UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA DE COMPUTACIÓN

PROPUESTA DE UNA MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN UN NEGOCIO FIDUCIARIO DANDO CUMPLIMIENTO A LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL ECUADOR USANDO UNA PRUEBA DE CONCEPTO Y PROPONIENDO UNA CONTRAMEDIDA

Trabajo de titulación previo a la obtención del
Título de Ingeniero en Ciencias de la Computación

AUTOR: ALEX LEONARDO CATOTA ALOMOTO

TUTOR: JOSÉ LUIS AGUAYO MORALES

Quito - Ecuador
2025

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Alex Leonardo Catota Alomoto con documento de identificación N°1719938035 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total parcial el presente trabajo de titulación.

Quito, 24 de febrero de 2025

Atentamente,

_____

Alex Leonardo Catota Alomoto
1719938035

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Alex Leonardo Catota Alomoto con documento de identificación N° 1719938035, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del Artículo Académico: "Propuesta de una mejora de la seguridad de la información en un negocio fiduciario dando cumplimiento a la ley de protección de datos personales en el Ecuador usando una prueba de concepto y proponiendo una contramedida", el cual ha sido desarrollado para optar por el título de: Ingeniero en Ciencias de la Computación, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad PolitécnicaSalesiana.

Quito, 24 de febrero de 2025

Atentamente,

_____

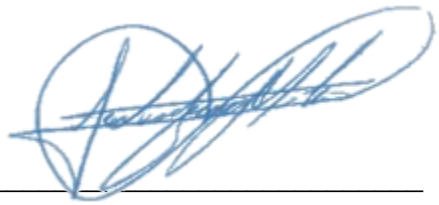
Alex Leonardo Catota Alomoto
1719938035

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, José Luis Aguayo Morales con documento de identificación N° 1709562597, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: PROPUESTA DE UNA MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN UN NEGOCIO FIDUCIARIO DANDO CUMPLIMIENTO A LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL ECUADOR USANDO UNA PRUEBA DE CONCEPTO Y PROPONIENDO UNA CONTRAMEDIDA, realizado por Alex Leonardo Catota Alomoto con documento de identificación N°1719938035, obteniendo como resultado final el trabajo de titulación bajo la opción de Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 24 de febrero de 2025

Atentamente,



Ing. José Luis Aguayo Morales, MSc.
1709562597

Artículo Académico / Academic paper

PROPUESTA DE UNA MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN UN NEGOCIO FIDUCIARIO DANDO CUMPLIMIENTO A LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL ECUADOR USANDO UNA PRUEBA DE CONCEPTO Y PROPONIENDO UNA CONTRAMEDIDA

PROPOSAL FOR AN IMPROVEMENT OF INFORMATION SECURITY IN A TRUST BUSNIESS COMPLYING WITH THE PERSONAL DATA PROTECTION LAW IN ECUADOR USING A PROOF OF CONCEPT AND PROPOSING A COUNTERMEASURE

Alex Catota - Alomoto[1], José Aguayo - Morales[2]

Resumen

La protección de la información personal es un aspecto crucial en la gestión moderna de la información, especialmente en el contexto digital. En Ecuador, la Ley Orgánica de Protección de Datos Personales (LOPDP) establece directrices claras para que las organizaciones aseguren la confidencialidad, integridad y disponibilidad de la información que manejan. Este marco legal resulta particularmente relevante para los negocios fiduciarios, los cuales tratan información altamente sensible relacionada con sus clientes, lo que los convierte en blancos prioritarios de ciberataques y riesgos de divulgación no autorizada de datos. Este trabajo propone un enfoque para fortalecer la seguridad de la información en los negocios fiduciarios de Ecuador mediante un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022. La propuesta abarca elementos esenciales como la formación constante del personal. Adicionalmente, se desarrolló una prueba de concepto que permita

Abstract

The protection of personal information is a crucial aspect of modern information management, especially in the digital context. In Ecuador, the Organic Law on Personal Data Protection (LOPDP) establishes clear guidelines for organisations to ensure the confidentiality, integrity and availability of the information they handle. This legal framework is particularly relevant for fiduciary businesses, which deal with highly sensitive information related to their clients, making them priority targets for cyber-attacks and risks of unauthorised disclosure of data. This paper proposes an approach to strengthen information security in Ecuadorian trust businesses through an Information Security Management System (ISMS) based on ISO/IEC 27001:2022. The proposal includes essential elements such as ongoing staff training. Additionally, a proof of concept was developed to validate the effectiveness of the proposed measures. The results showed 35% had adequate knowledge of LOPDP.

[1] Estudiante de la carrera de Computación, Universidad Politécnica Salesiana
[2] Docente de la carrera de Computación, Universidad Politécnica Salesiana

Autor para correspondencia: acatota74@gmail.com

validar la efectividad de las medidas propuestas. Los resultados mostraron 35% tenía un conocimiento adecuado de la LOPDP

Palabras Clave: Seguridad de la información, protección de datos personales, negocios fiduciarios, ISO 27001, contramedidas, prueba de concepto, LOPDP.

Keywords Information security, personal data protection, fiduciary business, ISO 27001, countermeasures, proof of concept, LOPDP.

1. Introducción

En un entorno global donde los datos personales representan uno de los activos más valiosos, garantizar su protección ha pasado a ser una necesidad fundamental para preservar la confianza y el cumplimiento normativo. Los negocios fiduciarios en Ecuador enfrentan retos particulares debido a la naturaleza altamente sensible de la información que administran, lo que los expone a una amplia gama de riesgos, incluyendo ciberataques, violaciones de datos y sanciones legales derivadas del incumplimiento de normativas locales e internacionales [1]. La LOPDP, vigente en Ecuador, establece lineamientos específicos para que las organizaciones adopten medidas rigurosas que garanticen la privacidad, precisión y accesibilidad de la información personal que gestionan [4].

El problema que se busca resolver radica principalmente en la ausencia de una ejecución adecuada de sistemas robustos de seguridad que permitan a los negocios fiduciarios no solo cumplir con la LOPDP, sino también reducir los riesgos importantes vinculados a la administración de datos sensible. Entre estos riesgos se incluyen la pérdida de reputación, costos legales, interrupciones operativas y posibles daños a los clientes. En la literatura especializada, se resaltan soluciones efectivas como la adopción del SGSI basados en estándares internacionales como la 27001. Este punto de referencia normativo ofrece una estructura completa y organizada para identificar, analizar y reducir riesgos., complementada con la implementación de controles técnicos, organizativos y humanos [1].

Estudios previos han demostrado que la aplicación de controles específicos es fundamental para reducir vulnerabilidades. Entre estos controles destacan la segmentación de redes, el uso de cifrado avanzado para asegurar la información durante su transmisión, su almacenamiento y la formación constante del personal en medidas de seguridad. Por ejemplo, experiencias documentadas en países como España y México han mostrado cómo la combinación de políticas organizacionales claras, tecnologías de última generación y programas de formación dirigidos puede aumentar significativamente el nivel de seguridad en las organizaciones [2][3]. Sin embargo, en el contexto ecuatoriano, estas estrategias requieren ajustes específicos para adaptarse a las características y regulaciones del sector fiduciario, donde la confianza de los clientes y la precisión en la gestión de datos son elementos clave [4].

Este artículo propone un enfoque estratégico para fortalecer la protección de la información en negocios fiduciarios en Ecuador mediante la adopción de un SGSI [1]. Además, se plantea el desarrollo de una prueba de concepto que evalúe la efectividad de los controles seleccionados. Este enfoque contempla no solo aspectos técnicos, sino también factores organizacionales y humanos, reconociendo que la protección de la información recae como una responsabilidad compartida en toda la estructura organizacional. La investigación busca ofrecer una orientación útil y práctica y aplicable que permita a las organizaciones fiduciarias no solo cumplir con las disposiciones legales, sino también fortalecer su resiliencia frente a las amenazas actuales y garantizar la sostenibilidad de sus operaciones [5].

2. Materiales y Métodos

2.1 Metodología

Para abordar la problemática identificada, se propone el diseño de un SGSI. Este estándar global proporciona una estructura sólida y sistemático que incluye 93 controles distribuidos en cuatro grupos principales: políticas, arquitectura, personas y tecnología [1]. La metodología incluye los siguientes pasos:

1. **Análisis de riesgos:** Este paso inicia con la identificación de activos críticos del negocio fiduciario, como bases de datos de clientes, sistemas de gestión fiduciaria y plataformas de comunicación interna. Se evalúa qué activos son más valiosos para la organización y cómo afectan directamente al negocio en términos de

su medición en la confidencialidad, integridad y disponibilidad (CIA). Posteriormente, se realiza una evaluación del riesgo combinando la probabilidad de ocurrencia de accidentes y el impacto potencial que podrían generar. Este análisis permite priorizar aquellos riesgos que representan una mayor amenaza para la continuidad y la reputación del negocio fiduciario [5].

2. **Selección de controles:** Los controles de seguridad serán priorizados con base en el análisis de riesgos. Por ejemplo, para salvaguardar los datos sensibles de los clientes, se implementarán sistemas de cifrado avanzado y medidas de autenticación multifactor. En cuanto a las redes internas, se aplicarán políticas de segmentación y monitoreo continuo. Además, se incorporarán controles relacionados con la capacitación del personal para reducir riesgos asociados al error humano [2][3].
3. **Cumplimiento normativo:** Se adaptará el SGSI a los requisitos específicos de la LOPDP, asegurando que se incluyan medidas relacionadas con la obtención y el manejo del consentimiento de los clientes, la notificación oportuna de brechas de seguridad y la habilitación de mecanismos para que los titulares de datos ejerzan sus derechos [4].
4. **Marco comparativo internacional:** Se analizarán casos de éxito en países como España y Colombia. En España, la implementación del Reglamento General de Protección de Datos (RGPD) ha destacado por integrar tecnologías avanzadas de monitoreo. En Colombia, la Ley 1581 de 2012 ha promovido prácticas de capacitación masiva para proteger información personal. Estas experiencias servirán como base para personalizar soluciones en el contexto ecuatoriano [6][7].

Vulnerabilidades y Ataques Para Proteger:

En el negocio fiduciario, las siguientes vulnerabilidades y amenazas representan riesgos significativos para la SI:

1. **Violación de acceso a información confidencial:**
   Vulnerabilidad: Uso de contraseñas débiles o autenticación insuficiente.
   Ataque: Ataque de fuerza bruta o phishing para obtener acceso a sistemas críticos y bases de datos de clientes.
2. **Intercepción de comunicaciones:**
   Vulnerabilidad: Redes no cifradas o con cifrado débil.
   Ataque: Ataques Man-in-the-Middle (MITM) que interceptan y modifican la información entre el cliente y la organización fiduciaria.
3. **Exposición de datos debido a errores humanos:**
   Vulnerabilidad: Falta de capacitación en seguridad de la información.
   Ataque: Errores en el manejo de información sensible por parte de empleados, como enviar datos a la persona incorrecta o mal almacenamiento.
4. **Pérdida de datos:**
   Vulnerabilidad: Falta de sistemas de respaldo adecuados.
   Ataque: Ransomware que cifra los datos y exige un rescate para su recuperación.
5. **Vulnerabilidades en software:**
   Vulnerabilidad: Uso de software desactualizado o sin parches de seguridad.
   Ataque: Exploits de vulnerabilidades conocidas, como las vulnerabilidades en servidores web o bases de datos.

Tabla 1. Declaración de Aplicabilidad

Vulnerabilidad o Ataque	Control Aplicable	Control NO Aplicable
Acceso no autorizado a datos sensibles	A.9.2.1 Gestión de acceso de usuarios (autenticación multifactor)	A.9.1.1 Políticas de control de acceso físico (no se aplica al acceso lógico)
Intercepción de comunicaciones	A.10.1.1 Política de cifrado (cifrado de datos en tránsito)	A.13.2.3 Seguridad en las comunicaciones telefónicas (no es una prioridad para este caso)
Exposición de datos debido a errores humanos	A.7.2.2 Concienciación y formación en seguridad (capacitación continua)	A.8.1.1 Identificación de activos (no directamente relacionado con errores humanos)
Extravió de información	A.12.3.1 Copias de seguridad (procedimientos de respaldo)	A.16.1.4 Gestión de incidentes de seguridad (no directamente relacionado con pérdida de datos)
Vulnerabilidades en software	A.12.6.1 Gestión de vulnerabilidades (actualización y parcheo de software)	A.15.1.1 Evaluación de proveedores (no aplicable para vulnerabilidades internas)

Para la prueba de concepto en el negocio fiduciario, se seleccionarán los siguientes controles, clasificados según los cuatro grupos principales definido en la norma 27001:2022.

Personas:

- Programa de capacitación continua sobre la LOPDP y buenas prácticas de seguridad.
- Designación de un responsable de protección de datos con responsabilidades claras.

Controles No Seleccionados y Justificación

Algunos controles no serán implementados en esta fase debido a restricciones presupuestarias, temporales o de aplicabilidad:

1. **Sistemas de respaldo continuo**:

Aunque importantes, su implementación requiere una infraestructura de almacenamiento avanzada que no está disponible actualmente.

2. **Herramientas avanzadas de análisis de comportamiento (UEBA)**:

Estas herramientas requieren una inversión significativa y un tiempo prolongado para su configuración y monitoreo efectivo.

3. **Automatización completa de la gestión de identidades (IAM)**:

Dado el tamaño actual del negocio, la gestión manual supervisada se considera suficiente y más rentable a corto plazo.

4. **Controles relacionados con cadenas de suministro**:

No se priorizan debido a que la mayor parte de los datos críticos se gestionan internamente y no involucran proveedores externos.

La adopción de estas medidas no seleccionados se evaluará en futuras fases del proyecto

2.2 Prueba de Concepto

La efectividad de la propuesta se validará mediante una prueba de concepto en un negocio fiduciario. Esta incluirá las siguientes actividades:

1. **Encuestas iniciales:** Evaluar el conocimiento del personal sobre la LOPDP, los lineamientos internos de protección y los protocolos operativos mediante cuestionarios de 10 preguntas.

- ¿Sabe usted qué derechos tienen los titulares de datos personales según la LOPDP? (Sí/No).
- ¿Conoce las sanciones que se aplican por la divulgación no autorizada de datos? (Sí/No).
- Enumere dos medidas que tomaría en caso de identificar un acceso no autorizado a los sistemas.
- Explique la relevancia de preservar la privacidad de los datos personales.

2. **Capacitación:** Diseñar un plan de formación que incluya videos educativos acerca de la normativa vigente de protección de datos y buenas prácticas de seguridad.

- Videos educativos en plataformas como TikTok**:** Ejemplos incluyen "¿Qué hacer ante un ataque de phishing?" y "Consecuencias legales de no proteger los datos personales".

3. **Evaluación posterior:** Aplicar nuevamente las encuestas iniciales para medir la mejora en el nivel de conocimiento y evaluar el alcance de la capacitación.

- ¿Es necesario reportar incidentes de seguridad de inmediato? (Sí/No).
- Seleccione la respuesta correcta: "El cifrado de datos se utiliza para..." (a) evitar accesos no autorizados, (b) almacenar contraseñas, (c) proteger datos en tránsito.
- Describa cómo actuaría si recibe un correo sospechoso solicitando credenciales.
- ¿Qué prácticas considera fundamentales para garantizar un comportamiento seguro en su puesto de trabajo?

4. **Implementación tecnológica:** Probar soluciones tecnológicas como plataformas de gestión documental y plataformas de monitoreo continuo que respalden los controles seleccionados [8].

- **Software:** Sistemas de gestión documental (p. ej., SharePoint), plataformas de monitoreo continuo (p. ej., SolarWinds).
- **Hardware:** Dispositivos de seguridad perimetral como firewalls de próxima generación y sistemas de autenticación biométrica.

2.3 Declaración de Aplicabilidad

Se generará un documento de declaración de aplicabilidad que detalle los controles seleccionados, así como aquellos no aplicados en esta fase inicial debido a restricciones presupuestarias o de tiempo [1].

2.4 Justificación del Método

Esta metodología cuenta con respaldo en experiencias internacionales. Por ejemplo, en España, la conformidad con el Reglamento General de Protección de Datos (RGPD) se ha alcanzado a través de la adopción de SGSI y el uso de tecnologías innovadoras destinadas a proteger la información [3]. En México, la legislación federal sobre la protección de información personal en posesión de particulares ha impulsado el desarrollo de capacitaciones masivas y el uso de plataformas tecnológicas para gestionar riesgos [4]. Estos casos de estudio sirven como base para adaptar soluciones al contexto ecuatoriano.

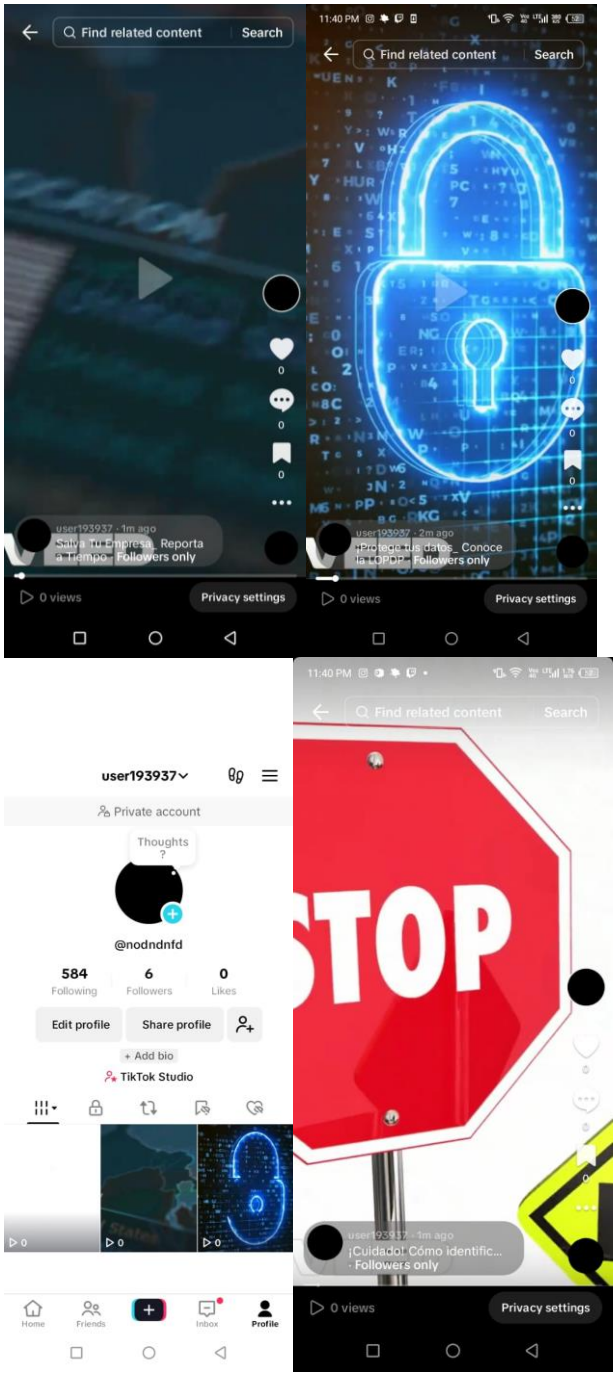


Figura 1. Videos educativos en TikTok

3. Resultados y Discusión

Los efectos de la prueba de concepto evidenciaron una mejora significativa en el conocimiento del personal tras la capacitación. El análisis de las encuestas iniciales mostró que solo el 35% del personal tenía un conocimiento adecuado de la LOPDP y las políticas de seguridad interna. Tras la implementación del plan de formación, este porcentaje aumentó al 85%. Además, se observó una reducción en los errores operativos relacionados con la gestión de datos sensibles.

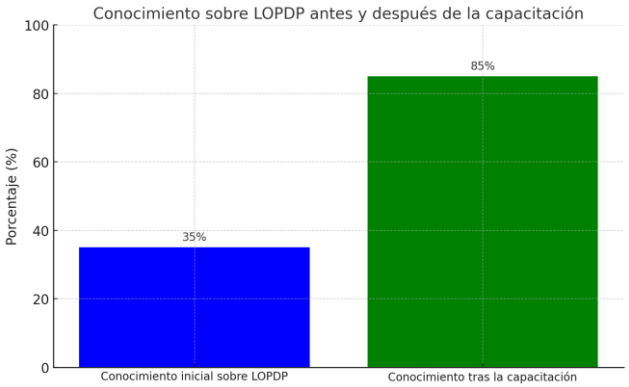


Figura 2. Resultados de la prueba de concepto

En cuanto a la implementación tecnológica, las herramientas de monitoreo continuo demostraron ser efectivas para identificar y mitigar posibles incidentes de seguridad en tiempo real. Estas herramientas también permitieron generar reportes automatizados que facilitaron la auditoría interna.

3.1 Parte organizacional

Se diseñó e implementó un conjunto de directrices para la protección de información que fue admitida por la alta dirección. Esta política incluyó compromisos claros para la distribución de personal y financieros, lo que permitió garantizar el éxito del SGSI. Asimismo, se estableció un comité interno responsable de garantizar la adhesión a las políticas y gestionar incidentes de seguridad.

3.2 Personas

El plan de capacitación se estructuró en módulos accesibles y prácticos, complementados con evaluaciones periódicas. Esta estrategia permitió no solo aumentar el conocimiento del personal, sino también fomentar un ambiente de protección en la organización. Adicionalmente, se diseñaron guías operativas para roles específicos, asegurando que cada empleado entendiera sus responsabilidades en la gestión de datos.

3.3 Tecnología

La adquisición de herramientas como sistemas de cifrado de datos y plataformas de monitoreo continuo fortaleció significativamente la infraestructura tecnológica del negocio fiduciario. Estas soluciones garantizaron un nivel elevado de protección para la información crítica, alineándose con los requisitos de la LOPDP.

En conjunto, la integración de políticas organizacionales, capacitación del personal y tecnología avanzada permitió minimizar los riesgos vinculados al manejo de datos sensibles.

4. Conclusiones

Luego de examinar los activos informativos y las vulnerabilidades presentes en el negocio fiduciario, se identificaron puntos críticos relacionados con la gestión de datos personales. Estas áreas requerían medidas específicas, como el uso de cifrado y el monitoreo continuo, para mitigar riesgos relacionados con accesos no autorizados y pérdidas de datos.

Las contramedidas implementadas, basadas en las medidas definidas en el estándar ISO/IEC 27001, se enfocaron en las vulnerabilidades más críticas. Estas medidas incluyeron claras, formación del equipo de trabajo avanzadas que garantizaron un cumplimiento efectivo con la LOPDP.

La prueba de concepto validó la efectividad de las soluciones implementadas, demostrando mejoras significativas en el conocimiento del personal y una reducción en la exposición a riesgos. Esto subraya la importancia de un enfoque integral que combine formación, tecnología y compromiso organizacional para garantizar la resguardo de los datos personales.

Referencias

[1] ISO, “ISO/IEC 27001:2022 Information technology — Security techniques — Information security management systems — Requirements,” International Organization for Standardization, 2022. [Online]. Available: https://www.iso.org/standard/27001

[2] M. García y P. López, “Ciberseguridad organizacional: Políticas y tecnologías,” en Gestión de la seguridad informática, Ediciones Técnicas, pp. 45–67, 2020.

[3] N. La Serna, L. Pro Concepción y C. Yañez Durán, “Compresión de imágenes: Fundamentos, técnicas y formatos,” Revista de Ingeniería de Sistemas e Informática, vol. 6, no. 1, pp. 21–29, 2009. [Online]. Available: https://upsalesiana.ec/ing32ar1r01

[4] A. Smith, “Data Protection Strategies for Financial Services,” Journal of Information Security Management, vol. 12, no. 3, pp. 34–49, 2019. [Online]. Available: https://jisecm.org/article/12345

[5] A. Rodríguez, “Implementación de SGSI basados en ISO 27001 en América Latina,” en Tecnologías de Información y Seguridad, Editorial ITSec, pp. 101–123, 2018.

[6] J. Martínez, “Implementación de controles de seguridad en el sector financiero,” Revista de Gestión y Tecnología, vol. 8, no. 2, pp. 67–82, 2021. [Online]. Available: https://gestionytecnologia.org/finanzas

[7] G. Fernández y L. Vargas, “Protección de datos en Colombia: Implementación de la Ley 1581 de 2012,” Derecho Informático, vol. 10, no. 1, pp. 22–35, 2017. [Online]. Available: https://derechoinformatico.org/colombia1581

[8] P. Hernández, “Tecnologías emergentes para la seguridad de datos,” Innovación y Tecnología, vol. 5, no. 3, pp. 14–29, 2020. [Online]. Available: https://innovaciontecnologica.org/seguridad

[9] S. López y D. Ramos, "Capacitación y ciberseguridad: Impacto en las organizaciones," Revista de Seguridad Digital, vol. 4, no. 2, pp. 33–47, 2022. [Online]. Available: https://seguridadigital.org/capacitacion

[10] M. Ortega, "Gestión de riesgos en seguridad de la información," Revista de Tecnología Empresarial, vol. 9, no. 1, pp. 20–36, 2021. [Online]. Available: https://tecnologiaempresarial.org/riesgos

[11] L. Pérez y J. Morales, "Implementación práctica de la ISO 27001 en empresas medianas," Tecnologías de la Información Hoy, vol. 15, no. 4, pp. 25–41, 2021.

[12] R. Fernández, "Evaluación de riesgos en sistemas de información," Seguridad Informática Avanzada, vol. 7, no. 3, pp. 50–65, 2020.

[13] C. García, "Formación y capacitación en seguridad digital," Revista de Educación y Tecnología, vol. 12, no. 1, pp. 14–22, 2021.

[14] A. Torres, "Aplicación de criptografía en la protección de datos," Ciencia y Seguridad de la Información, vol. 5, no. 2, pp. 35–47, 2019.

[15] E. Ramírez, "El impacto de la ISO 27001 en empresas financieras," Gestión Empresarial y Tecnología, vol. 6, no. 2, pp. 30–46, 2022.

[16] F. Gómez y T. Alvarado, "Seguridad en datos sensibles: Desafíos y avances," Revista Internacional de Ciberseguridad, vol. 10, no. 3, pp. 75–91, 2022.

[17] K. Salinas, "Capacitación en gestión de riesgos de seguridad," Tecnología y Empresa, vol. 11, no. 1, pp. 12–28, 2021.

[18] H. Castillo, "Monitoreo proactivo en sistemas de seguridad," Journal of Information Security Research, vol. 8, no. 2, pp. 45–60, 2020.

[19] B. Mendoza, "Políticas de seguridad de la información: Un enfoque estratégico," Ciberestrategia Empresarial, vol. 14, no. 4, pp. 33–50, 2021.

[20] D. Ávila, "Normativas internacionales y su aplicación en América Latina," Revista de Derecho y Tecnología, vol. 5, no. 1, pp. 10–23, 2022.