Gestión de Riesgos Emergentes

Tácito Augusto Silva Leite

La contribución de la ISO 31050 al sector de Seguridad

Costa Rica • 2024

Resumen

Este eBook complementa la presentación realizada por Tácito Augusto Silva Leite durante el Congreso de la ASIS Latam&CA en Costa Rica en 2024 – Congreso de Seguridad Integral, los días 18 y 19 de noviembre. Tácito presentó la ponencia titulada: Gestión de riesgos emergentes: La contribución de la ISO 31050 al sector de seguridad.

Este eBook explora cómo la norma ISO 31050 contribuye a la gestión de riesgos emergentes en el sector de seguridad. A través de un enfoque estructurado y adaptativo, la ISO 31050 proporciona directrices específicas para identificar y gestionar riesgos emergentes, caracterizados por su incertidumbre, complejidad y falta de patrones históricos. El contenido abarca la importancia de una gestión proactiva de riesgos emergentes, su integración con los objetivos estratégicos de las organizaciones, y la comparación con el enfoque de Enterprise Security Risk Management (ESRM) de ASIS, destacando cómo ambos enfoques pueden ser complementarios para lograr una gestión holística y eficaz.

El eBook también aborda los desafíos culturales y operacionales en la implementación de la ISO 31050, así como la importancia de superar las limitaciones de datos y el sesgo de percepción para lograr una gestión eficaz. Con ejemplos prácticos y estudios de caso, se ilustra cómo la anticipación de riesgos emergentes puede transformarse en una ventaja competitiva, mejorando la resiliencia y la sostenibilidad organizacional. Finalmente, se ofrecen recomendaciones prácticas para aplicar la ISO 31050 en el contexto de seguridad, complementando las prácticas actuales y fortaleciendo la capacidad organizacional para enfrentar un entorno cambiante.

Summary

This eBook complements the presentation given by Tácito Augusto Silva Leite during the ASIS Latam&CA Congress in Costa Rica in 2024 – Integrated Security Congress, on November 18 and 19. Tácito delivered the lecture titled: Emerging Risk Management: The Contribution of ISO 31050 to the Security Sector.

This eBook explores how ISO 31050 contributes to the management of emerging risks in the security sector. Through a structured and adaptive approach, ISO 31050 provides specific guidelines for identifying and managing emerging risks, characterized by their uncertainty, complexity, and lack of historical patterns. The content covers the importance of proactive management of emerging risks, their integration with the strategic objectives of organizations, and a comparison with the Enterprise Security Risk Management (ESRM) approach by ASIS, highlighting how both approaches can be complementary to achieve holistic and effective management.

The eBook also addresses cultural and operational challenges in the implementation of ISO 31050, as well as the importance of overcoming data limitations and perception bias to achieve effective management. With practical examples and case studies, it illustrates how anticipating emerging risks can be transformed into a competitive advantage, improving organizational resilience and sustainability. Finally, practical recommendations are offered for applying ISO 31050 in the security context, complementing current practices and strengthening organizational capacity to face a changing environment.

Palabras claves

ISO 31050; ISO 31000; Gestión de riesgos emergentes; Sector de seguridad; Incertidumbre y complejidad; Gestión proactiva; Enterprise Security Risk Management (ESRM); Resiliencia organizacional; Ventaja competitiva; Riesgos y oportunidades.

Acerca del autor

tacitoleite@totalrisk.com.br

www.linkedin.com/in/tacitoleite

http://lattes.cnpq.br/6763601233758573

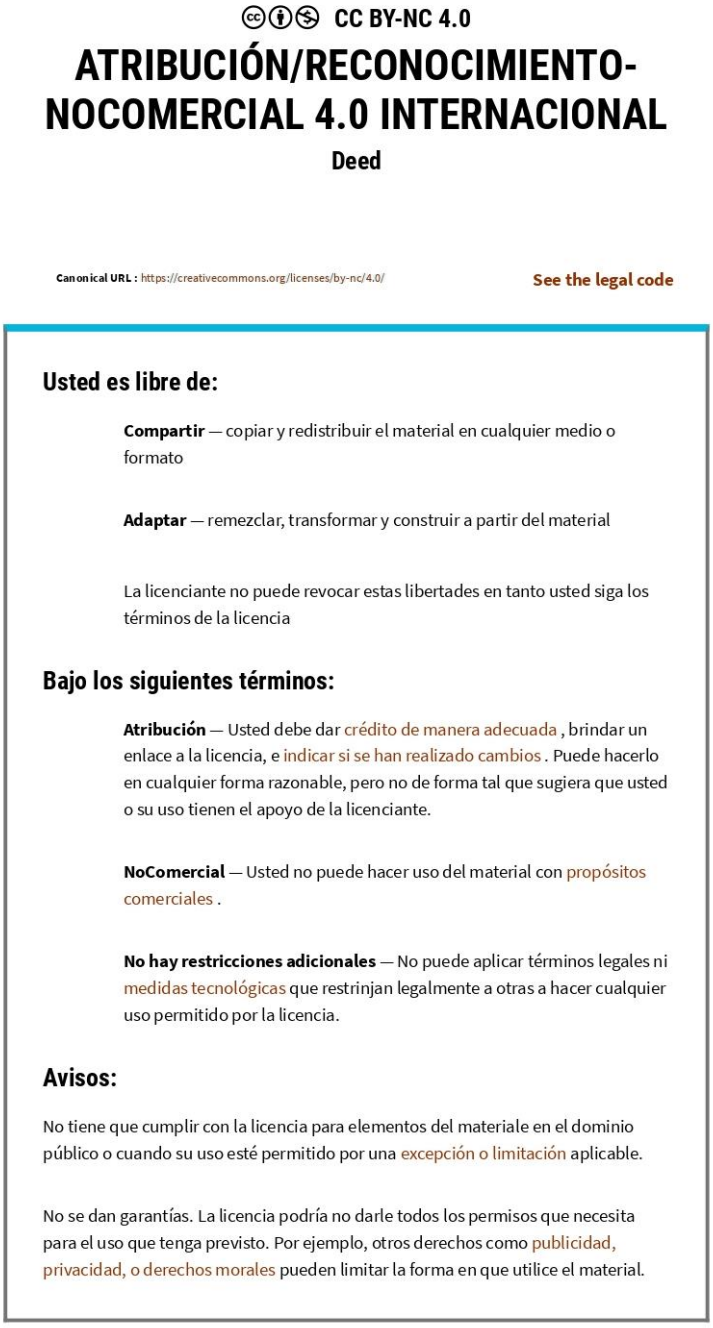
Tácito Augusto Silva Leite, MSc

DSE, C31000, ASE

Máster en Gestión de Riesgos por EALDE Business School y UCAM Universidad Católica San Antonio de Murcia, autor del libro *Gestión de Riesgos en la Seguridad Patrimonial* - consultoriadeseguranca.com.br, Creador de la Plataforma t-Risk - totalrisk.com.br, Posgraduado en Seguridad Empresarial por la Universidad Pontificia Comillas de Madrid, MBA en Gestión de Seguridad Empresarial por la Universidad Anhembi-Morumbi (Laureate), MBA en Sistemas de Información por la Universidad UnP con especialización en Seguridad de la Información, Curso de Gestión de Recursos de Defensa por la Escuela Superior de Guerra en Brasil, Curso de Formación en Gestión de Riesgos y Auditoría basada en Riesgos ISO 31000 por QSP, Curso de Terrorismo y Contraterrorismo por la Universiteit Leiden en los Países Bajos y Oficial de la Reserva del Ejército Brasileño. Trabaja desde 1994 en el área de gestión de riesgos, seguridad corporativa y seguridad de la información. CEO de la plataforma t-Risk y Director de ABSEG – Asociación Brasileña de Profesionales de Seguridad.

Licencia de Distribución

Haga clic en la imagen de abajo para acceder.



CC BY-NC 4.0

ATRIBUCIÓN/RECONOCIMIENTO-NOCOMERCIAL 4.0 INTERNACIONAL

Deed

Canonical URL : https://creativecommons.org/licenses/by-nc/4.0/

See the legal code

Usted es libre de:

Compartir — copiar y redistribuir el material en cualquier medio o formato

Adaptar — remezclar, transformar y construir a partir del material

La licenciante no puede revocar estas libertades en tanto usted siga los términos de la licencia

Bajo los siguientes términos:

Atribución — Usted debe dar crédito de manera adecuada , brindar un enlace a la licencia, e indicar si se han realizado cambios . Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que usted o su uso tienen el apoyo de la licenciante.

NoComercial — Usted no puede hacer uso del material con propósitos comerciales .

No hay restricciones adicionales — No puede aplicar términos legales ni medidas tecnológicas que restrinjan legalmente a otras a hacer cualquier uso permitido por la licencia.

Avisos:

No tiene que cumplir con la licencia para elementos del materiale en el dominio público o cuando su uso esté permitido por una excepción o limitación aplicable.

No se dan garantías. La licencia podría no darle todos los permisos que necesita para el uso que tenga previsto. Por ejemplo, otros derechos como publicidad, privacidad, o derechos morales pueden limitar la forma en que utilice el material.

CONTENIDO

Capítulo 1 – Introducción al Concepto de Riesgos Emergentes 9

1.1. Breve introducción sobre la ISO en el mundo y los comités técnicos (ABNT/CEE-063) 9

1.2. Definición y características de los riesgos emergentes (basado en la ISO 31050) 9

1.3. Ejemplos de riesgos emergentes en seguridad corporativa 10

1.4. La importancia de anticipar y gestionar riesgos emergentes 11

Capítulo 2 – ISO 31050: Perspectivas y Contribuciones 14

2.1. Visión general de la norma ISO 31050:2023 y su contexto de aplicación 14

2.2. Diferencias y similitudes entre ISO 31050 e ISO 31000:2018 15

2.3. Cómo la ISO 31050 complementa la ISO 31000 en la gestión de riesgos emergentes 15

2.4. Aplicación de los principios de la ISO 31050 en el aumento de la resiliencia organizacional 16

Capítulo 3 – Proceso de gestión de riesgos emergentes con ISO 31050 18

3.1. Ciclo de inteligencia de riesgo: conceptos y aplicación 18

3.2. Adopción de un enfoque integrado y holístico para la gestión de riesgos 20

3.3. La necesidad de acumulación de conocimiento verificable y la toma de decisiones bajo incertidumbre 20

Capítulo 4 – Comparación entre ESRM (Enterprise Security Risk Management) de ASIS e ISO 31050 23

4.1. Introducción al concepto de ESRM y su relevancia para la seguridad corporativa 23

4.2. Principios de la evaluación de riesgos de seguridad en el contexto del ESRM y la ISO 3105024

4.3. Comparación entre los principios del ESRM y el enfoque de la ISO 31050 25

4.4. Punto de convergencia: cómo alinear ESRM con ISO 31050 para una gestión estratégica 25

Capítulo 5 – Transformación de Incertidumbres en Oportunidades 28

5.1. Cómo la ISO 31050 facilita la transformación de riesgos en ventajas competitivas 28

5.2. Estudios de caso y ejemplos de aplicación en el sector de seguridad 28

5.3. Beneficios de la gestión de riesgos emergentes para la resiliencia y la sostenibilidad organizacional 30

Capítulo 6 – Integración de la Gestión de Riesgos Emergentes con los Objetivos Corporativos 32

6.1. La importancia de la integración con los objetivos estratégicos de la organización 32

6.2. Contribuciones de la ISO 31050 para el alineamiento de las estrategias de seguridad con las metas corporativas 33

6.3. Ejemplos prácticos de alineamiento y resultados obtenidos 33

Capítulo 7 – Desafíos en la Implementación de la ISO 31050 en el Sector de Seguridad 36

7.1. Principales barreras culturales y operativas 36

7.2. Superando limitaciones de datos y el sesgo de percepción 37

Capítulo 8 – Conclusión y Recomendaciones Estratégicas 39

8.1. La importancia de un enfoque proactivo para los riesgos emergentes 39

8.2. Recomendaciones para la aplicación práctica de la ISO 31050 en el sector de seguridad 40

8.3. Fortaleciendo la seguridad corporativa con ISO 31050 41

8.4. Pasos para implementar la ISO 31050 en complemento al proceso actual de gestión de riesgos de seguridad 41

ANEXO I – Análisis comparativo entre ESRM-ASIS e ISO 31000 45

ANEXO II – Referencias bibliográficas 47

Introducción al Concepto de Riesgos Emergentes

01

Capítulo 1 – Introducción al Concepto de Riesgos Emergentes

1.1. Breve introducción sobre la ISO en el mundo y los comités técnicos (ABNT/CEE-063)

La Organización Internacional de Normalización (ISO) está presente en más de 170 países y es una entidad internacional de normalización que se dedica a la creación y estandarización de normas técnicas aplicables en diversos sectores, incluyendo la gestión de riesgos. La ISO contribuye a la armonización global de prácticas, promoviendo la eficiencia y la seguridad en varios campos.

El Comité Técnico ISO/TC 262 (Brasil) es responsable del desarrollo de las normas ISO relacionadas con la gestión de riesgos, con una amplia contribución de más de 70 comités en todo el mundo, como el ABNT/CEE-063 en Brasil. Este comité es una referencia en términos de innovación en la gestión de riesgos, con la participación activa de profesionales de diversas industrias.

1.2. Definición y características de los riesgos emergentes (basado en la ISO 31050)

La ISO 31050 define los riesgos emergentes como fenómenos que no se comprenden o prevén completamente debido a su complejidad y a la rapidez con que surgen. Estos riesgos están asociados a incertidumbres que emergen de cambios dinámicos en los entornos sociales, tecnológicos, económicos, ambientales y políticos. A diferencia de los riesgos tradicionales, que pueden medirse y preverse a partir de datos históricos, los riesgos emergentes tienen una naturaleza disruptiva y, a menudo, se originan por fuerzas externas, desafiando los enfoques convencionales de gestión. La falta de un historial consolidado hace que su identificación y evaluación sean más complejas, requiriendo un enfoque adaptativo e innovador.

Los riesgos emergentes pueden clasificarse en varias categorías, dependiendo de sus orígenes e impactos potenciales. Entre las principales categorías se encuentran los riesgos tecnológicos, que surgen del desarrollo e implementación de nuevas tecnologías, como la inteligencia artificial y la automatización avanzada. También destacan los riesgos ambientales, especialmente debido al impacto del cambio climático y los eventos climáticos extremos. Además, existen riesgos sociales, relacionados con los cambios en las expectativas de la sociedad, como la mayor demanda de prácticas ESG, mientras que los riesgos regulatorios y políticos se refieren a la constante evolución de los marcos legales. Por último, los riesgos económicos, como las crisis financieras y la inestabilidad en los mercados, también representan un desafío constante para las organizaciones.

Los riesgos emergentes tienen características que los hacen desafiantes para la gestión de riesgos convencional. En primer lugar, implican un alto grado de incertidumbre y complejidad, resultado de las interacciones entre múltiples factores que no se comprenden bien. Además, su evolución es rápida y dinámica, lo que hace que las estrategias tradicionales de evaluación y tratamiento queden obsoletas. Tienen un impacto potencial amplio y sistémico, afectando no solo partes específicas de la organización, sino también toda la cadena de valor e incluso sectores enteros. Otra característica crítica es la falta de datos históricos, lo que dificulta la utilización de métodos cuantitativos tradicionales en la evaluación de estos riesgos.

Para identificar y gestionar eficazmente los riesgos emergentes, la ISO 31050 propone el uso de una combinación de técnicas cualitativas y cuantitativas, destacando métodos como la exploración de escenarios futuros, que considera variables económicas, sociales, tecnológicas y ambientales. Además, las consultas con expertos son fundamentales, así como el análisis de tendencias y señales débiles en el entorno externo, que permiten detectar cambios en una etapa inicial. El crowdsourcing y la innovación abierta también son técnicas útiles, ya que la colaboración con diversos stakeholders puede revelar información importante sobre posibles cambios y riesgos futuros.

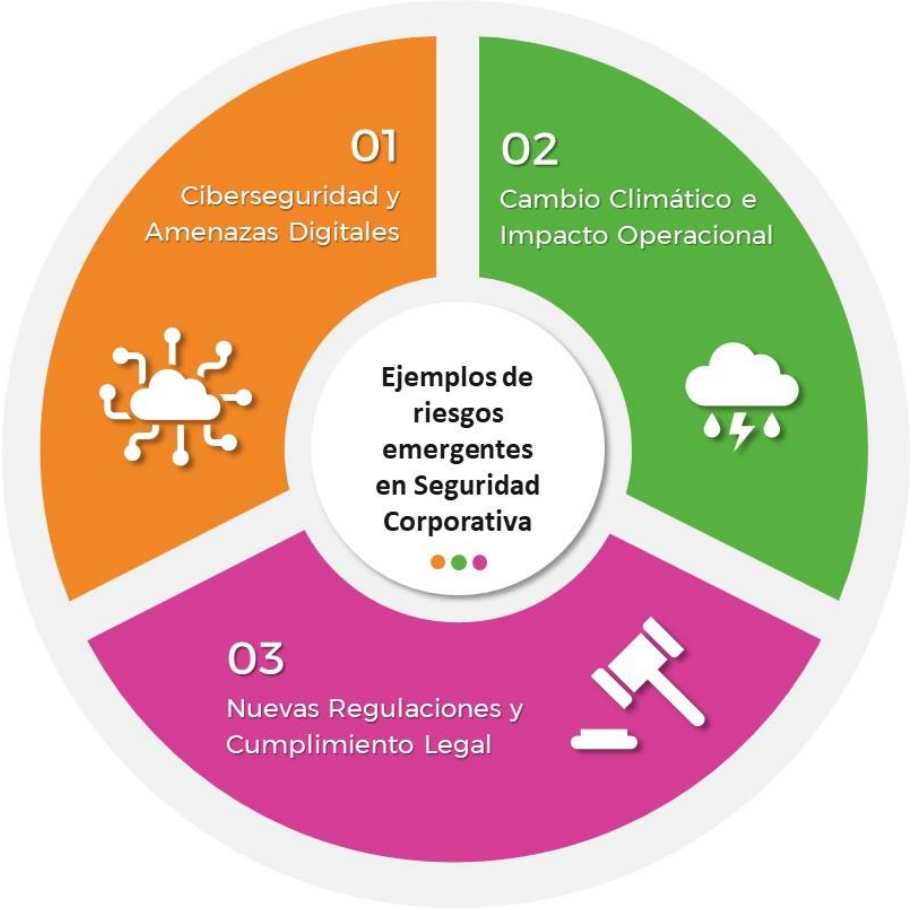
La gestión adecuada de los riesgos emergentes trae numerosos beneficios estratégicos para las organizaciones. Las empresas que logran anticipar y reaccionar rápidamente a los riesgos emergentes fortalecen su resiliencia, minimizando las pérdidas y adaptándose más fácilmente a los cambios. Además, la gestión proactiva de estos riesgos puede transformar la incertidumbre en oportunidades, fomentando la innovación y creando ventajas competitivas. Finalmente, demostrar una sólida capacidad para gestionar riesgos emergentes refuerza la reputación de la organización y la confianza de los stakeholders, clientes, inversores y socios, garantizando la estabilidad y la seguridad de las operaciones, incluso en situaciones de incertidumbre.

1.3. Ejemplos de riesgos emergentes en seguridad corporativa

- **Ciberseguridad y Amenazas Digitales**: Con el aumento de la digitalización, han surgido nuevos riesgos relacionados con ataques cibernéticos, secuestro de datos y violaciones de la privacidad. Estos riesgos impactan directamente la seguridad corporativa, ya que amenazan la integridad de los sistemas y los activos de información.
- **Cambio Climático e Impacto Operacional**: Los eventos climáticos extremos, como inundaciones, sequías y tormentas, están aumentando en frecuencia e

intensidad, creando riesgos que afectan directamente las operaciones y la resiliencia de las empresas.

- **Nuevas Regulaciones y Cumplimiento Legal**: La velocidad de los cambios regulatorios, especialmente en áreas como la protección de datos y ESG (Environmental, Social, and Governance), también representa riesgos emergentes que las empresas necesitan monitorear.



1.4. La importancia de anticipar y gestionar riesgos emergentes

Gestionar los riesgos emergentes es esencial para asegurar la continuidad de las operaciones y proteger los activos de las organizaciones, especialmente en el contexto actual, caracterizado por las dinámicas descritas en los mundos VUCA y BANI. El mundo VUCA (Volátil, Incierto, Complejo y Ambiguo) describe un escenario en el cual los cambios son rápidos e impredecibles, la incertidumbre es una constante, y la complejidad y la ambigüedad desafían los procesos tradicionales de toma de decisiones. Este entorno hace que los riesgos emergentes, que no tienen patrones históricos previsibles, sean mucho más difíciles de anticipar y controlar.

Por otro lado, el concepto de mundo BANI (Frágil, Ansioso, No lineal e Incomprensible) considera características aún más desafiantes del entorno actual, como la fragilidad de las estructuras frente a crisis inesperadas, la ansiedad generada por la imprevisibilidad, la no linealidad de los impactos y la dificultad de comprender la interrelación entre los eventos. Estos aspectos hacen que los riesgos emergentes no solo sean más frecuentes, sino también más amenazantes, ya que pequeños cambios pueden desencadenar efectos desproporcionados y, a menudo, incomprensibles para las organizaciones.

En este contexto, la anticipación de los riesgos emergentes se convierte en una ventaja estratégica fundamental. Las empresas que logran identificar señales débiles y anticipar cambios son capaces de adaptarse rápidamente a nuevos escenarios, garantizando una mayor resiliencia frente a cambios abruptos y eventos disruptivos. La ISO 31050 ofrece un enfoque estructurado para la gestión de estos riesgos, integrando conocimiento colectivo, tecnologías avanzadas y estrategias adaptativas. Este estándar enfatiza la importancia de una gestión proactiva, capaz de explorar escenarios, involucrar a los stakeholders y utilizar técnicas cualitativas para reconocer y mitigar riesgos antes de que se materialicen.

Así, la capacidad de gestionar riesgos emergentes en un mundo BANI y VUCA requiere que las empresas no solo se adapten, sino que también sean ágiles, flexibles y creativas en la manera en que responden a los desafíos. Esto incluye el desarrollo de una cultura organizacional que fomente la innovación, la colaboración y el aprendizaje continuo. La gestión eficaz de estos riesgos permite que las organizaciones transformen la incertidumbre en una oportunidad de crecimiento, reforzando su posición en el mercado y garantizando la sostenibilidad de sus operaciones en un entorno de constantes cambios.

ISO 31050: Perspectivas y Contribuciones

02

Capítulo 2 – ISO 31050: Perspectivas y Contribuciones

2.1. Visión general de la norma ISO 31050:2023 y su contexto de aplicación

La ISO 31050:2023 es una extensión importante de los conceptos y prácticas establecidos por la ISO 31000, específicamente orientada a la identificación y gestión de riesgos emergentes en un entorno global cada vez más dinámico y complejo. Esta norma fue desarrollada para atender las necesidades de organizaciones que enfrentan desafíos sin precedentes, como crisis ambientales, avances tecnológicos disruptivos, cambios sociales y desafíos regulatorios. La ISO 31050 proporciona directrices detalladas para el reconocimiento y tratamiento de riesgos que no presentan patrones tradicionales o históricos previsibles, ayudando a las organizaciones a identificar señales emergentes y tomar decisiones anticipadas.

El contexto de aplicación de la ISO 31050 incluye empresas de diferentes tamaños y sectores, ya que el riesgo emergente es transversal e impacta todas las áreas organizacionales. Desde el sector financiero, que enfrenta crecientes amenazas cibernéticas, hasta el sector manufacturero, que debe lidiar con cuestiones climáticas que afectan sus cadenas de suministro, la norma es una herramienta adaptable para mitigar riesgos que surgen en entornos inciertos. Además, la ISO 31050 es aplicable tanto a las operaciones internas como a las interacciones con stakeholders externos, promoviendo una visión holística e integrada de la gestión de riesgos.

2.2. Diferencias y similitudes entre ISO 31050 e ISO 31000:2018

La ISO 31050 y la ISO 31000 tienen objetivos complementarios, pero difieren en su alcance y enfoque. La ISO 31000:2018 es la norma de referencia para la gestión de riesgos de manera amplia, aplicable a cualquier tipo de riesgo en cualquier sector. Establece un marco general para identificar, analizar, evaluar y tratar riesgos de manera sistemática y repetible, siendo ampliamente utilizada para la creación de procesos y políticas de gestión de riesgos.

Por otro lado, la ISO 31050 se concentra específicamente en los riesgos emergentes. Mientras que la ISO 31000 aborda los riesgos de manera general, la ISO 31050 se destaca por su énfasis en anticipar y gestionar riesgos que son nuevos, inciertos y altamente impredecibles. La ISO 31050 proporciona directrices específicas para lidiar con riesgos emergentes en un entorno que es volátil, incierto, complejo y ambiguo (VUCA), y que a menudo tiene características asociadas al mundo BANI (Frágil, Ansioso, No lineal, Incomprensible). Una de las diferencias fundamentales es que la ISO 31050 promueve un enfoque más exploratorio y adaptativo, mientras que la ISO 31000 se enfoca en un marco estructurado y cíclico.

A pesar de las diferencias, ambas normas comparten la misma filosofía de que la gestión de riesgos es esencial para la creación y protección de valor en una organización. Ambas destacan la importancia del liderazgo y el compromiso de la alta dirección, así como la integración de la gestión de riesgos en la gobernanza y la cultura organizacional. Además, ambas normas refuerzan la necesidad de un proceso de mejora continua, lo que garantiza la adaptación constante de los sistemas de gestión de riesgos a los cambios en el entorno.

2.3. Cómo la ISO 31050 complementa la ISO 31000 en la gestión de riesgos emergentes

La ISO 31050 complementa la ISO 31000 al proporcionar un enfoque específico en los riesgos que surgen como resultado de eventos inesperados y dinámicas de cambio acelerado. Mientras que la ISO 31000 establece la estructura básica de gobernanza para el proceso de gestión de riesgos, la ISO 31050 avanza, permitiendo que las organizaciones sean más proactivas y resilientes respecto a los riesgos emergentes. La ISO 31050 sugiere enfoques que incluyen el uso de técnicas prospectivas, como análisis de escenarios, identificación de señales débiles y mapeo de tendencias, que permiten a las organizaciones detectar señales de riesgos antes de que se materialicen.

Además, la ISO 31050 refuerza la importancia de una cultura organizacional adaptativa, donde la capacidad de aprendizaje continuo y la colaboración son esenciales. Fomenta la integración de información obtenida de diversas fuentes, incluidos los stakeholders externos, expertos y el uso de herramientas de inteligencia artificial para el análisis de datos. De esta manera, la ISO 31050 fortalece los procesos establecidos por la ISO 31000, proporcionando a las organizaciones las herramientas necesarias para prepararse para lo inesperado y ser resilientes ante crisis y cambios.

2.4. Aplicación de los principios de la ISO 31050 en el aumento de la resiliencia organizacional

La resiliencia organizacional es uno de los principales objetivos de la aplicación de la ISO 31050. La norma proporciona una serie de principios y metodologías que ayudan a las organizaciones a adaptarse y prepararse para cambios súbitos y riesgos emergentes, fortaleciendo la capacidad de resistir, adaptarse y prosperar. Entre los principios más importantes se destaca la necesidad de un enfoque sistémico y holístico, que abarque no solo las operaciones internas, sino también toda la cadena de valor y los stakeholders externos.

La ISO 31050 también destaca la importancia de la flexibilidad y la adaptabilidad como componentes clave de la resiliencia. Esto incluye la adopción de planes de contingencia que sean ágiles y adaptables a los cambios en el contexto operacional, así como el desarrollo de competencias internas para la detección rápida de riesgos emergentes. La norma fomenta la adopción de prácticas como el desarrollo de escenarios y la exploración de incertidumbres para prever posibles impactos y preparar respuestas adecuadas, además de promover una cultura organizacional que priorice la comunicación abierta y la respuesta rápida a crisis.

Adoptar los principios de la ISO 31050 permite a las organizaciones desarrollar una postura más proactiva frente al riesgo, aumentando su resiliencia y la capacidad de transformar desafíos en oportunidades. Al promover el uso de tecnologías avanzadas para el monitoreo y análisis de riesgos, e integrar el conocimiento de los stakeholders en el proceso de gestión de riesgos, la ISO 31050 ayuda a fortalecer la capacidad de adaptación y la resiliencia de las organizaciones frente a un entorno cada vez más incierto y desafiante.

Proceso de gestión de riesgos emergentes con ISO 31050

03

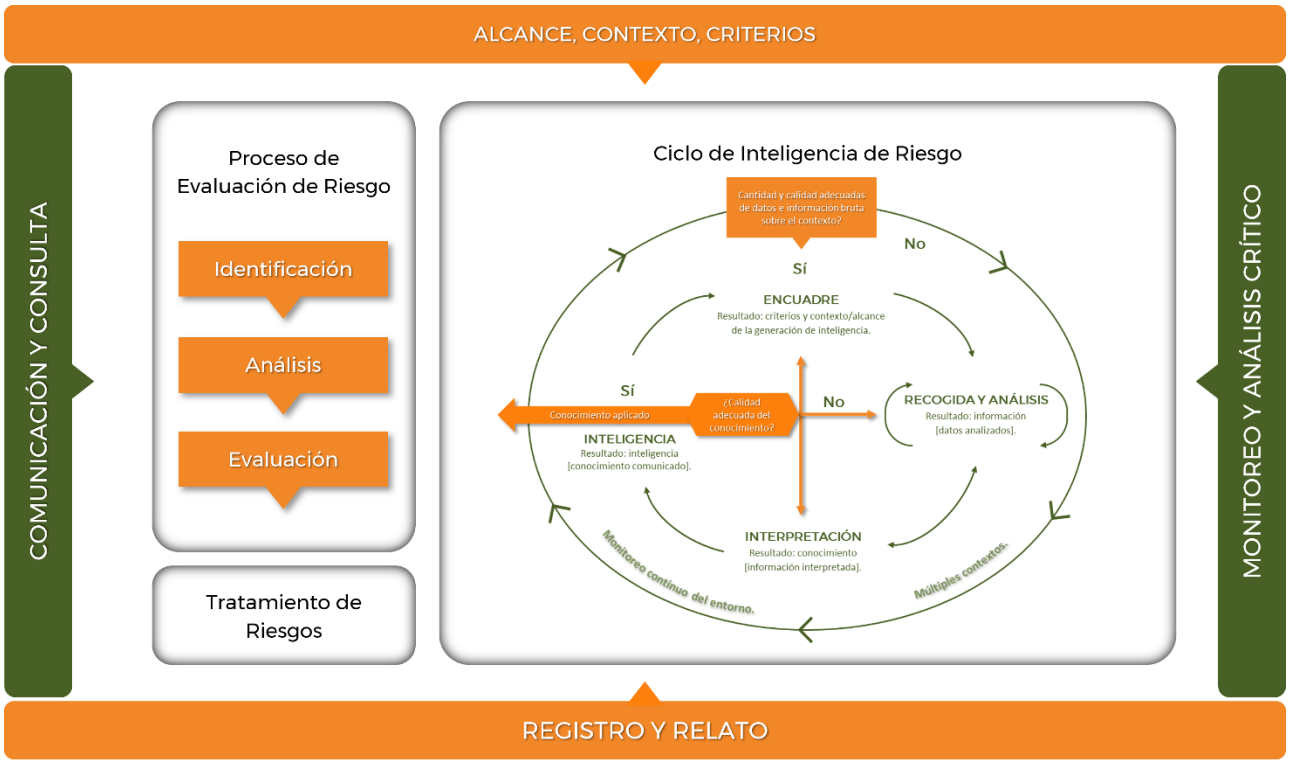
Capítulo 3 – Proceso de gestión de riesgos emergentes con ISO 31050

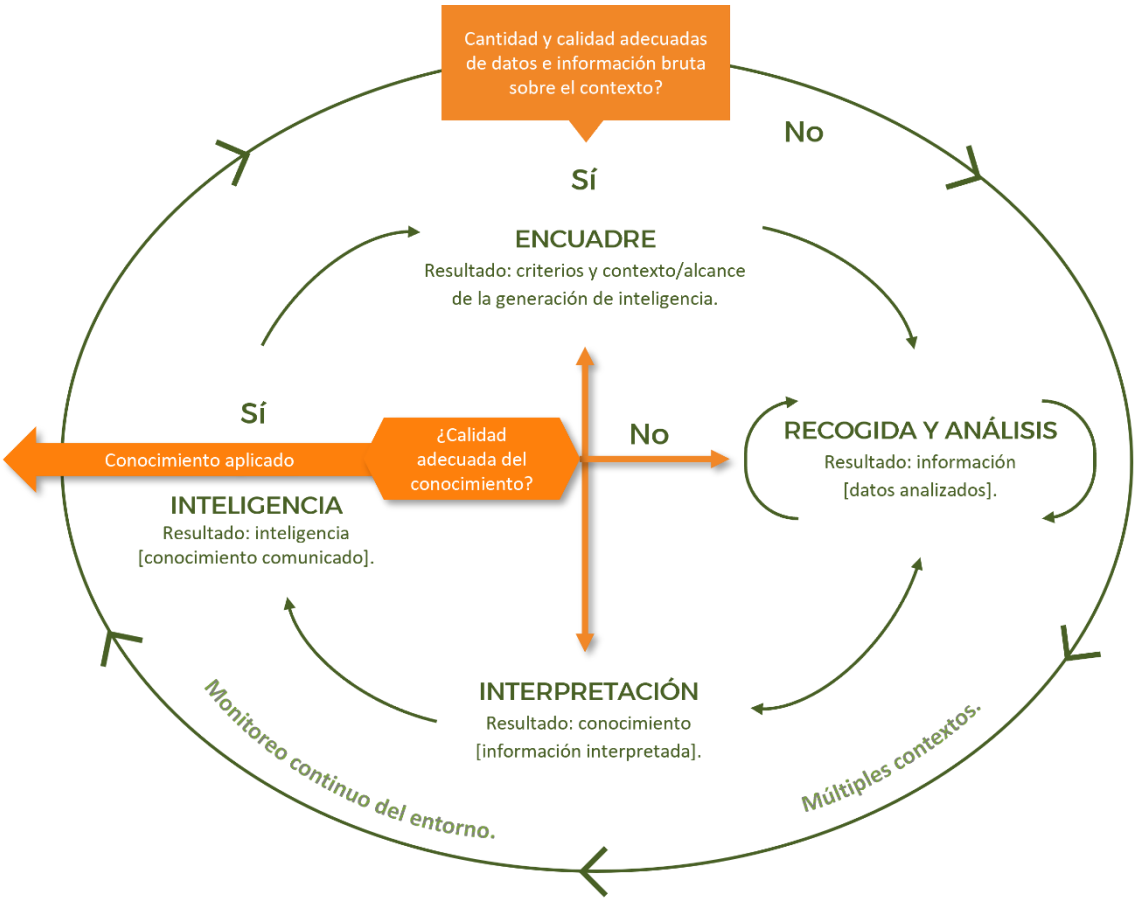
3.1. Ciclo de inteligencia de riesgo: conceptos y aplicación

El ciclo de inteligencia de riesgo es un concepto fundamental introducido por la ISO 31050 para lidiar con la incertidumbre asociada a los riesgos emergentes. Este ciclo se compone de varias etapas que buscan monitorear, identificar, evaluar y tratar riesgos de forma continua y adaptativa. El concepto de "inteligencia de riesgo" implica la recopilación sistemática de información relevante, el análisis de dicha información y la difusión del conocimiento obtenido para respaldar las decisiones estratégicas.

El proceso comienza con la identificación de señales débiles, que son indicadores iniciales de cambios en el entorno que, de manera aislada, pueden parecer insignificantes, pero que, al ser analizados en conjunto, pueden señalar la aparición de un riesgo significativo. El análisis de tendencias y señales débiles es una herramienta esencial para detectar riesgos emergentes antes de que se manifiesten de manera perjudicial. Posteriormente, la información recopilada se evalúa con el objetivo de determinar su relevancia y el posible impacto en la organización, integrando diferentes perspectivas para garantizar un análisis integral.

El ciclo de inteligencia de riesgo también incluye la etapa de análisis predictivo, en la que se utilizan escenarios futuros para explorar los posibles impactos de los riesgos emergentes. Con base en el análisis predictivo y la evaluación de los datos recopilados, las organizaciones pueden desarrollar estrategias proactivas para tratar los riesgos de manera eficiente. La aplicación del ciclo de inteligencia de riesgo permite que la gestión de riesgos emergentes sea una actividad continua, que utiliza el aprendizaje obtenido a lo largo del proceso para mejorar continuamente la respuesta de la organización.





Fuente: ISO 31050.

3.2. Adopción de un enfoque integrado y holístico para la gestión de riesgos

La ISO 31050 enfatiza la importancia de un enfoque integrado y holístico en la gestión de riesgos emergentes, reconociendo que los riesgos emergentes rara vez afectan solo una parte de la organización de manera aislada. Estos riesgos son multifactoriales y pueden impactar diversas áreas simultáneamente, requiriendo una visión amplia e integrada del contexto organizacional para gestionarlos adecuadamente. El enfoque integrado considera las interdependencias entre diferentes tipos de riesgos, ya sean estratégicos, operacionales, financieros, ambientales o sociales.

La integración de los procesos de gestión de riesgos con las áreas clave de la organización, incluyendo la gobernanza corporativa, operaciones, planificación estratégica y comunicación, es fundamental para garantizar que todos los aspectos del riesgo sean considerados y abordados de manera coordinada. Este enfoque también incluye la colaboración entre diferentes stakeholders, tanto dentro como fuera de la organización, como socios, proveedores, reguladores y la comunidad. Un aspecto importante del enfoque holístico es la coordinación transversal, que permite que diferentes departamentos compartan información y cooperen en la identificación y mitigación de riesgos.

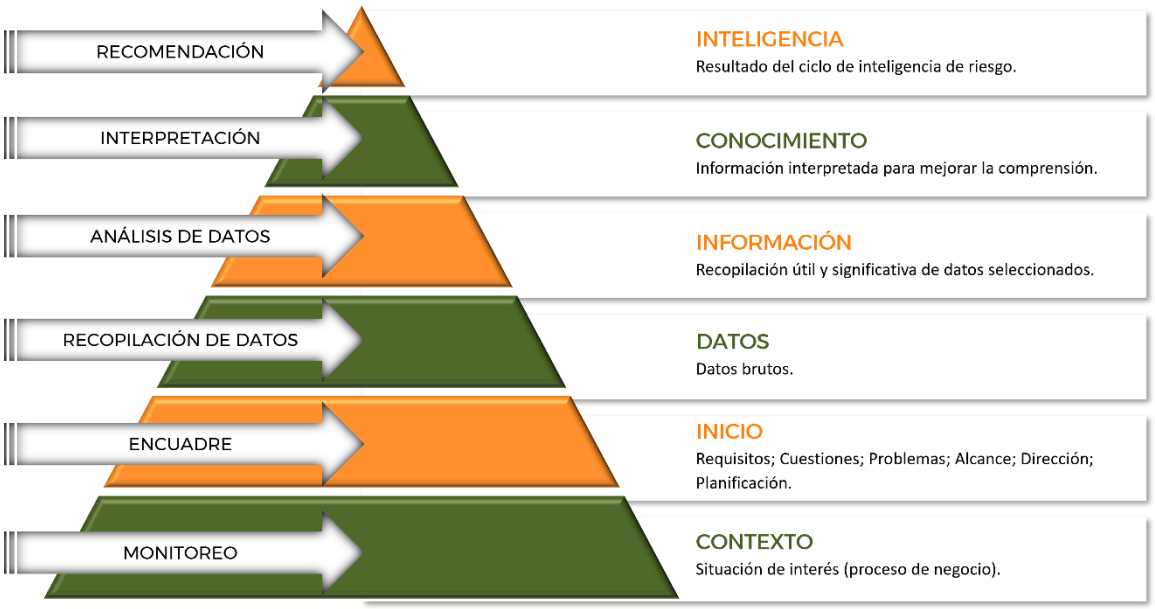
Además, el enfoque holístico fomenta la integración de la gestión de riesgos en el día a día de la organización, haciendo que todos los niveles jerárquicos, desde la alta dirección hasta los colaboradores de primera línea, participen en el proceso de identificación y respuesta a riesgos emergentes. Este enfoque no solo aumenta la eficacia de la gestión de riesgos, sino que también fortalece la cultura organizacional de resiliencia y adaptabilidad.

3.3. La necesidad de acumulación de conocimiento verificable y la toma de decisiones bajo incertidumbre

Una de las principales contribuciones de la ISO 31050 a la gestión de riesgos emergentes es el reconocimiento de la importancia de la acumulación de conocimiento verificable como base para la toma de decisiones bajo incertidumbre. A diferencia de los riesgos tradicionales, los riesgos emergentes no tienen un historial consistente que pueda utilizarse para prever comportamientos futuros, lo que hace que los datos tradicionales sean insuficientes para una evaluación precisa. Por lo tanto, la recopilación y verificación de información, a través de fuentes confiables y diversificadas, son fundamentales para construir una base de conocimiento que apoye decisiones informadas.

La acumulación de conocimiento debe ser continua, utilizando fuentes internas y externas, como análisis de tendencias, investigaciones académicas, informes de mercado y consultas con expertos. Se recomienda con frecuencia el uso de herramientas de análisis de datos e inteligencia artificial para identificar patrones emergentes y proporcionar información sobre posibles riesgos. La utilización de metodologías que permitan la verificación del conocimiento, como la validación cruzada con expertos y el análisis de evidencias históricas, es esencial para reducir la incertidumbre y aumentar la confianza en las decisiones tomadas.

La toma de decisiones bajo incertidumbre requiere que las organizaciones sean flexibles y capaces de ajustar sus estrategias conforme se obtengan nuevas informaciones e ideas. La ISO 31050 fomenta el uso de escenarios prospectivos y el análisis de múltiples alternativas para permitir que las organizaciones estén preparadas para una variedad de futuros posibles. La experimentación controlada, como la realización de simulaciones y ejercicios de respuesta a crisis, también es una práctica recomendada para probar diferentes enfoques y validar las mejores estrategias antes de que los riesgos se materialicen. De esta forma, las decisiones pueden adaptarse y refinarse con base en el aprendizaje continuo y la evolución de las circunstancias.



Fuente: ISO 31050.

Comparación entre ESRM (Enterprise Security Risk Management) de ASIS e ISO 31050

04

Capítulo 4 – Comparación entre ESRM (Enterprise Security Risk Management) de ASIS e ISO 31050

4.1. Introducción al concepto de ESRM y su relevancia para la seguridad corporativa

El concepto de Enterprise Security Risk Management (ESRM) fue desarrollado por ASIS para proporcionar un marco de gestión de riesgos de seguridad corporativa que abarque todos los niveles de una organización, con un enfoque prioritario en la seguridad. ESRM se centra en identificar, analizar, evaluar, controlar y gestionar los riesgos relacionados con la seguridad de los activos, ya sean físicos, digitales o humanos, siempre alineando las prácticas de seguridad con los objetivos estratégicos de la organización. Este concepto adopta un enfoque centrado en el negocio, buscando integrar la seguridad en la planificación estratégica y asegurando que todos los stakeholders comprendan el papel de la seguridad en la protección del valor organizacional.

La relevancia del ESRM en el contexto de la seguridad corporativa radica en su capacidad para integrar las funciones de seguridad en todos los niveles de la organización, promoviendo una visión clara y compartida de los riesgos de seguridad. El ESRM enfatiza el papel de la seguridad como facilitador del éxito empresarial, en lugar de ser visto solo como un costo o una actividad aislada. Proporciona un marco que abarca desde el análisis de amenazas y vulnerabilidades hasta la implementación de medidas de mitigación, garantizando que la seguridad sea una responsabilidad compartida y que los riesgos se gestionen de manera eficaz y continua.

ESRM - Enterprise Security Risk Management

4.2. Principios de la evaluación de riesgos de seguridad en el contexto del ESRM y la ISO 31050

El proceso de evaluación de riesgos descrito en el ESRM es idéntico al proceso descrito en la ISO 31000, que, a su vez, es la base para el desarrollo de la ISO 31050. Tanto el ESRM como la ISO 31000 comparten la estructura fundamental de la gestión de riesgos, que incluye etapas de identificación, análisis, evaluación y tratamiento de riesgos, siempre alineadas con los objetivos estratégicos de la organización. Esta estructura permite que la evaluación de riesgos se realice de manera sistemática y repetible, integrándose a las operaciones organizacionales y garantizando que todos los riesgos se consideren adecuadamente.

En el contexto del ESRM, la evaluación de riesgos de seguridad se lleva a cabo con el objetivo principal de proteger los activos más importantes de la organización, que pueden incluir personas, propiedades físicas, información y reputación. El ESRM busca evaluar no solo las amenazas identificables, sino también la vulnerabilidad de los activos y el impacto potencial en caso de incidentes. Con ello, es posible priorizar acciones de seguridad que generen mayor valor para el negocio, asegurando que la gestión de riesgos esté directamente conectada con los objetivos organizacionales y la protección del valor de la empresa.

Por otro lado, la ISO 31050 expande la perspectiva de la evaluación de riesgos para abarcar los riesgos emergentes, aquellos que surgen de cambios inesperados y, a menudo, disruptivos en el entorno organizacional o externo. La ISO 31050 se enfoca en identificar riesgos que son complejos, volátiles e inciertos, promoviendo un enfoque más amplio que trasciende la seguridad física o digital. Así, mientras que el ESRM tiene un enfoque específico en la protección de los activos actuales contra amenazas concretas, la ISO 31050 enfatiza la importancia de anticipar nuevos riesgos, analizar tendencias y preparar a la organización para desafíos futuros. Esta norma abarca un espectro más amplio de riesgos, incluidos aspectos operacionales, financieros y estratégicos, además de los riesgos de seguridad.

En resumen, tanto el ESRM como la ISO 31050 comparten la estructura de evaluación de riesgos de la ISO 31000, pero divergen en sus enfoques específicos. Mientras que el ESRM prioriza la mitigación de amenazas a la seguridad de los activos y la continuidad de las operaciones, la ISO 31050 se enfoca en la anticipación y preparación para riesgos emergentes, ayudando a la organización a adaptarse y responder a un entorno en constante transformación.

4.3. Comparación entre los principios del ESRM y el enfoque de la ISO 31050

La comparación entre los principios del ESRM y el enfoque de la ISO 31050 revela tanto convergencias como diferencias importantes que enriquecen la gestión de riesgos corporativos. El ESRM y la ISO 31050 comparten el principio de que la gestión de riesgos debe estar integrada en los objetivos estratégicos de la organización, promoviendo un enfoque proactivo y participativo. Ambos marcos reconocen que la gestión de riesgos debe ser parte integrante de la cultura organizacional y deben involucrar a todas las áreas y niveles jerárquicos de la empresa.

Una diferencia fundamental radica en el alcance y la forma de aplicación. El ESRM tiene un enfoque más específico en la seguridad corporativa, abordando riesgos que afectan directamente la integridad de los activos y la protección contra amenazas identificables. Está orientado a garantizar que las funciones de seguridad se alineen con las prioridades del negocio, mitigando las vulnerabilidades que puedan impactar directamente la continuidad de las operaciones y la protección de los activos. La ISO 31050, por otro lado, es más amplia y se preocupa por abordar riesgos emergentes y poco conocidos, promoviendo un enfoque exploratorio que implica el análisis de tendencias, la identificación de señales débiles y el desarrollo de estrategias adaptativas.

Mientras que el ESRM adopta un enfoque de "protección de activos", la ISO 31050 adopta un enfoque más orientado a la resiliencia organizacional. Esto significa que el ESRM prioriza la reducción de vulnerabilidades y la seguridad inmediata de los activos, mientras que la ISO 31050 se enfoca en preparar a la organización para enfrentar un entorno incierto y en constante cambio, capacitándola no solo para mitigar riesgos, sino también para encontrar oportunidades de crecimiento en medio de la incertidumbre.

4.4. Punto de convergencia: cómo alinear ESRM con ISO 31050 para una gestión estratégica

Los puntos de convergencia entre el ESRM y la ISO 31050 ofrecen una oportunidad única para alinear ambos enfoques y crear un marco robusto de gestión de riesgos y seguridad. Integrar el ESRM y la ISO 31050 permite que la organización no solo proteja sus activos de manera eficiente, sino que también esté preparada para adaptarse a cambios y responder a riesgos emergentes. Esta alineación crea un sistema de gestión que es tanto reactivo, en la protección contra amenazas y vulnerabilidades ya conocidas, como proactivo, en la anticipación y preparación para nuevos desafíos.

Un punto clave de alineación es el enfoque compartido en integrar la gestión de riesgos con los objetivos estratégicos de la organización. Ambos marcos enfatizan que las

actividades de seguridad y de gestión de riesgos no deben realizarse de manera aislada, sino que deben estar conectadas con los objetivos de crecimiento, innovación y sostenibilidad del negocio. Así, al implementar una estrategia combinada, la organización es capaz de proteger sus activos más importantes mientras construye resiliencia para enfrentar los riesgos del futuro.

Otro punto de convergencia es el énfasis en la colaboración entre stakeholders y en la difusión de la responsabilidad de la gestión de riesgos por todos los niveles de la organización. Utilizando los principios del ESRM, es posible garantizar que las funciones de seguridad sean reconocidas como parte integrante del proceso de creación de valor. Al aplicar la ISO 31050 en conjunto, las organizaciones pueden asegurarse de monitorear continuamente el entorno externo, identificando señales de cambio y ajustando sus estrategias para lidiar tanto con amenazas inminentes como con riesgos emergentes. De esta forma, la integración del ESRM con la ISO 31050 proporciona una visión holística de la seguridad y la gestión de riesgos, que fortalece la capacidad organizacional de responder a desafíos complejos e inciertos de manera estratégica y resiliente.

Transformación de Incertidumbres en Oportunidades

05

Capítulo 5 – Transformación de Incertidumbres en Oportunidades

5.1. Cómo la ISO 31050 facilita la transformación de riesgos en ventajas competitivas

La ISO 31050 proporciona una guía práctica para transformar los riesgos emergentes, que a menudo se presentan como incertidumbres complejas e impredecibles, en oportunidades estratégicas para la organización. La norma facilita esta transformación al fomentar un enfoque proactivo y adaptativo para la gestión de riesgos, integrando herramientas como el análisis predictivo y la exploración de escenarios futuros. La identificación temprana de riesgos emergentes permite a las organizaciones prepararse para responder rápidamente y posicionarse de forma ventajosa frente a sus competidores.

Por ejemplo, la ISO 31050 incentiva el desarrollo de estrategias que no solo minimicen los impactos de los riesgos, sino también maximicen las oportunidades que puedan surgir. Cuando se detecta un riesgo emergente, la organización tiene la oportunidad de innovar y adaptarse antes que otras, creando nuevas líneas de productos o servicios, ajustando procesos internos para una mayor eficiencia o incluso estableciendo alianzas estratégicas que aprovechen las condiciones del mercado. De esta manera, al abordar los riesgos emergentes como fuentes potenciales de innovación, las empresas pueden reforzar su posición competitiva y explorar nuevos mercados, promoviendo el crecimiento sostenible y la creación de valor a largo plazo.

5.2. Estudios de caso y ejemplos de aplicación en el sector de seguridad

Para ilustrar cómo la ISO 31050 puede transformar riesgos en oportunidades, podemos considerar algunos estudios de caso. Un ejemplo es el de una empresa de seguridad que, al adoptar la ISO 31050, logró identificar y prepararse para el aumento de las amenazas cibernéticas, impulsadas por la creciente digitalización de los servicios de seguridad. Esta empresa no solo implementó medidas de protección mejoradas, sino que también desarrolló nuevos servicios enfocados en la ciberseguridad, como consultoría en protección de datos y auditorías de seguridad digital. Como resultado, creó una nueva línea de negocios altamente demandada por sus clientes. Un ejemplo práctico es Prosegur/SegurPro – https://www.prosegur.com/sobre-nosotros/i-s. En Brasil, el promedio del ROI (retorno sobre la inversión) es de aproximadamente un 5% en vigilancia tradicional, un 25% en seguridad electrónica y más del 50% en ciberseguridad.

Un ejemplo que demuestra la criticidad de los riesgos emergentes es el de una gran empresa de logística que opera en un puerto internacional y enfrentó una combinación de riesgos relacionados con la ciberseguridad, el cambio climático y nuevas regulaciones. Imagine que un evento climático extremo, como una inundación significativa, afectó la infraestructura del puerto, causando la interrupción del suministro de energía y de los sistemas de comunicación. Durante la crisis, los hackers aprovecharon las vulnerabilidades creadas para lanzar un ataque cibernético dirigido, secuestrando datos críticos y exigiendo un rescate. Simultáneamente, la empresa enfrentaba presiones regulatorias para garantizar el cumplimiento de nuevas normas de ESG y protección de datos, que exigían transparencia sobre las acciones tomadas en respuesta a la crisis climática y sus impactos en los datos de los clientes.

Este escenario muestra cómo la combinación de diferentes tipos de riesgos emergentes puede resultar en una situación compleja y sistémica, en la cual los impactos se multiplican debido a la interacción entre eventos climáticos extremos, amenazas cibernéticas y exigencias regulatorias. La incapacidad de la empresa para responder adecuadamente a cada una de estas dimensiones resultó en una serie de desafíos operativos, financieros y de reputación que podrían tener efectos duraderos.

La aplicación de los principios de la ISO 31050 sería fundamental para mitigar los efectos de este tipo de riesgo emergente. La ISO 31050 recomienda un enfoque integrado y adaptativo para la gestión de riesgos, que incluye la identificación de señales débiles, la anticipación de posibles amenazas y el desarrollo de planes de contingencia sólidos. En el caso de esta empresa de logística, adoptar las prácticas de la ISO 31050 podría haber llevado a una preparación anticipada para escenarios de crisis climática, al fortalecimiento de las defensas cibernéticas y al establecimiento de mecanismos para garantizar el cumplimiento normativo incluso en situaciones adversas. De esta manera, el enfoque integrado de la ISO 31050 permitiría no solo la mitigación de los riesgos individuales, sino también la coordinación efectiva entre diferentes áreas, garantizando una respuesta cohesiva y minimizando los impactos negativos.

Estos ejemplos ilustran cómo la anticipación y la preparación proactivas para riesgos emergentes permiten que las organizaciones no solo resistan a los desafíos, sino que también se adapten y crezcan en medio de los cambios, transformando posibles amenazas en oportunidades de innovación y diferenciación.

5.3. Beneficios de la gestión de riesgos emergentes para la resiliencia y la sostenibilidad organizacional

La gestión de riesgos emergentes trae una serie de beneficios que son fundamentales para fortalecer la resiliencia y la sostenibilidad organizacional. En primer lugar, al implementar las directrices de la ISO 31050, las empresas logran anticipar riesgos y responder de manera ágil y coordinada, minimizando los impactos negativos y garantizando la continuidad de sus operaciones. Esta capacidad de respuesta rápida, especialmente en un contexto de cambios abruptos e impredecibles, es uno de los principales pilares de la resiliencia organizacional.

Además, la ISO 31050 promueve una visión estratégica a largo plazo que considera las incertidumbres del entorno y fomenta la innovación como respuesta adaptativa a los riesgos. De esta manera, las empresas están capacitadas no solo para reaccionar ante las amenazas, sino también para moldear su futuro, identificando y aprovechando oportunidades para crecer de forma sostenible. El enfoque orientado al futuro de la ISO 31050 refuerza la sostenibilidad organizacional, ya que considera no solo la supervivencia inmediata, sino también la capacidad de adaptarse continuamente y prosperar en un entorno en constante transformación.

La gestión eficaz de los riesgos emergentes también contribuye a la creación de una cultura organizacional resiliente, en la que la identificación de riesgos y la toma de decisiones bajo incertidumbre se perciben como oportunidades de aprendizaje y crecimiento. Esta cultura promueve la comunicación abierta, la participación de todos los niveles de la organización en la gestión de riesgos y la creación de estrategias que valoren tanto la mitigación de riesgos como la exploración de nuevas oportunidades. De esta manera, la ISO 31050 ayuda a transformar la gestión de riesgos emergentes en una herramienta esencial para el fortalecimiento de la resiliencia y la sostenibilidad a largo plazo.

Integración de la Gestión de Riesgos Emergentes con los Objetivos Corporativos

06

Capítulo 6 – Integración de la Gestión de Riesgos Emergentes con los Objetivos Corporativos

6.1. La importancia de la integración con los objetivos estratégicos de la organización

La integración de la gestión de riesgos emergentes con los objetivos estratégicos de la organización es fundamental para garantizar que la gestión de riesgos no sea una actividad aislada, sino una parte esencial de la planificación corporativa. En un entorno empresarial cada vez más volátil e incierto, gestionar riesgos emergentes de manera alineada con los objetivos estratégicos permite que la empresa esté preparada para adaptarse y responder rápidamente a los cambios, protegiendo su sostenibilidad y fortaleciendo su posición competitiva.

Cuando la gestión de riesgos está alineada con los objetivos estratégicos, las decisiones relacionadas con los riesgos se toman con una visión clara del impacto en las metas organizacionales. Esto permite que las acciones de mitigación se dirijan a proteger las áreas más críticas para el éxito de la organización. Además, la integración permite que la gestión de riesgos actúe como facilitadora de la innovación y del crecimiento sostenible, ya que identificar y gestionar riesgos emergentes también puede revelar nuevas oportunidades alineadas con las ambiciones de la empresa.

6.2. Contribuciones de la ISO 31050 para el alineamiento de las estrategias de seguridad con las metas corporativas

La ISO 31050 proporciona directrices para alinear la gestión de riesgos emergentes con los objetivos corporativos, promoviendo un enfoque holístico y adaptativo que contribuye a la sostenibilidad a largo plazo. La norma enfatiza la importancia de incorporar la evaluación de riesgos emergentes en el proceso de definición estratégica, considerando los escenarios futuros y las incertidumbres que pueden impactar el entorno empresarial. Al integrar los principios de la ISO 31050, las organizaciones logran adaptar sus estrategias de seguridad para no solo proteger sus activos y operaciones, sino también apoyar la ejecución de sus metas y objetivos.

Una de las principales contribuciones de la ISO 31050 es el enfoque prospectivo en la gestión de riesgos, que incentiva a las organizaciones a analizar tendencias y señales débiles para identificar riesgos que puedan afectar el futuro. Esto permite que la empresa adopte una postura proactiva, desarrollando estrategias de seguridad que están directamente vinculadas con el éxito corporativo. Además, la norma promueve una cultura de resiliencia organizacional, que es fundamental para alinear la gestión de riesgos con las metas estratégicas, garantizando que la empresa sea capaz de adaptarse a cambios abruptos e inesperados.

Otro punto importante es el cicloi”e in’eligencia, muy bien documentado y estructurado en la ISO 31050, que orienta a las organizaciones a recopilar, analizar y difundir información de manera continua. Este ciclo permite la anticipación de riesgos emergentes y una toma de decisiones fundamentada, reforzando la postura proactiva y adaptativa frente a los desafíos futuros.

6.3. Ejemplos prácticos de alineamiento y resultados obtenidos

Un ejemplo práctico de integración entre la gestión de riesgos emergentes y los objetivos corporativos puede observarse en una empresa del sector energético que, al adoptar la ISO 31050, logró alinear sus estrategias de seguridad con sus metas de crecimiento sostenible. La empresa identificó que los riesgos emergentes relacionados con el cambio climático y la transición energética podrían impactar sus operaciones y sus planes de expansión. Con base en los principios de la ISO 31050, la organización realizó un análisis prospectivo de los riesgos climáticos, desarrollando planes de adaptación que incluían la modernización de su infraestructura y la adopción de tecnologías verdes.

Este enfoque no solo mitigó los riesgos asociados a eventos climáticos extremos, sino que también creó nuevas oportunidades de crecimiento para la empresa, que se

posicionó como líder en la transición hacia fuentes de energía más limpias y sostenibles. Otro ejemplo puede verse en una empresa del sector financiero que, al integrar la gestión de riesgos emergentes con sus metas de innovación tecnológica, adoptó medidas proactivas de ciberseguridad que permitieron el desarrollo seguro de nuevos servicios digitales. Esta integración no solo minimizó los riesgos cibernéticos, sino que también contribuyó a la expansión de su base de clientes y al fortalecimiento de la confianza en el mercado.

Estos ejemplos demuestran cómo la aplicación de la ISO 31050 en la gestión de riesgos emergentes puede fortalecer la conexión entre seguridad, innovación y crecimiento estratégico, garantizando que las iniciativas de mitigación de riesgos estén siempre en sintonía con los objetivos corporativos.

Desafíos en la Implementación de la ISO 31050 en el Sector de Seguridad

07

Capítulo 7 – Desafíos en la Implementación de la ISO 31050 en el Sector de Seguridad

7.1. Principales barreras culturales y operativas

La implementación de la ISO 31050 en el sector de seguridad enfrenta una serie de barreras culturales y operativas que deben abordarse para que el proceso sea eficaz. En términos culturales, una de las mayores dificultades es promover un cambio de mentalidad dentro de la organización, que a menudo está acostumbrada a lidiar con los riesgos de manera reactiva, manejando las consecuencias solo cuando los riesgos se materializan. Esta cultura reactiva contrasta con el enfoque proactivo propuesto por la ISO 31050, que requiere la identificación temprana y la anticipación de riesgos emergentes antes de que causen daños significativos. Para muchos colaboradores y gestores, este cambio implica abandonar prácticas tradicionales, lo que puede generar resistencia, especialmente en industrias donde la gestión de riesgos se percibe como una responsabilidad exclusiva de los departamentos especializados, como seguridad patrimonial, seguridad laboral y ciberseguridad.

Otra barrera cultural es la dificultad de integrar la gestión de riesgos como una responsabilidad compartida por toda la organización. En muchos casos, la gestión de riesgos se percibe como una función periférica y no como un elemento central de la estrategia corporativa. Cambiar esta percepción y promover la concienciación sobre la importancia de los riesgos emergentes en todos los niveles de la empresa —desde la alta dirección hasta los colaboradores de primera línea— es esencial para la adopción efectiva de la norma. Esto requiere esfuerzos de comunicación interna, capacitaciones y, sobre todo, el compromiso de los líderes para fomentar la adopción de esta nueva cultura que valora la vigilancia constante y la respuesta anticipada a los signos de cambio.

Desde el punto de vista operativo, la integración de la ISO 31050 en los procesos organizacionales puede ser particularmente desafiante debido a la complejidad y la necesidad de coordinación entre diferentes áreas de la empresa. La norma propone un enfoque holístico e integrado que requiere la participación de equipos multidisciplinarios, lo que puede ser difícil de implementar en empresas con estructuras organizacionales compartimentadas, donde los departamentos funcionan de forma aislada y tienen poca comunicación entre sí. Para superar estos desafíos operativos, es necesario desarrollar procesos claros de colaboración y establecer canales eficientes de comunicación interna que fomenten el intercambio de información sobre posibles riesgos emergentes. Además, el enfoque de la ISO 31050 exige la capacitación de los equipos con nuevas competencias, desde el uso de herramientas tecnológicas de monitoreo hasta el análisis de datos cualitativos. La formación y el desarrollo de

habilidades son fundamentales, pero también pueden ser desafiantes para empresas que no tienen un historial de programas estructurados de capacitación en gestión de riesgos.

7.2. Superando limitaciones de datos y el sesgo de percepción

Uno de los principales desafíos en la implementación de la ISO 31050 es superar las limitaciones de datos y los sesgos de percepción que dificultan la gestión eficaz de los riesgos emergentes. A diferencia de los riesgos tradicionales, los riesgos emergentes generalmente no tienen suficientes datos históricos que permitan un análisis cuantitativo preciso. La falta de un historial consolidado hace que la evaluación de estos riesgos sea un desafío, ya que la mayoría de los métodos convencionales de gestión de riesgos dependen de una base de datos robusta para el análisis predictivo. Para superar esta limitación, la ISO 31050 recomienda el uso de técnicas cualitativas, como la exploración de escenarios, el análisis de tendencias y las consultas con expertos, que son herramientas valiosas para abordar la incertidumbre y la complejidad de los riesgos emergentes.

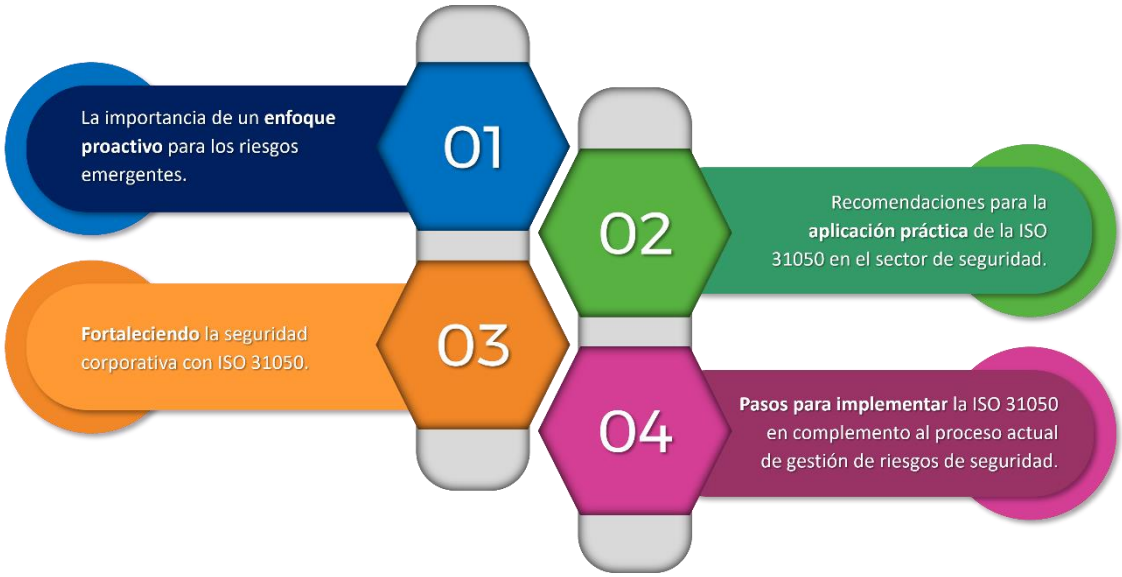
Otro aspecto importante para considerar es el sesgo de percepción, que puede influir negativamente en la forma en que se evalúan y priorizan los riesgos emergentes. Las personas tienden a subestimar riesgos menos conocidos que no se han materializado en el pasado, mientras que sobrestiman riesgos que ya han ocurrido o que parecen más tangibles e inminentes. Este sesgo puede llevar a que los riesgos emergentes se desatiendan hasta que ya sea demasiado tarde para una respuesta eficiente. Superar este desafío requiere no solo técnicas analíticas robustas, sino también un cambio cultural que valore el pensamiento crítico y la toma de decisiones basada en evidencias, y no solo en experiencias pasadas.

Para enfrentar las limitaciones de datos y el sesgo de percepción, es fundamental invertir en tecnologías de recopilación y análisis de información, como el análisis predictivo y la inteligencia artificial, que ayudan a identificar patrones y señales débiles que pueden ser indicios de riesgos emergentes. La creación de una base de conocimiento continua, donde la información de múltiples fuentes se actualice y analice constantemente, es fundamental para aumentar la capacidad de la organización para anticipar riesgos. Además, fomentar una cultura de aprendizaje continuo, donde todas las lecciones derivadas de la experiencia de la organización y de los análisis prospectivos se integren en los procesos de toma de decisiones, es esencial para eliminar prejuicios y aumentar la eficacia en la gestión de riesgos emergentes. Programas de capacitación destinados a sensibilizar a los colaboradores sobre la importancia de los riesgos emergentes,

Conclusión y Recomendaciones Estratégicas

08

Capítulo 8 – Conclusión y Recomendaciones Estratégicas



8.1. La importancia de un enfoque proactivo para los riesgos emergentes

En un escenario cada vez más volátil e impredecible, la importancia de un enfoque proactivo para la gestión de riesgos emergentes no puede subestimarse. A diferencia de los riesgos tradicionales, los riesgos emergentes se caracterizan por su complejidad, incertidumbre y rápida evolución. Estos riesgos pueden surgir repentinamente y tener impactos sistémicos en toda la organización, afectando las operaciones, las finanzas, la reputación e incluso la viabilidad del negocio. El enfoque reactivo, en el que las organizaciones responden solo después de la materialización de los riesgos, es ineficaz y peligroso en el contexto actual, donde los cambios son rápidos y los impactos pueden ser devastadores.

La ISO 31050 promueve la adopción de una postura proactiva, en la que la organización no solo reacciona ante los riesgos, sino que se anticipa a ellos. Esto implica la identificación temprana de señales de cambio, el análisis continuo del entorno externo y el desarrollo de estrategias adaptativas. El enfoque proactivo ayuda a transformar los riesgos emergentes en oportunidades de crecimiento e innovación, permitiendo que las organizaciones no solo mitiguen amenazas, sino que también exploren oportunidades y nuevas posibilidades de diferenciación en el mercado. Cuando los riesgos emergentes se gestionan de manera anticipada, la empresa está en una posición más favorable para minimizar los impactos negativos, proteger sus activos y, al mismo tiempo, fortalecer la confianza de sus stakeholders.

8.2. Recomendaciones para la aplicación práctica de la ISO 31050 en el sector de seguridad

Para aplicar la ISO 31050 de manera eficaz en el sector de seguridad, es esencial seguir algunas recomendaciones estratégicas que aseguren una implementación robusta e integrada. En primer lugar, es necesario que la alta dirección esté totalmente comprometida con la adopción de la norma. Sin el apoyo del liderazgo, es improbable que la cultura organizacional cambie para valorar la identificación y la anticipación de riesgos emergentes. Por lo tanto, el primer paso debe ser el compromiso de los líderes, demostrando que la gestión de riesgos emergentes es una prioridad estratégica.

Otro punto fundamental es la capacitación de los colaboradores y el desarrollo de competencias específicas para manejar riesgos emergentes. Esto incluye formación sobre los principios de la ISO 31050, además del uso de técnicas cualitativas, como el análisis de escenarios y la identificación de señales débiles, y el uso de tecnologías avanzadas, como la inteligencia artificial y el análisis predictivo. Crear una base de conocimiento dentro de la organización y capacitar a los colaboradores para monitorear y analizar riesgos emergentes son pasos esenciales para garantizar que todos los niveles jerárquicos estén alineados con el enfoque propuesto por la ISO 31050.

La integración de la gestión de riesgos emergentes en los procesos de negocio existentes es otra recomendación crítica. Esto requiere incorporar el análisis de riesgos emergentes en todas las fases de la planificación estratégica y la toma de decisiones, garantizando que la gestión de riesgos no sea un proceso aislado, sino una parte integral de las operaciones y la planificación corporativa. Para facilitar esta integración, es importante desarrollar una comunicación eficaz entre los departamentos y crear estructuras que promuevan la colaboración entre áreas, de modo que todos estén involucrados en la identificación y respuesta a riesgos emergentes.

Finalmente, se recomienda el uso de un ciclo continuo de inteligencia de riesgos, según lo descrito en la ISO 31050. Este ciclo implica la recopilación continua de información, el análisis de esa información para identificar riesgos potenciales y la difusión del conocimiento obtenido para los responsables de la toma de decisiones. Implementar un ciclo de inteligencia robusto ayudará a garantizar que la organización esté siempre preparada para responder a riesgos emergentes y ajustar sus estrategias según sea necesario, aumentando su resiliencia frente a cambios inesperados.

8.3. Fortaleciendo la seguridad corporativa con ISO 31050

La implementación de la ISO 31050 ofrece una oportunidad única para fortalecer la seguridad corporativa, convirtiendo la gestión de riesgos emergentes en un elemento central de la estrategia organizacional. La norma proporciona un marco integral e integrado que permite a las empresas anticiparse a los riesgos, ser proactivas en su mitigación y utilizar estos riesgos como oportunidades para el crecimiento y la innovación. Al integrar los principios de la ISO 31050, las organizaciones logran transformar un enfoque tradicionalmente reactivo en un proceso dinámico y proactivo, que contribuye a la construcción de una cultura de resiliencia y adaptabilidad.

En el sector de seguridad, la ISO 31050 se destaca por su enfoque en la identificación y gestión de riesgos complejos que no tienen un historial bien definido, como las ciberamenazas, el cambio climático y los desafíos regulatorios. Adoptar esta norma significa no solo estar preparado para enfrentar riesgos emergentes, sino también estar en posición de aprovechar las oportunidades que estos traen, como la innovación en procesos, la mejora de los servicios ofrecidos y el fortalecimiento de la confianza de los stakeholders. La ISO 31050 ayuda a promover una visión holística, donde la seguridad se considera un facilitador del éxito estratégico, contribuyendo directamente a la creación y protección del valor dentro de la organización.

Por lo tanto, al fortalecer sus prácticas de gestión de riesgos emergentes con la ISO 31050, las organizaciones estarán mejor preparadas para enfrentar las incertidumbres del entorno empresarial actual, garantizar la continuidad de sus operaciones y lograr un desempeño superior a largo plazo. La adopción de esta norma representa un paso importante para convertir la gestión de riesgos en un verdadero diferencial competitivo, asegurando no solo la protección contra amenazas, sino también la capacidad de evolucionar y prosperar en un mundo en constante cambio.

8.4. Pasos para implementar la ISO 31050 en complemento al proceso actual de gestión de riesgos de seguridad

La implementación de la ISO 31050 en el sector de seguridad puede integrarse al proceso de Enterprise Security Risk Management (ESRM) de ASIS para crear un sistema robusto y dinámico de gestión de riesgos emergentes.

Aquí se presentan 10 pasos para realizar esta implementación de manera eficaz:

1) **Compromiso del liderazgo y definición de objetivos estratégicos**: El primer paso es garantizar el compromiso de la alta dirección. El liderazgo debe

reconocer la importancia de los riesgos emergentes y definir objetivos estratégicos que alineen la gestión de riesgos emergentes con las metas corporativas. Esto incluye comunicar claramente cómo la ISO 31050 complementa el proceso actual de ESRM y cómo ambos marcos pueden ayudar a alcanzar los objetivos de la organización.

2) **Análisis del sistema actual de gestión de riesgos**: Antes de comenzar la implementación, es esencial analizar el sistema actual de gestión de riesgos de seguridad para identificar brechas y oportunidades. Esto implica revisar cómo se aplica actualmente el ESRM y determinar qué elementos de la ISO 31050 pueden añadirse para mejorar el enfoque de los riesgos emergentes, especialmente aquellos que trascienden las amenazas y vulnerabilidades físicas y operativas.

3) **Desarrollo de competencias y capacitación**: Capacitar al equipo es fundamental para implementar la ISO 31050. Esto incluye formar a los colaboradores sobre las diferencias entre el enfoque tradicional y el enfoque para riesgos emergentes, según lo descrito en la ISO 31050. Las capacitaciones específicas deben incluir la identificación de señales débiles, técnicas cualitativas como el análisis de escenarios y el uso de tecnologías como la inteligencia artificial para la predicción de riesgos.

4) **Creación de un ciclo de inteligencia de riesgo**: Establecer un ciclo de inteligencia de riesgo robusto es esencial. Este ciclo, descrito por la ISO 31050, debe implementarse para identificar, recopilar, analizar y difundir información relevante sobre riesgos emergentes. En el contexto del ESRM, esto puede significar un aumento en la frecuencia de las evaluaciones de riesgos, el monitoreo de tendencias y una mayor colaboración entre las áreas de TI, seguridad y gestión de riesgos corporativos.

5) **Integración con el ESRM: alineamiento con la gestión de activos**: La ISO 31050 debe integrarse al ESRM para garantizar un enfoque integral. El ESRM está enfocado en la protección de los activos más importantes de la organización, y la ISO 31050 puede complementar este enfoque ayudando a anticipar riesgos emergentes que puedan impactar esos activos. Esta integración asegura que la evaluación de riesgos emergentes se realice de forma coordinada, considerando tanto amenazas/vulnerabilidades conocidas como riesgos emergentes.

6) **Identificación y análisis de señales débiles**: Adoptar prácticas de identificación de señales débiles es un paso fundamental. Utilizando herramientas de análisis

de datos y monitoreo, la organización debe comenzar a detectar patrones o cambios en el entorno interno y externo que puedan indicar la posibilidad de un riesgo emergente. En el contexto del ESRM, esto puede incluir monitorear la seguridad cibernética de manera más amplia, incluyendo vulnerabilidades que puedan ser explotadas durante crisis climáticas.

7) **Creación de escenarios prospectivos**: La creación de escenarios prospectivos permite que la organización visualice posibles futuros y se prepare para ellos. Estos escenarios deben considerar una variedad de factores, como impactos regulatorios, cambio climático y posibles ataques cibernéticos. En el ESRM, esto puede adaptarse para analizar cómo diferentes tipos de amenazas y vulnerabilidades, combinadas, pueden afectar la seguridad de los activos críticos y cuál sería la respuesta más apropiada.

8) **Desarrollo de planes de contingencia y estrategias adaptativas**: Con base en los escenarios prospectivos y las señales débiles identificadas, la organización debe desarrollar planes de contingencia sólidos. Estos planes deben prever acciones a tomar en caso de crisis emergentes, como ataques cibernéticos durante desastres naturales, según lo discutido en ejemplos anteriores. La ISO 31050 orienta la adaptación continua, asegurando que los planes sean flexibles y puedan ajustarse según evolucione el escenario.

9) **Comunicación y colaboración transversal**: La comunicación eficaz entre las áreas de la organización es esencial para garantizar que la gestión de riesgos sea un esfuerzo colectivo. Tanto el ESRM como la ISO 31050 enfatizan la importancia de involucrar a diferentes stakeholders, y esto debe reflejarse en la práctica. Los equipos de seguridad física, TI, cumplimiento, operaciones y gestión de riesgos deben trabajar juntos para identificar, evaluar y responder a los riesgos de manera coordinada.

10) **Monitoreo continuo y mejora continua**: Finalmente, la implementación de la ISO 31050 debe incluir el monitoreo continuo de los riesgos emergentes y una evaluación regular de los procesos adoptados. Aprender de eventos pasados y ajustar las estrategias es fundamental para garantizar la eficacia de la gestión de riesgos. Esta etapa debe ser un ciclo constante de mejora, en el que se incorporen las lecciones aprendidas y se mejoren continuamente las prácticas de gestión de riesgos para adaptarse a los cambios del entorno empresarial.


10 pasos para realizar la implementación de la ISO 31050 de manera eficaz.
01. Compromiso del liderazgo y definición de objetivos estratégicos.
02. Análisis del sistema actual de gestión de riesgos.
03. Desarrollo de competencias y capacitación.
04. Creación de un ciclo de inteligencia de riesgo.
05. Integración con el ESRM: alineamiento con la gestión de activos.
06. Identificación y análisis de señales débiles.
07. Creación de escenarios prospectivos.
08. Desarrollo de planes de contingencia y estrategias adaptativas.
09. Comunicación y colaboración transversal.
10. Monitoreo continuo y mejora continua.

ANEXO I – Análisis comparativo entre ESRM-ASIS e ISO 31000

Resultado del análisis comparativo entre las dos normas (ISO 31000 y ESRM de ASIS), encontramos los siguientes resultados:

Similitudes:

1. **Gestión de Riesgos como Proceso Sistemático**: Ambas normas consideran la gestión de riesgos como un proceso sistemático, estructurado e iterativo, que involucra la identificación, análisis, evaluación y tratamiento de riesgos.
2. **Integración y Alineamiento con los Objetivos Organizacionales**: Las dos normas enfatizan la importancia de integrar la gestión de riesgos en los procesos estratégicos de la organización, alineando los esfuerzos de mitigación de riesgos con los objetivos y metas organizacionales.
3. **Participación de las Partes Interesadas**: Las normas destacan la importancia de la comunicación y consulta con las partes interesadas en el proceso de evaluación y mitigación de riesgos, garantizando que la información se considere en la toma de decisiones.

Diferencias:

1. **Enfoque Específico vs. Enfoque General**:
    - **ISO 31000**: Presenta un enfoque amplio para la gestión de cualquier tipo de riesgo, siendo aplicable a todo tipo de organizaciones, independientemente del sector.
    - **ESRM ASIS**: Se enfoca específicamente en los riesgos relacionados con la seguridad, incluyendo riesgos físicos, lógicos y no físicos, y está orientada a activos específicos que pueden ser impactados por amenazas y vulnerabilidades.
2. **Orientación hacia la Seguridad**:
    - La norma **ESRM ASIS** enfatiza la seguridad de los activos tangibles e intangibles, además de ofrecer directrices detalladas sobre la identificación de amenazas y el análisis de vulnerabilidades que afectan la seguridad.
    - La **ISO 31000** adopta una visión más amplia del riesgo, abarcando todo tipo de incertidumbres, sin enfocarse exclusivamente en la seguridad.

Complementariedad:

- La **ISO 31000** proporciona una base general y sólida para la gestión de riesgos, mientras que la **ESRM ASIS**detalla cómo aplicar estos conceptos específicamente

en el contexto de la seguridad. Una puede complementar a la otra de la siguiente manera:

  - La **ISO 31000** establece el proceso fundamental para la gestión de riesgos corporativos.
  - La **ESRM ASIS** complementa este proceso proporcionando directrices específicas para los riesgos de seguridad, ayudando a identificar y mitigar amenazas específicas que puedan comprometer los activos críticos de la organización.
- Juntas, estas normas ayudan a la empresa a gestionar no solo los riesgos generales que afectan sus operaciones, sino también los riesgos específicos relacionados con la seguridad de sus activos.

Puntos Antagónicos:

- No existe un punto explícitamente antagónico entre las normas, pero el enfoque difiere sustancialmente. La **ISO 31000** es más amplia y se aplica a una variedad de riesgos, mientras que la **ESRM ASIS** se centra estrictamente en la seguridad. Esta diferencia de enfoque puede llevar a diferentes enfoques en la priorización de riesgos, ya que la **ESRM** prioriza la seguridad física y operativa, lo cual puede no ser el foco principal en todos los contextos de gestión de riesgos definidos por la **ISO 31000**.

En resumen, ambas normas tienen enfoques que se alinean en muchos aspectos, siendo la **ISO 31000** adecuada para establecer una visión amplia de la gestión de riesgos, mientras que la **ESRM ASIS** ofrece un enfoque más práctico y detallado sobre la gestión de riesgos de seguridad. Son complementarias y pueden utilizarse conjuntamente para una gestión de riesgos más holística e integrada.

ANEXO II – Referencias bibliográficas

- ISO 31000:2018(en). Gestión del riesgo – Directrices. Organización Internacional de Normalización (ISO), 2018. Recuperado de https://www.iso.org/standard/65694.html;

- ISO/TS 31050:2023(en) Risk management – Guidelines for managing an emerging risk to enhance resilience. Recuperado de https://www.iso.org/standard/54224.html;

- ASIS STANDARD – Security Risk Assessment – ASIS SRA, 2024. Recuperado de https://store.asisonline.org/security-risk-assessment-standard-asis-sra-2024-softcover.html.

Sobre la Plataforma t-Risk

La **Plataforma t-Risk** (SaaS) está disponible **desde 2015** para apoyar a las organizaciones en la gestión de sus riesgos. Es una herramienta analítica que ayuda en la **identificación, análisis y evaluación** de riesgos, además de apoyar en los procesos de **priorización** de **controles y tratamiento de los riesgos**. Está en conformidad con el proceso de gestión de riesgos definido en las normas ISO 31000 e ISO 31050.

Disponible en **portugués, inglés y español**, aumenta la productividad hasta un **80%**. Después de definir los controles que se implementarán, mejorarán o mantendrán para mantener los riesgos dentro del apetito de riesgo de la organización, también será posible **monitorear** todos los proyectos, tareas y controles a través del **módulo 5W2H** para la gestión de proyectos.

Softwares t-Risk

Conozca todos los módulos y herramientas de la Plataforma t-Risk.

Módulo Gestión de Riesgos Corporativos

Análisis de riesgos integrados y planificación de los controles.

Módulo Análisis Preliminar de Riesgos

Evaluación previa sobre los principales riesgos en una organización.

Módulo Operador Económico Autorizado

Gestión de riesgos aduaneros y cadena de suministro.

Módulo Gestión de Riesgos de la Agenda ESG

Verificación de antecedentes y Due Diligence digital.

Módulo Evaluación de Madurez

Análisis del nivel de madurez de una organización en cada una de las 11 dimensiones críticas.

Aplicación de Evaluación de Riesgos Mobile

Integrada a la plataforma web, una solución completa para la recopilación de información en el campo.


POTENCIE SUS ANÁLISIS DE RIESGOS CON LA INTELIGENCIA ARTIFICIAL DE T-RISK!
Acceda ahora mismo y descubra esta innovación.
¡Haga clic aquí!

t-Risk

Método de Avaliação de Riscos

ASIS LATAM&CA Costa Rica 2024