593 Digital Publisher
CEIT
ISSN 2588-0705

Políticas de seguridad de la información según la norma iso 27001 para el municipio de Guaranda, Bolívar, Ecuador

Information security policies according to the ISO 27001 standard for the municipality of Guaranda, Bolívar, Ecuador

Xavier Efrain Mullo-Pilamunga[1]
Universidad Americana de Europa
xaviermullo@hotmail.com

Rosa Gabriela Camero-Berrones[2]
Universidad Americana de Europa
rosa.cb@cdmadero.tecnm.mx

doi.org/10.33386/593dp.2025.3.3134

V10-N3 (may-jun) 2025, pp 340-351 | Recibido: 26 de febrero del 2025 - Aceptado: 10 de marzo del 2025 (2 ronda rev.)

1 ORCID: https://orcid.org/0000-0002-8308-9279.
2 ORCID: https://orcid.org/0000-0003-4438-1645. Profesora en el Tecnológico Nacional de México, Campus Ciudad Madero y en la Universidad Americana de Europa. Doctora en Tecnología Avanzada.

340

Cómo citar este artículo en norma APA:

Mullo-Pilamunga, X, & Camero-Berrones, R., (2025). Políticas de seguridad de la información según la norma iso 27001 para el municipio de Guaranda, Bolívar, Ecuador. 593 Digital Publisher CEIT, 10(3), 340-351, https://doi.org/10.33386/593dp.2025.3.3134

Descargar para Mendeley y Zotero

RESUMEN

El estudio se centra en la implementación de políticas de seguridad de la información según la norma ISO 27001 en el Municipio de Guaranda, Ecuador. Se identificó la necesidad de mejorar las políticas existentes para proteger los datos sensibles contra las amenazas cibernéticas. A través de un enfoque cualitativo se evaluaron las prácticas de seguridad actuales y se diseñó un plan de acción basado en la norma ISO 27001. Los hallazgos revelan que, aunque se han implementado algunas medidas tecnológicas, persisten brechas en la adopción cultural y la capacitación de los empleados. personal, que son esenciales para una gestión eficaz de la seguridad. Los resultados subrayan la importancia de integrar una cultura organizacional sólida con tecnología avanzada y políticas de actualización continua para garantizar la protección de la información. Además, se destaca la necesidad de involucrar a todos los niveles de la organización en la gestión de la seguridad y realizar auditorías periódicas para garantizar la eficacia de las políticas implementadas.

Palabras claves: ISO 27001; seguridad de la información,; gestión de riesgos; Guaranda; amenazas cibernéticas.

ABSTRACT

The study focuses on the implementation of information security policies according to the ISO 27001 standard in the Municipality of Guaranda, Ecuador. The need to improve existing policies to protect sensitive data against cyber threats was identified. Through a qualitative approach, current security practices were evaluated and an action plan based on ISO 27001 was designed. The findings reveal that, although some technological measures have been implemented, gaps persist in cultural adoption and employee training. personnel, which are essential for effective security management. The results underscore the importance of integrating a strong organizational culture with advanced technology and continuously updating policies to ensure information protection. In addition, the need to involve all levels of the organization in security management and to carry out regular audits to ensure the effectiveness of the implemented policies is highlighted

Keywords: ISO 27001; information security; risk management; Guaranda; cyber threats.

Introducción

En la era digital actual, donde la información es uno de los activos más valiosos para cualquier organización, la protección de datos ha adquirido una importancia crítica. En este contexto, las políticas de seguridad de la información, basadas en estándares internacionales como la Norma ISO 27001, se han convertido en herramientas esenciales para garantizar la confidencialidad, integridad y disponibilidad de la información. Este estándar proporciona un marco robusto para la gestión de la seguridad de la información, permitiendo a las organizaciones identificar y mitigar riesgos de manera efectiva.

El presente estudio se enfoca en la implementación de políticas de seguridad de la información en la Unidad de Sistemas del Municipio de Guaranda, en la provincia de Bolívar, Ecuador, a través de la adopción de la Norma ISO 27001. Esta investigación surge de la necesidad de actualizar y fortalecer las políticas existentes para enfrentar las crecientes amenazas cibernéticas y garantizar la protección de datos sensibles, que son fundamentales para el funcionamiento eficiente y seguro del municipio.

El problema central en la Unidad de Sistemas del Municipio de Guaranda radica en la obsolescencia de sus políticas de seguridad de la información y la falta de cumplimiento de los procesos establecidos para asegurar un manejo seguro de los datos. Actualmente, se enfrentan a desafíos significativos como el incumplimiento en los procesos de verificación y el acceso a datos sensibles por parte de personas no autorizadas. Estas deficiencias no solo ponen en riesgo la integridad y confidencialidad de la información crítica, sino que también comprometen la confianza y la operatividad del municipio.

El objetivo general de este estudio es evaluar la situación actual de la seguridad de la información en la Unidad de Sistemas del Municipio de Guaranda, diagnosticar los procesos de cumplimiento de las políticas de seguridad existentes y desarrollar un plan de seguridad conforme a la Norma ISO 27001 que optimice la gestión y protección de la información en dicha unidad.

La importancia de este estudio radica en su potencial para mejorar la gestión de la seguridad de la información en una institución pública, alineando sus prácticas con estándares internacionales reconocidos. Esto no solo aumentará la capacidad del municipio para proteger sus activos informativos, sino que también reforzará la confianza de la ciudadanía en la gestión segura de sus datos, contribuyendo así al fortalecimiento de la transparencia y la eficacia administrativa.

Método

La investigación adoptó un enfoque mixto, combinando métodos cualitativos y cuantitativos para evaluar la implementación de la norma ISO 27001 en la Unidad de Sistemas del Municipio de Guaranda.

En la fase cualitativa, se realizaron observaciones directas para analizar la aplicación de las políticas de seguridad. En la fase cuantitativa, se aplicaron encuestas para medir la percepción y cumplimiento de las normativas.

El proceso se estructuró en varias etapas: integración de datos cualitativos y cuantitativos, diseño de un plan de acción alineado con ISO 27001 y evaluación de su efectividad mediante encuestas y observaciones.

Se empleó un método hipotético-deductivo, vinculando teoría y práctica. La hipótesis, basada en la literatura existente, sugería que la alineación de las políticas con ISO 27001 mejoraría la gestión de la seguridad de la información, lo que se validó mediante análisis documental y cuestionarios.

El diseño no experimental transversal permitió captar información sobre el estado actual de la seguridad en la organización, mientras que el enfoque cualitativo basado en estudios de caso exploró factores organizacionales y humanos. Esta combinación aseguró una visión integral de los desafíos y oportunidades en la implementación de la norma ISO 27001.

Desarrollo

Caso Ecuador: Municipio de Quito

En Ecuador, el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) elaboró en 2022 un diagnóstico de las capacidades de ciberseguridad del país. Este documento destaca la importancia de adoptar marcos de referencia basados en normas internacionales como la ISO 27001 para fortalecer la seguridad de la información en las instituciones públicas. El diagnóstico señala que, aunque existen avances, aún hay desafíos significativos en términos de infraestructura y capacitación del personal. Puedes acceder al documento completo aquí:

Además, un estudio de la Universidad Técnica del Norte propuso un marco de referencia basado en la norma ISO 27001 para su implementación obligatoria en instituciones públicas (Rodríguez, 2024). Este trabajo resalta la necesidad de adaptar la norma a las particularidades locales y de realizar evaluaciones periódicas para garantizar su efectividad. El estudio completo está disponible en:

Caso Colombia: Instituto Tecnológico Metropolitano de Medellín

En Colombia, el Instituto Tecnológico Metropolitano de Medellín llevó a cabo un proyecto de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001. El estudio identificó la importancia de realizar un diagnóstico exhaustivo de la situación actual de la entidad en relación con la seguridad y privacidad de la información, así como de desarrollar políticas y procedimientos alineados con los estándares internacionales (Prieto & Álvarez, 2024). Puedes consultar el informe final aquí:

La comparación de estos casos revela que la implementación efectiva de la norma ISO 27001 en municipios y entidades públicas depende de factores como:

Diagnóstico inicial: Realizar una evaluación detallada de la situación actual en materia de seguridad de la información. Repositorio UNAD+1Repositorio UNAD+1

Adaptación local: Ajustar la norma a las necesidades y contextos específicos de la entidad.

Capacitación continua: Formar al personal en aspectos de seguridad de la información.

Evaluaciones periódicas: Llevar a cabo auditorías internas para asegurar el cumplimiento y la mejora continua.

Seguridad de la Información

La seguridad de la información es fundamental en la era digital, abarcando estrategias y políticas para proteger la información contra accesos no autorizados y asegurar su confidencialidad, integridad y disponibilidad (Díaz, 2020). Los principios de la "Tríada CIA" —confidencialidad, integridad y disponibilidad— son la base para garantizar que los datos estén protegidos y accesibles solo para personas autorizadas, manteniéndose precisos y disponibles cuando se necesiten (Seminario, 2022).

Importancia de la Seguridad de la Información en el Contexto Actual

En un mundo cada vez más interconectado, la seguridad de la información es vital para proteger datos sensibles y cumplir con normativas legales como el GDPR, preservando la reputación organizacional y asegurando la continuidad del negocio frente a ciberataques y otras amenazas (Ñañez, 2021).

Amenazas y Vulnerabilidades en la Seguridad de la Información

Las amenazas a la seguridad de la información pueden ser externas (ciberataques, espionaje) o internas (errores humanos, malversación). Las vulnerabilidades, que son debilidades en sistemas y procesos, pueden ser explotadas por estas amenazas, comprometiendo la seguridad organizacional (Barrezueta, 2023).

Estrategias de Mitigación de Amenazas y Vulnerabilidades

Para proteger la información, es crucial evaluar riesgos, implementar controles de seguridad, y capacitar al personal de manera continua. Además, se deben desarrollar planes de respuesta y recuperación ante incidentes para mitigar el impacto de posibles brechas de seguridad (Chitacapa et al., 2023).

Políticas de Seguridad de la Información

Las políticas de seguridad establecen un marco para proteger la información dentro de las organizaciones, definiendo normas y procedimientos para mitigar riesgos y asegurar la confidencialidad, integridad y disponibilidad de los datos (Vega, 2021).

Desarrollo y Estructura de Políticas Efectivas de Seguridad de la Información

El desarrollo de políticas efectivas de seguridad de la información implica varios pasos esenciales. Primero, es fundamental realizar una evaluación de riesgos para identificar amenazas y vulnerabilidades (Morales et al., 2020). Luego, se deben definir objetivos claros de seguridad basados en esa evaluación. Es importante involucrar a todas las partes interesadas relevantes en el proceso de desarrollo, incluyendo la alta dirección y los departamentos clave. Una vez redactadas, las políticas deben ser revisadas legalmente para asegurar el cumplimiento con las regulaciones, y finalmente, deben ser aprobadas y comunicadas a todos los empleados.

La estructura recomendada de las políticas debe ser clara y lógica, comenzando con una introducción que resuma su propósito y alcance. Los objetivos de seguridad deben estar bien definidos, seguidos por el ámbito de aplicación, roles y responsabilidades, y procedimientos para la gestión de activos y control de acceso. Las políticas también deben incluir secciones sobre la gestión de incidentes, continuidad del negocio, y cumplimiento con las leyes y regulaciones aplicables (Morales et al., 2020).

Rol de las Políticas de Seguridad en la Protección de Datos y Sistemas

Las políticas de seguridad de la información son cruciales para establecer un marco de gobernanza que define responsabilidades y expectativas relacionadas con la seguridad de los datos (Aguerre, 2020). Estas políticas proporcionan estándares y directrices para proteger los sistemas de información, incluyendo el uso de cifrado y la gestión de contraseñas. Además, facilitan la gestión de riesgos, asegurando que las organizaciones puedan identificar, evaluar y mitigar riesgos de manera proactiva (Jiménez, 2022). El cumplimiento de estas políticas es esencial para evitar sanciones legales y mantener la confianza de los clientes.

Estrategias para la Implementación y Mantenimiento de Políticas de Seguridad de la Información

Para implementar y mantener políticas de seguridad de manera efectiva, es necesario desarrollar políticas basadas en un análisis de riesgos, involucrando a todas las partes interesadas en el proceso (Jurado et al., 2020). La comunicación clara y la capacitación continua son esenciales para asegurar que todos los empleados comprendan y sigan las políticas. Además, se deben establecer controles técnicos y administrativos, realizar auditorías regulares, y actualizar las políticas según sea necesario para adaptarse a las nuevas amenazas y cambios normativos.

Sistema de Gestión de Seguridad de la Información (SGSI)

El SGSI es un sistema documentado que incluye controles de seguridad implementados para proteger los activos de información de la organización. Este sistema sigue el ciclo de Planificar-Hacer-Verificar-Actuar (PDCA), comenzando con la identificación de riesgos, pasando por la implementación de controles, verificación de la eficacia, y ajustes según sea necesario (Yungán y Narváez, 2022). Un SGSI eficiente protege los datos confidenciales y debe integrarse en todas las áreas de la organización.

Digital Publisher

Evaluación y Auditoría Continuas

La revisión regular de los controles de seguridad y las prácticas de gestión de riesgos es crucial para asegurar su efectividad y relevancia. Las auditorías de seguridad ya sean internas o externas, permiten identificar debilidades y áreas de mejora en la estrategia de seguridad de la organización (Barrantes, 2023). Además, implementar un proceso de gestión de cambios efectivo es esencial para la infraestructura de TI, asegurando que los cambios no introduzcan nuevos riesgos o vulnerabilidades (Guevara et al., 2021).

Herramientas y Tecnologías para la Gestión de Riesgos

Las herramientas y tecnologías desempeñan un papel crucial en la gestión de riesgos de seguridad de la información. Plataformas como GRC proporcionan un marco integrado para la gestión de riesgos y cumplimiento, mientras que herramientas de análisis como FAIR y CRAMM facilitan la evaluación de riesgos (Hermawan & Novita, 2021). Los escáneres de vulnerabilidades y las herramientas de pruebas de penetración como Nessus y Metasploit son fundamentales para identificar y mitigar debilidades explotables (Ortiz, 2020). Sistemas de SIEM centralizan la gestión de eventos de seguridad, mientras que el software de continuidad del negocio y recuperación ante desastres asegura la resiliencia organizacional (Piñero & Brito, 2023).

Medidas de Protección y Control de Accesos

Las medidas de protección y control de accesos son fundamentales para la seguridad de los datos e infraestructuras. Tecnologías como la autenticación multifactor (MFA) y los sistemas de Gestión de Identidades y Accesos (IAM) refuerzan la seguridad al controlar quién puede acceder a los recursos de TI (Vargas, 2022). El cifrado de datos en reposo y en tránsito protege la información sensible, mientras que el control de acceso basado en roles (RBAC) asegura que los usuarios solo tengan acceso a los recursos necesarios para sus funciones (Cardona, 2021).

Tecnologías y Prácticas para la Protección de Datos e Infraestructuras

La seguridad de la red se fortalece con firewalls y sistemas de detección y prevención de intrusiones (IDS/IPS), que monitorizan el tráfico y bloquean actividades sospechosas (Velásquez, 2022). La seguridad física, a través de controles de acceso y videovigilancia, protege la infraestructura crítica de TI, mientras que la gestión de parches y vulnerabilidades asegura que el software esté actualizado contra amenazas conocidas (Padilla, 2023). Además, prácticas como el desarrollo seguro y la educación y concienciación en seguridad son esenciales para mitigar riesgos desde la base, fomentando una cultura de seguridad robusta (Pachacuti, 2020).

Constitución de la Constitución de la República del Ecuador

Sección cuarta Acción de acceso a la información pública Art. 91.- La acción de acceso a la información pública tendrá por objeto garantizar el acceso a ella cuando ha sido denegada expresa o tácitamente, o cuando la que se ha proporcionado no sea completa o fidedigna. Podrá ser interpuesta incluso si la negativa se sustenta en el carácter secreto, reservado, confidencial o cualquiera otra clasificación de la información. El carácter reservado de la información deberá ser declarado con anterioridad a la petición, por autoridad competente y de acuerdo con la ley.

Norma de control interno de la contraloría general del estado (2023)

Art 300

300 EVALUACIÓN DEL RIESGO

La máxima autoridad y el personal de la institución establecerán los mecanismos necesarios para identificar, analizar, valorar y responder a los riesgos a los que está expuesta la organización para el logro de sus objetivos, el cumplimiento de las disposiciones legales, la protección de recursos públicos y la generación de información oportuna y confiable.

El riesgo es la probabilidad de ocurrencia de un evento no deseado que pudiese perjudicar o afectar adversamente a la entidad o su entorno. La máxima autoridad, el nivel directivo y todo el personal de la entidad serán responsables de efectuar el proceso de administración de riesgos, que implica la metodología, estrategias, técnicas y procedimientos, a través de los cuales las unidades administrativas identificarán, analizarán, valorarán y responderán a los potenciales eventos que pudieran afectar la ejecución de sus procesos, el logro de sus objetivos, la protección de sus recursos y la generación de información; y emprenderán las medidas pertinentes para afrontar exitosamente tales riesgos.

Art 410-10 Mantenimiento, actualización y control de la infraestructura tecnológica

"…La unidad de tecnologías de la información y comunicaciones de cada organización definirá y regulará los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades".

1. Definición de procedimientos para mantenimiento y liberación de software de aplicación por planeación, por cambios a las disposiciones legales y normativas, por corrección y mejoramiento de los mismos o por requerimientos de los usuarios.

2. Los cambios que se realicen en procedimientos, procesos, sistemas y acuerdos de servicios serán registrados, evaluados y autorizados de forma previa a su implantación a fin de disminuir los riesgos de integridad del ambiente de producción. El detalle e información de estas modificaciones serán registrados en su correspondiente bitácora e informados a todos los actores y usuarios finales relacionados, adjuntando las respectivas evidencias.

3. Control y registro de las versiones del software que ingresa a producción.

4. Actualización de los manuales técnicos y de usuario por cada cambio o mantenimiento que se realice, los mismos que estarán en constante difusión y publicación.

5. Se establecerán ambientes de desarrollo/pruebas y de producción independientes; se implementarán medidas y mecanismos lógicos y físicos de seguridad para proteger los recursos y garantizar su integridad y disponibilidad a fin de proporcionar una infraestructura de tecnología de información confiable y segura.

6. Se elaborará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad

Ley Orgánica de transparencia y acceso a la información pública (2004)

Art. 5.- Información Pública. - Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado.

Art. 6.- Información Confidencial. - Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República.

Digital Publisher

Entrevistas

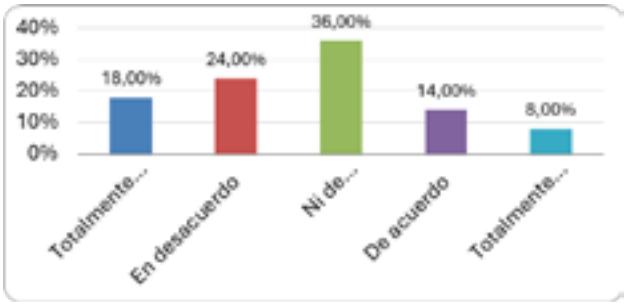
El personal del Municipio de Guaranda recibe capacitación adecuada para cumplir con las políticas de seguridad de la información basadas en ISO 27001.

Tabla 1

Capacitación del personal del Municipio de Guaranda para cumplir con las políticas de seguridad de la información según ISO 27001.

Respuesta	Recuento	Porcentaje
Totalmente en desacuerdo	9	18%
En desacuerdo	12	24%
Ni de acuerdo ni en desacuerdo	18	36%
De acuerdo	7	14%
Totalmente de acuerdo	4	8%
Total	50	100%

Gráfico 1.



Análisis e Interpretación

Los resultados de la encuesta indican que un 24% de los encuestados está en desacuerdo con las políticas de seguridad de la información en el Municipio de Guaranda, mientras que un 18% adicional está totalmente en desacuerdo. Esto sugiere que una proporción significativa de los participantes tiene una percepción negativa sobre la efectividad de estas políticas.

Por otro lado, un 36% de los encuestados se mantiene neutral, lo que podría indicar una postura indecisa o falta de claridad respecto a las políticas de seguridad de la información. En contraste, un 22% de los encuestados tiene una percepción positiva (14% de acuerdo y 8% totalmente de acuerdo), lo que muestra que, aunque en menor proporción, existe un grupo que valora de manera favorable las políticas implementadas, lo que podría servir como base para futuras mejoras en su aplicación.

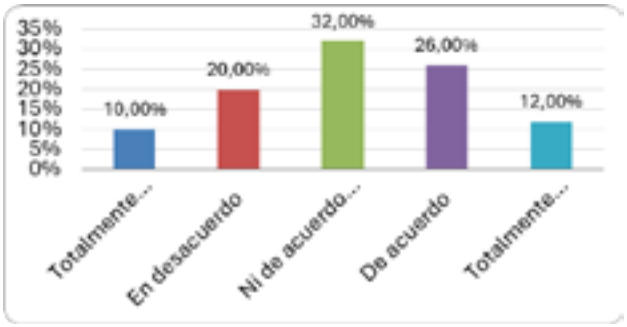
Los mecanismos de control y seguimiento implementados en el Municipio de Guaranda garantizan el cumplimiento continuo de la norma ISO 27001.

Tabla 2

Efectividad de los mecanismos de control y seguimiento en el Municipio de Guaranda para garantizar el cumplimiento continuo de la norma ISO 27001.

Respuesta	Recuento	Porcentaje
Totalmente en desacuerdo	5	10%
En desacuerdo	10	20%
Ni de acuerdo ni en desacuerdo	16	32%
De acuerdo	13	26%
Totalmente de acuerdo	6	12%
Total	50	100%

Gráfico 2.



Análisis e Interpretación

Los resultados de la encuesta muestran que un 20% de los encuestados está en desacuerdo con las políticas de seguridad de la información en el Municipio de Guaranda, mientras que un 10% adicional está totalmente en desacuerdo. Esto sugiere que un 30% de los participantes percibe deficiencias en la implementación de estas políticas.

Por otro lado, un 32% de los encuestados se mantiene neutral, lo que podría reflejar una postura indecisa o una falta de conocimiento suficiente sobre las políticas. En contraste, un 38% de los encuestados tiene una percepción positiva (26% de acuerdo y 12% totalmente de acuerdo),

lo que indica que una parte significativa de la población valora positivamente las políticas de seguridad de la información, lo que sugiere que hay aspectos bien implementados que pueden ser potenciados para mejorar la satisfacción general en la organización.

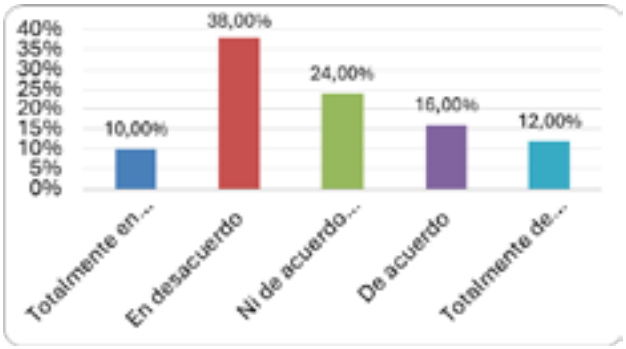
Los procesos de auditoría interna en el Municipio de Guaranda son efectivos para identificar y corregir incumplimientos de las políticas de seguridad de la información según ISO 27001.

Tabla 3

Efectividad de los procesos de auditoría interna en el Municipio de Guaranda para corregir incumplimientos de las políticas de seguridad según ISO 27001.

Respuesta	Recuento	Porcentaje
Totalmente en desacuerdo	5	10%
En desacuerdo	19	38%
Ni de acuerdo ni en desacuerdo	12	24%
De acuerdo	8	16%
Totalmente de acuerdo	6	12%
Total	50	100%

Gráfico 3.



Análisis e Interpretación

Los resultados de la encuesta revelan que un 38% de los encuestados está en desacuerdo con las políticas de seguridad de la información en el Municipio de Guaranda, lo que sugiere que una parte significativa de los participantes no está satisfecha con su implementación. Además, un 10% está totalmente en desacuerdo, lo que refleja un nivel de insatisfacción más profundo en un grupo minoritario.

Por otro lado, un 24% de los encuestados se mantiene neutral, lo que podría indicar indecisión o falta de información sobre el tema. En contraste, un 28% de los encuestados tiene una opinión positiva (16% de acuerdo y 12% totalmente de acuerdo), lo que indica que, aunque no mayoritaria, existe una valoración favorable de las políticas, sugiriendo que hay aspectos que funcionan bien y que podrían ser aprovechados para mejorar la percepción general en el municipio.

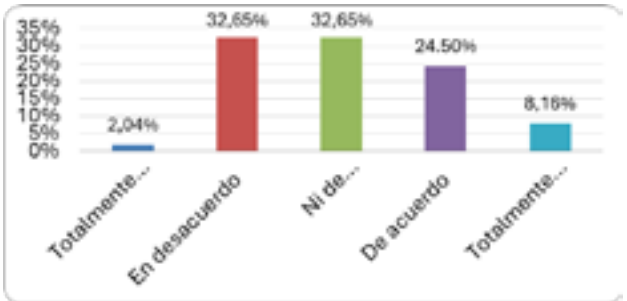
Las políticas de seguridad de la información en el Municipio de Guaranda contribuyen significativamente a la protección de los datos sensibles y a la mitigación de riesgos según los estándares de ISO 27001.

Tabla 4

Contribución de las políticas de seguridad de la información del Municipio de Guaranda a la protección de datos sensibles y mitigación de riesgos según ISO 27001.

Respuesta	Recuento	Porcentaje
Totalmente en desacuerdo	1	2.04%
En desacuerdo	16	32.65%
Ni de acuerdo ni en desacuerdo	16	32.65%
De acuerdo	12	24.50%
Totalmente de acuerdo	5	8.16%
Total	50	100%

Gráfico 4.



Análisis e Interpretación

Los resultados muestran que un 32.65% de los encuestados está en desacuerdo con las políticas de seguridad de la información en el Municipio de Guaranda, lo que sugiere que una parte considerable de los participantes percibe

Digital Publisher

deficiencias en su implementación o efectividad. Además, un pequeño porcentaje (2.04%) está totalmente en desacuerdo, lo que indica que hay una minoría con una opinión muy negativa al respecto.

Por otro lado, un 32.65% de los encuestados se mantiene neutral, lo que podría reflejar una falta de conocimiento o una posición indecisa respecto a la efectividad de las políticas. En contraste, un 32.66% de los encuestados tiene una percepción positiva (24.50% de acuerdo y 8.16% totalmente de acuerdo), lo que indica que un segmento significativo de la población valora positivamente estas políticas, sugiriendo que existen elementos que podrían ser fortalecidos para mejorar la percepción general en el Municipio.

Discusión

La seguridad de la información es un aspecto crucial en el entorno digital actual, especialmente en instituciones gubernamentales, donde la protección de datos sensibles es fundamental para el correcto funcionamiento y la confianza pública. Según Díaz (2020), la seguridad de la información se sustenta en la "Tríada CIA" (confidencialidad, integridad y disponibilidad), principios que garantizan que los datos solo sean accesibles por personas autorizadas y que mantengan su exactitud y disponibilidad cuando sean requeridos. En cambio, Seminario (2022) enfatiza que la aplicación de estos principios debe ir acompañada de normativas internacionales como la ISO 27001, para estandarizar y mejorar las prácticas de seguridad dentro de las organizaciones.

En relación con la implementación de políticas de seguridad, Vega (2021) argumenta que estas deben estar estructuradas de manera clara y contener normas específicas para mitigar riesgos. En contraste, Morales et al. (2020) destacan que el desarrollo de estas políticas requiere un análisis previo de riesgos, la definición de objetivos claros y la inclusión de todas las partes interesadas en su formulación. En el caso del Municipio de Guaranda, la necesidad de actualizar sus políticas de seguridad surge precisamente de la falta de procedimientos eficientes y del acceso no autorizado a datos sensibles, lo que compromete la integridad de la información.

Por otro lado, Jiménez (2022) resalta que el cumplimiento de las políticas de seguridad es esencial para evitar sanciones legales y fortalecer la confianza organizacional. Sin embargo, los resultados de la investigación realizada en el Municipio de Guaranda reflejan una percepción mixta respecto a la efectividad de estas políticas, ya que un 42% de los encuestados muestra desconfianza o desaprobación en su implementación. Esta situación coincide con los hallazgos de Barrantes (2023), quien sostiene que las auditorías de seguridad deben ser constantes para detectar debilidades y optimizar la gestión de riesgos.

Finalmente, Yungán y Narváez (2022) proponen la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en el ciclo PDCA (Planificar-Hacer-Verificar-Actuar), lo que permitiría un monitoreo continuo y mejoras constantes en la protección de datos. Esta estrategia podría ser una solución viable para el Municipio de Guaranda, ya que permitiría no solo mejorar la seguridad informática, sino también garantizar el cumplimiento de la norma ISO 27001 y fomentar una cultura organizacional orientada a la seguridad.

Conclusiones

La implementación de la norma ISO 27001 en la Unidad de Sistemas del Municipio de Guaranda ha sido fundamental para mejorar la seguridad de la información, pero los resultados muestran que es igualmente crucial fomentar una cultura organizacional comprometida con la seguridad. Sin un enfoque integral que incluya la capacitación del personal y la concienciación sobre las políticas de seguridad, las herramientas tecnológicas por sí solas no pueden garantizar la protección completa de la información.

El estudio ha demostrado que la gestión efectiva de riesgos de seguridad en la

información requiere más que solo la adopción de tecnologías avanzadas. Es necesario un enfoque holístico que combine estas tecnologías con prácticas operativas sólidas, auditorías regulares y, sobre todo, una cultura organizacional que priorice la seguridad. Solo así se pueden mitigar adecuadamente los riesgos y garantizar la protección continua de los datos.

La experiencia del Municipio de Guaranda subraya la importancia de la actualización constante de las políticas de seguridad de la información. Las políticas deben revisarse y adaptarse regularmente para seguir siendo efectivas frente a nuevas amenazas y cambios en el entorno tecnológico. Sin estas actualizaciones y una integración adecuada de todos los procesos organizacionales, incluso las mejores políticas pueden quedar obsoletas y perder su efectividad.

Referencias bibliográficas

Aguerre, C. (2020). Estrategias nacionales de IA y gobernanza de datos en la región. *Inteligencia Artificial en América Latina y el Caribe. Ética, Gobernanza y Políticas. Buenos Aires: CETyS Universidad de San Andrés.. Datoo y D. Indjic (eds.), The LegalTech Book: The Legal Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries*, 190-192.

Barrantes, L. F. (2023). *La auditoría interna en la gestión de la empresa EUROTUBO SAC, de la ciudad de Trujillo, 2017* [Universidad Nacional de Trujillo]. https://dspace.unitru.edu.pe/items/5fde4060-89e3-4af0-9d9b-9f75a19167d3

Barrezueta, V. F. (2023). *Guía de gestión de seguridad de la información para el Gobierno Provincial de Tungurahua* [Master's Thesis, Pontificia Universidad Católica del Ecuador]. https://repositorio.puce.edu.ec/server/api/core/bitstreams/8d01a825-05c1-4416-b08c-6574a9b1110a/content

Cardona, P. A. (2021). *Diseño de un modelo centralizado de autorizaciones para mejorar la seguridad en aplicaciones desarrolladas a la medida.* http://repositorio.itm.edu.co/handle/20.500.12622/4680

Chitacapa, J. P., Torres, C. A., & Lugo, J. (2023). Análisis de riesgos y fortalecimiento de la seguridad de la información en el Centro de Capacitación y Actualización Profesional de la Universidad Católica de Cuenca. *MQRInvestigar*, *7*(4), 500-514.

Díaz, J. (2020). *Sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en la biblioteca de la universidad de la costa*. https://repositorio.cuc.edu.co/bitstream/handle/11323/7436/SISTEMA%20DE%20GESTI%c3%93N%20PARA%20LA%20SEGURIDAD%20DE%20LA%20INFORMACI%c3%93N%20BASADO%20EN%20METODOLOG%c3%8dA%20DE%20IDENTIFICACI%c3%93N%20Y%-20AN%c3%81LISIS%20DE%20RIESGO%20EN%20LA.pdf?sequenc

Guevara, H. E. G., Huarachi, L. A., & Zanelly, G. A. L. (2021). Gestión del cambio en organizaciones educativas pospandemia. *Revista Venezolana de Gerencia*, *26*(93), 178-191.

Hermawan, A., & Novita, N. (2021). The Effect of Governance, Risk Management, and Compliance on Efforts to Minimize Potential Fraud Based on the Fraud Pentagon Concept. *Asia Pacific Fraud Journal*, *6*(1), 82-95.

Jiménez, F. A. (2022). *Guía metodológica de gestión de riesgos de seguridad de la información para la administración de los servidores virtualizados.* [Escuela Superior Politécnica de Chimborazo]. http://dspace.espoch.edu.ec/handle/123456789/18017

Morales, F., Toapanta, S., & Toasa, R. M. (2020). Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información. *Revista*

Iberica de sistemas e tecnologías de informacao, *E27*, 553-565.

Ñañez, O. (2021). *Modelo gestión de riesgos para la seguridad de la información, Universidad Nacional Toribio Rodríguez de Mendoza-Chachapoyas*. Universidad César Vallejo. https://repositorio.ucv.edu.pe/handle/20.500.12692/67841

Ortiz, A. M. (2020). *Introducción a las pruebas de penetración*. https://repository.unipiloto.edu.co/handle/20.500.12277/6863

Pachacuti, M. (2020). *Modelo de seguridad para el desarrollo de software* [PhD Thesis]. https://repositorio.umsa.bo/handle/123456789/27697

Padilla, E. P. (2023). *Análisis y evaluación de protocolos de comunicación en sistemas de video vigilancia en zonas remotas para garantizar disponibilidad del servicio.* http://dspace.espoch.edu.ec/handle/123456789/18311

Piñero, I., & Brito, G. (2023). *Prueba de un plan de contingencia y continuidad de negocio para fallo de dispositivo de borde*. https://repositorio.uci.cu/handle/123456789/10690

Prieto, Y. A., & Alvarez, J. W. (2024). *Fortalecimiento de la seguridad y privacidad de la información en una entidad pública del estado colombiano a través de la implementación de los Modelos de Seguridad y Privacidad de la Información (MSPI), Modelo de Gestión de Riegos de Seguridad Digital (MGRSD) y la Norma ISO 27001*. https://repository.unad.edu.co/handle/10596/60771

Rodríguez, D. L. (2024). *Evaluación de la seguridad de tecnología de información del Gad Municipal de Esmeraldas basado en las normas de control interno* [masterThesis]. https://repositorio.utn.edu.ec/handle/123456789/16461

Seminario, R. A. (2022). *Plan de mejora de seguridad de la información basado en la ISO/IEC 27001: 2013 en la empresa BROZZANDII Pastelería SAC Piura, 2022.* [Universidad Católica Los Ángeles de Chimbote]. https://repositorio.uladech.edu.pe/handle/20.500.13032/31892

Vargas, D. (2022). *Propuesta de solución para la modernización de accesos e identidades, bajo principios de cero confianza.* [PhD Thesis, Universidad Cenfotec]. http://repositorio.ucenfotec.ac.cr/handle/123456789/389

Vega, E. (2021). *Seguridad de la Información*. https://3ciencias.com/wp-content/uploads/2021/03/LIBRO-SEGURIDAD-INFORMACIO%CC%81N.pdf

Velásquez, E. (2022). *Metodología de evaluación para preservar la seguridad y privacidad de la información en la interoperabilidad de nubes híbridas, tomando como modelo de prueba un entorno virtual experimental*. http://repositorio.itm.edu.co/handle/20.500.12622/5786

Yungán, J. C., & Narváez, C. V. (2022). Aplicación de la Norma ISO 27001 para la seguridad de los Sistemas de Información. *Dominio de las Ciencias*, *8*(3), 1025-1041.