Machine Translated by Google

RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año V, vol. 2, 2024 | Envío: 16/02/2024 | Aceptado: 19/02/2024 | Publicación: 22/02/2024

Gobernanza de la información corporativa: seguridad, privacidad de datos y gestión ejecutiva en la era de la inteligencia artificial.

Gobernanza de la información corporativa: seguridad, privacidad de datos y gestión ejecutiva en la era de la inteligencia artificial.

Gobernanza de la información corporativa: seguridad, privacidad de datos y gestión ejecutiva en la era de la inteligencia artificial.

Ricardo Saddi Becker es
licenciado en Informática por la Universidad Federal de Mato Grosso (2009).
Especialista certificado en continuidad del negocio por DRII

RESUMEN

La información se ha convertido en uno de los principales activos estratégicos de las organizaciones contemporáneas, desempeñando un papel clave en la generación de valor, innovación y competitividad.
Paralelamente al crecimiento exponencial del volumen de datos y la incorporación de tecnologías basadas en inteligencia artificial (IA), se han intensificado los desafíos relacionados con la seguridad de la información, la privacidad de los datos personales y la gobernanza corporativa. En este contexto, este estudio analiza la integración entre la gobernanza de la información, la protección de datos, la gestión ejecutiva y la ciberseguridad, y examina cómo estos elementos contribuyen a la creación de organizaciones más resilientes, transparentes y orientadas a los datos. La investigación se desarrolló mediante una revisión bibliográfica exploratoria y descriptiva, basada en literatura científica, estándares internacionales y marcos de gobernanza ampliamente adoptados en el entorno corporativo. Los resultados muestran que la protección de la información ha dejado de ser una mera responsabilidad operativa de las áreas de tecnología de la información para convertirse en una responsabilidad estratégica compartida entre ejecutivos, consejos de administración y líderes organizacionales. Se concluye que los modelos de gobernanza integrados, combinados con la adopción de prácticas estructuradas de seguridad, privacidad y gestión de riesgos, son factores esenciales para garantizar el cumplimiento normativo, la sostenibilidad empresarial y la confianza institucional en un escenario caracterizado por la creciente digitalización de las relaciones económicas y sociales.

PALABRAS CLAVE: Gobernanza de la información; Seguridad de la información; Privacidad de datos; Inteligencia artificial; Dirección ejecutiva.

ABSTRACTO

La información se ha convertido en uno de los activos estratégicos más valiosos de las organizaciones contemporáneas, desempeñando un papel decisivo en la creación de valor, la innovación y la competitividad. Paralelamente al crecimiento exponencial del volumen de datos y la incorporación de tecnologías de inteligencia artificial (IA), se han intensificado los desafíos relacionados con la seguridad de la información, la privacidad de los datos y el gobierno corporativo. Este estudio examina la relación entre la gobernanza de la información, la protección de datos, la alta dirección y la ciberseguridad, analizando cómo estos elementos contribuyen al desarrollo de organizaciones resilientes, transparentes y basadas en datos. La investigación se llevó a cabo mediante una revisión bibliográfica exploratoria y descriptiva basada en publicaciones científicas, estándares internacionales y marcos de gobernanza reconocidos. Los resultados demuestran que la protección de la información ya no es únicamente responsabilidad operativa de los departamentos de Tecnologías de la Información, sino que se ha convertido en una preocupación estratégica compartida por los ejecutivos, los consejos de administración y el liderazgo organizacional. El estudio concluye que los modelos de gobernanza integrados, combinados con prácticas estructuradas en seguridad, privacidad y gestión de riesgos, son fundamentales para garantizar el cumplimiento normativo, la sostenibilidad empresarial y la confianza institucional en una economía cada vez más digital.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año V, vol. 2, 2024 | Envío: 16/02/2024 | Aceptado: 19/02/2024 | Publicación: 22/02/2024

PALABRAS CLAVE: Gobernanza de la información; Seguridad de la información; Privacidad de datos; Inteligencia artificial; Dirección ejecutiva.

INTRODUCCIÓN

La economía digital ha transformado profundamente la forma en que las organizaciones producen.
El conocimiento les permite tomar decisiones y establecer ventajas competitivas. La expansión de los entornos
Las tecnologías conectadas, la computación en la nube, las plataformas digitales y la inteligencia artificial se han expandido...
Incrementando significativamente el valor estratégico de los datos, convirtiendo la información en un recurso indispensable.
para la innovación, el desarrollo de nuevos modelos de negocio y el fortalecimiento de
competitividad empresarial.

Sin embargo, ese mismo escenario que fomenta las oportunidades también aumenta la complejidad de la gestión.
Corporativo. El crecimiento exponencial del volumen de información, la circulación continua de datos.
personal, la integración entre diferentes ecosistemas tecnológicos y la creciente dependencia de
Los servicios digitales conllevan mayores riesgos relacionados con la privacidad, la ciberseguridad y...
Cumplimiento normativo y gobernanza de los activos de información. Como consecuencia,
La gestión de estos recursos ha dejado de ser una tarea exclusivamente técnica.
asumir una dimensión estratégica en las organizaciones.

En los últimos años se ha promulgado legislación destinada a proteger los datos personales, como el Reglamento General de Protección de Datos.
La Ley General de Protección de Datos (LGPD) de Brasil y el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.
Los europeos reforzaron la necesidad de mecanismos capaces de garantizar la transparencia,
responsabilidad y control sobre el manejo de la información. Paralelamente, la rápida evolución de
Las soluciones basadas en inteligencia artificial han planteado nuevos desafíos relacionados con su uso ético.
Desde los datos, hasta la transparencia de los algoritmos y la rendición de cuentas por las decisiones automatizadas. En este
En este contexto, la gobernanza de la información emerge como una disciplina responsable de establecer políticas,
Procesos y responsabilidades que garantizan el uso seguro, ético y estratégico de los activos.
Informativo. Más que garantizar el cumplimiento normativo, su propósito es promover
Calidad de los datos, fortalecimiento de la toma de decisiones, reducción de los riesgos corporativos y expansión...
La capacidad de generar valor a partir de la información.

La participación de los líderes ejecutivos está adquiriendo cada vez más importancia en este proceso. Consejos de
administración, directores ejecutivos, gerentes de tecnología y responsables de la protección de datos.
Compartirán responsabilidades relacionadas con la definición de estrategias de gobernanza, y...

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año V, vol. 2, 2024 | Envío: 16/02/2024 | Aceptado: 19/02/2024 | Publicación: 22/02/2024

gestión de riesgos digitales y el establecimiento de una cultura organizacional orientada hacia
Protección de la información y uso responsable de la Inteligencia Artificial.
Ante este escenario, este estudio pretende analizar la relación entre la gobernanza y...
Información, seguridad de la información, privacidad de datos y gestión ejecutiva, analizando cómo
Estos elementos se complementan entre sí para construir organizaciones capaces de conciliar la innovación.
tecnología, cumplimiento normativo y sostenibilidad empresarial en un entorno caracterizado
debido a la creciente complejidad digital.

METODOLOGÍA

Esta investigación se caracteriza por ser un estudio exploratorio y descriptivo.
desarrollado a través de una revisión de la literatura. Según Gil (2019), este procedimiento
El enfoque metodológico permite recopilar, organizar y analizar críticamente diferentes perspectivas teóricas sobre...
un fenómeno dado, que facilita la comprensión de las transformaciones conceptuales y prácticas.
observado en contextos organizacionales contemporáneos.
La revisión de la literatura incluyó libros, artículos científicos, normas internacionales,
Publicaciones institucionales y directrices de gobernanza relacionadas con la seguridad de la información.
protección de datos personales, gobierno corporativo, inteligencia artificial, gestión de riesgos y
Transformación digital. Se dio prioridad a los proyectos reconocidos por la comunidad académica y técnica.
así como los documentos producidos por organizaciones internacionales dedicadas al desarrollo de
Mejores prácticas en gobernanza de la información.
Las fuentes seleccionadas fueron sometidas a un análisis cualitativo con el fin de identificar puntos en común.
marcos conceptuales, modelos de gestión ampliamente adoptados y tendencias observadas en la evolución de
Prácticas de gobernanza de la información corporativa. Para promover un enfoque sistemático,
El contenido se organizó en cinco áreas temáticas: fundamentos de la gobernanza de la información;
Privacidad de datos y cumplimiento normativo; Inteligencia artificial y gestión de riesgos; Seguridad
Información desde una perspectiva ejecutiva; y liderazgo estratégico basado en datos.
Además de la literatura clásica sobre gobernanza y gestión de la información, se consideraron los siguientes elementos como puntos de referencia.
desarrollos recientes relacionados con la regulación de la Inteligencia Artificial y con los principios internacionales de
Ética y estándares digitales destinados a proteger la privacidad y la seguridad de los activos de información.
Este enfoque permite integrar los principios establecidos en la literatura con los desafíos.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año V, vol. 2, 2024 | Envío: 16/02/2024 | Aceptado: 19/02/2024 | Publicación: 22/02/2024

factores emergentes derivados de la rápida evolución tecnológica y de los nuevos requisitos normativos.
a las organizaciones.

1. FUNDAMENTOS DE LA GOBERNANZA DE LA INFORMACIÓN

La transformación digital ha cambiado sustancialmente la forma en que las organizaciones crean valor.
haciendo de la información uno de los principales activos estratégicos en el entorno corporativo. Datos generados
operaciones, clientes, proveedores, dispositivos conectados y plataformas digitales se han convertido
para respaldar las decisiones empresariales, impulsar las iniciativas de innovación y orientar las estrategias.
crecimiento. En este contexto, la gobernanza de la información deja de ser una actividad restringida.
La tecnología de la información está asumiendo un papel transversal, que involucra diferentes áreas de
Organización y niveles de liderazgo.

La gobernanza de la información puede entenderse como el conjunto de políticas, procesos,
responsabilidades y mecanismos de control diseñados para garantizar que los activos de información
Deben gestionarse de forma coherente a lo largo de todo su ciclo de vida. Su propósito no es...
Se limita a la protección de datos, pero busca garantizar que la información sea confiable, completa,
accesible, utilizado de forma ética y alineado con los objetivos estratégicos de la institución.
La forma, la calidad, la seguridad, el cumplimiento normativo y la creación de valor se convierten en dimensiones inseparables.
de gestión de la información.

La consolidación de esta disciplina surge de la comprensión de que las decisiones organizacionales son
influenciada directamente por la calidad de los datos disponibles. Información incompleta,
Los datos inconsistentes o desactualizados comprometen los análisis de gestión y dificultan el cumplimiento de...
Los requisitos normativos pueden tener repercusiones financieras, operativas y en la reputación.
relevante. Desde esta perspectiva, la gobernanza de la información establece criterios para la estandarización,
clasificación, retención, intercambio y eliminación de activos de información, reducción
Eliminar ambigüedades y reforzar la fiabilidad de las decisiones corporativas.

Entre los pilares más relevantes de este modelo, la clara definición de roles y...
responsabilidades. Las organizaciones con un mayor grado de madurez tienden a distinguir entre asignaciones.
entre los ejecutivos patrocinadores, los propietarios de datos y los gerentes responsables de
calidad de la información (administradores de datos) y equipos técnicos encargados de gestionar la
entornos tecnológicos. Esta segregación fomenta una mayor responsabilidad institucional, amplía la
Transparencia en los procesos y reducción de conflictos relacionados con el uso de datos.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año V, vol. 2, 2024 | Envío: 16/02/2024 | Aceptado: 19/02/2024 | Publicación: 22/02/2024

Otro elemento esencial se relaciona con la gestión del ciclo de vida de la información. Desde su creación o
Desde la recopilación hasta el archivo y la eliminación final, los datos pasan por diferentes etapas que requieren...
Controles específicos. La ausencia de políticas de retención, clasificación o eliminación de documentos.
Los seguros aumentan la exposición a riesgos regulatorios y comprometen la eficiencia de la gestión documental.
Por este motivo, los modelos de gobernanza modernos establecen criterios objetivos para cada fase de este proceso.
ciclo, conciliando los requisitos legales, las necesidades operativas y los intereses estratégicos de
organización.

La calidad de los datos también ocupa una posición central en las prácticas de gobernanza. Dimensiones como
La precisión, la coherencia, la exhaustividad, la puntualidad y la singularidad influyen directamente en la fiabilidad.
a partir de análisis realizados por áreas de negocio. La expansión de las iniciativas de Business Intelligence,
El análisis y la inteligencia artificial han hecho aún más evidente que los modelos analíticos producen
Los resultados solo se logran en la medida en que se utilizan bases de datos confiables. Por lo tanto, las inversiones en
Las tecnologías avanzadas tienden a presentar un rendimiento limitado cuando no van acompañadas de...
programas estructurados de calidad de la información.

Más allá de los aspectos operativos, la gobernanza de la información fortalece la adaptabilidad de
Organizaciones que se enfrentan a cambios regulatorios y tecnológicos. La existencia de políticas.
Las responsabilidades institucionalizadas y formalmente definidas, así como los procesos documentados, facilitan la
La incorporación de nuevos requisitos legales reduce el impacto derivado de las transformaciones.
Mejora la organización y aumenta la previsibilidad en la gestión de los activos de información.

En este escenario, se observa una importante evolución conceptual: la información deja de ser tratada...
meramente como un recurso operativo para consolidarse como un activo estratégico de la organización.
Una gobernanza adecuada influye directamente en la capacidad de innovar, competir y satisfacer las demandas.
Cumplimiento normativo y establecimiento de relaciones de confianza con clientes, socios, inversores y organismos reguladores.
supervisión. En las organizaciones basadas en datos, la madurez de la gobernanza de la información
Se ha convertido en un indicador relevante de la capacidad de la propia institución para generar valor de forma sostenible.

2. PRIVACIDAD DE DATOS Y CUMPLIMIENTO NORMATIVO

La intensificación de la recopilación, el intercambio y el procesamiento de información personal.
Esto ha convertido la privacidad en uno de los principales desafíos de la gobernanza corporativa contemporánea.
El crecimiento de los servicios digitales, la computación en la nube, las plataformas colaborativas y...
Las aplicaciones basadas en inteligencia artificial han ampliado significativamente el flujo de datos entre

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año V, vol. 2, 2024 | Envío: 16/02/2024 | Aceptado: 19/02/2024 | Publicación: 22/02/2024

organizaciones, proveedores y usuarios, que requieren mecanismos capaces de garantizar el tratamiento
Responsable de la información y el respeto de los derechos de los interesados.

La evolución de este escenario ha impulsado el fortalecimiento de los marcos regulatorios destinados a la protección.
de datos personales. La entrada en vigor de la Ley General de Protección de Datos (LGPD) en Brasil y de
El Reglamento General de Protección de Datos (RGPD) en la Unión Europea ha consolidado un cambio.
Este cambio de paradigma establece que el uso de datos personales debe ajustarse a principios relacionados.
al propósito, la necesidad, la transparencia, la seguridad, la rendición de cuentas y la presentación de informes.
La legislación representa no solo instrumentos legales para la supervisión, sino también puntos de referencia capaces de...
para orientar modelos más maduros de gobernanza de la información.

Desde esta perspectiva, el cumplimiento normativo no debe entenderse como una actividad limitada.
En cumplimiento de los requisitos legales. Organizaciones que gestionan exclusivamente la protección de datos.
Como obligación regulatoria, tienden a adoptar medidas específicas y reactivas. Por el contrario,
Las instituciones que incorporan la privacidad en su estrategia organizativa desarrollan políticas al respecto.
Medidas permanentes de gestión de datos que refuercen la confianza de los titulares de los datos y reduzcan los riesgos asociados.
debido al mal uso de la información.

Uno de los principios más relevantes en este contexto es el concepto de Privacidad desde el Diseño, según el cual
Los requisitos de privacidad deben tenerse en cuenta desde las primeras etapas del diseño del producto.
Servicios y procesos organizacionales. En lugar de implementar controles solo después de la identificación.
Para abordar estos problemas, este enfoque fomenta la integración proactiva de la protección de datos en
Desarrollar soluciones tecnológicas, reducir los costes de adaptación y aumentar la eficacia.
de los mecanismos de seguridad.

Además, el principio de privacidad por defecto establece que la configuración predeterminada de
Los sistemas deben priorizar el menor procesamiento posible de datos personales, limitando la recopilación y el procesamiento de dichos datos.
Compartir únicamente la información estrictamente necesaria para cada propósito. Esta directriz refuerza
la idea de que la protección de la privacidad no depende exclusivamente del comportamiento del usuario,
pero también las decisiones arquitectónicas adoptadas durante el desarrollo y la operación de
sistemas.

La implementación de programas de privacidad estructurados también requiere mecanismos permanentes para
Gobernanza. Inventarios de datos, mapeo de flujos de información, registros de actividad.
tratamiento, evaluaciones de impacto en la protección de datos y procesos formales para abordar
Los derechos de los interesados son instrumentos fundamentales para garantizar el cumplimiento continuo de la normativa.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año V, vol. 2, 2024 | Envío: 16/02/2024 | Aceptado: 19/02/2024 | Publicación: 22/02/2024

Estas prácticas también promueven una mayor transparencia con las autoridades reguladoras y reducen la
tiempo necesario para responder a incidentes que involucren información personal.
Otro aspecto cada vez más relevante se refiere a la gestión de los riesgos derivados del uso compartido.
Compartir datos con terceros. Cadenas de suministro complejas, servicios subcontratados, plataformas en
La computación en la nube y los ecosistemas digitales aumentan la necesidad de una evaluación continua de las prácticas adoptadas.
por socios comerciales. Por lo tanto, el cumplimiento organizacional ya no depende únicamente de
Se están implementando controles internos y se están incorporando mecanismos de debida diligencia y cláusulas contractuales.
auditorías específicas y periódicas y criterios objetivos para la selección y el seguimiento de los operadores.
datos.

La figura del Responsable de Protección de Datos, conocido internacionalmente como
El Responsable de Protección de Datos (RPD) refuerza este modelo de gobernanza actuando como un elemento de
Integración entre la organización, las partes interesadas y las autoridades de supervisión. Más que simplemente cumplir una función.
En su función de asesor, este profesional contribuye a difundir una cultura de protección de datos y a apoyar la toma de decisiones.
Planificación estratégica y orientación de programas de cumplimiento alineados con los requisitos reglamentarios y las mejores prácticas.
prácticas internacionales.

A medida que evoluciona la economía digital, la privacidad ya no se percibe simplemente como un requisito.
legal para consolidarse como un diferenciador competitivo y un elemento esencial de la reputación institucional.
Organizaciones capaces de demostrar transparencia, rendición de cuentas y compromiso con la protección.
Los datos fortalecen las relaciones de confianza con clientes, socios e inversores, transformando...
El cumplimiento normativo como componente estratégico de la sostenibilidad y la gobernanza.
corporativo.

3. INTELIGENCIA ARTIFICIAL, GOBIERNO ALGORÍTMICO Y GESTIÓN DE RIESGOS

La incorporación de la Inteligencia Artificial (IA) en los procesos organizacionales representa uno de los
Las transformaciones más significativas de la actualidad. Sistemas capaces de analizar grandes volúmenes de datos.
El análisis de datos, la identificación de patrones complejos y el apoyo a las decisiones en tiempo real se han empleado en
sectores como la salud, las finanzas, la industria, la logística, la educación y la administración pública. Aunque estos
Tecnologías que mejoran la eficiencia operativa y las capacidades analíticas de las organizaciones, su adopción
También plantea desafíos relacionados con la gobernanza, la transparencia de las decisiones automatizadas y...
Gestionar los riesgos asociados a los modelos algorítmicos.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año V, vol. 2, 2024 | Envío: 16/02/2024 | Aceptado: 19/02/2024 | Publicación: 22/02/2024

A diferencia de los sistemas tradicionales, las aplicaciones basadas en aprendizaje automático
Presentan un comportamiento dinámico, condicionado por la calidad de los datos utilizados en el entrenamiento.
a las características de los algoritmos utilizados y a los cambios que se han producido en el entorno operativo.
En consecuencia, las decisiones generadas por estos modelos pueden sufrir un deterioro.
rendimiento a lo largo del tiempo, reproduciendo sesgos estadísticos presentes en las bases de datos o generando
resultados cuya lógica no es comprendida completamente por los propios usuarios. Esta característica
Esto refuerza la necesidad de mecanismos de gobernanza específicos para garantizar la fiabilidad.
Trazabilidad y supervisión humana.

En este contexto, la gobernanza algorítmica emerge como una disciplina centrada en establecer
Políticas, responsabilidades y controles aplicables al ciclo de vida de los modelos de inteligencia.
Inteligencia artificial. Su objetivo es garantizar el desarrollo de sistemas automatizados.
implementado y supervisado de manera coherente con los principios éticos, los requisitos legales y los objetivos.
Objetivos estratégicos de la organización. La gobernanza no busca limitar la innovación tecnológica, sino garantizarla.
que su uso se produzca de forma transparente y responsable, y que esté alineado con el interés institucional.

Entre los principales desafíos se encuentra la calidad de las bases de datos utilizadas para el entrenamiento y
Validación de los modelos. Información incompleta, desactualizada o estadísticamente desequilibrada.
Comprometen la capacidad predictiva de los algoritmos y aumentan el riesgo de decisiones inconsistentes.
En solicitudes relacionadas con la concesión de crédito, la contratación de personal, el diagnóstico médico o
Análisis de riesgos: pequeñas distorsiones en los datos pueden tener repercusiones significativas en las personas.
y organizaciones. Por lo tanto, los programas de gobernanza de IA dependen directamente de la madurez.
de la gobernanza de la información analizada en capítulos anteriores.

Otro aspecto cada vez más relevante se refiere a la explicabilidad de los modelos (Inteligencia Artificial Explicable).
Inteligencia – XAI). En aplicaciones críticas, las decisiones automatizadas no deben evaluarse únicamente
por la precisión estadística, pero también por la capacidad de proporcionar justificaciones comprensibles para

La transparencia fomenta las auditorías independientes y fortalece la confianza de los usuarios. Sus resultados se ven potenciados por la transparencia, que facilita las auditorías independientes y refuerza la confianza de los usuarios.

y permite identificar factores que influyen en el comportamiento de los algoritmos, especialmente en
sectores sujetos a una alta regulación.

La supervisión humana sigue siendo igualmente indispensable. Aunque los modelos avanzados son
capaz de automatizar actividades complejas, la responsabilidad de las decisiones organizativas
El derecho a participar recae en las personas e instituciones que utilizan estas tecnologías.
expertos en la validación de resultados, la revisión periódica de modelos y la definición de límites.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año V, vol. 2, 2024 | Envío: 16/02/2024 | Aceptado: 19/02/2024 | Publicación: 22/02/2024

La automatización reduce la probabilidad de decisiones inapropiadas y preserva los principios relacionados con responsabilidad corporativa.

La rápida evolución de las soluciones de IA también ha aumentado la importancia de la gestión continua de Riesgos tecnológicos. Las organizaciones maduras establecen procesos continuos para monitorearlos. rendimiento del modelo, identificación de la deriva estadística (deriva del modelo), revisión de los parámetros de capacitación y evaluación de los impactos de los cambios en los conjuntos de datos. Este enfoque Permite la detección de degradaciones antes de que produzcan consecuencias significativas para los procesos de negocio.

En los últimos años, las organizaciones internacionales han comenzado a estructurar marcos específicos para Gobernanza de la Inteligencia Artificial. Destacan las iniciativas centradas en la gestión de riesgos y los principios. Principios éticos para el uso responsable de la IA y directrices para la transparencia algorítmica, que reflejan una Tendencia global hacia el fortalecimiento de los mecanismos regulatorios aplicables a las tecnologías. tendencias emergentes. Estas iniciativas refuerzan la idea de que la innovación y la responsabilidad deben evolucionar de manera que... integrado, evitando que se logren mejoras en la eficiencia a expensas de una menor confianza. institucional.

Desde esta perspectiva, la Inteligencia Artificial deja de representar simplemente una herramienta de La automatización se está convirtiendo en una parte permanente del gobierno corporativo. Su uso responsable. Depende de la integración entre la calidad de los datos, la supervisión humana, la evaluación continua de riesgos y... mecanismos capaces de garantizar la transparencia, el cumplimiento normativo y la rendición de cuentas en decisiones automatizadas.

4. La seguridad de la información como herramienta de gobernanza y valor organizacional.

Durante muchos años, la seguridad de la información se trató predominantemente como una función. técnica, centrada en la administración de controles informáticos diseñados para proteger la entornos tecnológicos. Sin embargo, la evolución de los modelos de negocio digitales se ha expandido significativamente su relevancia estratégica. Actualmente, los incidentes que involucran fugas de información, compromiso de la integridad de los datos o interrupción del servicio producen impactos que van más allá del ámbito tecnológico y que afectan a la reputación y al rendimiento institucional. Seguridad financiera, cumplimiento normativo y la confianza de clientes, inversores y socios comerciales.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año V, vol. 2, 2024 | Envío: 16/02/2024 | Aceptado: 19/02/2024 | Publicación: 22/02/2024

Esta transformación ha cambiado la forma en que las organizaciones estructuran sus programas de seguridad.

La responsabilidad de proteger la información ya no se limita a los equipos técnicos, sino que se ha convertido en responsabilidad compartida.

Integrarse en la agenda de los consejos de administración y la alta dirección. Gestión de riesgos

La ciberseguridad ha llegado a entenderse como un componente del gobierno corporativo, influyendo en

decisiones relacionadas con la expansión empresarial, la innovación tecnológica, la gestión de terceros y

sostenibilidad organizacional.

En este contexto, la cultura organizacional desempeña un papel crucial. La eficacia de los controles...

La seguridad no solo depende de la adopción de tecnologías especializadas, sino también de...

El comportamiento de las personas que producen, comparten y utilizan información a diario.

Programas permanentes de sensibilización, formación y desarrollo de habilidades.

Refuerzan la percepción de los riesgos asociados con el manejo inadecuado de los datos y reducen...

La ocurrencia de incidentes resultantes de errores humanos sigue siendo responsable de una parte significativa.

de incidentes de seguridad registrados en organizaciones públicas y privadas.

Otro aspecto relevante se refiere a la integración entre la seguridad de la información y la gestión de riesgos.

Los programas de seguridad corporativa, en lugar de operar de forma aislada, deberían participar en...

procesos de planificación estratégica, evaluación de los impactos potenciales en los objetivos institucionales,

Continuidad de las operaciones, cumplimiento normativo y reputación organizacional. Esta integración

Favorece decisiones más equilibradas en cuanto a la priorización de inversiones y la aceptación de riesgos.

controles residuales y la definición de controles compatibles con el contexto de cada organización.

La creciente dependencia de proveedores especializados también ha aumentado la importancia de la gestión.

de los riesgos asociados a las cadenas de suministro digitales. Servicios en la nube, plataformas

empresas subcontratadas, proveedores de software, socios tecnológicos y empresas responsables de

El procesamiento de datos se ha integrado en ecosistemas altamente conectados, en los que

Las vulnerabilidades externas pueden tener un impacto significativo en la organización contratante.

Por lo tanto, procesos estructurados de evaluación de proveedores, auditorías periódicas y

La monitorización continua se ha convertido en un elemento esencial de la gobernanza de la seguridad.

Desde una perspectiva ejecutiva, los indicadores de desempeño adquieren un papel estratégico. Métricas

relacionado con la madurez de los controles, el tiempo de respuesta ante incidentes y el cumplimiento de las políticas.

Datos corporativos, resultados de auditorías, cumplimiento normativo y evolución del nivel de riesgo.

Proporcionan información relevante para respaldar las decisiones de la alta dirección. A diferencia de

Indicadores operativos utilizados tradicionalmente por equipos técnicos, estos instrumentos

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año V, vol. 2, 2024 | Envío: 16/02/2024 | Aceptado: 19/02/2024 | Publicación: 22/02/2024

Permiten traducir los riesgos tecnológicos en información comprensible para los gerentes responsables.
a través de la dirección estratégica de la organización.

La evolución de los entornos digitales también ha reforzado la necesidad de enfoques basados en
Mejora continua. Evaluaciones periódicas de madurez, revisiones de políticas institucionales,
Ejercicios de gestión de crisis, auditorías independientes y procesos de aprendizaje sistemáticos.
Las mejoras organizativas contribuyen a la mejora continua de los programas de seguridad, haciéndolos...
mayor adaptabilidad a los cambios tecnológicos y normativos.

Finalmente, se observa que la seguridad de la información ha llegado a desempeñar un papel relevante en la generación de
Valor institucional. Organizaciones capaces de demostrar un alto grado de madurez en la protección...
Sus activos informativos tienden a fortalecer las relaciones de confianza con clientes, inversores y...
socios estratégicos, ampliando su capacidad competitiva en mercados cada vez más orientados al mercado.
por datos. En este escenario, la seguridad deja de representar exclusivamente un centro de costos para
consolidarse como una inversión estratégica capaz de respaldar la innovación, el cumplimiento y
crecimiento sostenible.

5. Liderazgo ejecutivo y toma de decisiones basada en datos

La consolidación de la economía digital ha alterado significativamente el papel del liderazgo en las organizaciones.
La creciente disponibilidad de información, junto con el avance de las plataformas analíticas y...
La inteligencia artificial ha ampliado la capacidad de las empresas para comprender su entorno empresarial.
y responder más rápidamente a los cambios del mercado. En este contexto, la toma de decisiones
La toma de decisiones basada en datos ya no representa una ventaja competitiva.
Es circunstancial, pero se está convirtiendo en un componente esencial de la estrategia corporativa.
Esta transformación exige que los ejecutivos desarrollen habilidades que vayan más allá de los conocimientos básicos.
gestión tradicional. Comprender los principios relacionados con la gobernanza de
La información, la protección de datos, la ciberseguridad y la inteligencia artificial están ahora integradas en...
un conjunto de habilidades necesarias para guiar las inversiones, evaluar los riesgos y establecer
Prioridades organizativas. El rol del liderazgo ya no se centra exclusivamente en la gestión.
financiera y operativa, incorporando responsabilidades relacionadas con un uso ético, seguro y eficaz.
gestión estratégica de activos de información.

La madurez digital de las organizaciones está directamente relacionada con su capacidad para integrar datos.
Información procedente de diferentes áreas de negocio en procesos de toma de decisiones coherentes.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año V, vol. 2, 2024 | Envío: 16/02/2024 | Aceptado: 19/02/2024 | Publicación: 22/02/2024

producido por sistemas corporativos, plataformas de relaciones con el cliente, indicadores
Las tecnologías financieras, los sensores industriales y los entornos digitales permiten una visión más completa.
del desempeño institucional. Sin embargo, la mera disponibilidad de estos datos no garantiza
mejores decisiones. Su eficacia depende de la existencia de mecanismos de gobernanza capaces de
Para garantizar la calidad, la fiabilidad y el contexto en la interpretación de la información.
En este escenario, la inteligencia empresarial, el análisis de datos y la inteligencia artificial desempeñan papeles clave.
Complementario. Si bien las plataformas analíticas ofrecen apoyo para identificar tendencias.
y patrones de comportamiento, los modelos de IA amplían la capacidad predictiva de las organizaciones y
Ayudan a simular escenarios complejos. Sin embargo, el uso de estas tecnologías debe
permanecer subordinado a los objetivos estratégicos definidos por la dirección, evitando que se tomen decisiones indiscriminadamente.
Los procesos automatizados sustituyen el análisis crítico necesario para la gestión organizacional.
Acción integrada entre el Consejo de Administración, el Director Ejecutivo (CEO), el Director
Director de Información (CIO), Director de Seguridad de la Información (CISO) y Persona a Cargo de
El responsable de protección de datos (DPO) se ha convertido en uno de los principales indicadores de madurez en
Gobierno corporativo. La coordinación entre estas funciones fomenta una mayor alineación con la innovación.
objetivos tecnológicos, de gestión de riesgos, de cumplimiento normativo e institucionales, reduciendo la
Fragmentación de las decisiones relacionadas con la transformación digital.
Otro elemento relevante se refiere al establecimiento de indicadores capaces de traducir
Información técnica en métricas comprensibles para la alta dirección. Indicadores clave de rendimiento de
Indicadores de rendimiento (KPI) e indicadores clave de riesgo (KRI) relacionados con la calidad de los datos,
cumplimiento normativo, madurez de la gobernanza, protección de la privacidad y eficiencia
Los datos operativos proporcionan apoyo objetivo para monitorear el desarrollo institucional y para
Definir las prioridades estratégicas.
La sostenibilidad de las organizaciones digitales también depende de la consolidación de una cultura.
impulsado por los datos. Esta transformación no proviene exclusivamente de la adopción de nuevas tecnologías,
pero también la capacidad institucional para incorporar evidencia objetiva en los procesos de planificación,
Innovación y toma de decisiones. Entornos organizativos que fomentan la transparencia.
El intercambio responsable de información y el aprendizaje continuo presentan mayores ventajas.
Capacidad para adaptarse a los cambios normativos, tecnológicos y de mercado.
Finalmente, se observa que el liderazgo contemporáneo ahora desempeña un papel integrador entre
Tecnología, gobernanza y estrategia. La capacidad de transformar datos en conocimiento fiable.
Promover la innovación de forma responsable y equilibrar las oportunidades con los riesgos se ha convertido en un factor clave.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año V, vol. 2, 2024 | Envío: 16/02/2024 | Aceptado: 19/02/2024 | Publicación: 22/02/2024

crucial para las organizaciones que buscan competitividad en un entorno caracterizado por
Rápida evolución tecnológica y creciente dependencia de los activos de información.

CONCLUSIÓN

La creciente importancia de la información en las actividades económicas e institucionales ha redefinido la forma
Cómo las organizaciones estructuran sus procesos de gestión, innovación y creación de valor. En un
un entorno marcado por la intensificación de la transformación digital y la expansión de la inteligencia artificial.
Artificial y mediante el fortalecimiento de los requisitos reglamentarios relacionados con la protección de datos, la
La gobernanza de la información se está consolidando como un elemento estratégico para la sostenibilidad.
organizativo.

El análisis desarrollado en este estudio muestra que la seguridad de la información, la privacidad de los datos,
El gobierno corporativo y la dirección ejecutiva son dimensiones interdependientes de una misma entidad.
sistema de gestión. La efectividad de estas iniciativas no depende exclusivamente de la implementación de
tecnologías especializadas, pero también la construcción de estructuras organizativas capaces de integrar
políticas institucionales, procesos de toma de decisiones, responsabilidades y mecanismos claramente definidos
Estrategias de seguimiento permanente y mejora continua.

Se observó que la calidad de la información tiene una influencia directa en la capacidad de
Las organizaciones desarrollan modelos analíticos fiables e implementan soluciones basadas en
Inteligencia artificial y la satisfacción de las crecientes demandas relacionadas con la transparencia y
cumplimiento normativo. En este contexto, los programas de gobernanza de la información dejan de ser
tener un carácter puramente administrativo para poder asumir un papel decisivo en la creación de valor.
institucional y en la reducción de los riesgos asociados al uso de activos digitales.

La evolución de las tecnologías de Inteligencia Artificial introduce nuevos desafíos relacionados con
transparencia algorítmica, mitigación de sesgos, supervisión humana y rendición de cuentas por
Decisiones automatizadas. Estos aspectos demuestran que la innovación tecnológica debe ser...
acompañado de mecanismos de gobernanza robustos capaces de garantizar un equilibrio entre
Eficiencia operativa, protección de los derechos fundamentales y responsabilidad corporativa.

Otro aspecto que se destaca a lo largo de este trabajo se refiere a la importancia de la participación de las personas mayores.
Gestión en la implementación de estrategias de gobernanza de la información. Integración entre consejos de administración.
administración, ejecutivos, áreas tecnológicas, seguridad de la información y protección de datos

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año V, vol. 2, 2024 | Envío: 16/02/2024 | Aceptado: 19/02/2024 | Publicación: 22/02/2024

Fortalece la capacidad institucional para responder a las transformaciones del entorno digital, promoviendo
Mayor alineación entre los objetivos estratégicos, la innovación y la gestión de riesgos.

Aunque este estudio se desarrolló a través de una revisión de la literatura, las referencias
Los análisis muestran una convergencia en cuanto a la necesidad de tratar la información como un activo.
Estratégico para las organizaciones. La madurez de la gobernanza de la información comienza a reflejar no solo
el nivel de cumplimiento normativo alcanzado por la institución, pero también su capacidad de innovar,
para preservar la confianza de diferentes públicos y respaldar las decisiones basadas en datos.
confiable.

En cuanto a las perspectivas para futuras investigaciones, se recomienda seguir investigando temas relacionados.
Impacto de la inteligencia artificial generativa en la gobernanza corporativa y la regulación.
sistemas inteligentes internacionales, hasta modelos de gobernanza para ecosistemas digitales.
distribuido y al uso de métricas capaces de medir el retorno estratégico de la inversión.
en gobernanza de la información y protección de la privacidad.

Entendemos, por lo tanto, que la gobernanza de la información corporativa representa uno de los principales
pilares de las organizaciones basadas en datos. Al integrar la seguridad de la información, la privacidad,
La inteligencia artificial, la gestión de riesgos y el liderazgo ejecutivo hacen posible la creación de entornos.
más transparente, resiliente, innovador y preparado para afrontar los desafíos tecnológicos,
Factores regulatorios y competitivos que caracterizan la economía digital contemporánea.

REFERENCIAS

- GIL, AC Cómo Desarrollar Proyectos de Investigación. 6ª edición. São Paulo: Atlas, 2019.

Gobernanza de la información y los datos

- DAMA INTERNATIONAL. DAMA-DMBOK: Cuerpo de conocimientos sobre gestión de datos. 2.ª ed. Bradley Beach: Technics Publications, 2017.
- WEILL, P.; ROSS, JW. Gobernanza de TI: Cómo las empresas de alto rendimiento gestionan los derechos de decisión en TI para obtener resultados superiores. Boston: Harvard Business School Press, 2004.
- DAVENPORT, TH. Competir con análisis: La nueva ciencia del éxito. Boston: Harvard Business School Press, 2007.
- REDMAN, TH. Datos orientados: Cómo obtener beneficios de su activo empresarial más importante. Boston: Harvard Business Review Press, 2008.

Seguridad y gestión de la información

- WHITMAN, ME; MATTORD, HJ Principios de seguridad de la información. 7.ª ed. Boston: Cengage Learning, 2022.
- ISACA. Marco COBIT 2019: Gobernanza y objetivos de gestión. Schaumburg: ISACA, 2019.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año V, vol. 2, 2024 | Envío: 16/02/2024 | Aceptado: 19/02/2024 | Publicación: 22/02/2024

- ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información: requisitos.
- ISO/IEC 27701:2019. Gestión de la información de privacidad.
- ISO/IEC 38500:2015. Gobernanza de las TI para la organización.

Privacidad e inteligencia artificial

- NIST. Marco de gestión de riesgos de inteligencia artificial (AI RMF 1.0). Gaithersburg: Instituto Nacional de Estándares y Tecnología, 2023.
- NIST. Marco de Ciberseguridad (CSF 2.0). Gaithersburg: Instituto Nacional de Estándares y Tecnología. Tecnología, 2024.
- OCDE. Recomendación del Consejo sobre Inteligencia Artificial. París: Organización para la Cooperación y el Desarrollo Económicos (OCDE). Cooperación y Desarrollo Económicos, 2019.
- BRASIL. Ley n.º 13.709, de 14 de agosto de 2018. Ley General de Protección de Datos Personales (LGPD).
- REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Reglamento General de Protección de Datos (RGPD).

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.