

Año 1, N.º 01

Octubre 2026

RIESGO ENSERIO

El boletín de noticias de **APE**  **RI**

El boletín **RIESGO ENSERIO** de **APEGRI** es distribuido bajo la
Licencia de **CREATIVE COMMONS CC BY-NC-SA 4.0**
Atribución/Reconocimiento – No Comercial – Compartir Igual
(<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

CONTENIDO

EDITORIAL.....	4
EL CONCEPTO DE RIESGO INHERENTE HA CAMBIADO... Y POR QUÉ ESTO ES IMPORTANTE.....	5
EL SUPERPODER TIENE UN COSTO.....	9
RIESGO, CONTINUIDAD DEL NEGOCIO Y SEGURO	12
NOVEDADES.....	15

EDITORIAL

¿Qué es el riesgo? Varias organizaciones y personas en el mundo han realizado, desde su punto de vista, descripciones para poder responder la pregunta. Esto demuestra que el riesgo es importante y abarca todas las dimensiones que conocemos, quizás también las dimensiones que no conocemos en un espacio determinado del tiempo.

Varios factores que han acontecido en los últimos tiempos han hecho que se tome con importancia al riesgo y a su debida gestión, tanto a nivel individual como personas y a nivel empresarial de cualquier tamaño. En esta línea, se puede distinguir al riesgo en distintas, por llamarlo así, vertientes que se van a aplicar a un contexto, sector o área en específico. Aceptando la diversidad de enfoques, y mejor si se tienen consensos, es que vamos a poder entendernos y por ende tener una buena gestión del riesgo.

La gestión del riesgo, en forma propia, determina una acción preventiva para ayudar a los que la utilizan, personas o empresas de cualquier tamaño, a tomar decisiones informadas para alcanzar sus objetivos.

Riesgo enserio nace con el fin de aportar pautas para la realización de una mejor práctica de la gestión del riesgo; permitiendo que sus asociados, profesionales competentes en distintas áreas del riesgo, compartir sus conocimientos y experiencias. De esta manera, APEGRI busca la pluralidad en las actividades que realiza y aportar al bienestar de la sociedad.



Gustavo Vallejo La Torre
Editor

<https://www.linkedin.com/in/gvallejolt/>

EL CONCEPTO DE RIESGO INHERENTE HA CAMBIADO... Y POR QUÉ ESTO ES IMPORTANTE



Figura 1. Dos maneras, un término.

El término «riesgo inherente» se utiliza ampliamente en los ámbitos de la gestión de riesgos, la auditoría interna, el cumplimiento normativo y la gobernanza. Sin embargo, a pesar de su popularidad, no posee un significado único y universalmente aceptado. Con el tiempo, han surgido dos interpretaciones distintas; cada una es válida en su propio contexto, pero a menudo se utilizan indistintamente, lo que genera confusión en la práctica.

Históricamente, el riesgo inherente se refería al peligro intrínseco propio de una actividad, producto o situación. Esta perspectiva ontológica concibe el riesgo como algo que existe independientemente de los controles. Un vehículo en movimiento, una reacción química o una industria de alto riesgo, como la construcción, conllevan un peligro inherente que no puede eliminarse, sino únicamente gestionarse. Desde este punto de vista, el riesgo está vinculado a la naturaleza misma de la realidad, no a la presencia o ausencia de medidas de mitigación.

Más recientemente, no obstante, ha cobrado fuerza una segunda interpretación, especialmente en los entornos de auditoría, cumplimiento y regulación. En este caso, el riesgo inherente se define como el nivel de riesgo existente antes de aplicar cualquier control. Este enfoque basado en controles trata el riesgo inherente como una línea base hipotética utilizada para medir la eficacia de los controles y para comparar los niveles de riesgo bruto, neto y residual.

Ambas interpretaciones son útiles, pero sirven para fines muy diferentes.



Figura 2: El paso del peligro intrínseco a los modelos basados en el control

La perspectiva ontológica se alinea mejor con la toma de decisiones en el mundo real, sobre todo en contextos operativos, de ingeniería, jurídicos y estratégicos. Reconoce que algunos riesgos son irreducibles. Por ejemplo, trabajar en altura siempre conlleva un riesgo de caída, independientemente de las medidas de seguridad.

En tales casos, la función de la gestión de riesgos no es «eliminar» el riesgo, sino comprender, comunicar y gestionar la exposición al mismo. Por el contrario, el enfoque basado en controles resulta muy adecuado para entornos estructurados donde el énfasis recae en la eficacia de los controles y en la garantía de su funcionamiento. Permite a las organizaciones modelar la reducción del riesgo, probar controles y respaldar los procesos de auditoría. Sin embargo, también puede crear la impresión errónea de que todos los riesgos son controlables o de que el riesgo es simplemente una consecuencia de la falta de controles.

Esta dualidad plantea un desafío crítico: un mismo término —riesgo inherente— puede dar lugar a interpretaciones fundamentalmente distintas según quién lo utilice y en qué contexto.

Función / Departamento	Vista preferida de riesgo inherente
Auditoría interna	✗ Basado en controles
Cumplimiento / Asuntos regulatorios	✗ Basado en controles
Operaciones / Gestión de línea	✓ Peligro inherente
Ingeniería / Salud y seguridad / Seguridad	✓ Peligro inherente
Legal / Consejo general	✓ Peligro inherente

Función / Departamento	Vista preferida de riesgo inherente
Finanzas / Tesorería	⚠ Ambos (depende del contexto)
Recursos Humanos (p. ej., riesgos laborales, viajes)	✅ Peligro inherente
TI / Ciberseguridad	⚠ Both
Gestión de proyectos / PMO	✅ Peligro inherente
Consejo de Administración / Ejecutivos	✅ Peligro inherente (preferido); ❌ Basado en controles (si está influido por la auditoría)
Ejecutivos Función de gestión de riesgos	⚠ Both (se deben traducir ambos)

Tabla 1. El significado del peligro intrínseco en los distintos departamentos de una organización.

Esta brecha es claramente visible en todas las organizaciones. Las funciones de auditoría interna y cumplimiento tienden a adoptar la definición basada en controles, ya que sus marcos de trabajo se estructuran en torno a la evaluación de dichos controles. Por otro lado, las áreas de operaciones, ingeniería y legal, así como la alta dirección, suelen pensar en términos de peligro inherente, centrándose en la exposición real implícita en las actividades o decisiones. Se espera que los propios gestores de riesgos sepan desenvolverse entre ambos mundos, traduciendo conceptos entre las distintas funciones.

Las consecuencias de esta ambigüedad no son meramente teóricas; afectan directamente a la comunicación, la toma de decisiones y la gobernanza. Cuando las partes interesadas utilizan el mismo término con significados diferentes, las evaluaciones de riesgos pueden volverse incoherentes, engañosas o desconectadas de la realidad.

La solución no consiste en imponer una definición única, sino en **priorizar la claridad sobre la costumbre**.

Los profesionales deben especificar qué interpretación están utilizando y adaptar su lenguaje al contexto. Al referirse a la exposición intrínseca, términos como «peligro inherente» o «riesgo intrínseco» aportan mayor precisión. Cuando se alude a

escenarios hipotéticos sin controles, resultan más adecuados términos como «riesgo previo al control» o «riesgo bruto».

En última instancia, una gestión de riesgos eficaz no trata sobre terminología, sino sobre facilitar mejores decisiones.

El lenguaje debe respaldar ese objetivo, no oscurecerlo. Por tanto, reconocer la evolución del concepto de riesgo inherente es algo más que un ejercicio semántico: es un paso necesario hacia unas prácticas de gestión de riesgos más coherentes, transparentes y orientadas a la toma de decisiones en las organizaciones modernas.



Alex Dali

Fundador y miembro de la Junta Directiva G31000 Risk Institute
<https://www.linkedin.com/in/alex dali/>

EL SUPERPODER TIENE UN COSTO

Cinco pestañas abiertas. Cinco procesos en paralelo, cada uno delegado a una herramienta distinta de inteligencia artificial. Uno te resume un informe, otra arma un análisis, otro redacta un correo, otro consulta una base de datos, el quinto te devuelve código. Todos exigen lo mismo de vos: revisar la salida, validar que tenga sentido, decidir si la usas tal cual. Por un rato, es la sensación del superpoder: haces en una hora lo que antes te llevaba un día.

Cuando termina la jornada, la cuenta llega. Dolor de cabeza. Vista cansada. Mal humor sin causa clara. Y peor todavía: la sensación de no haber producido tanto como creías. Bienvenidos a la productividad de la era de la IA, y al costado que las organizaciones todavía no están midiendo.

La eficiencia tiene un costado que no se está midiendo

Las empresas incorporan IA con la misma lógica con que incorporaron cualquier tecnología productiva: optimizar tiempos. Reducir costos. Ampliar capacidad. Esa lógica no está mal. Le falta una segunda mirada: qué le pasa a la salud de la gente que sostiene esos procesos.

En marzo de 2026, Harvard Business Review publicó “When Using AI Leads to ‘Brain Fry’” realizado por investigadores de Boston Consulting Group junto con la Universidad de California, Riverside. El hallazgo central: ciertos patrones de uso de IA generan fatiga cognitiva, lo que los propios autores bautizaron “brain fry” (fritura cerebral), mientras que otros la reducen. Reportes sobre el estudio ubican el quiebre a partir de tres aplicaciones de IA gestionados en simultáneo: hasta ahí la productividad sube, de ahí en más empieza a caer, aunque la sensación de estar rindiendo siga intacta.

No es la IA en abstracto la que enferma. Es la forma en que la usamos dentro del trabajo. Eso convierte a la implementación de IA en un asunto de riesgo psicosocial, no solo de tecnología o cumplimiento.

Lo que dice la ISO/IEC 45003

La norma ISO/IEC 45003:2021 ubica el riesgo psicosocial en cuatro dimensiones: carga y exigencia cognitiva, autonomía y claridad de rol, relaciones sociales en el trabajo, organización del entorno laboral. La adopción mal gestionada de IA pega directo sobre las cuatro.

Una persona que supervisa tres, cuatro o cinco procesos de IA en simultáneo no está delegando tareas. Está auditando salidas con responsabilidad final sobre cada una. El alcance del puesto se corre sin que nadie lo redefina. Y cuando el

resultado de la IA reemplaza la consulta con un par, el tejido social del equipo se erosiona sin que nadie lo decida.

Si tu organización tiene una matriz de riesgos psicosociales y ahí no figura la implementación de IA, esa matriz ya está desactualizada.

Dimensión ISO/IEC 45003	Cómo la golpea la IA mal gestionada
Carga y exigencia cognitiva	Supervisión simultánea de múltiples agentes, sin límite definido
Autonomía y claridad de rol	El alcance del puesto se corre sin rediseño formal
Relaciones sociales en el trabajo	La consulta con un par se reemplaza por la consulta a la IA
Organización del entorno laboral	No hay pauta de simultaneidad ni de pausas cognitivas

Tabla 1. Riesgo psicosocial e implementación de IA. Fuente: elaboración propia sobre ISO/IEC 45003:2021.

La paradoja productiva

La sensación inicial es la opuesta a la fatiga: es la del superpoder. Y es real, durante un rato. Pasado cierto umbral de procesos simultáneos, la productividad real cae, aunque la productividad percibida siga subiendo. Aparecen los errores. Las decisiones apuradas. Los retrabajos. Más adelante: ausentismo, problemas de salud, accidentes en operaciones críticas, sin que nadie lo haya visto venir con un dato.

Ahí está el problema de fondo: la mayoría de las organizaciones todavía no tiene una cifra propia de cuánto cuesta esto. Lo que se vendió como eficiencia termina siendo costo oculto, y los costos ocultos de riesgo psicosocial son los más caros porque no aparecen en ninguna cuenta hasta que estallan. Medirlo (frecuencia de eventos, ausentismo asociado, rotación en los equipos con mayor simultaneidad) es el paso que falta antes de poder ponerle un número.

Qué pueden hacer las organizaciones

Limitar la simultaneidad. Poner como pauta que nadie gestione más de dos procesos paralelos asistidos por IA en la misma franja horaria. No es una restricción arbitraria: es, según el propio estudio de BCG, la línea que separa la ganancia de productividad de la fatiga.

Diseñar pausas cognitivas reales, no el café de cinco minutos frente a otra pantalla. Pausas que saquen a la persona del entorno de supervisión.

Formar antes de delegar. Si alguien pasa a auditar resultados de IA en un ámbito donde antes no operaba (finanzas, legales, control interno), la organización tiene la responsabilidad de formarlo antes, no de corregir después. La IA habilita el rol y la formación lo sostiene.

Una observación final

El superpoder existe. El costo también. La gestión de riesgos no apareció en las organizaciones para frenar la innovación: apareció para sostenerla. Incorporar IA sin gestionar su impacto psicosocial no construye una revolución productiva. Construye una ola de agotamiento que la propia tecnología no va a poder revertir.

Fuente de referencia

- Harvard Business Review “When Using AI Leads to ‘Brain Fry’”
 - <https://hbr.org/2026/03/when-using-ai-leads-to-brain-fry>
- ISO/IEC 45003:2021
 - <https://www.iso.org/standard/64283.html>



Ezequiel Bossio
Gobernanza y Riesgo en IA
www.ezequielbossio.com

RIESGO, CONTINUIDAD DEL NEGOCIO Y SEGURO

El riesgo y su normalización por ISO

Acorde con la definición de riesgo como efecto de la incertidumbre en los objetivos de las organizaciones, según lo establecido en la norma ISO 31000:2009 y su revisión de 2018, la gestión del riesgo se ha centrado históricamente en los efectos negativos y especialmente en los eventos que causan grandes daños patrimoniales como incendios, terremotos o inundaciones.

La normalización de la gestión del riesgo iniciada en el presente siglo XXI ha evolucionado desde la tradicional consideración del seguro como fórmula preferente de tratamiento del riesgo al nuevo concepto de seguro como respuesta al riesgo compartida con los aseguradores, tal y como se está proponiendo en la revisión de la norma ISO 31000 en curso en esta década de los 2020s.

El seguro de daños materiales y de pérdida de beneficios

Las pólizas de seguro suelen ser la piedra angular de la respuesta a estos riesgos de catastróficas consecuencias y baja probabilidad para las organizaciones industriales, pero en muchas ocasiones las pólizas tradicionales del siglo XX no llegaban a cumplir con su objetivo de restaurar de forma integral a la empresa a la situación anterior al siniestro con la simple contratación de coberturas de daños materiales.

Si el evento es disruptivo y se produce la paralización total de la organización durante un periodo significativo, la falta de liquidez en la empresa para mantener sus gastos permanentes (nóminas de los empleados, impuestos y amortizaciones, entre otros) puede llevarla a desaparecer, incluso aunque pueda reparar o reponer los bienes productivos indemnizados por la compañía de seguros. En tales situaciones de necesidad financiera por falta de actividad productiva, la respuesta bancaria es menos eficaz que la aseguradora.

Por ello los aseguradores complementaron, ya mediado el siglo XX, las pólizas de daños materiales con la cobertura de lucro cesante o de pérdida de beneficios para posibilitar la supervivencia del negocio durante los periodos de paralización por un evento asegurado por la cobertura de daños materiales (ver fig.1), indemnizando los gastos permanentes de la empresa y, en caso de solicitarlo, el beneficio neto de los accionistas

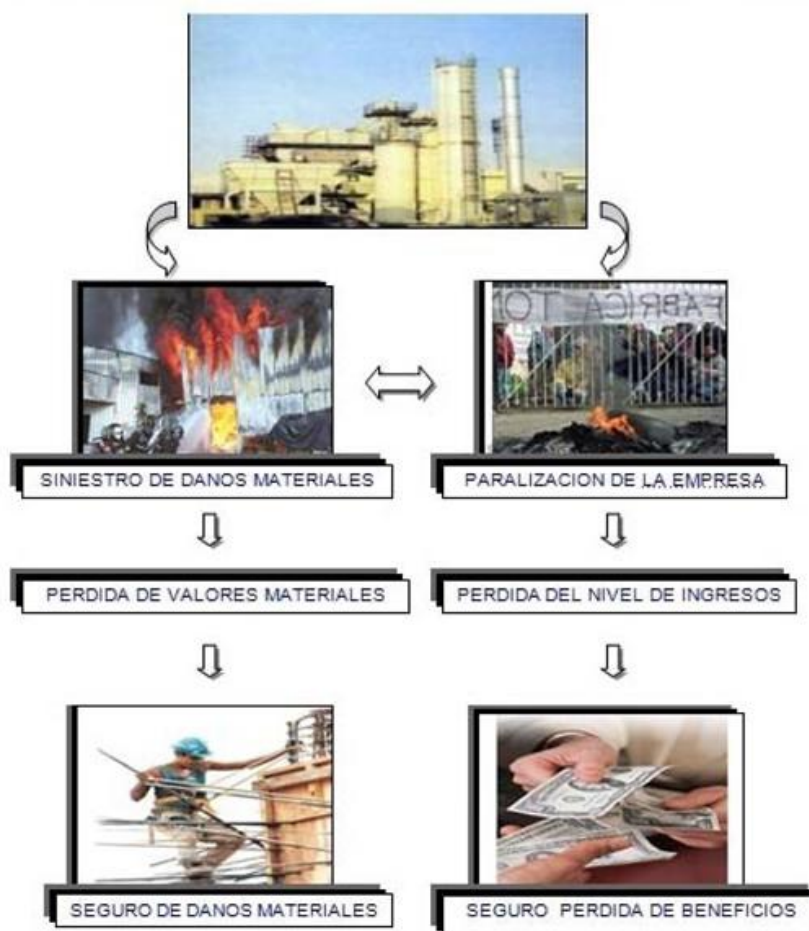


Figura.1 proporcionada por Suárez Consultores

Esta cobertura, vinculada siempre a la existencia de una cobertura de daños materiales, permite devolver de forma plena a la empresa a la situación anterior al siniestro catastrófico de daños materiales que paraliza su actividad.

La respuesta complementaria al seguro de los planes tras siniestro

Ha llevado décadas que las organizaciones aprecien el valor añadido de la garantía de pérdida de beneficios, pero hoy en día es una cobertura muy extendida en el seguro industrial, hasta el punto de que muchos aseguradores exigen para aceptar esta cobertura disponer de medidas preventivas complementarias, al igual que tradicionalmente han venido exigiendo medios de protección (como sectorización, detectores o hidrantes) para asegurar el riesgo de incendio en algunas industrias de alta exposición.

En esta línea, se han extendido en los últimos años las exigencias de respuestas mediante planes de contingencia y de continuidad del negocio frente a eventos disruptivos para algunos sectores industriales que requieran largos periodos de indemnización en el contrato asegurador. De esta forma, estas organizaciones industriales tienen en la consultoría de planes de contingencia una herramienta que les permite cumplir con este requisito asegurador, pero lo que es más importante, les

ayuda a garantizar una respuesta de mínimos y un retorno a la normalidad en plazos aceptables.

Adicionalmente, esta planificación puede servir de punto de partida para que la organización desarrolle un sistema de gestión de la continuidad del negocio conforme a la norma ISO 22301 que no solo será valorada por los aseguradores sino también por sus partes interesadas de la cadena de suministro y por la propia organización que gestionará este riesgo de una forma eficaz incluida su imagen en la gestión de crisis aplicando la norma ISO 22361.

El desarrollo y la implantación de planes de continuidad del negocio como respuesta a los riesgos disruptivos de las industrias son importantes en las grandes organizaciones, pero adquieren el carácter de elemento crítico en el caso de PYMEs sin plantas alternativas dentro de la organización a las que poder desplazar temporalmente la actividad productiva paralizada.



Angel Escorial Bonet
Profesor en ENAE Business School
<https://www.linkedin.com/in/angel-escorial/>

NOVEDADES

1

APEGRI actualizó su página web:

www.apegri.org

2

Se realiza la publicación de la ISO 19011:2026 – Directrices para la auditoría de sistemas de gestión

<https://www.iso.org/standard/19011>

4

Se realiza la publicación de la ISO 9001:2026 – Sistema de gestión de la calidad

<https://www.iso.org/standard/9001.html>

APEGRI

<https://www.linkedin.com/company/apeгри/>

<https://apeгри.org/>