

MUST UNIVERSITY
MASTER IN BUSINESS ADMINISTRATION

ELIEZER JAFET JURADO YELA

**Propuesta de un modelo estratégico de protección de datos
mediante Inteligencia de Negocios en la implementación de ERP**

FLORIDA – USA
2024

ELIEZER JAFET JURADO YELA

**Propuesta de un modelo estratégico de protección de datos
mediante Inteligencia de Negocios en la implementación de ERP**

Trabajo de Conclusión Final presentado como
requisito parcial para la obtención del título de
MAESTRÍA en el Curso de MASTER IN
BUSINESS ADMINISTRATION de MUST
UNIVERSITY – Florida USA.

Orientador(a): Prof. Dr. Diego Fernando Cardona Madariaga

FLORIDA – USA
2024

MUST UNIVERSITY

LISTA DE FIGURAS

Ilustración 1 Modelo Estratégico	18
Ilustración 2 Fase de Implementación. Elaboración Propia	20

LISTA DE TABLAS

Tabla 1 Indicadores Claves. Elaboración Propia..... 23

LISTA DE ABREVIATURAS Y SIGLAS

BI - Business Intelligence (Inteligencia de Negocios)

ERP - Enterprise Resource Planning (Planificación de Recursos Empresariales)

GDPR - General Data Protection Regulation (Reglamento General de Protección de Datos)

CCPA - California Consumer Privacy Act (Ley de Privacidad del Consumidor de California)

KPI - Key Performance Indicator (Indicador Clave de Desempeño)

FAIR - Factor Analysis of Information Risk (Análisis de Factores de Riesgo de Información)

ROI - Return on Investment (Retorno de la Inversión)

ISO - International Organization for Standardization (Organización Internacional de Normalización)

LEF - Loss Event Frequency (Frecuencia de Eventos de Pérdida)

LM - Loss Magnitude (Magnitud de la Pérdida)

RESUMEN

El objetivo de esta investigación fue desarrollar un modelo estratégico que integre la Inteligencia de Negocios (BI) con sistemas de planificación de recursos empresariales (ERP) para optimizar la protección de datos y garantizar el cumplimiento normativo en empresas en proceso de digitalización. El estudio se centró en identificar vulnerabilidades críticas en la implementación de ERP, evaluar el rol de BI en la gestión de riesgos de seguridad y definir indicadores clave para medir la efectividad del modelo propuesto.

Se utilizó un enfoque teórico-documental basado en una revisión exhaustiva de literatura académica y regulaciones internacionales relevantes, complementado con el análisis de casos y metodologías reconocidas para la gestión de riesgos y protección de datos. Este método permitió establecer un marco conceptual sólido y proponer métricas específicas que guían la implementación del modelo estratégico.

Los resultados destacan que la integración de herramientas BI en sistemas ERP proporciona monitoreo en tiempo real, análisis predictivo y automatización de reportes, lo que reduce significativamente las vulnerabilidades de seguridad y mejora el cumplimiento normativo. Asimismo, los indicadores propuestos, como la tasa de incidentes prevenidos y el porcentaje de datos cifrados, permiten una evaluación continua del impacto del modelo.

En conclusión, el modelo estratégico desarrollado representa una solución innovadora y adaptable que no solo mitiga riesgos, sino que también incrementa la eficiencia operativa y la competitividad empresarial, proporcionando un enfoque integral para la transformación digital segura en las organizaciones.

Palabras clave: Negocios. Datos. ERP. Cumplimiento. Seguridad.

ABSTRACT

The objective of this research was to develop a strategic model that integrates Business Intelligence (BI) with Enterprise Resource Planning (ERP) systems to optimise data protection and ensure regulatory compliance in companies undergoing digital transformation. The study focused on identifying critical vulnerabilities during ERP implementation, evaluating the role of BI in risk management, and defining key performance indicators to measure the effectiveness of the proposed model.

A theoretical-documentary approach was employed, based on an extensive review of academic literature and relevant international regulations, complemented by the analysis of case studies and recognised methodologies for risk management and data protection. This method enabled the establishment of a solid conceptual framework and the proposal of specific metrics to guide the implementation of the strategic model.

The results highlight that the integration of BI tools into ERP systems provides real-time monitoring, predictive analysis, and automated reporting, significantly reducing security vulnerabilities and improving regulatory compliance. Additionally, the proposed indicators, such as the rate of prevented incidents and the percentage of encrypted data, allow continuous evaluation of the model's impact.

In conclusion, the developed strategic model represents an innovative and adaptable solution that not only mitigates risks but also increases operational efficiency and business competitiveness, providing an integral approach for secure digital transformation in organizations.

Keywords: Business. Data. ERP. Compliance. Security.

Propuesta de un modelo estratégico de protección de datos mediante Inteligencia de Negocios en la implementación de ERP

Eliezer Jafet Jurado Yela

SUMARIO

1.	INTRODUCCIÓN	9
1.1.	Problema de Investigación	9
1.2.	Justificación	10
1.3.	Objetivos de la Investigación	11
1.3.1.	Objetivo general	11
1.3.2.	Objetivo específico	11
2.	MARCO TEÓRICO	12
2.1.	Inteligencia de Negocio (BI)	12
2.2.	Protección de Datos y Privacidad	12
2.3.	Implementación de Sistemas ERP	13
2.4.	Relación entre BI y Protección de Datos en ERP	14
2.5.	Normativas y Regulaciones en Protección de Datos	14
4.	DESARROLLO DEL MODELO	17
4.1.	Componentes del Modelo Estratégico	18
4.2.	Fases de Implementación	19
4.2.1.	Diagnóstico inicial	20
4.2.2.	Diseño del modelo estratégico	21
4.2.3.	Ejecución piloto	21
4.2.4.	Escalamiento y seguimiento	22
6.	Consideraciones Finales	24
6.1.	Relevancia de la Propuesta	24
6.2.	Aportes al Conocimiento	24
6.3.	Limitaciones del Estudio	25
6.4.	Recomendaciones	25
6.5.	Conclusión	25
7.	Referencias Bibliográficas	27

1. INTRODUCCIÓN

1.1. Problema de Investigación

En el entorno empresarial actual, donde los datos son uno de los activos más valiosos, muchas organizaciones enfrentan serias dificultades para garantizar la protección y seguridad de la información dentro de sus sistemas de planificación de recursos empresariales (ERP). La implementación de ERP permite la centralización y automatización de procesos, lo que aumenta la eficiencia operativa; sin embargo, también amplifica la exposición a riesgos de seguridad y vulnerabilidades cibernéticas, especialmente si no se aplican estrategias sólidas de protección de datos.

Esta problemática se agrava debido a las exigencias de cumplimiento normativo, como el Reglamento General de Protección de Datos (GDPR), que impone estrictos controles sobre la gestión y seguridad de la información. Aunque la Inteligencia de Negocios (BI) tiene un gran potencial para mejorar la visibilidad de los datos y facilitar la toma de decisiones en tiempo real, todavía existe una notable carencia de orientación sobre cómo integrarla efectivamente en la protección de datos a lo largo de cada etapa de implementación de un ERP.

La falta de un enfoque claro sobre la manera en que la Inteligencia de Negocios puede reforzar la seguridad de los datos, mitigar riesgos cibernéticos y garantizar el cumplimiento normativo durante la implementación de sistemas ERP, representa un vacío significativo. Esto plantea la necesidad urgente de investigar y desarrollar estrategias que permitan a las organizaciones enfrentar estos desafíos de manera eficaz y segura.

1.2. Justificación

La creciente digitalización de las empresas y el volumen masivo de datos generados a diario han hecho que la protección de datos sea una prioridad crítica en cualquier organización. En particular, la implementación de sistemas ERP (Planificación de Recursos Empresariales), que centralizan y gestionan procesos clave, incrementa significativamente la exposición a riesgos de seguridad y privacidad de datos. En este contexto, surge la necesidad de estrategias más robustas y eficientes que aseguren la integridad de la información en todas las etapas de la implementación de ERP.

La Inteligencia de Negocios (BI), como conjunto de tecnologías y prácticas enfocadas en el análisis de datos, tiene un papel fundamental en la toma de decisiones estratégicas y en la optimización del uso de la información dentro de las organizaciones. A pesar de su amplio uso para la mejora de procesos empresariales, se ha explorado menos su potencial en el ámbito de la protección de datos durante la implementación de ERP.

Este estudio es necesario para llenar el vacío en la literatura actual, investigando cómo la Inteligencia de Negocios puede convertirse en una herramienta clave para fortalecer la seguridad de los datos en la implementación de ERP, minimizando riesgos cibernéticos y asegurando el cumplimiento de normativas internacionales de protección de datos, como el GDPR o el CCPA.

El impacto práctico de esta investigación radica en que ofrecerá un marco que permita a las organizaciones optimizar sus estrategias de protección de datos mediante BI, lo cual no solo mejorará la seguridad de la información, sino que también aumentará la eficiencia operativa y reducirá las vulnerabilidades. Esto no solo aporta valor a las empresas, sino que también contribuye a la seguridad en la economía digital global.

1.3. Objetivos de la Investigación

1.3.1. Objetivo general

Desarrollar un esquema preliminar para la integración de la Inteligencia de Negocios (BI) en sistemas ERP, con el fin de optimizar la protección de datos y asegurar el cumplimiento normativo en entornos empresariales.

1.3.2. Objetivo específico

1. Identificar las vulnerabilidades críticas en la protección de datos que ocurren durante la implementación de un sistema ERP, con el fin de definir los componentes clave que el marco estratégico debe abordar para garantizar la seguridad de la información.
2. Evaluar el papel de la Inteligencia de Negocios en la mejora de la toma de decisiones en la gestión de riesgos de protección de datos, explorando cómo las herramientas de BI pueden integrarse eficazmente en el proceso de implementación de un ERP.
3. Definir un conjunto básico de indicadores de éxito que permita evaluar la efectividad de la integración de BI en la protección de datos durante la implementación de ERP, estableciendo métricas preliminares para medir la seguridad de la información y el cumplimiento normativo.

2. MARCO TEÓRICO

2.1. Inteligencia de Negocio (BI)

La Inteligencia de Negocios (BI) se ha consolidado como una herramienta estratégica clave para transformar datos en información valiosa que facilite la toma de decisiones empresariales. BI permite analizar grandes volúmenes de datos provenientes de diversas fuentes, integrándolos en sistemas que generan dashboards interactivos y análisis predictivos. Según (Hernández Silva, Estrategias para la Implementación Efectiva de Soluciones de Inteligencia de Negocios Basadas en Big Data, 2023), su implementación contribuye a optimizar operaciones, mejorar la eficiencia y fortalecer la seguridad en los procesos organizacionales.

La capacidad de la BI para identificar patrones y anomalías en tiempo real la posiciona como un componente esencial en entornos de alta complejidad, como los sistemas ERP. A través de la visualización de indicadores clave de desempeño (KPIs), es posible monitorear aspectos críticos relacionados con el acceso, la integridad y el uso de la información. Esto refuerza la capacidad de las organizaciones para anticiparse a incidentes de seguridad y cumplir con normativas internacionales.

2.2. Protección de Datos y Privacidad

La protección de datos y la privacidad son componentes esenciales en el manejo de información sensible dentro de las organizaciones. En un entorno digital donde los datos son un activo estratégico, garantizar su integridad y confidencialidad se convierte en un imperativo. Regulaciones internacionales como el GDPR y la CCPA han establecido estándares rigurosos

que obligan a las empresas a implementar medidas de seguridad robustas en todos los niveles de operación.

El enfoque moderno de protección de datos incluye el uso de herramientas avanzadas como el cifrado, controles de acceso basados en roles y auditorías automatizadas. Según (Molina Marin & Orozco, 2020), estos mecanismos permiten mitigar riesgos de seguridad y asegurar la privacidad en cada etapa del ciclo de vida de la información. La incorporación de tecnologías analíticas y de monitoreo continuo fortalece aún más la capacidad de las organizaciones para adaptarse a un entorno regulatorio en constante evolución.

2.3. Implementación de Sistemas ERP

La adopción de sistemas ERP implica centralizar procesos operativos y de datos en una única plataforma integrada, lo que representa tanto una ventaja estratégica como un desafío en términos de seguridad. Durante su implementación, es crucial garantizar que los datos almacenados y procesados cumplan con estándares de calidad y seguridad, minimizando vulnerabilidades que puedan comprometer su integridad.

El éxito de un ERP depende de la alineación entre los objetivos de negocio y las estrategias tecnológicas. (Molina Marin & Orozco, 2020) destacan la importancia de establecer políticas claras de gobernanza de datos y capacitar al personal para gestionar los riesgos asociados a la centralización de información. Adicionalmente, la integración de herramientas analíticas desde las primeras etapas del proyecto puede optimizar la supervisión y el control del sistema, asegurando un manejo seguro y eficiente de los datos.

2.4. Relación entre BI y Protección de Datos en ERP

La combinación de BI con sistemas ERP representa una solución poderosa para gestionar datos de manera segura y estratégica. Mientras que los ERP centralizan la información, BI proporciona las herramientas necesarias para analizarla, detectando patrones y posibles riesgos en tiempo real. Según (Serrano, 2023), esta sinergia no solo mejora la eficiencia operativa, sino que también fortalece el cumplimiento normativo mediante la creación de alertas tempranas y el monitoreo continuo de los accesos a la información.

La implementación de sistemas integrados que combinen estas tecnologías facilita el diseño de estrategias preventivas, permitiendo a las organizaciones responder rápidamente a amenazas cibernéticas y asegurar la privacidad de los datos. Además, el uso de dashboards especializados en riesgos y conformidad fortalece la toma de decisiones informadas, alineadas con los estándares internacionales de protección de datos.

2.5. Normativas y Regulaciones en Protección de Datos

El marco normativo global, liderado por regulaciones como el Reglamento General de Protección de Datos (GDPR) y la Ley de Privacidad del Consumidor de California (CCPA), establece requisitos claros sobre el manejo responsable de la información. Estas normativas no solo buscan proteger los derechos de los usuarios, sino también fomentar la transparencia y responsabilidad en las prácticas empresariales.

El GDPR exige implementar medidas técnicas y organizativas que aseguren un nivel adecuado de protección, incluyendo el derecho al acceso, rectificación y eliminación de datos. Por su parte, la CCPA otorga a los consumidores un mayor control sobre su información personal. El cumplimiento de estas regulaciones requiere de herramientas tecnológicas que monitoreen y

auditen el manejo de datos, garantizando la seguridad en cada etapa del proceso. Estas normativas se convierten así en un punto de partida esencial para cualquier estrategia de protección de datos.

3. METODOLOGÍA

3.1. Tipo de Investigación

Este proyecto es de carácter teórico y se enmarca en una revisión bibliográfica-documental, centrada en el análisis de la literatura existente y los estudios previos sobre la Inteligencia de Negocios (BI), protección de datos, y la implementación de sistemas ERP. El enfoque bibliométrico será utilizado para identificar patrones y tendencias relevantes en las publicaciones sobre estos temas, mientras que los relatos de experiencia, presentes en estudios de caso y análisis de implementación en el ámbito empresarial, proporcionarán perspectivas prácticas sin la participación directa de personas.

3.2. Fuentes de Información

- Investigación Documental

La metodología empleará una revisión de la literatura académica, documentos técnicos y reportes de organismos especializados. Se recopilarán artículos de revistas científicas, tesis académicas, libros, informes de consultoras y publicaciones de instituciones especializadas en BI y ERP, priorizando fuentes recientes y de alta confiabilidad.

- Fuentes Primarias y Secundarias:

Fuentes Primarias: En este caso, se considerarán fuentes primarias los estudios originales y las investigaciones de expertos en BI y ERP que presentan datos originales y conclusiones

fundamentadas en el análisis empírico, aunque no se involucrará la recolección de datos de campo.

Fuentes Secundarias: La investigación se complementará con fuentes secundarias, como revisiones de la literatura, estudios de casos documentados y análisis bibliográficos sobre la integración de BI y la protección de datos en sistemas ERP. Estas fuentes proporcionarán un contexto amplio y detallado sobre el estado actual del conocimiento en este campo.

3.3. Procedimientos de Recolección y Análisis de Datos

La recolección de datos se basará en la búsqueda sistemática de literatura en bases de datos académicas (como Google Scholar, Scopus y JSTOR) y sitios de referencia especializados en tecnología y seguridad de la información (como IEEE Xplore y ScienceDirect). Para seleccionar el material, se aplicarán criterios de inclusión y exclusión específicos, priorizando documentos publicados en los últimos cinco años que aborden la relación entre BI, ERP y protección de datos.

El análisis de datos se centrará en la sistematización de información para identificar patrones comunes, tendencias en la investigación, y hallazgos significativos que contribuyan al desarrollo del marco teórico y a la formulación de un esquema preliminar de prácticas recomendadas.

3.4. Métodos de Evaluación

Se utilizará un enfoque de análisis cualitativo para evaluar la información recopilada. El estudio comparará los enfoques teóricos y prácticos presentes en la literatura, identificando puntos de convergencia y disonancia en las soluciones propuestas para la protección de datos en sistemas ERP mediante BI. Los estudios de caso y las experiencias documentadas permitirán evaluar el impacto de distintas prácticas y enfoques sobre la seguridad y el cumplimiento normativo.

3.5. Herramientas y Técnicas para el Análisis de Datos

Para el análisis bibliométrico, se utilizarán herramientas como VOSviewer o Bibliometrix, que permiten visualizar redes de co-ocurrencia de términos, autores y temas recurrentes en la literatura científica. Además, el uso de software de gestión de referencias como Mendeley o Zotero facilitará la organización de las fuentes, la extracción de datos y la creación de citas y referencias de manera coherente y precisa. Estas herramientas asegurarán que la información recopilada esté debidamente organizada y que se pueda acceder a ella de forma rápida y eficiente para elaborar un análisis exhaustivo y estructurado del tema en estudio.

4. DESARROLLO DEL MODELO

El avance de la digitalización ha llevado a las empresas a implementar sistemas de planificación de recursos empresariales (ERP) para centralizar procesos y mejorar la eficiencia operativa. Sin embargo, esta centralización incrementa los riesgos de seguridad de datos, exponiendo a las organizaciones a posibles brechas y sanciones regulatorias. La integración de Inteligencia de Negocios (BI) en estos sistemas no solo fortalece la toma de decisiones, sino que también ofrece una oportunidad única para optimizar la protección de datos y garantizar el cumplimiento normativo.

Esta propuesta presenta un modelo estratégico diseñado para abordar las vulnerabilidades críticas de la implementación de ERP, utilizando herramientas de BI para monitorear, proteger y gestionar la información sensible. A través de un enfoque estructurado, se busca proporcionar a las empresas un marco práctico que garantice la seguridad y la privacidad de los datos en entornos altamente regulados.

4.1. Componentes del Modelo Estratégico



Ilustración 1 Modelo Estratégico

1. Gobernanza de Datos

- Clasificación y segmentación de datos sensibles según su importancia y nivel de exposición.
- Establecimiento de políticas claras de acceso y manejo de datos, basadas en estándares internacionales como ISO/IEC 27001.

2. Inteligencia de Negocios

- Implementación de herramientas BI para monitorear en tiempo real la seguridad de datos.
- Diseño de dashboards interactivos con métricas clave como incidentes detectados, acceso no autorizado y cumplimiento normativo.

3. Gestión de Riesgos

- Identificación y priorización de vulnerabilidades críticas durante las fases de implementación del ERP.
- Integración de análisis predictivos para anticipar posibles amenazas.

4. Cumplimiento Normativo

- Alineación con regulaciones internacionales como GDPR y CCPA.
- Automatización de auditorías internas y generación de reportes regulatorios.

4.2. Fases de Implementación

La fase de implementación del modelo estratégico propuesto se estructura en una serie de pasos progresivos diseñados para garantizar la integración eficiente de la Inteligencia de Negocios (BI) con los sistemas ERP, optimizando la protección de datos y asegurando el cumplimiento normativo. Esta fase comprende cuatro etapas principales: diagnóstico inicial, diseño del modelo, ejecución piloto y escalamiento.

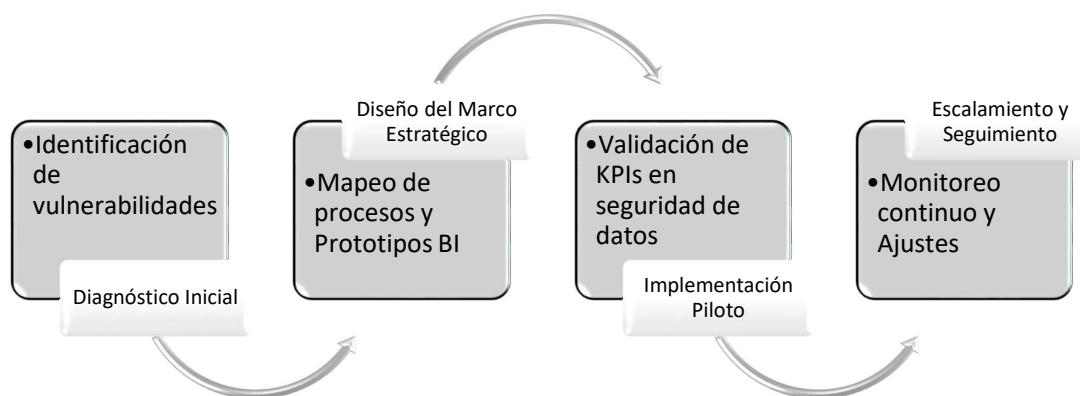


Ilustración 2 Fase de Implementación. Elaboración Propia

4.2.1. Diagnóstico inicial

El objetivo de esta etapa es evaluar el estado actual de la infraestructura tecnológica y de los procesos de gestión de datos en la organización, identificando brechas y vulnerabilidades críticas.

Actividades clave:

- Realizar entrevistas con las partes interesadas para comprender los flujos de datos y las políticas actuales de seguridad. Analizar el estado de cumplimiento con normativas como GDPR o CCPA.
- Identificar los riesgos asociados con la implementación del ERP, clasificándolos por su impacto y probabilidad.

Resultados esperados:

- Informe detallado del estado actual de la seguridad de los datos y el cumplimiento normativo.
- Lista priorizada de riesgos y vulnerabilidades que el modelo debe abordar.

4.2.2. Diseño del modelo estratégico

En esta etapa, se configura el marco estratégico que será implementado en la organización. Esto incluye la definición de procesos, herramientas y métricas para monitorear la seguridad de los datos.

Actividades clave:

- Configurar dashboards de BI que integren los indicadores clave de desempeño (KPIs).
- Establecer políticas de acceso a los datos basadas en roles y niveles de autorización.
- Diseñar protocolos de respuesta a incidentes que incluyan acciones preventivas y correctivas.

Resultados esperados:

- Plan de implementación detallado del modelo estratégico.
- Prototipos de dashboards y reportes automatizados.

4.2.3. Ejecución piloto

Esta etapa consiste en probar el modelo en un entorno controlado o en un área específica de la organización para validar su efectividad y realizar ajustes necesarios antes de su escalamiento.

Actividades clave:

- Implementar el modelo estratégico en una unidad de negocio o proceso específico.
- Monitorear los KPIs definidos para evaluar el impacto en tiempo real.
- Ajustar los procesos y herramientas en función de los resultados obtenidos.

Resultados esperados:

- Validación de la viabilidad del modelo en un entorno operativo.
- Recomendaciones para mejoras antes de la implementación a nivel organizacional.

4.2.4. Escalamiento y seguimiento

Tras la validación del piloto, el modelo se implementa en toda la organización, asegurando un monitoreo continuo y la capacidad de adaptación a nuevas necesidades o regulaciones.

Actividades clave:

- Extender el modelo a todas las áreas de la organización, integrando BI y ERP.
- Realizar auditorías periódicas para garantizar el cumplimiento de las normativas.
- Proporcionar capacitación continua al personal en el uso de herramientas BI y mejores prácticas en protección de datos.

Resultados esperados:

- Implementación completa del modelo estratégico.
- Monitoreo continuo de los KPIs y generación de reportes automatizados.
- Organización alineada con las normativas y con procesos seguros y optimizados

5. Indicadores Claves de Desempeño

Los indicadores clave permiten evaluar la efectividad del modelo en tiempo real:

Tabla 1 Indicadores Claves. Elaboración Propia

KPI	Descripción	Fórmula / Medición	Meta
Tasa de Incidentes Prevenidos	Porcentaje de amenazas detectadas y mitigadas frente al total identificado.	$Tasa = \frac{Incidentes\ Prevenidos}{Total\ de\ Incidentes\ Detectados} \times 100$	$\geq 85\%$
Tiempo de Respuesta a Incidentes	Tiempo promedio entre la detección y resolución de una brecha de seguridad.	$Tasa = \frac{Tiempo\ Total\ de\ Respuestas}{Número\ de\ Incidentes}$	≤ 24 horas
Porcentaje de Datos Cifrados	Proporción de datos sensibles protegidos mediante cifrado en tránsito y en reposo.	$\% = \frac{Datos\ Cifrados}{Total\ de\ Datos\ Sensibles} \times 100$	$\geq 90\%$
Cumplimiento Normativo	Nivel de conformidad del sistema ERP con normativas internacionales como GDPR o CCPA.	Evaluación mediante auditorías internas y externas.	$\geq 95\%$
Frecuencia de Auditorías Realizadas	Número de auditorías internas o externas completadas dentro de un periodo definido.	Numero de auditorías realizadas anualmente	4 auditorías/año

6. Consideraciones Finales

El desarrollo de este proyecto de investigación ha permitido abordar de manera integral los desafíos relacionados con la protección de datos en el contexto de la implementación de sistemas ERP, destacando el rol estratégico de la Inteligencia de Negocios (BI) como una solución innovadora y eficaz. A lo largo de este trabajo, se ha planteado una propuesta que combina prácticas avanzadas de seguridad, herramientas analíticas de BI y el cumplimiento de normativas internacionales, ofreciendo a las empresas un modelo estratégico adaptado a las exigencias del entorno digital actual.

6.1. Relevancia de la Propuesta

El modelo propuesto no solo responde a la necesidad crítica de proteger los datos en sistemas centralizados, sino que también permite a las organizaciones optimizar sus procesos de toma de decisiones mediante la integración de herramientas de BI. Al abordar las vulnerabilidades críticas y establecer indicadores clave para medir la efectividad de la implementación, se garantiza que las empresas puedan gestionar sus riesgos de manera proactiva, minimizando los costos asociados con incidentes de seguridad y maximizando el retorno de su inversión en tecnologías digitales.

6.2. Aportes al Conocimiento

Este proyecto contribuye al campo de la gestión de tecnología al proporcionar un marco teórico-práctico que conecta directamente la seguridad de los datos con la inteligencia de negocios, creando una sinergia que puede ser replicada en diferentes sectores industriales. Además, la metodología aplicada y los resultados esperados ofrecen una base para futuras investigaciones que profundicen en la relación entre BI, ERP y la protección de datos.

6.3. Limitaciones del Estudio

A pesar de los avances logrados, el alcance de este proyecto se limitó a un enfoque teórico-documental, lo que deja abierta la posibilidad de realizar estudios empíricos que validen y ajusten el modelo estratégico propuesto en escenarios reales. Asimismo, la aplicación de normativas como el GDPR y la CCPA puede variar según las particularidades legales y culturales de cada región, lo que implica que el modelo debe ser adaptado en cada caso.

6.4. Recomendaciones

Validación en Campo: Se recomienda implementar el modelo propuesto en empresas piloto para evaluar su efectividad en un entorno práctico, ajustando los indicadores clave según las necesidades específicas del sector.

Monitoreo Continuo: Las empresas deben establecer un sistema de revisión periódica del modelo para adaptarlo a nuevas amenazas cibernéticas y actualizaciones normativas.

Capacitación Constante: La formación de los equipos internos en BI y seguridad de datos es crucial para garantizar el éxito del modelo a largo plazo.

Investigaciones Futuras: Se sugiere explorar cómo otras tecnologías emergentes, como la inteligencia artificial y el aprendizaje automático, pueden complementar las capacidades de BI en la protección de datos.

6.5. Conclusión

El proyecto demuestra que la integración de Inteligencia de Negocios en la implementación de ERP no solo fortalece la protección de datos, sino que también genera valor estratégico para las empresas. Este modelo estratégico se presenta como una herramienta esencial para enfrentar los retos de la era digital, garantizando la seguridad de la información y el cumplimiento

normativo, al tiempo que impulsa la eficiencia operativa y la competitividad empresarial. Con esta base, se espera que las organizaciones puedan adoptar un enfoque más proactivo y sostenible en su transformación digital.

7. Referencias Bibliográficas

Álvarez Carrillo, P. A., Hernández Medina, M. Á., Bernal Agramón, M. d., & Muñoz Palma, M. (13 de abril de 2023). Universidad Nacional Autónoma de México, Facultad de Contaduría y Administración. doi:<http://dx.doi.org/10.22201/fca.24488410e.2023.4587>

Asamblea Legislativa del Estado de California. (2018). Obtenido de https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Ballard, C., Abdel-Hamid, A., Frankus, R., Hasegawa, F., Larrechart, J., Leo, P., & Ramos, J. (2006). *Improving Business Performance Insight with Business Intelligence and Business Process Management*.

Barahona, J. C., & Murillo, D. (2022). ¿Cómo lograr que las decisiones sean guiadas por datos?: Una guía práctica para implementar su proyecto de inteligencia de negocios. *INCAE Business Review*, 3(3), 75-83. Obtenido de <https://research.ebsco.com/c/m2vuqh/viewer/pdf/sed4qj63qz>

California State Legislature (o Asamblea Legislativa de California). (2018). *Código Civil de California*. Obtenido de <https://oag.ca.gov/privacy/ccpa>

Gesto, M. (24 de may. de 2018). *Deloitte*. Obtenido de <https://www.deloitte.com/es/es/services/risk-advisory/perspectives/gdpr-retos.html>

Hernández Silva, J. D. (2023). *Estrategias para la Implementación Efectiva de Soluciones de Inteligencia de Negocios Basadas en Big Data*. Obtenido de <https://revistas.udistrital.edu.co/index.php/vinculos/article/view/16887>

Hernández Silva, J. D. (04 de 10 de 2023). *Universidad Distrital San Francisco José de Caldas*. Obtenido de <https://revistas.udistrital.edu.co/index.php/vinculos/article/view/16887>

Molina Marin, Y., & Orozco, L. G. (2020). Vulnerabilidades de los Sistemas de Información: una revisión. *Tecnológico de Antioquia, Institución Universitaria*. Obtenido de <https://dspace.tdea.edu.co/handle/tdea/1398>

Parlamento Europeo y Consejo de la Unión Europea. (27 de abril de 2016). *Diario Oficial de la Unión Europea*. Obtenido de <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679>

SAP. (2023). *SAP*. Obtenido de <https://www.sap.com/latinamerica/insights/erp-security.html>

Serrano, V. (11 de abril de 2023). *DATATEC*. Obtenido de <https://www.datadec.es/blog/el-bi-el-complemento-perfecto-de-un-erp>

Wolters Kluwer TAA España. (11 de 08 de 2024). *Business intelligence: qué es y cómo integrarla en tu ERP*. Obtenido de Wolters Kluwer: <https://www.wolterskluwer.com/es-es/expert-insights/business-intelligence-que-es-bi>