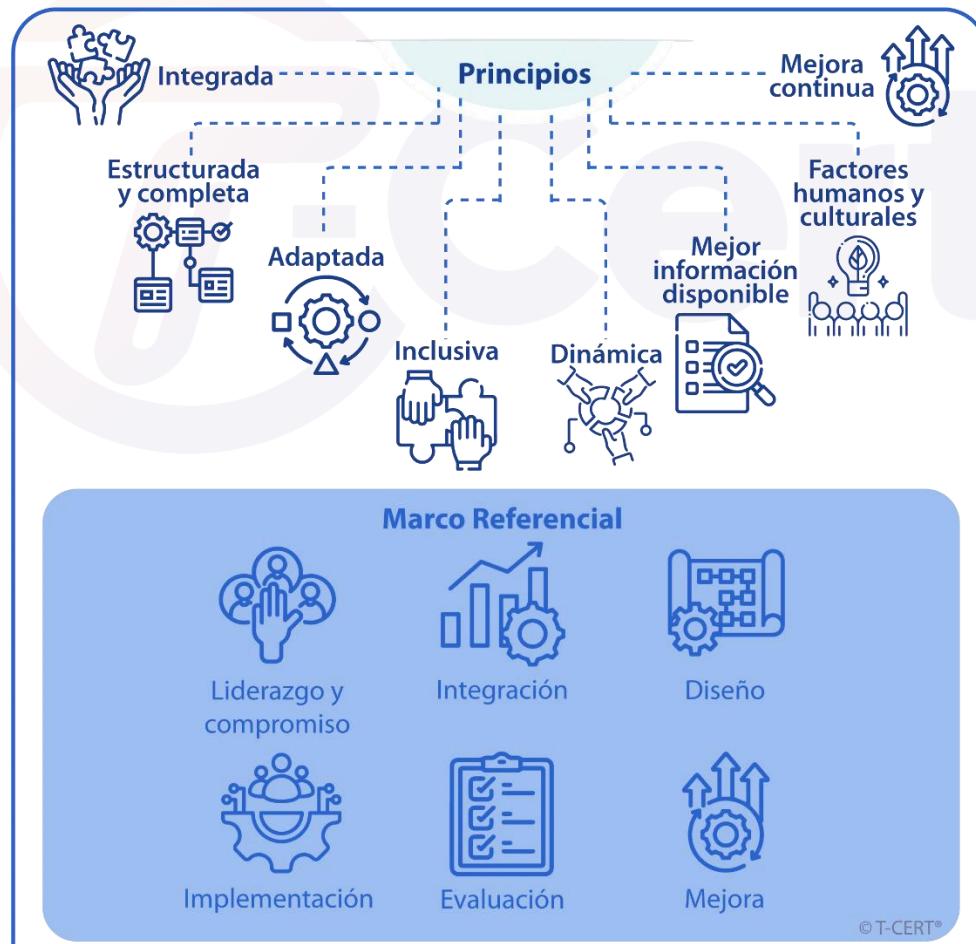


- Se simplifica el contenido con un mayor enfoque en mantener un modelo de sistemas abiertos para adaptarse a múltiples necesidades y contextos.

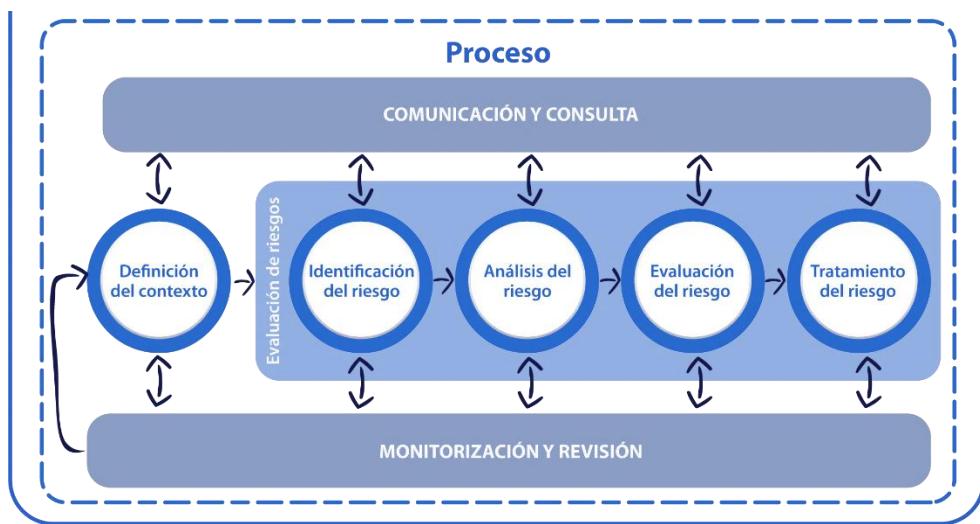
1.1. Estructura de la norma

La norma cuenta con 3 componentes principales: los principios, el marco referencial y el proceso para la gestión de riesgos. Adicionalmente cuenta con una bibliografía y un anexo el cual contiene los principales cambios de la versión anterior de la norma y figuras explicativas para manejo de temas como principios, marcos y procesos.

Estructura de la norma ISO 31000:2018



Continua en la siguiente pagina



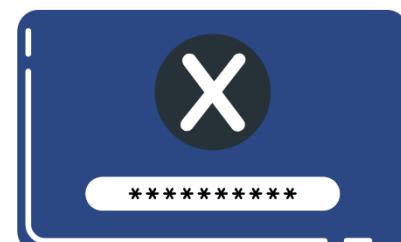
1.2. Objeto y campo de aplicación

La norma ISO 31000 proporciona las directrices para gestionar el riesgo al que se enfrentan las organizaciones. La aplicación de estas directrices puede adaptarse a cualquier organización y a su contexto.

Además, proporciona un enfoque común para gestionar cualquier tipo de riesgo y no es específico de una industria o un sector. Puede utilizarse a lo largo de la vida de la organización y puede aplicarse a cualquier actividad, incluyendo la toma de decisiones a todos los niveles.

1.3. Referencias normativas

La norma ISO 31000 no contiene referencias normativas.



1.4. Términos y definiciones

Para los fines de este documento, se requiere conocer los siguientes conceptos clave:

RIESGO

Efecto de la incertidumbre sobre la consecución de los objetivos.

GESTIÓN DE RIESGOS

Actividades coordinadas para dirigir y controlar la organización con relación al riesgo.

PARTE INTERESADA

Persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad.

FUENTE DE RIESGO

Elemento que, por sí solo o en combinación con otros, tiene el potencial de generar riesgo.

EVENTO

Ocurrencia o cambio de un conjunto particular de circunstancias. Un evento puede tener una o más ocurrencias y puede tener varias causas y varias consecuencias.

Un evento puede ser una fuente de riesgo.

CONSECUENCIA

Resultado de un evento que afecta a los objetivos.

Una consecuencia puede ser cierta o incierta y puede tener efectos positivos o negativos, directos o indirectos sobre los objetivos.

PROBABILIDAD

Posibilidad de que algo suceda.

CONTROL

Medida que mantiene y/o modifica un riesgo.

Los controles incluyen, pero no se limitan a cualquier proceso, política, dispositivo, práctica u otras condiciones y/o acciones que mantengan y/o modifiquen un riesgo.

Adicionalmente, se hace énfasis en un concepto llamado “Iteración” que significa el acto de repetir un proceso con el objetivo de alcanzar una meta deseada, objetivo o resultado.

La gestión del riesgo basada en este concepto se logra con el ejercicio de repetición ya que los riegos son seres vivos que están en evolución, se transforman, mutan y están en constante cambio.

Módulo II.

El riesgo

Módulo II. El riesgo

Comenzamos este apartado con esta introducción que nos permite entender que todo el tiempo convivimos con el **riesgo** y hace parte fundamental de nuestra vida y nuestros negocios.

EL RIESGO

Reír es correr el riesgo de parecer tonto.

Llorar es arriesgarse a parecer sentimental.

Acerca a otro ser es arriesgarse a comprometerse.

Mostrar emoción es arriesgarse a que se te conozca.

Someter a la gente tus ideas y sueños es ponerlos en riesgo.

Amar es correr el riesgo de no ser correspondido.

Vivir es arriesgarse a morir.

En toda esperanza hay el riesgo del desespero.

En todo intento el riesgo de fracasar.

Pero los riesgos se han de tomar porque el mayor peligro en esta vida es no arriesgar nada.

Porque el que nada arriesga nada hace.... Nada tiene..... Nada es.

Tal vez pueda ahorrar sufrimiento y dolor, pero, a fin de cuentas, no puede aprender, ni sentir, ni cambiar, ni crecer, ni amar, ni vivir.

Encadenado por las certidumbres será un esclavo. Sacrificará el ser libre.

Sólo arriesgando se consigue la libertad.

Autor: Anónimo

RIESGO

Es la probabilidad de que un hecho ocurra en el futuro, dependiendo de factores al azar, de personas o de situaciones imprevisibles.

“EFECTO DE LA INCERTIDUMBRE SOBRE LA CONSECUCIÓN DE LOS OBJETIVOS”

El riesgo también puede definirse como la probabilidad de ocurrencia de un evento no deseable, que afecte el logro de los objetivos y metas de una organización.

Para las organizaciones el concepto de riesgo esta referido a la **incertidumbre** sobre los efectos que nuestras acciones generen sobre los objetivos trazados por las mismas.

❖ Dimensiones del riesgo

- La **posibilidad** de que un evento se produzca.
- Las **consecuencias** que se podrían generar como consecuencia de ese evento.

En la mayoría de las definiciones de **riesgo**, se mencionan palabras claves como **probabilidad e incertidumbre**, para la Norma ISO 31000 no resulta ajeno, esta define el riesgo como: “efecto de la incertidumbre sobre la consecución de los objetivos” y lo trabaja en 2 dimensiones, una es la **posibilidad** y la otra es la **consecuencia**.



Sobre los riesgos se pueden sumar estas preguntas, que nos ayudaran a administrar y gestionar el riesgo:

- **¿Qué puede pasar?** Escenarios, cómo pueden verse afectados los objetivos.
- **¿De qué depende que pase?** Variables y factores.
- **¿Qué control tengo sobre esas variables y factores?** Azar y probabilidad.
- **¿Qué efecto tendrá sobre mis objetivos?** Escenarios, consecuencias positivas y negativas.



2.1. Contexto del riesgo

Siniestro	Riesgo
Ya ocurrió	No ha ocurrido
 A photograph of a sunken shipwreck underwater, showing the hull and debris on the ocean floor. Sunlight filters down from the surface.	 A photograph of a steamboat on a river at sunset. The boat is illuminated from within, and steam is rising from its funnels against a backdrop of hills and a colorful sky.
PASADO	FUTURO

2.2. ¿Dónde aplica el riesgo?

El riesgo aplica durante toda la vida de la organización, aplica a todas las actividades, incluyendo la más importante como base para tomar la de decisiones.

¹ Foto tomada de: <https://es.gizmodo.com/un-hallazgo-extraordinario-en-el-mar-negro-el-naufragio-griego-mejor-conservado-de-la-antiguedad-2000139192>.

Las organizaciones están trabajando todo el tiempo en intentar predecir y gestionar riesgos, para esto es importante que se responda a:

- **¿Dónde puede suceder?** Se buscar predecir el lugar físico o geográfico donde se pueda materializar el riesgo.
- **¿Quién lo puede generar?** se intenta buscar los actores generadores de Riesgo.
- **¿Como puede suceder?** Encontrar las diferentes fuentes que puedan materializar Riesgo.
- **¿Cuándo puede suceder?** Entender y análisis el marco de tiempo donde se puede manifestar el riesgo.



2.3. El riesgo y la ISO 31000

La norma ISO 31000 es utilizada como guía en diversos modelos de seguridad o de gestión y aporta las directrices que sirven de guía para la gestión de los riesgos en cualquier ciclo de administración de riesgos.

Es a la gerencia de riesgos, como el agua al ser humano: sirve para todo y se mezcla bien con todo.

Cuando se intenta aplicar este enfoque tan universal en las organizaciones, se encuentra la dificultad de que no se sabe por dónde empezar, ni se realiza de forma correcta una diferenciación por tipo de riesgos, ni mucho menos se crea el espacio para el mejoramiento continuo.

La norma ISO 31000 es una directriz transversal y se puede integrar con cualquier sistema de gestión basado en ISO entre ellos ISO 27001, ISO 9001, ISO 14001, ISO 45001, ISO 28000, ISO 22301 entre otros.



También, se puede integrar con otras metodologías apropiadas que utilizan entes reguladores del gobierno para atención de lavado de activos, financiación del terrorismo (SARLAFT, SIPLAFT, SAGRILAFT y PTTE) así como iniciativas de seguridad como OEA (Operador Económico Autorizado).

Aplicación de gestión del riesgo



El riesgo basa sus premisas en eventos que no han ocurrido, siempre camina hacia adelante, buscar predecir. Sin embargo, se debe aprender de eventos pasados,

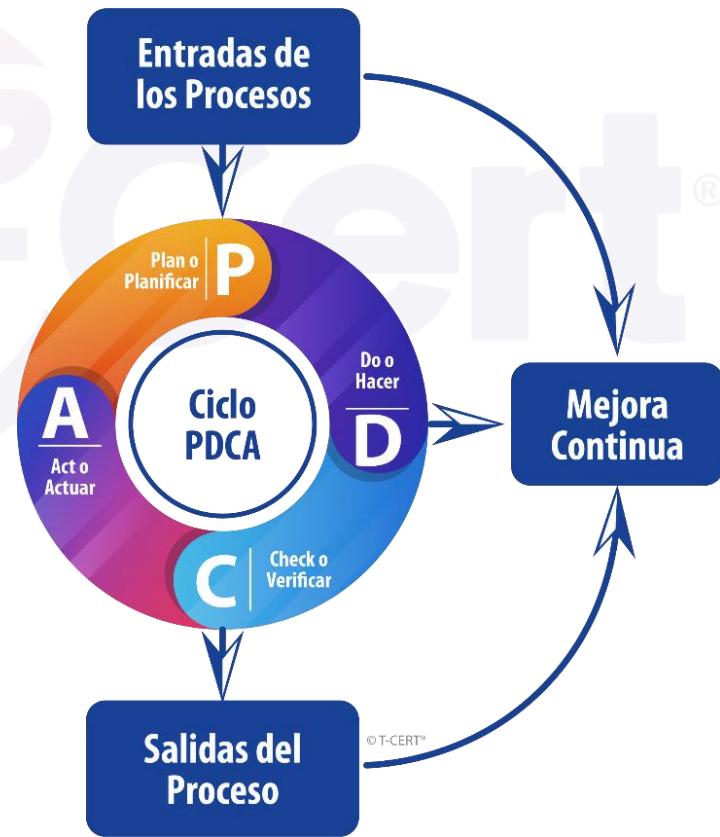
esos hechos que ya ocurrieron, con el fin de generar planes de acción y lecciones aprendidas para administrar de mejor manera.

2.3.1. El ciclo PDCA

La norma trabaja con metodología PDCA o “ciclo de Deming”, como todas las normas ISO existentes.

El PDCA es un método norteamericano que pone en práctica la filosofía de la mejora continua. 4 pasos que deben realizarse cíclicamente, donde es posible identificar el problema, analizarlo, crear un plan de acción, ejecutar, verificar, normalizar y actuar para mejorar.

1. *Plan* (planificar)
2. *Do* (hacer)
3. *Check* (verificar)
4. *Act* (actuar)



Para la “P” podemos ubicar temas como: establecer el contexto, identificar el riesgo, análisis del riesgo y evaluación del riesgo.

Do o
Hacer | **D**

Para la “D” se puede ubicar el tratamiento del riesgo.

Check o
Verificar | **C**

Para la “C” se puede ubicar el monitoreo y revisión

Act o
Actuar | **A**

Y para la “A” se puede ubicar a la mejora y acciones.

2.4. Conceptos Clave

2.4.1. Taxonomía Básica Del Riesgo

2.4.1.1. Amenaza

AMENAZA

Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Es importante identificar hechos que pueden producir daños personales, económicos, de imagen, al cliente y la seguridad.



2.4.1.2. Vulnerabilidad

VULNERABILIDAD

Debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

Se deben determinar las condiciones de factores o procesos físicos, sociales, económicos y ambientales que aumentan la susceptibilidad de impacto de amenazas.

Ejemplo

AMENAZA	RIESGO	IMPACTO O CONSECUENCIA
 ²	 ³	 ⁴

En este ejemplo se puede entender de mejor manera las definiciones ya vistas, en el caso de la amenaza, no es el Toro, es lo que puede causar y el impacto o consecuencia puede variar desde una simple caída hasta corneada y porque no la muerte.

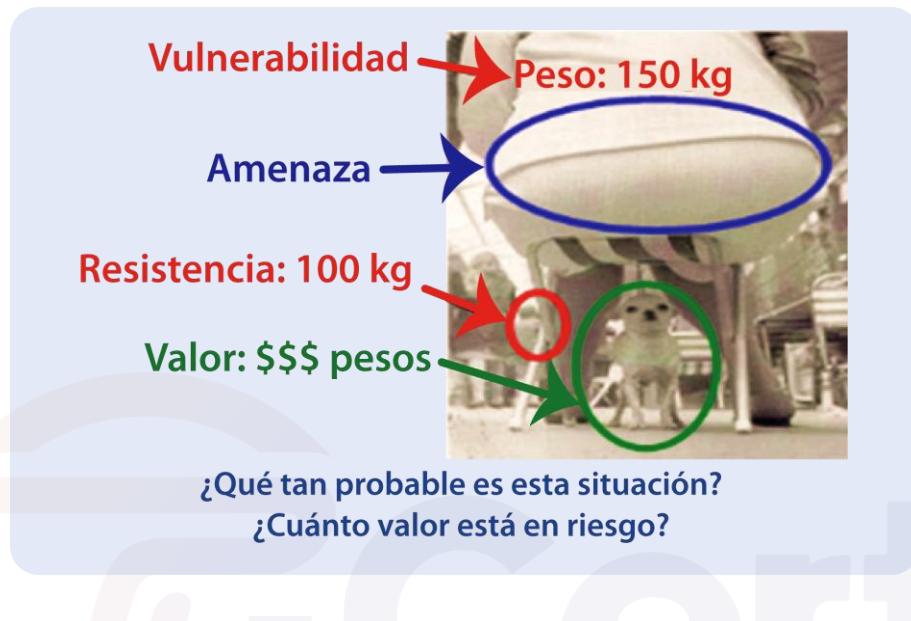
² Foto tomada de: <https://www.intagri.com/articulos/ganaderia/toros-de-lidia>

³ Foto tomada de: https://www.diariodecadiz.es/cadizfornia/son-pueblos-cadiz-celebran-domingo_0_2003771994.html

⁴ Foto tomada de: <https://navarra.okdiario.com/articulo/san-fermin-encierro-pamplona-running-of-the-bulls-2022/cebada-gago-encierro-sanfermines-pamplona-heridos-cogidas/20220711073621422404.html>

2.4.2. Elementos adicionales del Riesgo

La amenaza y la vulnerabilidad nos dan la **probabilidad** de materialización del riesgo. El valor del activo (A) nos da el impacto.



De la foto anterior se puede realizar un análisis de la amenaza, ratificando que no es la señora la verdadera amenaza, es el peso de la señora que puede hacer que la silla ceda y de esta forma se materializaría el riesgo.

De aquí se desprende otro concepto importante, **la vulnerabilidad** que para este caso es la resistencia de la silla, ya que puede que suceda el evento como puede que no pase, en caso de materializarse el riesgo se pone en juego un activo, que se debe validar y cuantificar.

La gestión del riesgo permite detectar a tiempo y gestionar el riesgo, que es asintomático en las primeras etapas. La función de los equipos de administración del riesgo, la alta dirección y los dueños de procesos es poder detectar a tiempo y frenar el “efecto dominó”.

Un claro ejemplo es, cuando en su primera etapa el riesgo se manifiesta en la parte operacional, posteriormente se genera el contagio, o como llamamos en ejemplo de

cáncer la “metástasis” que se riega y genera nuevos tumores posteriores, si la afectación es grave se materializa el **Riesgo Legal** y finalmente termina afectándose una de las variables más importantes de las empresas la **Reputación**, siendo la más crítica.



Recuerda

La gestión de riesgos es responsabilidad de la alta dirección, líderes de procesos y dueños de riesgos.

2.4.3. Tipología de riesgos

Existe una gran diversidad de riesgos, como:

- Riesgo ocupacional
- Riesgo informático
- Riesgo de mercado
- Riesgo ambiental
- Riesgo público
- Riesgo reputacional
- Riesgo operacional



- Riesgo de contagio
- Riesgo legal
- Riesgo financiero

Para la norma ISO 31000 es importante realizar énfasis en los riesgos operacionales y de tecnología.

2.4.3.1. Riesgo operacional

Un riesgo operacional es la posibilidad de pérdidas ocasionadas en la ejecución de los procesos y funciones de la empresa por una falla en el sistema, en los procedimientos, modelos o personas.

2.4.3.2. Riesgo de tecnología de información

Es un tipo de riesgo empresarial que se define como la posibilidad de que una falla tecnológica afecte negativamente a una empresa, aquí entran desde ataques cibernéticos hasta interrupciones del servicio, o novedades de infraestructura que no satisfacen las necesidades de la organización, que pueden ser:



Obsolescencia
del software



Obsolescencia
del hardware



Infraestructura
tradicional

© T-CERT™



Resiliencia
digital



Pérdida de
información

2.4.4. Beneficios de Gestión De Riesgos

Algunos de los beneficios para las organizaciones que gestionan y administran riesgos son:

- Toma de decisiones / no en factores aleatorios.
- Mejora la rentabilidad de negocios (costos de eventualidades).
- Protege los bienes y recursos de las organizaciones y su capacidad productiva disminuyendo impactos.
- Mejora el uso de los recursos asignado en forma racional.
- Implementa cultura preventiva en la organización en lugar de un manejo reactivo y tardío a los problemas.

2.4.5. Planificación estratégica VS Riesgos

Integrar la gestión de riesgos en la planificación estratégica es esencial para las organizaciones que buscan alcanzar sus objetivos a largo plazo mientras minimizan posibles contratiempos. Esta integración implica un enfoque sistemático donde las consideraciones de riesgo se incorporan en el proceso de planificación estratégica desde el principio. Para poder integrarlas se necesita:





1

Identificar Objetivos Estratégicos: Comienza definiendo claramente los objetivos estratégicos de la organización. Esto podría incluir la expansión del mercado, el desarrollo de productos o la eficiencia operativa. Comprender estos objetivos es crucial, ya que establece la base para identificar los riesgos asociados.

2

Realizar una Evaluación de Riesgos: Una vez establecidos los objetivos, realiza una evaluación de riesgos integral, para identificar los riesgos potenciales que podrían obstaculizar el logro de estos objetivos. Esta evaluación debe considerar tanto factores internos como externos, incluyendo la volatilidad del mercado, cambios regulatorios y desafíos operativos.

3

Priorizar Riesgos: No todos los riesgos son iguales. Utiliza métodos cualitativos y cuantitativos para priorizar los riesgos según su impacto potencial y probabilidad. Herramientas como matrices de riesgo pueden ayudar a visualizar y categorizar los riesgos, permitiendo a los tomadores de decisiones centrarse en las amenazas más críticas.

4

Desarrollar Estrategias de Mitigación de Riesgos: Para cada riesgo priorizado, desarrolla estrategias para mitigarlos o gestionarlos. Esto podría implicar la implementación de controles, la transferencia de riesgos a través de seguros o el desarrollo de planes de contingencia. Asegúrate de que estas estrategias se alineen con los objetivos estratégicos generales.

5

Monitorear y Revisar: La gestión de riesgos no es una actividad única. Establece un marco para el monitoreo y la revisión continua de los riesgos y las estrategias de mitigación. Esto debe incluir actualizaciones regulares de la evaluación de riesgos a medida que el entorno empresarial cambia y surgen nuevos riesgos.

6

Comunicar y Colaborar: La comunicación efectiva es vital para integrar la gestión de riesgos en la planificación estratégica. Involucra a las partes interesadas en toda la organización para asegurarte de que todos comprendan los riesgos y sus roles en la gestión de estos. Este enfoque colaborativo fomenta una cultura de conciencia y responsabilidad en torno al riesgo.

Al incorporar la gestión de riesgos en el proceso de planificación estratégica, las organizaciones pueden tomar decisiones informadas que se alineen con su apetito de riesgo y mejorar su resiliencia ante las incertidumbres.

2.4.6. Medición de un programa de gestión de riesgos

Medir la efectividad de un programa de gestión de riesgos es crucial para asegurar que cumpla con sus objetivos y proporcione valor a la organización. Varios indicadores clave de rendimiento (KPI) y métricas pueden utilizarse para evaluar la efectividad de las iniciativas de gestión de riesgos, algunos son:



© T-CERT®



Reducción de Riesgos

Reducción de Riesgos: Uno de los objetivos primordiales de un programa de gestión de riesgos es reducir la probabilidad y el impacto de los riesgos. Mide la reducción en la exposición al riesgo a lo largo del tiempo comparando los resultados de la evaluación de riesgos antes y después de implementar estrategias de mitigación de riesgos.



Frecuencia de Incidentes



Tiempo de Respuesta

Tiempo de Respuesta: Evalúa el tiempo de respuesta de la organización a eventos de riesgo. Un tiempo de respuesta más rápido puede indicar una organización bien preparada con procesos de gestión de riesgos efectivos en su lugar.



Retroalimentación de las Partes Interesadas

Retroalimentación de las Partes Interesadas: Recopila comentarios de las partes interesadas, incluyendo empleados, gerentes y socios externos, sobre sus percepciones del programa de gestión de riesgos. Encuestas y entrevistas pueden proporcionar información valiosa sobre la efectividad del programa y áreas de mejora.



regulatorios.

Métricas de Cumplimiento: Para las organizaciones en industrias reguladas, medir el cumplimiento de leyes y regulaciones relevantes es esencial. Realiza un seguimiento de las métricas de cumplimiento para asegurar que el programa de gestión de riesgos aborde efectivamente los requisitos

Análisis de Costo-Beneficio: Realiza un análisis de costo-beneficio para evaluar el impacto financiero del programa de gestión de riesgos. Compara los costos de implementar estrategias de gestión de riesgos con las pérdidas financieras evitadas debido a una mitigación de riesgos efectiva.



Revisar regularmente estas métricas y KPI permite a las organizaciones evaluar la efectividad de su programa de gestión de riesgos y hacer los ajustes necesarios para mejorar su rendimiento.



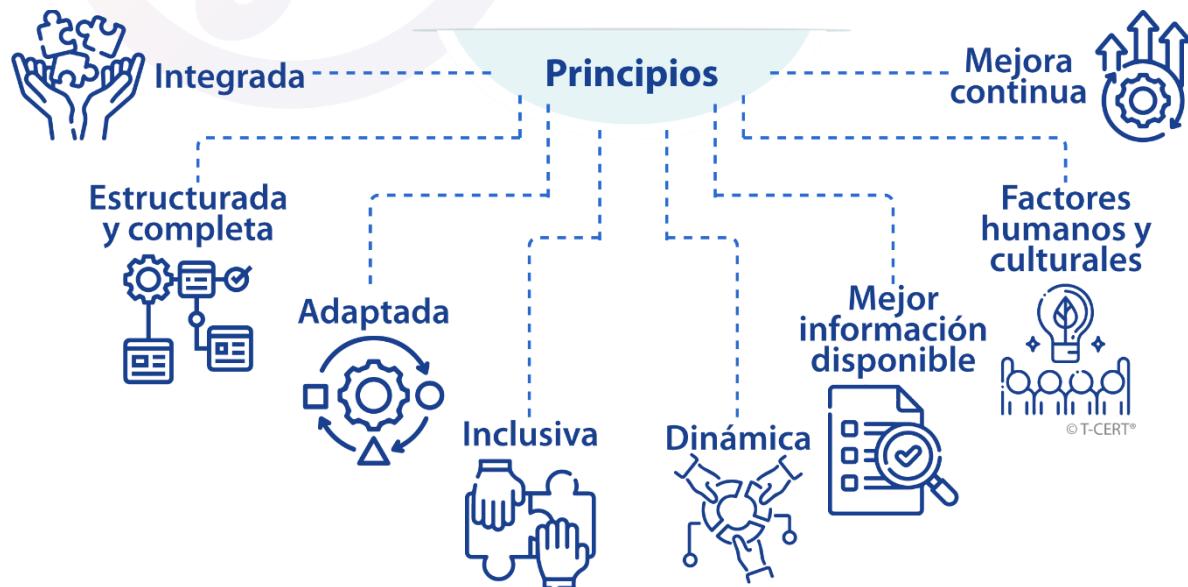
Módulo III. Principios de la Gestión del Riesgo

Módulo III. Principios de la Gestión del Riesgo

Los principios se basan en la creación y protección del valor, el cual es el eje principal y articulador de los principios en la gestión de riesgo.

Según la norma ISO 31000 se busca que las organizaciones puedan cumplir sus objetivos de manera eficaz, teniendo en cuenta la participación de las partes interesadas, puntos de vista y percepciones. Permitiendo anticiparse, detectar, reconocer y responder a los cambios del entorno y adaptándose al contexto de la organización.

Para esto es necesario basarse en la mejor información disponible, fuentes de información fiables, experiencia, análisis y las opiniones de expertos, gestores de riesgos y líderes de procesos buscando como todo sistema de gestión la mejora continua, que tiene una premisa fundamental que se basa en el aprendizaje y mejora mediante la experiencia.



3.1. Integrada

La gestión del riesgo es parte integral de todas las actividades de la organización.

Involucra todos los procesos, subprocessos y actividades.



Este principio es muy importante porque involucra todos los macroprocesos, procesos, subprocessos y actividades.

3.2. Estructurada y completa

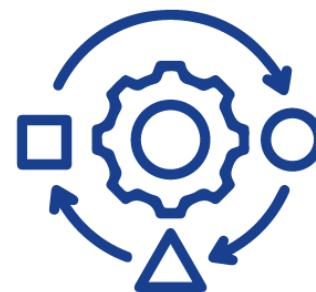


Un enfoque estructurado y exhaustivo hacia la gestión del riesgo contribuye a resultados coherentes y comparables.

Este principio es relevante ya que maneja un marco referencial que da pautas para su implementación y cubre por completo a toda la organización.

3.3. Adaptada

El marco de referencia y el proceso de la gestión del riesgo se adaptan y son proporcionales a los contextos externo e interno de la organización relacionados con sus objetivos. Los contextos pueden cambiar dependiendo de factores internos y externos a los que la organización este expuesta.



La adaptabilidad es una gran virtud, ya que ante cualquier cambio de alcance, contexto, variable interna o externa de la organización la norma se ajusta y amolda antes los cambios tan dinámicos de las organizaciones y su entorno.

3.4. Inclusiva



La participación apropiada y oportuna de las partes interesadas permite que se considere su conocimiento, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y una gestión del riesgo informada. Hoy la gestión apropiada del riesgo genera inclusión de todos los colaboradores de la organización, líderes y gestores de riesgos.

La gestión del riesgo es responsabilidad de todos en la organización, es cultural y exige el compromiso de todos.

3.5. Dinámica

Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de la organización. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.



Los riesgos son cambiantes, activos y vitales para sustentabilidad de organización razón por la cual siempre están en constante evolución.

3.6. Mejor información disponible



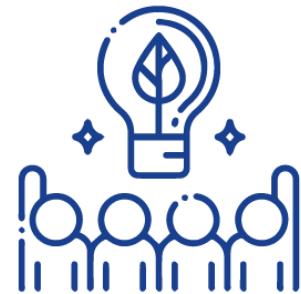
Las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en expectativas. La gestión del riesgo tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tal información y

expectativas. La información debe ser oportuna, clara y estar disponible para las partes interesadas pertinentes.

La administración de riesgo exige poder tener a la mano información de hechos y datos del pasado para saber si se materializó el riesgo, o de lo contrario buscar predecir y ver el futuro basado en visión de posibles eventos que puedan presentarse.

3.7. Factores humanos y culturales

El comportamiento humano y la cultura influyen considerablemente en todos los aspectos de la gestión del riesgo, en todos los niveles y etapas.



Los colaboradores, socios, gerencia y terceros outsourcing entre otros sumados a una cultura son las bases sólidas que permiten que la organización estructure e implemente un sistema de gestión de riesgos que asegure la sustentabilidad.

3.8. Mejora continua



La gestión del riesgo mejora continuamente mediante el aprendizaje y la experiencia.

Como todo sistema de gestión la búsqueda de mejora continua la madurez y expertiz de adecuado anejo y administración del riesgo se logra con compromiso liderazgo y capacitación constante.

Módulo IV. Marco Referencial

Módulo IV. Marco Referencial

El marco referencial pretende asistir a la organización en integrar la gestión del riesgo en todas sus actividades y funciones significativas. La eficacia de la gestión del riesgo dependerá de su integración en la gobernanza de la organización, incluyendo la toma de decisiones. Esto requiere el apoyo de las partes interesadas, particularmente de la alta dirección.



El marco de referencia con sus 6 etapas gobernanza, integración, diseño, evaluación, apoyada en la implementación y mejora continua marca el norte del sistema y hace parte integral de la planeación dentro ciclo PDCA.

4.1. Liderazgo y compromiso



Liderazgo y compromiso

La alta dirección y los órganos de supervisión, cuando sea aplicable, deberían asegurar que la gestión del riesgo esté integrada en todas las actividades de la organización.

El liderazgo y compromiso se demostrará:

- Adaptando e implementando todos los componentes del marco de referencia.
- Publicando una declaración o una política que establezca un enfoque, un plan o una línea de acción para la gestión del riesgo.

Recuerda

La política puede estar integrada en otros sistemas integrados de gestión que pueda tener la organización.

- Asegurando que los recursos necesarios se asignan para gestionar los riesgos (físicos, económicos, infraestructura, personal).
- Asignando autoridad, responsabilidad y obligación de rendir cuentas en los niveles apropiados dentro de la organización (líder de gestión de riesgos, oficiales de cumplimiento, gestores de riesgos, etc.).

Este capítulo se considera muy importante, ya que es uno de los puntos importantes de la modificación respecto a la versión anterior del año 2009. Se hace un numeral muy relevante, ya que el liderazgo y el compromiso hacen parte fundamental para que el sistema de gestión riesgos cumpla su función y objetivos esperados.

Variables que debe incluir el liderazgo y compromiso



Se consideran cuatro aspectos importantes para ejercer un verdadero liderazgo, se habla de una participación activa en la implementación del marco de referencia, la construcción de objetivos y política de riesgos, la asignación de los recursos necesarios para sostener el sistema y una correcta asignación de roles, funciones y delegación.

Un adecuado liderazgo y compromiso puede lograr los siguientes resultados:

1. Alinear la gestión del riesgo con sus objetivos, estrategia y cultura

Ejemplo de interacción de la política y la matriz de riesgos con mejora continua y monitoreo



En la figura anterior ponemos como ejemplo que luego de definida la política, esta se articula con la matriz de riesgos que a su vez determina el camino a seguir con protocolos de monitoreo y administración para asegurar la mejora continua.

Cumplimiento de política



En esta figura se muestra que para poder cumplir la política es necesario establecer objetivos claros y definidos, así como metas alcanzables y programas que impulsen el cumplimiento de los dos ítems anteriores.

Condiciones mínimas para definir objetivos



Para definir los objetivos es necesario que estos sean coherentes con la política, sean medibles, tengan seguimiento y trazabilidad, sean comunicados y actualizados si hay cambios y que adicional sean parte de la información documentada y controlada.

Ejemplo de un objetivo: Gestionar los RIESGOS derivados de nuestra actividad a través de su identificación, evaluación y control. Gestionar e implementar estrategias en seguridad de la información con el fin de prevenir hurtos, robos, contaminación de carga.

Ejemplo de una meta: 0% de sanciones originada en el cumplimiento de la normatividad, licencias, permisos de software utilizados en los equipos e infraestructura de la organización.

Ejemplo de programa: Bautizamos el programa normalmente con un nombre “Proveedores Estratégicos” Este programa pretende contratación y supervisión de proveedores de servicios tecnológicos y suministros de Hardware seguros y confiables.

2. Reconocer y abordar todas las obligaciones, así como sus compromisos voluntarios.
3. Establecer la magnitud y el tipo de riesgo que puede o no ser tomado para guiar el desarrollo de los criterios del riesgo, asegurando que se comunican a la organización y a sus partes interesadas.

4. Comunicar el valor de la gestión del riesgo a la organización y sus partes interesadas.
5. Promover el seguimiento sistemático de los riesgos.
6. Asegurarse de que el marco de referencia de la gestión del riesgo permanezca ajustado al contexto de la organización, si este cambia se debería adaptar a las nuevas condiciones del entorno.

En la gestión del riesgo existen dos responsabilidades claves, estas son que:

1. La alta dirección es quien rinde cuentas por gestionar el riesgo en la organización.
2. Los órganos de supervisión rinden cuentas por la supervisión de la gestión del riesgo.

Actualmente, en muchos países de Latinoamérica los organismos estatales de control como superintendencias, entidades de control, organismos evaluadores de conformidad validan en espacio de auditoría, vistas e inspección el cumplimiento de administración de riesgo como pilar de cumplimiento y sostenibilidad supervisando las siguientes variables:



- Se aseguren de que los riesgos se consideran apropiadamente cuando se establezcan los objetivos de la organización.
- Comprendan los riesgos a los que hace frente la organización en la búsqueda de sus objetivos.

- Se aseguren de que los sistemas para gestionar estos riesgos se implementen y operen eficazmente.
- Se aseguren de que estos riesgos sean apropiados en el contexto de los objetivos de la organización.
- Se aseguren de que la información sobre estos riesgos y su gestión se comunique de la manera apropiada.

4.2. Integración



Integración

La integración de la gestión de riesgos depende de la comprensión de las estructuras y el contexto de las organizaciones. Las estructuras difieren dependiendo del propósito, las metas y la complejidad de las organizaciones.

La integración de la gestión del riesgo depende de varios factores como:

- Entender la estructura, procesos y contexto de la organización ya que el riesgo se gestiona en cada uno de ellos.
- La gobernanza guía el curso de la organización, estrategia y los objetivos asociados requeridos para lograr los niveles deseados de desempeño sistema de gestión del riesgo, definición de roles y supervisión.
- Es un proceso dinámico e iterativo, y se debería adaptar a las necesidades y a la cultura de la organización.

Recuerda

Todos los miembros de una organización tienen la responsabilidad de gestionar el riesgo.

4.3. Diseño



Diseño

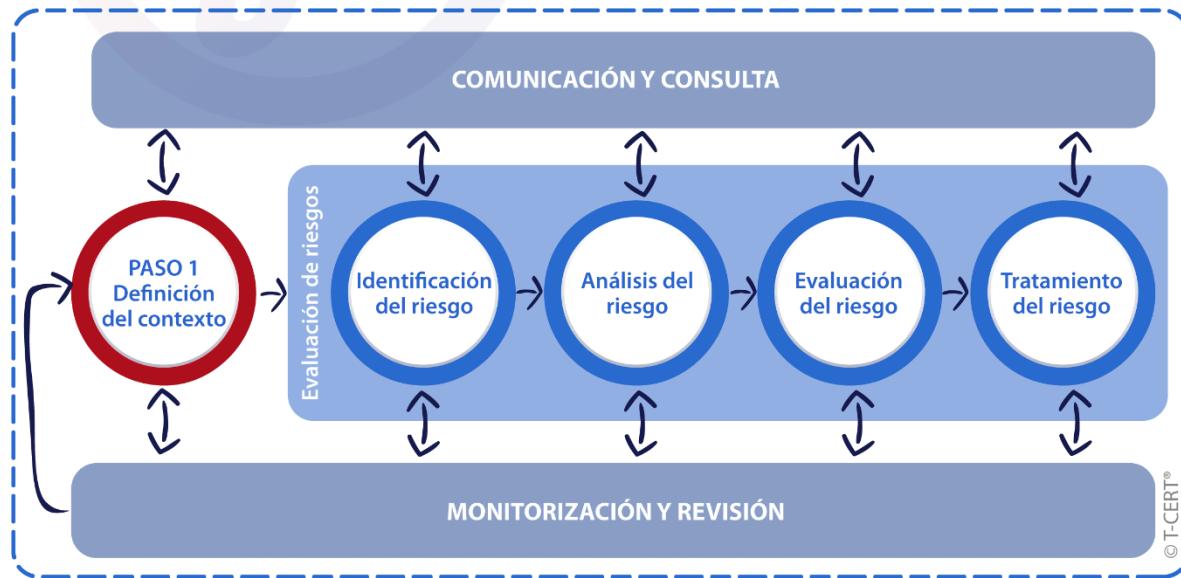
La organización debe analizar y comprender sus contextos externo e interno cuando diseña el marco de referencia para gestionar el riesgo.

4.3.1. Comprensión de la organización y de su contexto

Es importante responder como compañía y entender ¿dónde estamos operando? entender el contexto nos ayuda a identificar riesgos, administrarlos y controlarlos.

Hay que destacar que si no está bien definido, estructurado y acorde a la realidad actual de la compañía el contexto puede desviar los objetivos que se persiguen en resto de pasos para administrar y gestionar los riesgos en la organización.

Paso 1 del proceso de administración de gestión del riesgo



Establecer el contexto es el paso 1 del proceso de administración de gestión del riesgo e implica:

- Establecer el contexto estratégico y organizacional.
- Establecer el contexto de la gestión del riesgo.
- Definir la estructura.



Es fundamental y determinante conocer el contexto en que se desenvuelve la organización para poder cumplir con los siguientes pasos de la gestión del riesgo.

Existen diferentes metodologías para establecer el contexto de las organizaciones entre ellas se encuentran la matriz DOFA, las 5 fuerzas de Michael Porter, Kambas entre otras.

4.3.2. Articulación del compromiso con la gestión del riesgo

La alta dirección y los organismos de supervisión, cuando sea aplicable, deben articular y demostrar su compromiso continuo con la gestión del riesgo mediante una política, una declaración u otras formas que expresen claramente los objetivos y el compromiso de la organización con la gestión del riesgo.

El compromiso debe incluir, pero no limitarse a:

- Propósito de la organización para gestionar el riesgo y los vínculos con sus objetivos y otras políticas.
- El refuerzo de la necesidad de integrar la gestión del riesgo en toda la cultura de la organización.

- El liderazgo en la integración de la gestión del riesgo en las actividades principales del negocio y la toma de decisiones.
- Las autoridades, las responsabilidades y la obligación de rendir cuentas.
- La disponibilidad de los recursos necesarios.
- La manera de manejar los objetivos en conflicto.
- La medición e informe como parte de los indicadores de desempeño de la organización.
- La revisión y la mejora.

El compromiso con la gestión del riesgo se debería comunicar dentro de la organización y a las partes interesadas, de manera apropiada.

EJEMPLO POLITICA INTEGRAL

Esta política involucra un manejo integral riesgos en diferentes sistemas de gestión para esta compañía.

POLITICA INTEGRAL (Incluye varios sistemas gestión)

Somos una empresa que presta servicios de vigilancia y seguridad privada, estamos comprometidos con la Satisfacción de nuestros Clientes y demás grupos de interés, orientamos nuestra labor hacia la prevención y control de pérdidas implementando mecanismos apropiados para la **gestión del riesgo**.

Entendemos y practicamos el mejoramiento continuo como parte integral de cada una de nuestras acciones. Fundamentamos nuestra gestión en la utilización de herramientas tecnológicas, talento humano altamente calificado al que brindamos espacios para su crecimiento personal y

profesional, orientamos nuestra gestión hacia el mejoramiento de la calidad de vida de nuestros colaboradores, promovemos el trabajo en equipo y la construcción de una sociedad incluyente y equitativa.

Nuestro compromiso se fundamenta en:

- El estricto cumplimiento de los requisitos legales, los que la organización suscriba y los estándares aplicables a nuestra actividad económica.
- **La identificación, valoración y control de los riesgos** ocupacionales e impactos socio ambientales derivados del ejercicio de nuestra actividad, a través de la implementación de programas encaminados hacia la prevención de incidentes (con o sin lesión), enfermedades profesionales y la contaminación del ambiente.
- Implementar, mantener y mejorar anualmente el conjunto de controles de **riesgos y seguridad** de la información recomendados por el modelo de seguridad y privacidad de la información mediante la aplicación del plan de seguridad y privacidad de la información para mantener en niveles aceptables los riesgos residuales.
- El desarrollo de **estrategias en riesgos y seguridad** que nos permitan la prevención del contrabando de drogas, el terrorismo, el lavado de activos y en general cualquier actividad ilegal en nuestras operaciones a fin de fomentar un comercio interior y exterior lícito.
- La adopción de prácticas socialmente responsables en todos los ámbitos de influencia de la organización.

Todo esto enmarcado en la optimización de los recursos necesarios, dentro de parámetros de rentabilidad y una sólida estructura organizacional, que nos permite ser líderes en el sector.

4.3.3. Asignación de roles, autoridades, responsabilidades y obligación de rendir cuentas en la organización

La alta dirección y los órganos de supervisión, cuando sea aplicable, deben asegurarse de que las autoridades, las responsabilidades y la obligación de rendir cuentas de los roles relevantes con respecto a la gestión del riesgo se asignen y comuniquen a todos los niveles de la organización, es decir que deben:

- Enfatizar en que la gestión del riesgo es una responsabilidad principal.
- Identificar a las personas que tienen asignada la obligación de rendir cuentas y la autoridad para gestionar el riesgo (dueños del riesgo).

Es importante que estos roles, especialmente los que tienen funciones dentro la organización tomen conciencia de su labor y se empoderen para asegurar el tiempo y compromiso que demanda además de sus labores diarias esta importante adjudicación.



4.3.4. Asignación de recursos

La alta dirección y los órganos de supervisión, cuando sea aplicable, deberían asegurar la asignación de los recursos apropiados para la gestión del riesgo, que puede incluir, pero no limitarse a:

- Las personas, las habilidades, la experiencia y las competencias.
- Los procesos, los métodos y las herramientas de la organización a utilizar para gestionar el riesgo.
- Los procesos y procedimientos documentados.
- Los sistemas de gestión de la información y del conocimiento.

- El desarrollo profesional y las necesidades de formación.
- La organización debería considerar las competencias y limitaciones de los recursos existentes.

Dentro de la asignación de recursos es importante que desde la parte financiera se ejecute un presupuesto anual de mantenimiento del sistema.

Garantizar las habilidades del personal, implica que estos comprendan lo que significan para la organización y como contribuyen para el cumplimiento de los requisitos de la gestión de riesgos.

Por esta razón, la organización debe contar con una gestión de comunicación y un proceso de capacitación donde:

- Se proporcione capacitación o se tomen medidas para asegurar que las personas cuenten con las habilidades necesarias para el cumplimiento de competencia dentro de la gestión de riesgos.
- Se monitorean constantemente los niveles de competencia, para definir posibles brechas.
- Planificar lo que se haría, es decir, el paso a seguir en caso de encontrar brechas.

Es importante que cuando se ejecute un proceso de capacitación, se integre dentro de este, un formato de evaluación, que ayude a determinar que las habilidades de cada persona han mejorado y que así mismo se vea reflejado en el desempeño de sus tareas. Esto también hace parte de determinar la competencia del personal, con respecto a la gestión de riesgos.

4.3.5. Establecimiento de la comunicación y la consulta

La organización debe establecer un enfoque aprobado con relación a la comunicación y la consulta, para apoyar el marco de referencia y facilitar la aplicación eficaz de la gestión del riesgo. La comunicación implica compartir información con el público objetivo.

La consulta además implica que los participantes proporcionen retroalimentación con la expectativa de que ésta contribuya y de forma a las decisiones u otras actividades. Los métodos y el contenido de la comunicación y la consulta deberían reflejar las expectativas de las partes interesadas, cuando sea pertinente.

La comunicación y la consulta deberían ser oportunas y asegurar que se recopile, consolide, sintetice y comparta la información pertinente, cuando sea apropiado, y que se proporcione retroalimentación y se lleven a cabo mejoras.

Esto se puede lograr con información documentada, por ejemplo, de:



- Actas de reuniones.
- Tabloides de anuncios con información sobre seguridad.
- Boletines internos.
- Buzones o programas de sugerencias.
- Sitios web y correo electrónico,
- Reuniones.
- Acceso para la participación en investigaciones sobre incidentes e inspecciones de seguridad.

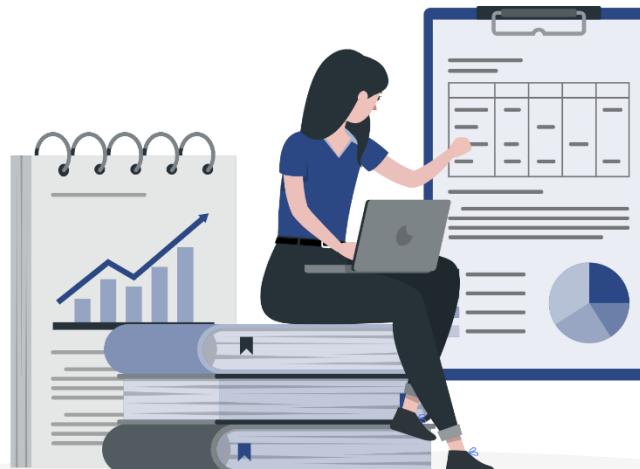
Dentro de las organizaciones existe comunicación interna y externa, por lo que se debe establecer una necesidad en las comunicaciones que se realicen, en donde se indique:

- Lo que se debe comunicar.
- Cuando se debe hacer una comunicación.
- A quien dirigir la comunicación.
- Como se debe comunicar.

Recuerde que todo hay que documentarlo, esto es necesario para:

- **Garantizar la repetición en el tiempo de un proceso:** la base para garantizar la aplicación sistemática de un proceso es su documentación.
- **Establecer un proceso de mejora:** la documentación de un proceso permite el acceso a información valiosa cuando se decida evaluar la eficacia de la gestión de riesgos.

Mantener información documentada es el medio para justificar el cumplimiento con los requisitos de la norma. Si no se crean registros de lo que se hace, no se puede conseguir la mejora continua.



4.4. Implementación



Implementación

La implementación es el proceso de poner en práctica los principios y directrices de la ISO 31000 para gestionar los riesgos de manera efectiva.

La organización debe implementar el marco de referencia de la gestión del riesgo mediante:

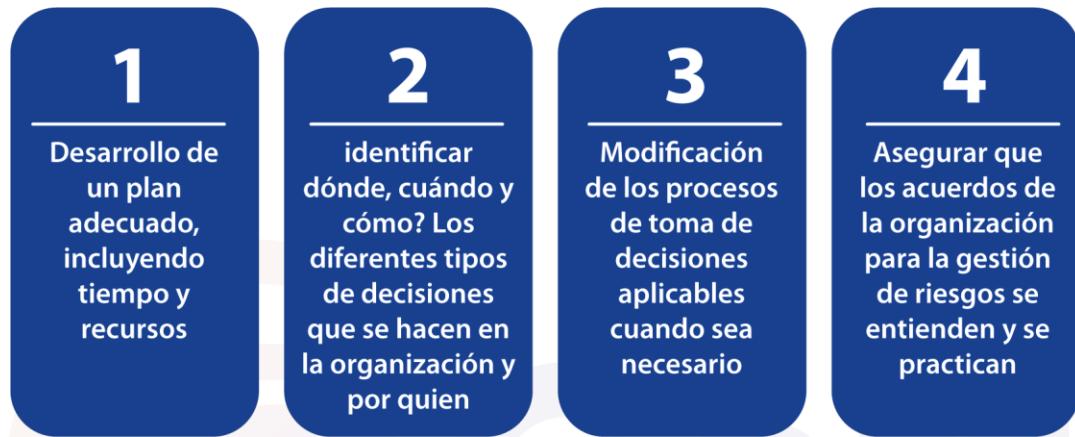
- El desarrollo de un plan apropiado incluyendo plazos y recursos.
- La identificación de dónde, cuándo, cómo y quién toma diferentes tipos de decisiones en toda la organización.
- La modificación de los procesos aplicables para la toma de decisiones, cuando sea necesario.
- El aseguramiento de que las disposiciones de la organización para gestionar el riesgo son claramente comprendidas y puestas en práctica.

La implementación con éxito del marco de referencia requiere el compromiso y la toma de conciencia de las partes interesadas. Esto permite a las organizaciones abordar explícitamente la incertidumbre en la toma de decisiones, al tiempo que asegura que cualquier incertidumbre nueva o subsiguiente se pueda tener en cuenta cuando surja.

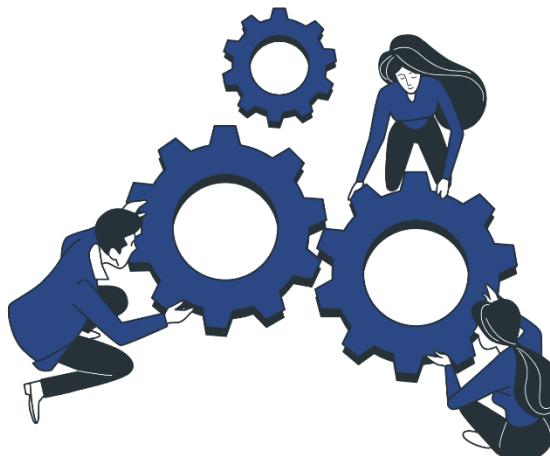


Si se diseña e implementa correctamente, el marco de referencia de la gestión del riesgo asegurará que el proceso de la gestión del riesgo sea parte de todas las actividades en toda la organización, incluyendo la toma de decisiones, y que los cambios en los contextos externo e interno se captarán de manera adecuada.

4.4.1. Proceso de implementación de riesgos basado en decisiones



Hemos simplificado el proceso de implementación de riesgos en cuatro pasos, que van desde el desarrollo del plan atendiendo unidad de tiempo y recursos suministrados por la dirección, así como identificación de preguntas claves como: ¿Dónde? ¿cuándo? ¿cómo? se toman decisiones y como se ajustan al principal proceso gerencial de la toma de decisiones y al final asegurar que acuerdos tomados que apliquen, se lleven a la práctica y se repliquen.



4.5. Evaluación



Evaluación

La evaluación, es un proceso crucial en la gestión de riesgos que implica medir periódicamente el desempeño del marco de referencia de la gestión del riesgo con relación a su propósito, sus planes para la implementación, sus indicadores y el comportamiento esperado. Además, determina si permanece idóneo para apoyar el logro de los objetivos de la organización.

Hoy existen diferentes metodologías para medición sean cuantitativas o cualitativas aquí traemos una metodología que permite generar KPI's, llamada SMART.

Metodología SMART construcción de indicadores



Para valorar la eficacia del marco de referencia de la gestión del riesgo, la organización debe:

- Medir periódicamente el desempeño del marco de gestión de riesgos contra su propósito, planes e implementación, indicadores y comportamiento esperado.

- Determinar si sigue siendo adecuada para soportar la consecución de los objetivos de la organización.

4.6. Mejora



Mejora

La organización tiene la responsabilidad de generar una cultura que se centre en la importancia de mejorar continuamente.

4.6.1. Adaptación

La organización debe realizar el seguimiento continuo y adaptar el marco de referencia de la gestión del riesgo en función de los cambios externos e internos. Al hacer esto, la organización puede mejorar su valor.

4.6.2. Mejora continua

MEJORA CONTINUA

Práctica de gestión enfocada en la mejora constante de procesos operativos, con el objetivo de ser más eficiente y tener un mejor rendimiento.

La organización debe mejorar continuamente la idoneidad, adecuación y eficacia del marco de referencia de la gestión del riesgo y la manera en la que se integra el proceso de la gestión del riesgo.

Cuando se identifiquen brechas u oportunidades de mejora pertinentes, la organización debería desarrollar planes y tareas y asignarlas a quienes tuviesen que rendir cuentas de su implementación. Una vez implementadas, estas mejoras deberían contribuir al fortalecimiento de la gestión del riesgo.

Al igual que otros sistemas de gestión basados en ISO la mejora continua hace parte importante de poder cerrar el ciclo PDCA Y asegurar madurez el sistema, así como si existen desviaciones y/o oportunidad de mejorar implementar cambios necesarios.

Se habla de que la mejora continua se basa en tres pilares principales, los cuales son:



1 **Continuidad:** siempre hay una forma de mejorar y esta búsqueda debe ser constante, ya que no existe la perfección en los procesos.

2

Cultura: es importante que dentro de la organización se forme una cultura de mejora, para que la continuidad sea posible, es necesario volver esa cultura en un hábito.

3

Bueno para todos: las mejoras deben estar pensadas y deben ejecutarse para que contribuyan beneficios a todas las áreas de la organización. Involucre a todas las partes interesadas.

La organización puede buscar apoyarse en procesos y tareas automatizadas, buscando siempre la forma de reducir los riesgos.

Incorporar la mejora continua implica:



1. Identificar lo que hay que mejorar



2. Creación de procesos



3. Seguimiento de la mejora



4. Adoptar métodos de mejora continua



1. Identificar lo que hay que mejorar:

Identifiqué y evalúe todos los procesos. Cree prioridades y analice si el proceso impacta en la estrategia general y los objetivos de la organización.

2. Creación de procesos

Estandarice y mapee los procesos de todas las tareas, actividades, personas interesadas, objetivos y todo lo relacionado con la operación de la empresa.



3. Seguimiento de la mejora

Cree métricas y KPI's (indicadores de rendimiento) para medir con datos reales los resultados de la mejora. De esta forma será más fácil la comparación y el análisis de las versiones, para saber realmente que resultados se obtuvieron y si hay más puntos de mejora.

4. Adoptar métodos de mejora continua

Adopte métodos que optimicen los procesos y ayuden con la mejora continua, como:

- **El ciclo PDCA**

Cuatro pasos que deben realizarse cíclicamente, donde es posible identificar el problema, analizarlo, crear un plan de acción, ejecutar, verificar, normalizar y actuar para mejorar.



1. *Plan* (planificar)
2. *Do* (hacer)
3. *Check* (verificar)
4. *Act* (actuar)



- **Kaizen**

Metodología japonesa de mejora continua, que reconoce la mejora constante de los procesos, productos o servicios. Kaizen en japonés significa “mejora”.

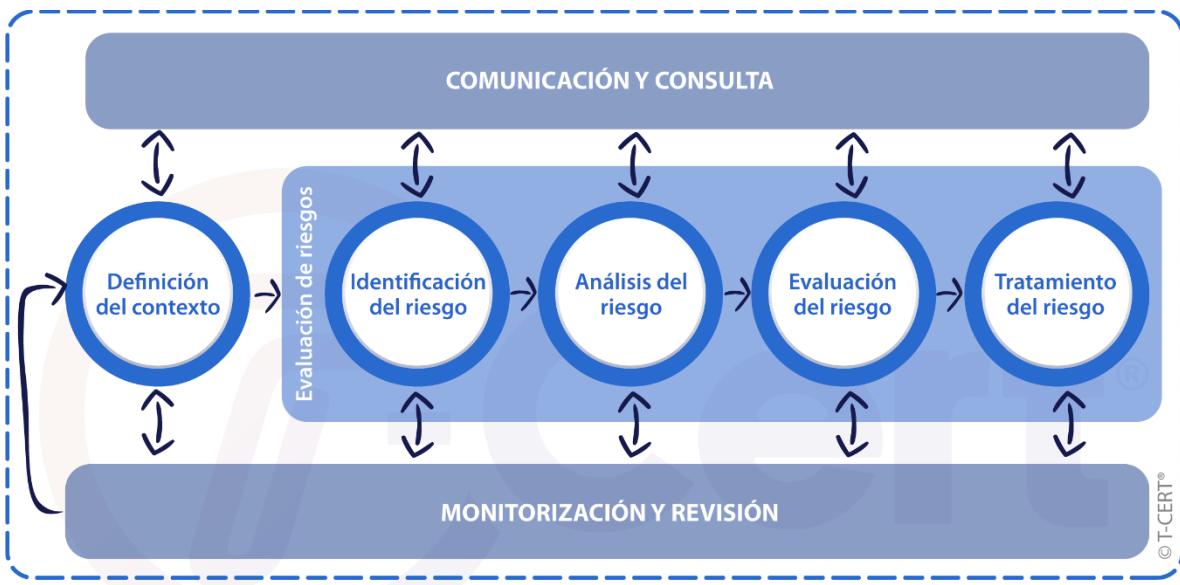
- **Six Sigma**

Estrategia de gestión que entiende que las producciones tienen variaciones y es necesario eliminar estas fuentes de variabilidad. Six sigma sigue las fases denominadas DMAIC: definir, medir, analizar, mejorar, controlar.

Módulo V. Proceso

Módulo V. Proceso

El proceso de la gestión del riesgo implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo.



Puede haber muchas aplicaciones del proceso de la administración/gestión de riesgos dentro de las organizaciones, adaptadas para lograr objetivos, y apropiadas a los contextos interno y externo en los cuales se aplican.

Aunque el proceso de gestión de riesgos se presenta frecuentemente como secuencial, en la práctica es iterativo.

5.1. Comunicación y consulta

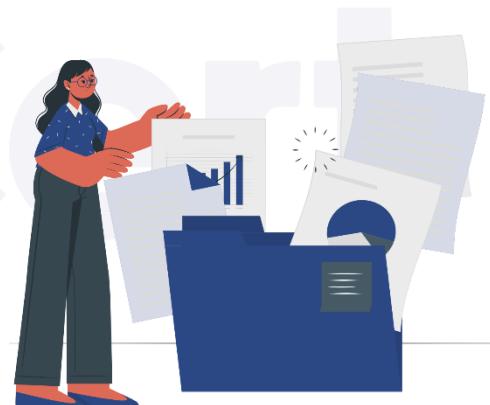
El propósito de la comunicación y consulta es asistir a las partes interesadas pertinentes a comprender el riesgo, las bases con las que se toman decisiones y las razones por las que son necesarias acciones específicas.

La comunicación busca promover la toma de conciencia y la comprensión del riesgo, mientras que la consulta implica obtener retroalimentación e información para apoyar la toma de decisiones.

Una coordinación cercana entre ambas debería facilitar un intercambio de información basado en hechos, oportuno, pertinente, exacto y comprensible, teniendo en cuenta la confidencialidad e integridad de la información, así como el derecho a la privacidad de las personas.

La comunicación y consulta con las partes interesadas apropiadas, externas e internas, se debería realizar en todas y cada una de las etapas del proceso de la gestión del riesgo.

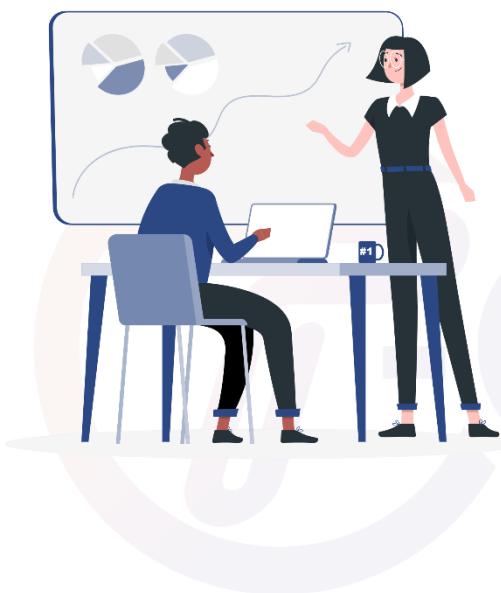
La comunicación y consulta pretende:



- Reunir diferentes áreas de experiencia para cada etapa del proceso de la gestión del riesgo.
- Asegurar que se consideren de manera apropiada los diferentes puntos de vista cuando se definen los criterios del riesgo y cuando se valoran los riesgos.
- Proporcionar suficiente información para facilitar la supervisión del riesgo y la toma de decisiones.
- Construir un sentido de inclusión y propiedad entre las personas afectadas por el riesgo.

5.2. Alcance, Contexto y Criterios

El propósito del establecimiento del alcance, contexto y criterios es adaptar el proceso de la gestión del riesgo, para permitir una evaluación del riesgo eficaz y un tratamiento apropiado del riesgo. El alcance, el contexto y los criterios implican definir el alcance del proceso, y comprender los contextos externo e interno.



Definimos alcance como la delimitación de las partes de una organización que están sujetas a dicho sistema, así como los productos, servicios y ubicaciones físicas que se incluyen.

El alcance puede abarcar toda la organización, funciones específicas, procesos concretos o áreas específicas. Es importante definir el alcance de un sistema de gestión con claridad antes de empezar a trabajar en su implantación

5.2.1. Definición del alcance

La organización debe definir el alcance de sus actividades de gestión del riesgo. Como el proceso de la gestión del riesgo puede aplicarse a niveles distintos es importante tener claro el alcance considerado, los objetivos pertinentes a considerar y su lineamiento con los objetivos de la organización.

Por ejemplo: Niveles estratégicos, operacionales, de programa, de proyecto u otras actividades.

En la planificación del enfoque se incluyen las siguientes consideraciones:

- Los objetivos y las decisiones que se necesitan tomar.
- Los resultados esperados de las etapas a ejecutar en el proceso.
- El tiempo, la ubicación, las inclusiones y las exclusiones específicas.
- Las herramientas y las técnicas apropiadas de evaluación del riesgo.
- Los recursos requeridos, responsabilidades y registros a conservar.
- Las relaciones con otros proyectos, procesos y actividades.



La política se debe alinear con el alcance, el contexto y los riesgos para no ir en contravía de las directrices organizacionales, el alcance delimita los límites y cobertura hasta donde nuestro sistema pueda generar valor.

5.2.2. Contextos externo e interno

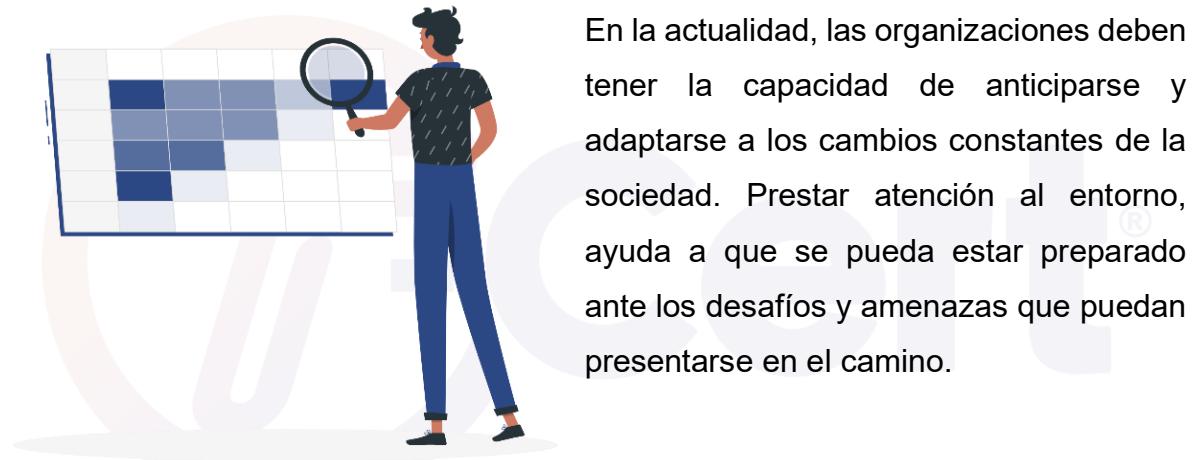
Los contextos externo e interno son el entorno en el cual la organización busca definir y lograr sus objetivos.

El contexto del proceso de la gestión del riesgo se debería establecer a partir de la comprensión de los entornos externo e interno en los cuales opera la organización y debería reflejar el entorno específico de la actividad en la cual se va a aplicar el proceso de la gestión del riesgo.

La comprensión del contexto es importante porque:

- La gestión del riesgo tiene lugar en el contexto de los objetivos y las actividades de la organización.
- Los factores organizacionales pueden ser una fuente de riesgo.
- El propósito y alcance del proceso de la gestión del riesgo puede estar interrelacionado con los objetivos de la organización como un todo.

La organización debe establecer los contextos externo e interno del proceso de la gestión del riesgo considerando los factores mencionados.



En la actualidad, las organizaciones deben tener la capacidad de anticiparse y adaptarse a los cambios constantes de la sociedad. Prestar atención al entorno, ayuda a que se pueda estar preparado ante los desafíos y amenazas que puedan presentarse en el camino.

5.2.2.1. **Modelo PESTEL**

El entorno externo de una organización implica factores políticos, económicos, sociales, tecnológicos, ambientales y legales. Estos elementos ofrecen una comprensión clara de los riesgos y oportunidades que pueden impactar en la organización.

En el contexto de los factores externos, el análisis PESTEL (o PESTLE) se ha convertido en una herramienta invaluable, que ayuda a las organizaciones a estar preparadas ante los desafíos y amenazas.

El análisis PESTEL, es un método representativo usado para conocer el contexto de una empresa. Ahora veamos cada factor:



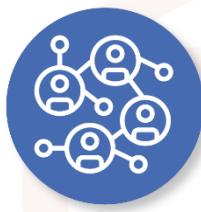
Políticos

Factores Políticos: Se deben analizar las políticas del país donde opera la empresa, políticas del sector, la estabilidad estatal y los cambios en los acuerdos internacionales.



Económicos

Factores Económicos: Los cambios en la normativa fiscal, la inflación, los tipos de cambio e interés, el crecimiento económico, así como la tasa de empleo, son también factores externos que afectan a una empresa.



Sociales

Factores sociales: Se refiere a la valoración de los patrones culturales, valores compartidos, movimientos geográficos de los consumidores y estilo de vida, hábitos y tendencias de consumo.



Tecnológicos



Ambientales

Factores ambientales: Son todos los aspectos relacionados con la preservación del medioambiente, desde la contaminación que emite la actividad empresarial y el uso de los recursos naturales, hasta la gestión de los residuos. Para este punto se deben tener presentes las políticas de cada país.



Legales

Factores legales: Aquí se deben incluir leyes que puedan afectar y limiten a la organización, como: derechos de autor, licencias, reglas sanitarias, seguridad laboral, salarios, protección del consumidor, etc.

5.2.2.2. Análisis FODA

El análisis FODA o DOFA, es otra herramienta que sirve para evaluar los factores externos, pero también internos de la organización. Esta puede usarse desde el contexto unipersonal, así como también en grandes proyectos, ya que aporta una visión diferente del cómo se encuentra la organización actualmente.

El análisis FODA está diseñado para comprender la situación de la organización a través del análisis de las fortalezas, oportunidades, debilidades y amenazas. Analizar las áreas clave en función de las oportunidades y amenazas, ayudará a obtener la información que se necesita para una toma de decisiones estratégica.



Fortalezas: Son las partes de la organización que funcionan bien.



Oportunidades: Las oportunidades en FODA son el resultado de las fortalezas y las debilidades. Son esas partes que se pueden y se quieren mejorar, y que son aplicables a cualquier actividad de la organización.



Debilidades: Son las actividades internas que no funcionan como debe ser. Al analizar las fortalezas antes que las debilidades, se puede generar una referencia de lo que es exitoso y de lo que no. La identificación de estas debilidades ayuda a generar un punto de partida para mejorar.



Amenazas: Las amenazas son externas, por lo que generalmente están fuera de nuestro control.

Tabla 1. Ejemplo de Matriz FODA

	FORTALEZAS	DEBILIDADES
Factores Internos	<ul style="list-style-type: none">• ¿Qué es lo que hacemos bien?• ¿Qué hace que seamos especiales?• ¿Qué es lo que le gusta de nosotros a nuestro público objetivo?	<ul style="list-style-type: none">• ¿Qué decisiones no funcionan bien y por qué?• ¿Qué podemos mejorar?• ¿Qué recursos o equipos, pueden ayudar al rendimiento?
Factores Externos	OPORTUNIDADES	AMENAZAS
	<ul style="list-style-type: none">• ¿Qué podemos usar para mejorar nuestras debilidades?• ¿Hay brechas en nuestros servicios?• ¿Cuáles son nuestros objetivos, en X tiempo?	<ul style="list-style-type: none">• ¿Qué cambios en el sector son preocupantes?• ¿Hay nuevas tendencias en el mercado?• ¿En qué es mejor la competencia?

Por último, se debe ejecutar una última revisión para confirmar los elementos que determinan la situación actual de la organización.

En ejercicios anteriores validamos metodologías para poder definir el contexto interno y externo. A continuación, se muestra el análisis de contexto elaborado para la gestión de riesgo “LAFT” Lavado de Activos y Financiación de Terrorismo.

Tabla 2. Ejemplo de Matriz FODA de riesgos LAFT (Lavado de activos y financiación del terrorismo)

	FORTALEZAS	DEBILIDADES
Factores Internos	<ul style="list-style-type: none"> • Cumplimiento normativo y compromiso con la calidad. • Compromiso con la transparencia y la ética empresarial. • Diversificación de productos y servicios. • Red de distribución establecida. 	<ul style="list-style-type: none"> • Riesgo de cumplimiento normativo. • Dependencia proveedores y terceros. • Transparencia en la cadena de suministro. • Seguridad laboral y ética empresarial.
Factores Externos	OPORTUNIDADES	AMENAZAS
	<ul style="list-style-type: none"> • Sostenibilidad del negocio. • Nuevos negocios y nuevas inversiones. • Seguridad y confianza en el sector. • Toma de decisiones estratégicas para gerencias. • Competencia legítima. 	<ul style="list-style-type: none"> • Deficiencia de conocimiento de terceros. • Riesgo regulatorio y de cumplimiento. • Crisis de mercados financieros mundiales. • Cambio en la demanda y crisis de energía. • Crecimiento de economía criminal.

5.2.3. Definición de los criterios del riesgo

La organización debe precisar la cantidad y el tipo de riesgo que puede o no puede tomar, con relación a los objetivos. Además, debe definir los criterios para valorar la importancia del riesgo y para apoyar los procesos de toma de decisiones.

Los criterios del riesgo se deben alinear con el marco de referencia de la gestión del riesgo y adaptar al propósito y al alcance específicos de la actividad considerada.

Los criterios del riesgo deben reflejar los valores, objetivos y recursos de la organización y ser coherentes con las políticas y declaraciones acerca de la gestión del riesgo. Los criterios se deben definir teniendo en consideración las obligaciones de la organización y los puntos de vista de sus partes interesadas.

Aunque los criterios del riesgo se deberían establecer al principio del proceso de la evaluación del riesgo, éstos son dinámicos, y deben revisarse continuamente y si fuese necesario, modificarse.

Para establecer los criterios del riesgo, se debería considerar lo siguiente:

- La naturaleza y los tipos de las incertidumbres que pueden afectar a los resultados y objetivos (tanto tangibles como intangibles).
- Cómo se van a definir y medir las consecuencias (tanto positivas como negativas) y la probabilidad.
- Los factores relacionados con el tiempo.
- La coherencia en el uso de las mediciones.
- Cómo se va a determinar el nivel de riesgo.
- Cómo se tendrán en cuenta las combinaciones y las secuencias de múltiples riesgos.
- La capacidad de la organización.



Además, se debe considerar la siguiente calificación de riesgos:

- **Los riesgos aceptables:** que están definidos en el apetito de riesgo de cada organización y son riesgos inherentes donde cada compañía convive en su core business y son administrables debido a su bajo impacto y probabilidad.
- **Los riesgos tolerables:** son los de carácter medio, pero con la premisa de trabajar en procesos de mitigación y control.
- **Los riesgos no tolerables:** son los altos e inaceptables, se deben intervenir de inmediato para el control y la mitigación, son los que están en zona de cuarentena y son como pacientes en cuidado intensivo.

Criterio y calificación de Riesgos



Estos criterios se validan en el “mapa de calor” donde la organización dependiendo su apetito de riesgo definirá los umbrales y categorías acorde a sus productos y servicios.

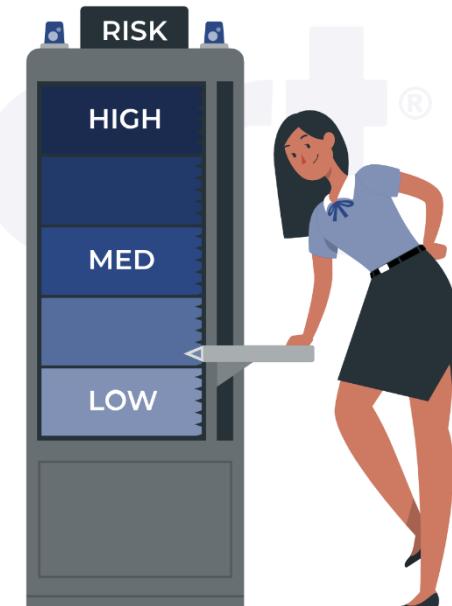
5.3. Evaluación de riesgos

5.3.1. Identificación del riesgo

El propósito de la identificación del riesgo es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos. Para la identificación de los riesgos es importante contar con información pertinente, apropiada y actualizada.

La organización puede utilizar un rango de técnicas para identificar incertidumbres que pueden afectar a uno o varios objetivos. Se deberían considerar los factores siguientes y la relación entre estos factores:

- Las fuentes de riesgo tangibles e intangibles.
- Las causas y los eventos.
- Las amenazas y las oportunidades.
- Las vulnerabilidades y las capacidades.
- Los cambios en los contextos externo e interno.
- Los indicadores de riesgos emergentes.
- La naturaleza y el valor de los activos y los recursos.
- Las consecuencias y sus impactos en los objetivos.
- Las limitaciones de conocimiento y la confiabilidad de la información.
- Los factores relacionados con el tiempo.
- Los sesgos, los supuestos y las creencias de las personas involucradas.



La organización debe identificar los riesgos, tanto si sus fuentes están o no bajo su control. Se debería considerar que puede haber más de un tipo de resultado, que puede dar lugar a una variedad de consecuencias tangibles o intangibles.



Existen varios métodos para identificación de riesgos como los son listas de chequeo, experiencia y juicios de pasados eventos y registros existentes, entrevistas con expertos y personas que hayan sido expuestas al riesgo o posean conocimientos específicos.

La lluvia de ideas una de las más usadas ya que permite que todos los integrantes de equipos puedan hacer aportes y genere participación colectiva, las auditorias pasadas y reportes de operaciones también son fuentes de información importante, así como análisis de escenarios y flujos, por esta razón es importante la información documentada.



5.3.2. Análisis del riesgo

5.3.2.1. Tipos de riesgos

Algunos tipos de riesgos son:

- **Riesgos inherentes:** Son los que se pueden sufrir por el entorno de las operaciones empresariales.
- **Riesgos externos:** son los riesgos que se pueden sufrir por acciones de terceros o eventos externos, de los que no se puede tener ningún tipo de control.
- **Riesgos residuales:** Son los que se pueden sufrir, después de haber aplicado las medidas de control necesarias en la mitigación de riesgos.
- **Riesgos potenciales:** Son los que se pueden sufrir cuando se opera bajo un contexto global, en donde todos los cambios económicos y políticos aumentan los riesgos.

5.3.2.2. Clasificación de riesgos

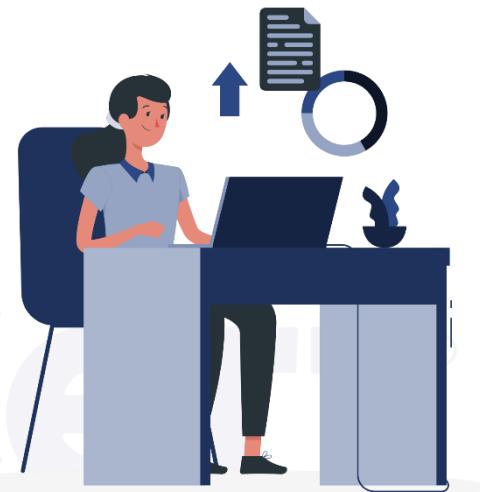
Los riesgos se pueden clasificar en una escala por niveles, así:



Lo anterior es una base de lo que puede usar una organización para la gestión de sus riesgos, ya que, cada empresa debe definir los tipos y clasificación de sus propios riesgos. Teniendo en cuenta los factores internos y externos, los requisitos de las partes interesadas, su política y objetivos.

El análisis de riesgos implica:

- Analizar el estado actual (contexto).
- Definir el método a emplear.
- Variables: probabilidad e impacto (independientes).
- Subjetividad en las valoraciones (análisis).
- No deben existir prejuicios.
- No dejarse influenciar por el cliente.
- Valor del analista.



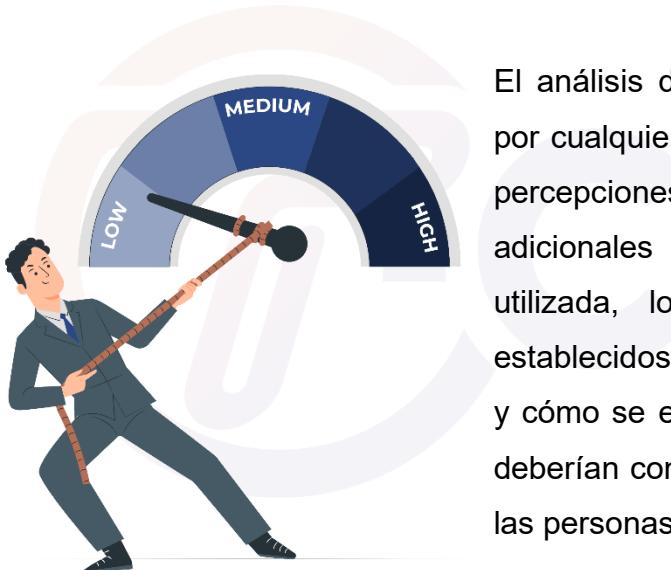
El propósito del análisis del riesgo es comprender la naturaleza del riesgo y sus características, incluyendo cuando sea apropiado, el nivel del riesgo. El análisis del riesgo implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia. Un evento puede tener múltiples causas y consecuencias y puede afectar a múltiples objetivos.

El análisis del riesgo se puede realizar con diferentes grados de detalle y complejidad, dependiendo del propósito del análisis, la disponibilidad y la confiabilidad de la información y los recursos disponibles. Las técnicas de análisis

pueden ser cualitativas, cuantitativas o una combinación de éstas, dependiendo de las circunstancias y del uso previsto.

El análisis del riesgo debería considerar factores tales como:

- La probabilidad de los eventos y de las consecuencias.
- La naturaleza y la magnitud de las consecuencias.
- La complejidad y la interconexión.
- Los factores relacionados con el tiempo y la volatilidad.
- La eficacia de los controles existentes.
- Los niveles de sensibilidad y de confianza.



El análisis del riesgo puede estar influenciado por cualquier divergencia de opiniones, sesgos, percepciones del riesgo y juicios. Las influencias adicionales son la calidad de la información utilizada, los supuestos y las exclusiones establecidos, cualquier limitación de las técnicas y cómo se ejecutan éstas. Estas influencias se deberían considerar, documentar y comunicar a las personas que toman decisiones.

Los eventos de alta incertidumbre pueden ser difíciles de cuantificar. Esto puede ser una cuestión importante cuando se analizan eventos con consecuencias severas. En tales casos, el uso de una combinación de técnicas generalmente proporciona una visión más amplia.

El análisis del riesgo proporciona una entrada para la valoración del riesgo, para las decisiones sobre la manera de tratar los riesgos y si es necesario hacerlo y sobre la estrategia y los métodos más apropiados de tratamiento del riesgo.

Los resultados proporcionan un entendimiento profundo para tomar decisiones, cuando se está eligiendo entre distintas alternativas, y las opciones implican diferentes tipos y niveles de riesgo.

La norma ISO 31010 tiene a su disposición y comparación diferentes metodologías que permiten el análisis con diferentes opciones y adaptabilidad a diferentes sectores de la economía, cada metodología cuenta con aplicabilidad y mejor adaptabilidad.

Sin embargo, la ISO 31000 demuestra su versatilidad y facilita tanto la implementación como la adaptabilidad a cualquier tipo de empresa, negocio y/o sector económico donde se desarrolle el negocio.

5.3.3. Valoración del riesgo

La evaluación de los riesgos implica:

- Definir niveles de riesgo.
- Mantener la independencia entre probabilidad e impacto.
- Clasificar los riesgos.
- Priorizar.
- Permite orientar la toma de decisiones.
- De la criticidad se desprende el tratamiento y control.



El propósito de la valoración del riesgo es apoyar a la toma de decisiones. La valoración del riesgo implica comparar los resultados del análisis del riesgo con los criterios del riesgo establecidos para determinar cuándo se requiere una acción adicional.

Esto puede conducir a una decisión de:

- No hacer nada más.
- Considerar opciones para el tratamiento del riesgo.
- Realizar un análisis adicional para comprender mejor el riesgo.
- Mantener los controles existentes.
- Reconsiderar los objetivos.

Las decisiones deben tener en cuenta un contexto más amplio y las consecuencias reales y percibidas por las partes interesadas externas e internas.

Los resultados de la valoración del riesgo se deben registrar, comunicar y luego validar a los niveles apropiados de la organización.

Para efectuar análisis de riesgos se puede utilizar la metodología de mapa de calor que, a través de variables como el **impacto** y la **probabilidad**, una tipificación de cada variable y una ponderación generar una calificación del estado actual del riesgo sin todavía ejecutar un tratamiento ósea elaborar un diagnóstico actual.

Tabla 3. Matriz de evaluación del riesgo - Mapa de calor

Probabilidad		Nivel del Riesgo (Probabilidad x Impacto)				
Cierto	5	5	10	15	20	25
Probable	4	4	8	12	16	20
Possible	3	3	6	9	12	15
Improbable	2	2	4	6	8	10
Raro	1	1	2	3	4	5
IMPACTO	1	2	3	4	5	
	Insignificante	Menor	Moderado	Mayor	Catastrófico	
	Riesgo Externo	Riesgo Alto	Riesgo Moderado	Riesgo Bajo		

Ahora veamos la relación con un ejemplo para establecer variables para el manejo de probabilidad y de impacto.

Tabla 4. Ejemplo definición variables de probabilidad

NIVEL	DESCRIPCIÓN	DESCRIPCIÓN
5	Inminente	<ul style="list-style-type: none"> • Ha ocurrido más de dos veces en el último semestre. • No se cuenta con los procedimientos, medidas de control, seguridad ni elementos de protección.
4	Probable	<ul style="list-style-type: none"> • Ha ocurrido al menos una vez en el último semestre. • Las medidas de control, seguridad y elementos de protección no se aplican o no son eficientes.
3	Possible	<ul style="list-style-type: none"> • Ha ocurrido al menos una vez en el último año. • Existen medidas de control, seguridad y elementos de protección.
2	Improbable	<ul style="list-style-type: none"> • Ha ocurrido una vez en los últimos 3 años. • Las medidas de control, seguridad y elementos de protección son verificadas en cada operación.
1	Raro	<ul style="list-style-type: none"> • Ha ocurrido una vez en los últimos 5 años. • Las medidas de control, seguridad y elementos de protección son verificadas en cada operación y se mejoran continuamente.

Tabla 5. Ejemplo definición variables de impacto

NIVEL	DESCRIPCIÓN	DESCRIPCIÓN
5	Catastrófico	<p>Requiere rediseño de los procedimientos vigentes.</p> <ul style="list-style-type: none"> • Hay afectación severa del sistema con demoras superiores a los 3 días de operación.

NIVEL	DESCRIPCIÓN	DESCRIPCIÓN
		<ul style="list-style-type: none"> • Pérdidas financieras superiores a treinta salarios mínimos mensuales legales vigentes. • Muerte o lesiones mayores con incapacidad total y permanente. • Hay daños severos en las estructuras físicas de la empresa que deben ser atendidas por profesionales y que suspende la operación. • Su imagen corporativa se afecta frente al cliente interno y externo a nivel regional y nacional.
4	Mayor	<p>Requiere ajustes y supervisión a los procedimientos vigentes.</p> <ul style="list-style-type: none"> • Hay afectación del sistema con demoras de hasta 3 días en la operación. • Perdidas financieras que oscilan entre los ocho y treinta salarios mínimos mensuales vigentes. • Lesiones mayores que requieren hospitalización y originan incapacidad de hasta 3 meses. • Hay daños mayores en las estructuras físicas de la empresa que deben ser atendidas por profesionales y que limitan la operación. • Su imagen corporativa se afecta frente al cliente interno y externo a nivel local.
3	Moderada	<p>Requiere ajustes a los procedimientos vigentes.</p> <ul style="list-style-type: none"> • Hay afectación del sistema con demoras de hasta 4 horas en la operación. • Perdidas financieras que oscilan entre los cuatro y ocho salarios mínimos mensuales vigentes. • Lesiones menores con incapacidad de un día de trabajo.

NIVEL	DESCRIPTOR	DESCRIPCIÓN
		<ul style="list-style-type: none"> • Hay daños leves en las estructuras físicas de la empresa atendidas por mano de obra no calificada. • Su imagen corporativa se afecta frente al cliente interno.
2	Menor	<p>Requiere revisión de los procedimientos vigentes.</p> <ul style="list-style-type: none"> • No hay afectación del sistema, continúa trabajando por sí solo. • Perdidas financieras que oscilan entre uno y cuatro salarios mínimos mensuales vigentes. • Lesiones leves que requieren primeros auxilios sin más procedimientos. • No hay daños en las estructuras físicas de la empresa. • No hay daño en su imagen corporativa.
1	Insignificante	<p>No requiere tratamiento.</p> <ul style="list-style-type: none"> • El sistema continúa trabajando por sí solo. • Perdidas financieras inferiores a un salario mínimo mensual vigente. • No hay afectaciones de la integridad de las personas. • No hay daños en las estructuras físicas de la empresa. • No hay daño en su imagen corporativa.

5.4. Tratamiento del riesgo

El tratamiento de riesgos debe realizarse después de cada iteración del proceso de evaluación de riesgos de la seguridad de la información. Es decir, siempre que se actualice la evaluación de riesgos la organización se debe aplicar y actualizar el plan del tratamiento de riesgos.

Para desarrollar un plan de tratamiento de riesgos y la implementación de controles y procesos de seguridad es fundamental asignar tareas y responsabilidades. Asignar un responsable, permitirá:

- Establecer los objetivos.
- Hacer efectivas las medidas organizativas.
- Implantar y ejecutar las tareas técnicas planificadas.
- Supervisar las actividades.
- Recabar y analizar la información de los indicadores.
- La detección y notificación de las incidencias.

Para hacer efectivo el tratamiento de riesgos puede generar modelos o plantillas que ayuden en la recolección de información sobre el proceso de implantación de controles y las medidas de seguridad que se derivan del tratamiento de riesgos.

Cuando un proceso se ha definido, planificado, tiene responsables, se encuentra integrado a los procesos de la organización y se ha integrado por un periodo de tiempo para la toma de efectividad, se puede decir que se ha pasado la primera fase de la implementación.



El propósito del tratamiento del riesgo es seleccionar e implementar opciones para abordar el riesgo. Para esto debe:

- Considerar la valoración del riesgo.
- Entender que en este punto se convierte en una herramienta gerencial.
- Valorar la eficacia del tratamiento.

El tratamiento del riesgo implica un proceso iterativo de:

- Formular y seleccionar opciones para el tratamiento del riesgo.
- Planificar e implementar el tratamiento del riesgo.
- Evaluar la eficacia de ese tratamiento.
- Decidir si el riesgo residual es aceptable.
- Si no es aceptable, efectuar tratamiento adicional.

5.4.1. Selección de las opciones para el tratamiento del riesgo



En la figura anterior se muestran cuatro opciones que se pueden tomar para tratar los riesgos, ya sea aceptando y administrándolo, mitigándolo y generando dispersión de este para no concentrado en una sola alternativa, transfiriéndolo con opciones diferentes y evitándolo, rediciendo o definitivamente cancelando o cerrando. Ahora veamos de qué trata cada uno:

Mitigar el riesgo

- Fortalece el control interno en los procesos del negocio.
- Diversificación de productos.

Transferir el riesgo

- Compra de seguros contra perdidas inesperadas significativas.
- Contratación de outsourcing para procesos del negocio.
- Compartir el riesgo con acuerdos sindicales o contractuales con clientes, proveedores u otros socios del negocio.

Evitar el riesgo

- Reducir la expansión de una línea de productos a nuevos mercados.
- Vender una división, unidad de negocio o segmento geográfico altamente riesgoso.
- Dejar de producir un producto o servicio altamente riesgoso.

Aceptar el riesgo

- Auto asegurarse contra perdidas.
- Aceptar los riesgos de acuerdo con los niveles de tolerancia del riesgo.

La selección de las opciones más apropiadas para el tratamiento



del riesgo implica hacer un balance entre los beneficios potenciales, derivados del logro de los objetivos contra costos, esfuerzo o desventajas de la implementación.

Las opciones de tratamiento del riesgo no necesariamente son mutuamente excluyentes o apropiadas en todas las circunstancias. Las opciones para tratar el riesgo pueden implicar una o más de las siguientes:

- Evitar el riesgo decidiendo no iniciar o continuar con la actividad que genera el riesgo.
- Aceptar o aumentar el riesgo en busca de una oportunidad.
- Eliminar la fuente de riesgo.
- Modificar la probabilidad.
- Modificar las consecuencias.
- Compartir el riesgo.
- Retener el riesgo con base en una decisión informada.

La justificación para el tratamiento del riesgo es más amplia que las simples consideraciones económicas y debería tener en cuenta todas las obligaciones de la organización, los compromisos voluntarios y los puntos de vista de las partes interesadas. La selección de las opciones para el tratamiento del riesgo debe realizarse de acuerdo con los objetivos de la organización, los criterios del riesgo y los recursos disponibles.



Al seleccionar opciones para el tratamiento del riesgo, la organización debe considerar los valores, las percepciones, el involucrar potencialmente a las partes interesadas y los medios más apropiados para comunicarse con ellas y consultarlas.

A igual eficacia, algunas partes interesadas pueden aceptar mejor que otras los diferentes tratamientos del riesgo.

Los tratamientos del riesgo, a pesar de un cuidadoso diseño e implementación, pueden no producir los resultados esperados y puede producir consecuencias no previstas. El seguimiento y la revisión necesitan ser parte integral de la implementación del tratamiento del riesgo para asegurar que las distintas maneras del tratamiento sean y permanezcan eficaces.

El tratamiento del riesgo a su vez puede introducir nuevos riesgos que necesiten gestionarse.

Si no hay opciones disponibles para el tratamiento o si las opciones para el tratamiento no modifican suficientemente el riesgo, éste se debería registrar y mantener en continua revisión.

Las personas que toman decisiones y otras partes interesadas deberían ser conscientes de la naturaleza y el nivel del riesgo residual después del tratamiento del riesgo. El riesgo residual se debería documentar y ser objeto de seguimiento, revisión y, cuando sea apropiado, de tratamiento adicional.



5.4.2. Preparación e implementación de los planes de tratamiento del riesgo

El propósito de los planes de tratamiento del riesgo es especificar la manera en la que se implementarán las opciones elegidas para el tratamiento, de manera tal que los involucrados comprendan las disposiciones, y que pueda realizarse el seguimiento del avance respecto de lo planificado.

El plan de tratamiento debe identificar claramente el orden en el cual el tratamiento del riesgo se debe implementar.

Los planes de tratamiento deben integrarse en los planes y procesos de la gestión de la organización, en consulta con las partes interesadas apropiadas. La información proporcionada en el plan del tratamiento debería incluir:

- El fundamento de la selección de las opciones para el tratamiento, incluyendo los beneficios esperados.
- Las personas que rinden cuentas y aquellas responsables de la aprobación e implementación del plan.
- Las acciones propuestas.
- Los recursos necesarios, incluyendo las contingencias.
- Las medidas del desempeño.
- Las restricciones.
- Los informes y seguimiento requeridos.

Apreciación del riesgo



Inicialmente cuando apreciamos los riesgos partimos del hecho de una identificación y un análisis del riesgo, validamos la calidad de riesgo inherente y el apetito de riesgo que la compañía tienen definido lo que esperamos es decantar el riesgo y con el plan implementado generar un riesgo administrado y controlado llamado riesgo residual.

5.5. Seguimiento y revisión

El propósito del seguimiento y la revisión es asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados del proceso. El seguimiento continuo y la revisión periódica del proceso de la gestión del riesgo y sus resultados debe ser una parte planificada del proceso de la gestión del riesgo, con responsabilidades claramente definidas.

El seguimiento y la revisión deben tener lugar en todas etapas del proceso. El seguimiento y la revisión incluyen planificar, recopilar y analizar información, registrar resultados y proporcionar retroalimentación.

Los resultados del seguimiento y la revisión deben incorporarse a todas las actividades de la gestión del desempeño, de medición y de informe de la organización.

Pilares de administración del riesgo



En la figura anterior se muestra que luego de trabajar en la prevención y de materializarse el riesgo la organización debe administrarlo, controlarlo y lograr reducirlo en impacto y probabilidad, quedando el riesgo residual, que deja experiencias y consecuencias de las cuales con los planes de tratamiento y mecanismos de control se acepta o se transfiere.

5.6. Registros e informes

El proceso de la gestión del riesgo y sus resultados se deben documentar e informar a través de los mecanismos apropiados. El registro e informe pretenden:

- Comunicar las actividades de la gestión del riesgo y sus resultados a lo largo de la organización.
- Proporcionar información para la toma de decisiones.
- Mejorar las actividades de la gestión del riesgo.
- Asistir la interacción con las partes interesadas, incluyendo a las personas que tienen la responsabilidad y la obligación de rendir cuentas de las actividades de la gestión del riesgo.

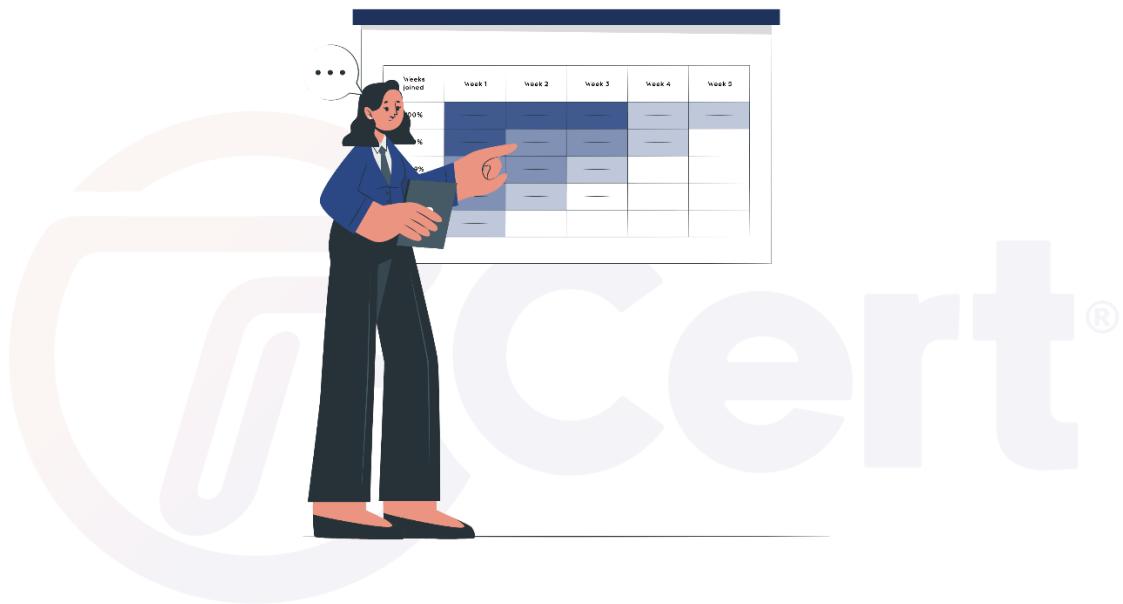
Las decisiones con respecto a la creación, conservación y tratamiento de la información documentada deberían tener en cuenta, pero no limitarse a su uso, la sensibilidad de la información y los contextos externo e interno.



El informe es una parte integral de la gobernanza de la organización y debería mejorar la calidad del diálogo con las partes interesadas, y apoyar a la alta dirección y a los órganos de supervisión a cumplir sus responsabilidades.

Los factores para considerar en el informe incluyen, pero no se limitan a:

- Las diferentes partes interesadas, sus necesidades y requisitos específicos de información.
- El costo, la frecuencia y los tiempos del informe.
- El método del informe.
- La pertinencia de la información con respecto a los objetivos de la organización y la toma de decisiones.



Módulo VI.

Riesgos para el

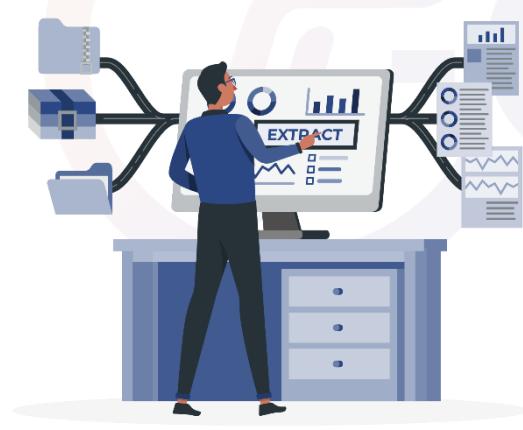
Sector T.I.

Módulo VI. Riesgos para el Sector T.I

El riesgo de Tecnología de la Información (TI) se refiere a la posibilidad de que los sistemas de información, datos o procesos tecnológicos de una organización se vean comprometidos y afectados.

Esto puede tener como resultado pérdidas financieras daños a la reputación, interrupciones operativas o violaciones de la seguridad. En el mundo digital actual, donde la mayoría de las organizaciones dependen en gran medida de la tecnología para llevar a cabo sus operaciones y cumplir como áreas de apoyo o Core de negocio que ejecutan a diario.

6.1. ISO 31000 y las Tecnologías de la Información



Ahora que hemos plantado la semilla de la curiosidad, profundicemos en cómo la ISO 31000 se aplica a las tecnologías de la información. En un mundo impulsado por datos y tecnología, los riesgos cibernéticos y la seguridad de la información son temas candentes.

La ISO 31000 actúa como un faro que guía a las organizaciones a través de las aguas tumultuosas de la ciberseguridad y la gestión de riesgos en TI.

6.2. ¿Por qué la ISO 31000 en TI es esencial?

Imagina esto, tu empresa se enfrenta a una violación de seguridad de datos. ¿Estás preparado para lidiar con las consecuencias? La norma ISO 31000 te ofrece una estructura sólida para anticipar y abordar estos riesgos. Esto no solo te protege de

eventos adversos, sino que también te permite capitalizar las oportunidades que el mundo digital tiene para ofrecer.

6.3. Beneficios de adoptar la ISO 31000

La implementación de la ISO 31000 ofrece una serie de ventajas clave, como lo son:

- 1. Gestión integral de riesgos:** La norma proporciona un marco estructurado para identificar y abordar riesgos, lo que ayuda a evitar sorpresas desagradables.
- 2. Protección de datos:** En un mundo donde los datos son un activo crítico, la ISO 31000 contribuye a salvaguardar la información confidencial.
- 3. Cumplimiento regulatorio:** Cumplir con regulaciones es un requisito legal. La ISO 31000 te ayuda a cumplir con los requisitos de gestión de riesgos establecidos por reguladores.
- 4. Mejora en la toma de decisiones:** La Gestión de Riesgos efectiva proporciona información valiosa para la toma de decisiones estratégicas. Esto te ayuda a asignar recursos de manera más inteligente.
- 5. Aprovechamiento de oportunidades:** La ISO 31000 no se enfoca solo en mitigar riesgos, sino también en identificar y aprovechar oportunidades, impulsando el crecimiento.



6.4. Implementación de la ISO 31000

Puede parecer un desafío, pero la implementación de la ISO 31000 se desglosa en pasos lógicos:

1. **Comprende el contexto:** Antes de comenzar, comprende tu organización y su entorno. Esto incluye identificar los objetivos, partes interesadas y el alcance de la gestión de riesgos.
2. **Identifica los riesgos:** Ahora es el momento de identificar riesgos, analizando amenazas y oportunidades que pueden afectar a tu organización.
3. **Evalúa los riesgos:** Una vez identificados, evalúa los riesgos, determinando su probabilidad e impacto potencial.
4. **Trata los riesgos:** Desarrolla estrategias para abordar los riesgos. Esto puede incluir evitar, mitigar, transferir o aceptar riesgos.
5. **Supervisión y revisión:** la gestión de riesgos no es un proceso estático. Debe ser monitoreada y revisada constantemente para mantenerse al día con los cambios en el entorno empresarial.

6.5. El futuro de la gestión de riesgos en TI

En un mundo en constante evolución, la gestión de riesgos se convierte en un pilar fundamental de cualquier organización. La norma ISO 31000 proporciona una base

sólida para abordar riesgos y oportunidades de manera efectiva, y su importancia en el campo de las tecnologías de la información no debe subestimarse.

Hoy las compañías trabajan en categorizar sus riesgos de T.I en:

- Riesgos de Ciberseguridad.
- Riesgos de Infraestructura Tecnológica.
- Riesgos de Acceso y Autenticación.
- Riesgos de Cumplimiento y Regulatorios.
- Riesgos Humanos.
- Riesgos de Terceros.

Adicional la Inteligencia Artificial (IA), tecnología de automatización, Internet de las Cosas (IoT), Robótica, Impresión 3D, servicios en la nube, ciberseguridad y otras que ofrece innumerables prestaciones para incrementar la productividad e incluso la seguridad de las organizaciones.

El reto para áreas de T.I está en que la “IA” es responsable de muchos de los riesgos tecnológicos y deben ser debidamente administrados.



Mediante estos sistemas, los ciberdelincuentes pueden diseñar ataques de ingeniería social y de phishing más convincentes. También crear malwares adaptativos. Dos acciones que ponen en jaque la integridad de cualquier compañía. Con el desarrollo de tecnología iCloud los riesgos que se pueden materializar están a la orden del día, así como afectación a las soluciones de la nube.

En la implementación y en sistemas de almacenamiento virtual, se corre el riesgo de que los datos se pierdan o caigan en manos inadecuadas por brechas de ciberseguridad o los accesos no autorizados, se requiere un extra de seguridad y controles para mitigar la pérdida de control de la información de la compañía y de los procesos y no afectar a la confidencialidad empresarial.

6.5.1. Formación del personal

Enseñar a la plantilla a manejar los últimos sistemas tecnológicos, bien sean soluciones iCloud o de IA, es el primer paso hacia la prevención de los riesgos y el aumento de la productividad.



Hoy en rol de la tecnología como articulador de áreas de apoyo y eje fundamental de seguridad, riesgos y productividad deberá manejar políticas de gobernanza dirigido a la protección integral de los datos, manejo estructurado de información sensible, en términos de ciberseguridad con implementación de identidad en la nube, integración de soluciones de acceso privado y optimización los algoritmos de la IA para evitar manipulaciones maliciosas.

Es muy importante el monitoreo constante en gestión de riesgos tecnológicos y auditorias periódicas para detectar no confirmades y hallazgos que permitan fomentar planes de acción preventivos.

6.5.2. Riesgos asociados a la seguridad de la información

- **Amenazas cibernéticas:** Este tipo de riesgo incluye ataques maliciosos realizados por hackers, crackers y otros actores. Estos ataques pueden

incluir malware, como virus y ransomware, así como ataques de denegación de servicio (DDoS), phishing y ataques de ingeniería social.

- **Brechas de seguridad:** Las brechas de seguridad ocurren cuando se producen vulnerabilidades en los sistemas de información, permitiendo el acceso no autorizado a datos confidenciales. Estas vulnerabilidades pueden ser el resultado de configuraciones incorrectas, falta de actualizaciones de seguridad, o debilidades en el diseño de los sistemas.



- **Pérdida o robo de datos:** La pérdida o robo de datos ocurre cuando información sensible o confidencial cae en manos equivocadas. Esto puede suceder debido a brechas de seguridad, errores humanos, dispositivos perdidos o robados, o espionaje.
- **Fallas en la infraestructura tecnológica:** Las fallas en la infraestructura tecnológica, como servidores, redes o sistemas de almacenamiento, pueden resultar en la pérdida de datos o interrupciones en los servicios. Estas fallas pueden ser causadas por errores de configuración, sobrecargas de tráfico, problemas de hardware o software, o desastres naturales.
- **Acceso no autorizado:** El acceso no autorizado se refiere a la intrusión en sistemas de información por parte de personas no autorizadas. Esto puede suceder debido a contraseñas débiles, falta de controles de acceso adecuados, o incluso por empleados deshonestos.
- **Riesgos internos:** Los riesgos internos provienen de personas dentro de la organización, como empleados, contratistas o socios comerciales. Esto puede incluir el uso indebido de datos, la divulgación de información

confidencial, o la negligencia en la protección de la seguridad de la información.

- **Riesgos de cumplimiento:** Los riesgos de cumplimiento se refieren a la posibilidad de no cumplir con las leyes, regulaciones o estándares relacionados con la seguridad de la información. Esto puede resultar en sanciones legales, multas o pérdida de reputación para la organización.

6.5.3. Riesgos de ciberseguridad

- **Malware:** Incluye virus, gusanos, troyanos y ransomware, que pueden comprometer la integridad y confidencialidad de los datos.
- **Ataques de phishing:**
Intentos de engañar a usuarios para que revelen información confidencial, como contraseñas o información de tarjetas de crédito, mediante correos electrónicos fraudulentos.An illustration showing a woman with dark hair sitting at a desk, looking at a laptop screen with a confused expression. A thought bubble above her contains a question mark. To her right, a male hacker wearing a black hoodie and a cap is holding a large sword-like tool. He is pointing it towards the woman's laptop. On the screen of the laptop, there is a gauge or meter with a needle pointing to the right. The background features a faint watermark of a medical cross symbol.
- **Ataques de Denegación de Servicio (DDoS):** Sobrecargan un sistema o red con tráfico falso, impidiendo que los usuarios legítimos accedan a los servicios.
- **Ingeniería social:** Manipulación psicológica para obtener información confidencial o acceso no autorizado a sistemas.
- **Fuga de datos:** Pérdida o filtración de información sensible a través de brechas de seguridad.

6.5.4. Riesgos de Infraestructura Tecnológica

- **Fallas de hardware:** Interrupciones en el funcionamiento de equipos informáticos, como servidores, routers o switches.
- **Fallas de software:** Errores en aplicaciones o sistemas operativos que pueden provocar pérdida de datos o violaciones de seguridad.
- **Desastres naturales:** Eventos como terremotos, incendios o inundaciones que pueden dañar la infraestructura física y tecnológica.

6.5.5. Riesgos de acceso y autenticación



- **Contraseñas débiles:** Contraseñas fáciles de adivinar que pueden ser explotadas por atacantes.
- **Acceso no autorizado:** Usuarios sin permisos adecuados que intentan acceder a sistemas o datos sensibles.
- **Fallo en la autenticación multifactorial:** Ausencia de métodos adicionales de autenticación, como códigos de seguridad enviados por mensaje de texto o autenticación biométrica.

6.5.6. Riesgos de cumplimiento y regulatorios

- **Incumplimiento de normativas:** Falta de conformidad con regulaciones y estándares de seguridad de la información, como GDPR, HIPAA o PCI-DSS.
- **Falta de políticas y procedimientos:** Ausencia de directrices claras y procedimientos establecidos para proteger la seguridad de la información.

6.5.7. Riesgos Humanos

- **Errores y negligencia:** Acciones humanas involuntarias que pueden resultar en vulnerabilidades de seguridad o pérdida de datos.
- **Acciones malintencionadas:** Comportamientos intencionales de empleados deshonestos o empleados que buscan dañar la seguridad de la información.



6.5.8. Riesgos de terceros y asociados de negocio

- **Proveedores y contratistas:** Riesgos asociados con proveedores externos que tienen acceso a sistemas o datos de la organización.
- **Subcontratistas:** Riesgos derivados de proveedores de terceros contratados por los proveedores principales.

Al clasificar los tipos de riesgos de IT – Seguridad de la Información de esta manera, las organizaciones pueden identificar áreas específicas de vulnerabilidad y desarrollar estrategias de mitigación adecuadas.

Es importante abordar estos riesgos de manera integral y proactiva para proteger los activos digitales y garantizar la continuidad del negocio.



Glosario

Glosario

Amenaza: Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Consecuencia: Resultado de un evento que afecta a los objetivos. Una consecuencia puede ser cierta o incierta y puede tener efectos positivos o negativos, directos o indirectos sobre los objetivos.

Control: Medida que mantiene y/o modifica un riesgo. Los controles incluyen, pero no se limitan a cualquier proceso, política, dispositivo, práctica u otras condiciones y/o acciones que mantengan y/o modifiquen un riesgo.

Evento: Ocurrencia o cambio de un conjunto particular de circunstancias. Un evento puede tener una o más ocurrencias y puede tener varias causas y varias consecuencias. Un evento puede ser una fuente de riesgo.

Fuente de riesgo: Elemento que, por sí solo o en combinación con otros, tiene el potencial de generar riesgo.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar la organización con relación al riesgo.

Mejora continua: Práctica de gestión enfocada en la mejora constante de procesos operativos, con el objetivo de ser más eficiente y tener un mejor rendimiento.

Parte interesada: Persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad.

Probabilidad: Posibilidad de que algo suceda.

Riesgo: Efecto de la incertidumbre sobre la consecución de los objetivos.

Vulnerabilidad: Debilidad de un activo o de un control que puede ser explotada por una o más amenazas.