UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN

TEMA: ANÁLISIS DEL NIVEL DE CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LOS GAD'S CANTONALES CAÑAR, EL TAMBO Y SUSCAL.

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

AUTOR: CLAUDIO XAVIER ZHAO YUQUIPA

DIRECTOR: ING. CRISTHIAN FLORES URGILES

CAÑAR - ECUADOR

2023

DIOS, PATRIA, CULTURA Y DESARROLLO

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE

INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN

(TEMA): ANÁLISIS DEL NIVEL DE CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LOS GAD'S CANTONALES CAÑAR, EL TAMBO Y SUSCAL.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

AUTOR: CLAUDIO XAVIER ZHAO YUQUIPA

DIRECTOR: ING. CRISTHIAN FLORES URGILES

CAÑAR – ECUADOR

2023

DIOS, PATRIA, CULTURA Y DESARROLLO

DECLARACIÓN

Yo, Claudio Xavier Zhao Yuquipa, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

La Universidad Católica de Cuenca extensión Cañar puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y la Normativa actual de la institución.

Claudio Xavier Zhao Yuquipa

C.I: **030260222-2**

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por el Est. Claudio Xavier Zhao , bajo mi supervisión.

Ing. Cristhian Flores Urgilés.

DIRECTOR DEL TRABAJO INVESTIGATIVO

UNIVERSIDAD CATÓLICA DE CUENCA EXTENSION CAÑAR

Resumen

El propósito de esta investigación es evaluar hasta qué punto se desempeñan las políticas de seguridad de la información en los GAD's cantónales de Cañar El Tambo y Suscal. El enfoque de este estudio es cuantitativo, descriptivo y explicativo. Para la evaluación, se aplica la norma ISO 27001:2013 y la guía de buenas prácticas ISO 27002, permitiendo la evaluación de cada dominio y objetivos de control. El marco teórico se establece a través del análisis de documentos relacionados con el Sistema de Gestión de Seguridad de la Información (SGSI), ISO 27000, la Ley de Protección de Datos, la normativa de seguridad informática para entidades públicas en Ecuador y las directrices de seguridad de la información emitidas por las entidades reguladoras. Para entender la condición actual de los GAD's, se llevó a cabo una investigación mediante una encuesta a los administradores de las áreas tecnológicas de la información, obteniendo como resultados 2 dominios con riesgo alto, 10 con riesgo medio y 2 con riesgo bajo.

Palabras Clave: ISO, SGSI, GAD's, Datos, Dominios.

Abstract

The purpose of this research is to assess the extent to which information security policies are implemented in the Cantonal GADs (Decentralized Autonomous Governments) of Cañar. The focus of this study is quantitative, descriptive, and explanatory. For the evaluation, the ISO 27001:2013 standard and the ISO 27002 best practices guide are applied, allowing the assessment of each domain and control objective. The theoretical framework is established through the analysis of documents related to the Information Security Management System (ISMS), ISO 27000, the Data Protection Law, the computer security regulations for public entities in Ecuador, and the information security guidelines issued by regulatory entities.

To understand the current condition of the GAD's, an investigation was carried out through a survey of administrators in the information technology departments, obtaining the following results: 2 domains with high risk, 10 with medium risk, and 2 with low risk.

Keywords: ISO, SGSI, GAD's, Data, Domains.

e-ISSN: 2588-1000

Pro Sciences

Revista de Producción, Ciencias e Investigación

Análisis del nivel de cumplimiento de las Políticas de Seguridad de la Información de los GAD's cantonales Cañar, El Tambo y Suscal.

Analysis of the Compliance Level of Information Security Policies of the cantonal GAD's of Cañar, Tambo, and Suscal.

Claudio Xavier Zhao Yuquipa[1]
Categoría profesional, Universidad Católica de Cuenca, Ecuador,
cxzhaoy@est.ucacue.edu.ec

Cristhian Humberto Flores Urgilés[2]
Docente, Universidad Católica de Cuenca, Ecuador
chfloresu@ucacue.edu.ec

Cristina Mariuxi Flores Urgilés[3]
Docente, Universidad Católica de Cuenca, Ecuador
cmfloresu@ucacue.edu.ec

José Antonio Carrillo Zenteno[4]
Docente, Universidad Católica de Cuenca, Ecuador
J acarri l l oz @ucacue.edu.ec

Danny Patricio Andrade Cárdenas[5]
Docente, Universidad Católica de Cuenca, Ecuador
dp and radec@ucacue.edu.ec

ORCID

[1] Egresado (Ingeniería de Sistema).
[2]Docente Universitario
[3]Docente Universitario
[4] Docente Universitario
[5] Docente Universitario

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

INTRODUCCIÓN

En la era digital actual, la Seguridad de la Información (SI) son importantes para mantener la integridad, disponibilidad y confidencialidad de los datos y la información (Briceño, 2021). Actualmente, la información que se maneja en los Gobiernos Autónomos Descentralizados (GAD's), es aún más crítica, ya que la gestión segura y eficiente de la información es vital para la funcionalidad y confiabilidad del gobierno.

Es relevante destacar que cuando una entidad integra las Tecnologías de Información y Comunicación (TIC), es ineludible instaurar directrices de seguridad de la información con la intención de proteger datos delicados y preservar los tres cimientos esenciales de la información (Karlsson, Kolkowska, & Petersson, 2022).

Además, con el incremento de las ciberamenazas las políticas de seguridad de la información permiten asegurar resiliencia para que una organización se encuentre preparada y sea capaz de responder de manera efectiva ante un incidente, minimizando el impacto potencial.

Por lo mismo, el presente artículo se orienta en verificar el cumplimiento de las políticas de seguridad de la información para los GAD's cantonales Cañar, El Tambo y Suscal.

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

Bases Teóricas

Seguridad de la Información

Briceño (2021) comenta que:

> Es una disciplina que abarca políticas, procedimientos, tecnología y controles para minimizar los riesgos asociados con la información de una organización, incluyendo los datos de sus clientes y usuarios. Estas medidas pueden incluir firewalls, programas antivirus, cifrado de datos, políticas de contraseña, programas de formación para empleados, y más.

"Considerando el enfoque de la seguridad de la información es necesario tomar en cuenta tres elementos fundamentales como son: la confidencialidad, integridad y disponibilidad" (Baca, Vega, Corredor, & Diaz, 2020, pág. 3)

Sistema de gestión de Seguridad de la Información

Un Sistema de Gestión de Seguridad de la Información (SGSI). es un marco de trabajo que consiste en políticas, procedimientos, técnicas y sistemas que ayudan a prevenir, detectar, documentar y contrarrestar amenazas a la información (Mogollón Jimenez, 2022).

Mora et al. (2020) manifiesta que:

> Un SGSI puede ser certificado conforme a la norma ISO/IEC 27001, ya que esta norma es reconocida internacionalmente, que proporciona las especificaciones para un SGSI. Esta norma incluye aspectos como la evaluación de riesgos, el desarrollo e implementación de

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

una política de seguridad de la información, y el establecimiento de controles de seguridad.

Estándares de seguridad de la información

ISO/IEC 27001:2013

Según Álvarez (2015), es un modelo desarrollado para el estudio, implementación, control y mantenimiento de un (SGSI). En donde la seguridad de la información es "la protección de la confidencialidad, integridad, y disponibilidad, así como de los sistemas comprometidos en el procedimiento de la información" (p. 40), este debe ser un proceso dinámico que se adapte a las demandas particulares de cada organización, así como al diseño y ejecución de requisitos de seguridad acorde con la naturaleza de los procesos, la estructura organizativa y la magnitud de la entidad.

Beneficios de la Norma ISO / IEC 27001: 2013

Este estándar proporciona recursos para la instauración de un (SGSI), presentándose como una regulación que facilita a las organizaciones, tanto públicas como privadas, la administración y aplicación efectiva de las directrices de seguridad, las mismas que son indispensables para supervisar la condición y el uso de la información, entre otras alternativas (LASSO & LÓPEZ, p. 21).

e-ISSN: 2588-1000

Pro Sciences

Revista de Producción, Ciencias e Investigación

*Tabla 1. Beneficios de ISO/IEC 27001:2013. **Fuente**: (LASSO & LÓPEZ, 2016).*

	Beneficios de ISO/ IEC 27001:2013
1	Establece un compromiso significativo con la protección de la información. Hay protocolos y estrategias de control en marcha la misma que certifican la integridad de la información, y todos los esfuerzos realizados en esta dirección son verificables y demostrables.
2	Cumplimiento de requisitos legales.
3	Ayuda a una misión eficiente de las inseguridades. La organización tiene un entendimiento profundo de su estructura y de los Sistemas de Información que emplea, de los desafíos que enfrenta y de las normas de protección pertinentes. Además, se debe certificar una óptima disponibilidad de recursos y antecedentes, asegurando una continuidad ininterrumpida de las operaciones.
4	Se obtiene confianza entre todos los trabajadores de la organización.
5	Disminuye los costos con respecto a los distintos sucesos por lo que se consigue minimizar los servicios brindados de los mecanismos con los que tienen convenidos.

ISO/IEC 27002: 2013

La norma ISO/IEC 27002:2013 es una norma internacional que proporciona directrices para las mejores prácticas en la gestión de la seguridad de la información. Especifica recomendaciones para la implementación de controles de seguridad seleccionados basados en la ISO/IEC 27001. Esta norma contiene 114 controles, 35 objetivos de control y 14 dominios (Valencia-Duque & Orozco-Alzate, 2017).

e-ISSN: 2588-1000

Pro Sciences

Revista de Producción, Ciencias e Investigación

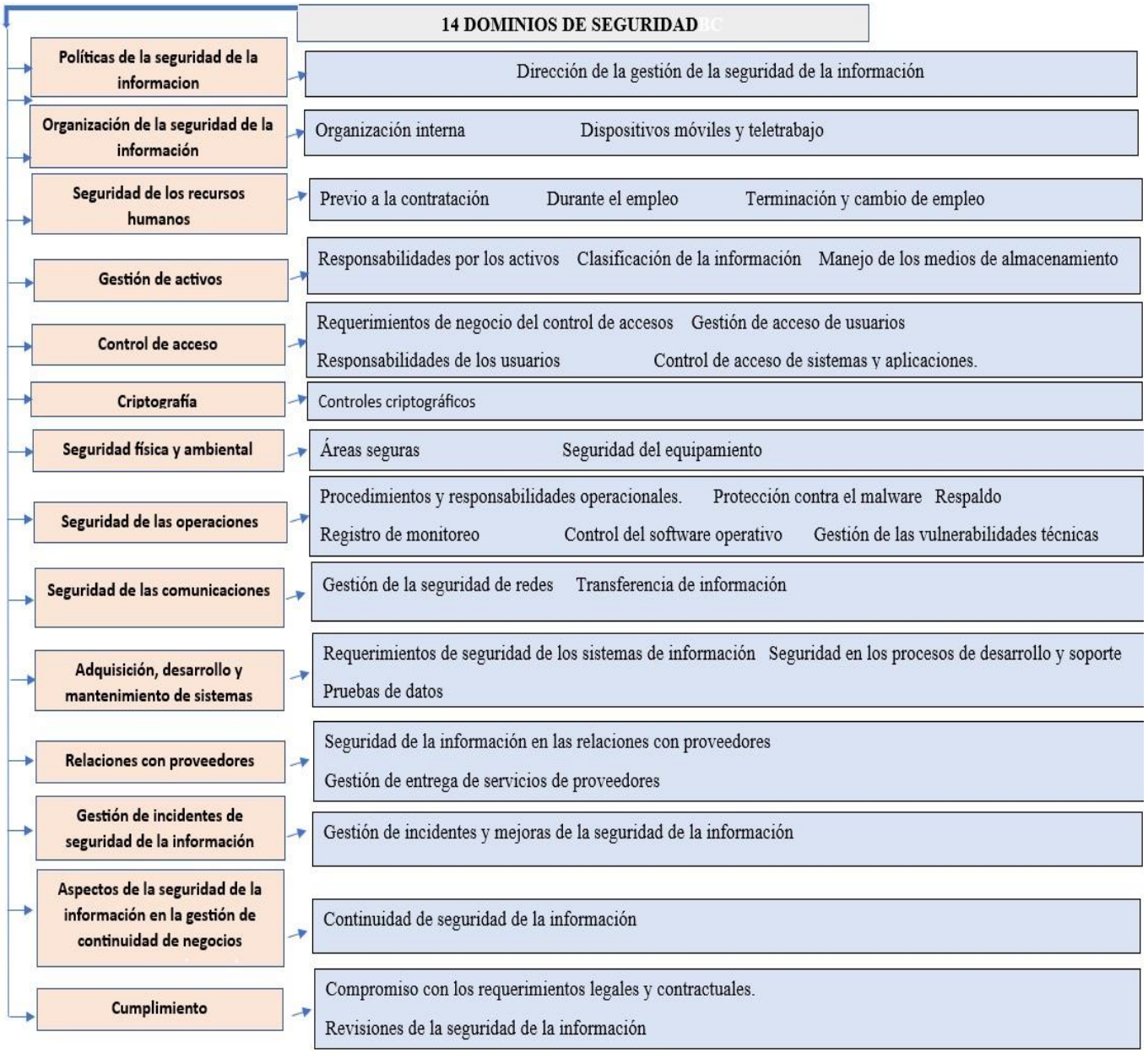

Ilustración 1. Estructura del estándar ISO 2002(dominios y controles). ***Fuente:*** (iso27000, 2012)

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

Políticas de seguridad de la información

Los objetivos de las organizaciones, empresas, en cuanto a la seguridad de la información se ven reflejadas en las normas de seguridad, junto con el compromiso de la dirección de alcanzar los objetivos propuestos teniendo en cuenta los requisitos lógicos y reglamentarios pertinentes. La política se reconoce como el primer control de la norma ISO/IEC 27002 y sirve de guía que facilita el cumplimiento de los objetivos. Es importante saber que existe una única política básica de seguridad a partir de la cual pueden establecerse diversas normas, incluidas las que rigen el acceso, el uso de dispositivos móviles, las copias de seguridad y otros temas, a distintos niveles (Valencia-Duque & Orozco-Alzate, 2017).

Ley de Protección de datos

(Álvarez L. E., 2017) , Afirma que, en febrero de 2022, Ecuador promulgó su Ley Orgánica de Protección de Datos Personales, consolidando su posición como una de las naciones latinoamericanas que más ha avanzado en este campo. Cualquier tratamiento de datos personales, ya sea público o privado, realizado en suelo ecuatoriano por personas naturales o jurídicas está sujeto a la ley.

El marco legal señala los derechos y responsabilidades asociados al tratamiento de datos personales, que puede incluir, entre otros, la recolección, almacenamiento, uso, distribución, supresión y transmisión de datos personales.

A continuación, se exponen algunos de los principales principios de la Ley Orgánica de Protección de Datos de Carácter Personal de Ecuador:

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

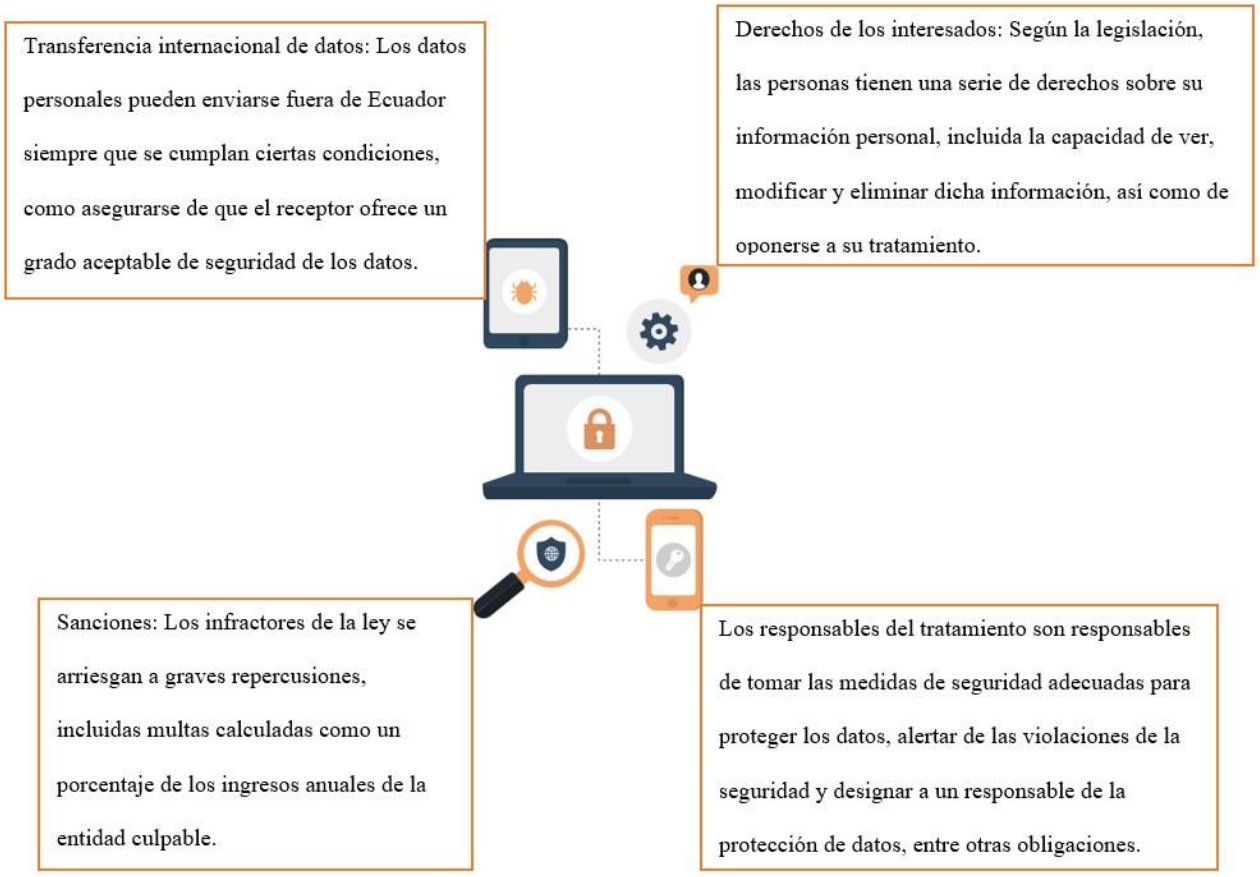

Ilustración 2. *Principios de la Ley Organiza de Protección de Datos en Ecuador.* ***Fuente****: (Álvarez L. E., 2017)*

Como con cualquier regulación, debe enfatizarse que las empresas que manejan datos personales en Ecuador deben ser plenamente conscientes de sus responsabilidades bajo este estatuto y tomar las medidas apropiadas para cumplirlo. Además, un plan integral de gestión de la información y ciberseguridad debe incluir el cumplimiento de la normativa (Lombarte, 2019).

Normativa de seguridad Informática para las Entidades Públicas en el Ecuador

La Comisión de Seguridad Informática y Tecnologías de la Información y Comunicación para el Control de las Empresas Públicas fue creada mediante

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

acuerdos ministeriales que fueron publicados en la Gaceta Oficial No. 837 del 19 de agosto de 2011 y No. 837 del 29 de julio de 2011, respectivamente, el establecimiento de normas de seguridad informática es una de las funciones importantes las distintas organizaciones ya sean públicas, instituciones o centrales, la comisión crea el Esquema Gubernamental de Seguridad de la Información (EGSI), basado en la norma ISO/IEC 27001. El EGSI forma un proceso de desarrollo que mejora continuamente en las organizaciones de la dirección pública ecuatoriana e instituye un conjunto de criterios clave para la gestión de la seguridad de la información (Orozco & Paulina, 2021, p. 45).

GAD´s Municipales

Las entidades conocidas como Gobiernos Autónomos Descentralizados (GAD) constituyen la estructura territorial del Estado Ecuatoriano y están sujetas a las regulaciones de la Constitución de la República del Ecuador (Art. 238-241) y el Código Orgánico de Organización Territorial, Autonomías y Descentralización (COOTAD) (Cepal).

"Los GAD's son organismos descentralizados con autonomía política, administrativa y financiera, y se rigen por los principios de solidaridad, subsidiariedad, equidad, integración y participación ciudadana" (Reyes, 2020, p. 198).

METODOLOGÍA

Este estudio se basa en un enfoque cuantitativo para investigar las características singulares de la gestión de seguridad en los Gobiernos Autónomos Descentralizados (GAD's) cantonales de Cañar, El Tambo y Suscal, cimentado en la norma ISO/IEC

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

27001:2013. La metodología será de naturaleza descriptiva. Esto se debe a que se realizará una encuesta, la cual facilitará la recopilación de información y permitirá explorar específicas situaciones o poblaciones determinadas.

Para recolectar datos, se utilizó una encuesta implementada en los GAD's cantonales mencionados. El diseño de la encuesta se orientó en torno a las pautas de la guía de buenas prácticas ISO/IEC 27002:2013.

En un esfuerzo por identificar los dominios de la norma que requieren mayor atención por su relevancia en la seguridad de la información, se realizó una clasificación basada en los porcentajes de cumplimiento. Para este propósito, se hizo una matriz de madurez visualizado en la Tabla 2. Este estudio promovió la selección de políticas necesarias para su incorporación en los GAD's cantonales, con el propósito de optimizar la seguridad de la información.

Tabla 2. *Porcentajes de Madurez.* ***Fuente****: (Perez, 2018)*

Riesgo	Nivel de Madurez	Límite Inferior	Límite superior
Bajo	Optimizado	91%	100%
	Administrado	71%	90%
Medio	Definido	61%	70%
	Repetible	40%	60%
Alto	Inicial	16%	39%
	Inexistente	0%	16%

e-ISSN: 2588-1000

Pro Sciences

Revista de Producción, Ciencias e Investigación

*Tabla 3. Detalle del Nivel de Madures y Riesgo. **Fuente**: (Perez, 2018, p. 30)*

Niveles de Madurez		Riesgos	
Nivel 0: Inexistente	La organización no reconoce la existencia de un problema que requiere resolución.	**Bajo**	Si la madurez se gestiona y se optimiza, el riesgo es manejable y ya ha sido evaluado en la entidad.
Nivel 1: Inicial	La organización admite que existe un problema que necesita una solución, pero no dispone de un proceso estándar que facilite una resolución completa del problema.	**Medio**	Si el nivel de madurez es repetible y definido, el riesgo es aceptable.
Nivel 2: Repetible	La organización tiene procedimientos documentados, pero no ha implementado un plan de capacitación.	**Alto**	Si el nivel de madurez es inexistente o inicial, el riesgo es inaceptable, requiere la implementación inmediata de controles.
Nivel 3: Definido	Los procedimientos están estandarizados, documentados y difundidos, pero la elección de su uso depende de cada individuo, siendo poco probable la detección de desviaciones.		
Nivel 4: Administrados	Es factible supervisar y evaluar el cumplimiento de los procesos y adoptar acciones si no funcionan eficientemente.		
Nivel 5: Optimizado	Los procesos tecnológicos se centran en la automatización de las tareas, por lo que los problemas son escasos y no impactan en el rendimiento de la organización.		

e-ISSN: 2588-1000

Pro Sciences

Revista de Producción, Ciencias e Investigación

RESULTADOS

A continuación, se muestra una representación gráfica de los resultados obtenidos en base a cada dominio de la ISO/IEC 27002: 2013.

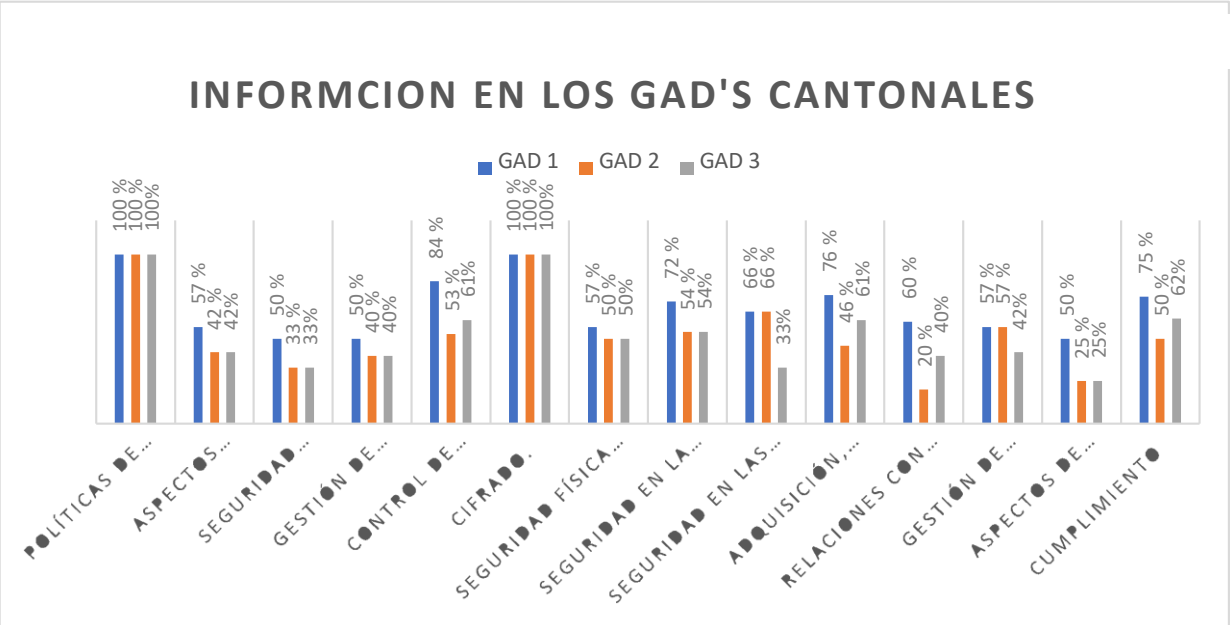

***Ilustración 3**. Nivel de Porcentaje de cada GAD, en cuanto a la Seguridad de Información en los GAD's Cantonales.*

El primer dominio, Políticas de Seguridad, muestra un cumplimiento total del 100% en los tres GAD's. Según la encueta realizada, todos poseen documentación de seguridad actualizada.

El dominio Aspectos Organizativos de la Seguridad de la Información, presenta un cumplimiento del 57% en el GAD 1 y un 42% en los GAD's 2 y 3. Este nivel más bajo se atribuye a la falta de acuerdos interinstitucionales que proporcionen servicios de seguridad.

En cuanto al dominio Seguridad Ligada a los Recursos Humanos, el GAD 1 tiene un cumplimiento del 57%, mientras que los GAD's 2 y 3 tienen un 33%. Esto se debe a

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

la ausencia de normas, en donde se dé a conocer las cláusulas respectivas de contratación y las directrices de cambios o renuncia de puestos de cargo.

El dominio Gestión de Activos muestra un cumplimiento medio del 50% en el GAD 1 y un 40% en los GAD's 2 y 3. La baja puntuación en este dominio se debe a la falta de un uso adecuado de los activos, su etiquetado y manipulación correcta.

En el dominio Control de Acceso, el GAD 1 y el GAD 3 muestran un cumplimiento del 84% y 61%, respectivamente. Esto indica que ambos GAD's cumplen con la mayoría de los controles de este dominio. Sin embargo, el GAD 2 muestra un cumplimiento del 53%, señalando deficiencias en el control de acceso y la revisión de usuarios.

En el dominio Cifrado, los tres GAD's presentan un cumplimiento perfecto del 100%. Todos ellos utilizan claves para el acceso a las instalaciones y sistemas de información.

El dominio Seguridad Física y Ambiental muestra un cumplimiento del 57% en el GAD 1, y un 50% en los GAD's 2 y 3, debido a la falta de cumplimiento de controles esenciales como el trabajo en áreas seguras y el movimiento de activos.

En la Seguridad Operativa, el GAD 1 muestra un cumplimiento del 72%, mientras que los GAD's 2 y 3 tienen un 54%, atribuido a deficiencias en restricciones para la instalación de software y la ausencia de auditorías regulares de los sistemas de información.

En el dominio Adquisición, Desarrollo y Mantenimiento del Sistema, se encontró un cumplimiento del 76% en el GAD 1 y del 61% en el GAD 3, mientras que el GAD 2

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

presenta deficiencias en los requisitos de protección y las políticas de desarrollo de sistemas.

En cuanto a las Relaciones con los Proveedores, el GAD 1 presenta un cumplimiento aceptable del 60%, mientras que el GAD 2 y 3 muestran niveles preocupantes del 20% y 40%, respectivamente, debido a la falta de políticas de seguridad de la información en relación con los proveedores.

En el dominio Gestión de Incidentes de Seguridad de la Información, los GAD's 1 y 2 muestran un cumplimiento aceptable del 57%, mientras que el GAD 3 presenta un cumplimiento menor del 42%.

En el dominio Gestión de Continuidad del Negocio, el GAD 1 muestra un cumplimiento del 50%, mientras que los GAD's 2 y 3 presentan un bajo cumplimiento del 25%, debido a deficiencias en sus planes de continuidad del negocio.

Por último, en el dominio Cumplimiento, el GAD 1 muestra un cumplimiento superior del 75%, mientras que el GAD 2 y 3 presentan un cumplimiento del 50% y 62%, respectivamente, debido a la falta de cumplimiento con los requisitos legales, contractuales, políticas y normas de seguridad.

Resultados Generales

En el ámbito de las políticas de seguridad, se ha logrado un 100% de cumplimiento, lo que indica que los GAD's cantonales están implementando todos los controles de seguridad de manera eficiente.

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

En cuanto a los aspectos organizativos de la seguridad de la información, sólo se alcanza un 47% de cumplimiento. Esta cifra refleja que la seguridad en estas áreas aún no es total.

En el dominio de la seguridad asociada a los recursos humanos, el nivel de cumplimiento es alarmantemente bajo, con tan solo un 37%. Esto sugiere una ausencia de controles o políticas que establezcan las condiciones en el momento de firmar contratos, la investigación de antecedentes, las capacitaciones y los procesos disciplinarios.

En la gestión de activos, se logra un 43% de cumplimiento. El bajo porcentaje se debe a la falta de control de activos y a la ausencia de documentación que detalle el inventario de activos, incluyendo qué activos se han devuelto, si los hubiera.

En el dominio de control de acceso, se obtiene un nivel de cumplimiento del 66%, indicando que los GAD's cantonales están implementando adecuadamente la mayoría de los controles, como la autenticación de usuarios y las restricciones de acceso a la información, redes y servicios.

En el dominio del cifrado, se logra un cumplimiento del 100% entre los GAD's cantonales. Esto significa que se están tomando medidas adecuadas para garantizar la seguridad de la información en los diversos sistemas, redes o servicios, a través de la utilización de claves de seguridad.

El dominio de seguridad física y ambiental muestra un cumplimiento del 52%, lo que indica falencias en la seguridad de los despachos. Adicionalmente, se observa una carencia en los controles para supervisar equipos o activos fuera de las instalaciones.

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

En el dominio de la seguridad operativa, se obtiene un nivel del 60%, reflejando que se están cumpliendo con la mayoría de los controles, como la protección contra código malicioso, la protección de los registros de información, y las restricciones para la instalación de software.

El dominio de seguridad de las telecomunicaciones muestra un cumplimiento del 55%, evidenciando que no se están implementando los dispositivos de seguridad inscritos a la red ni las normativas para el intercambio seguro de información.

En el dominio de adquisición, desarrollo y mantenimiento de sistemas, el nivel de cumplimiento es del 46%, lo que indica que no se están alcanzando objetivos fundamentales como el análisis y la especificación de los requisitos de seguridad de la información, el control de protección en los cambios de sistemas y el mantenimiento de un entorno seguro para el desarrollo del sistema.

Respecto a las relaciones con proveedores, el cumplimiento es del 40%, lo cual es preocupante. Esto evidencia una falta de seguimiento adecuado al gestionar cambios en los servicios de los proveedores y ausencia de políticas y condiciones específicas al firmar acuerdos.

En el dominio de gestión de incidentes de seguridad de la información, se obtiene un 52% de cumplimiento, lo cual resulta alarmante, pues se están ignorando la evaluación de eventos de seguridad de la información y la realización de informes pertinentes.

En cuanto a la seguridad de la información en la gestión de continuidad del negocio, el nivel de cumplimiento es críticamente bajo, solo un 33%, evidenciando que no se están tomando en cuenta las medidas esenciales al planificar la continuidad de la

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

seguridad de la información, ni se está garantizando la disponibilidad de las instalaciones para el procesamiento de la información.

Finalmente, en el dominio de cumplimiento, se alcanza un 62%. Aunque este porcentaje es aceptable, se requiere la implementación de varios controles, como la regulación de los controles criptográficos, la realización de una revisión independiente de la seguridad de la información y la identificación de la legislación aplicable necesaria.

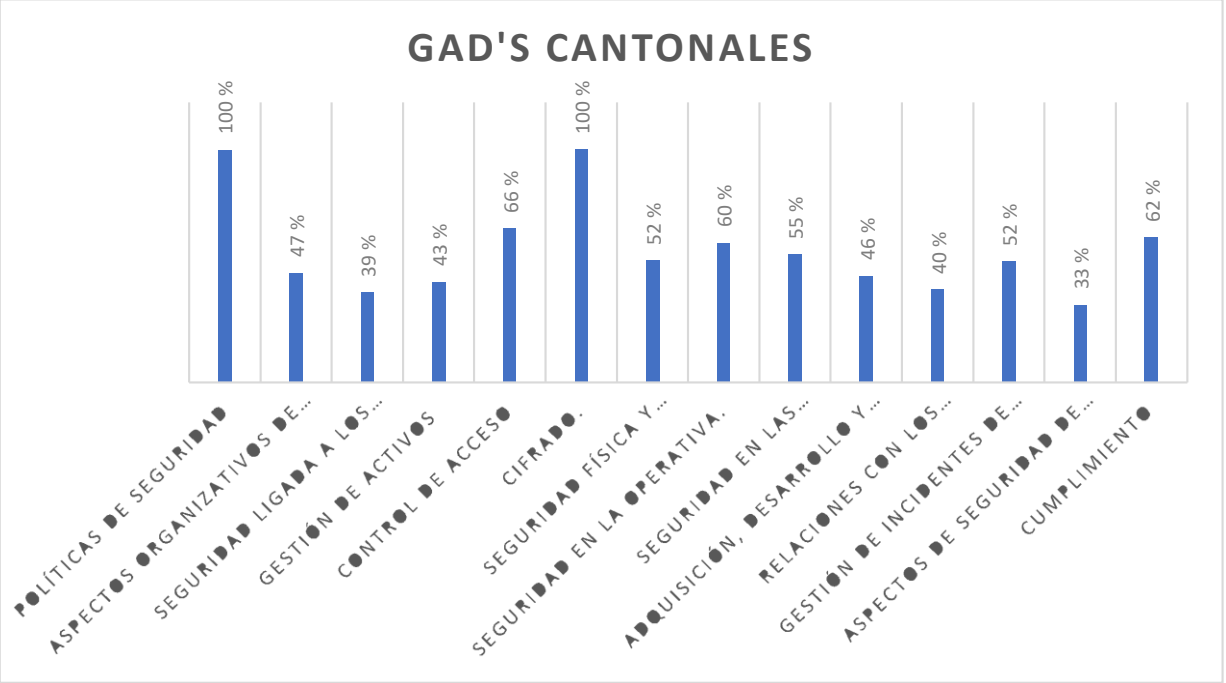

Ilustración 4. *Nivel de Porcentaje obtenido de acuerdo al cumplimiento de los dominios de seguridad de la Información.* ***Fuente:*** *Autoría Propia*

e-ISSN: 2588-1000

Pro Sciences

Revista de Producción, Ciencias e Investigación

Tabla 4: Matriz de nivel de Madurez y Riesgo. ***Fuente:*** *Autoría Propia*

Dominios ISO 27001	% de Madurez	Meta	Nivel de Madurez	Riesgo

e-ISSN: 2588-1000

Pro Sciences

Revista de Producción, Ciencias e Investigación

Gestión de incidentes de seguridad de la información	52%	100%	Repetible	
Aspectos de seguridad de la información de la Gestión de continuidad de Negocio.	33%	100%	Inicial	Alto
Cumplimiento	62%	100%	Definido	

DISCUSIÓN

En el dominio de Políticas de Seguridad, los tres GAD's han demostrado una total adherencia al mantenimiento y revisión de la documentación de seguridad, un logro importante que muestra su compromiso con los estándares de seguridad de la información.

Sin embargo, el dominio de Aspectos Organizativos presenta un cumplimiento notablemente menor, especialmente en los GAD's 2 y 3. Este resultado subraya la necesidad de establecer acuerdos interinstitucionales que proporcionen servicios de seguridad y aumenten la eficacia de las medidas de seguridad existentes.

El cumplimiento también es bajo en la Seguridad Ligada a los Recursos Humanos, lo que indica una falta de políticas claras sobre las condiciones de contratación y las directrices en caso de cambios en los roles laborales. Esto es crítico, ya que las personas

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

son a menudo el eslabón más débil en la seguridad de la información, y políticas claras en este dominio pueden mitigar el riesgo.

La Gestión de Activos y el Control de Acceso son áreas de gran importancia en la seguridad de la información. En estos dominios, se observa un cumplimiento variable entre los GAD’s, con el GAD 1 superando generalmente a los GAD’s 2 y 3. En particular, el GAD 2 muestra un cumplimiento especialmente bajo en Control de Acceso, una brecha crítica que debe ser abordada.

En el dominio de Cifrado, se alcanza el nivel máximo de cumplimiento en todos los GAD's, un aspecto esencial para la protección de la información.

Aunque el dominio de Seguridad Física y Ambiental muestra una adhesión moderada, hay margen para mejorar los controles de seguridad en el lugar de trabajo y la gestión de los activos.

La seguridad operativa, aunque con un nivel decente de cumplimiento en el GAD 1, también muestra un margen de mejora en los GAD's 2 y 3, sobre todo en aspectos como las restricciones de instalación de software y la realización de auditorías regulares.

Las Relaciones con Proveedores y la Gestión de Incidentes de Seguridad de la Información, así como la Continuidad del Negocio, también presentan deficiencias que deben ser abordadas para mitigar los riesgos y garantizar la resiliencia de las operaciones.

Finalmente, en el dominio de Cumplimiento, la discrepancia en los niveles de cumplimiento entre los GAD’s sugiere la necesidad de abordar los requisitos legales y contractuales, así como las políticas y normas de seguridad, de manera más efectiva.

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

Aunque se han hecho avances significativos en algunos dominios, queda mucho por hacer para mejorar el cumplimiento global de las políticas de seguridad de la información en los GAD's cantonales de Cañar, El Tambo y Suscal. Las áreas de enfoque clave deberían incluir la mejora de los aspectos organizativos, la seguridad ligada a los recursos humanos, la gestión de activos y el control de acceso.

CONCLUSIONES

La normativa ISO27001:2013 incorpora todos los elementos necesarios para que una organización pueda establecer un Sistema de Gestión de Seguridad de la Información (SGSI), uno de los cuales es la implementación de políticas de seguridad de la información. Dado que este SGSI se fortalece con los controles o buenas prácticas propuestas por la ISO 27002, se procedió a realizar una evaluación de estas políticas de acuerdo con los dominios y controles que la ISO 27002 define.

La inspección efectuada a los diferentes GAD's, permitió obtener un panorama fidedigno contrastado con los dominios que establece la ISO 27001. Durante este proceso, se pudo constatar que una de las principales falencias en estas instituciones financieras es la carencia de controles de seguridad de la información que la ISO 27002 recomienda.

Tras el diagnóstico realizado en los Gobiernos Autónomos Descentralizados (GAD) cantonales, se han identificado áreas de fortaleza en los dominios de *'Políticas de seguridad de la información*' y '*Cifrado*'. Sin embargo, es crucial que la organización enfoque sus esfuerzos renovados en los dominios de *'Seguridad en los Recursos Humanos*' y '*Aspectos de seguridad de la información de la Gestión de continuidad de*

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

Negocio'. Además, es necesario continuar trabajando en el resto de los dominios para seguir elevando el nivel de madurez en seguridad de la información.

e-ISSN: 2588-1000

Pro Sciences

Revista de Producción, Ciencias e Investigación

Referencias

Mogollón Jimenez, K. A. (01 de 01 de 2022). *repository.unimilitar.edu.co.* Obtenido de repository.unimilitar.edu.co: https://repository.unimilitar.edu.co/bitstream/handle/10654/41450/MogollonJimenezKarenAndrea2022.pdf?sequence=1&isAllowed=y

Álvarez, L. E. (2017). Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales. *FORO*, 19.

Álvarez, V. R. (05 de 2015). *https://tesis.pucp.edu.pe.* Obtenido de https://tesis.pucp.edu.pe: https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/6092/TALAVERA_VASCO_DISE%c3%91O_SISTEMA_GESTION.pdf?sequence=1&isAllowed=y

Baca, L. S., Vega, C. F., Corredor, C. M., & Diaz, M. A. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *scielo*, 1-11.

Briceño, E. V. (2021). *Seguridad de la información.* Editorial área de Innovación y Desarrollo, S.L.

Cepal. (s.f.). *https://observatorioplanificacion.cepal.org*. Obtenido de https://observatorioplanificacion.cepal.org/: https://observatorioplanificacion.cepal.org/es/instituciones/gobiernos-autonomos-descentralizados-de-ecuador#:~:text=Los%20Gobiernos%20Aut%C3%B3nomos%20Descentralizados%20(GAD,Autonom%C3%ADas%20y%20Descentralizaci%C3%B3n%20(COOTAD).

Guaman, A. (2022). *https://dspace.ucacue.edu.ec/*. Obtenido de https://dspace.ucacue.edu.ec/:

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

https://dspace.ucacue.edu.ec/bitstream/ucacue/12815/1/FormatoProyectoFinal%20%281%29.pdf

iso27000. (01 de 01 de 2012). *iso27000.es.* Obtenido de https://www.iso27000.es/iso27000.html

Karlsson, F., Kolkowska, E., & Petersson, J. (2022). Information security policy compliance-eliciting requirements for a computerized software to support value-based compliance analysis. *Science Direct*, 1-11.

LASSO, D. B., & LÓPEZ, N. Y. (06 de 2016). *https://repositorio.uniautonoma.edu.co/.* Obtenido de https://repositorio.uniautonoma.edu.co/: https://repositorio.uniautonoma.edu.co/bitstream/handle/123456789/551/T%20S-M%20245%202016.pdf?sequence=1&isAllowed=y

Lombarte, R. (2019). EL NUEVO DERECHO DE PROTECCIÓN DE DATOS. *Revista Española de Derecho Constitucional*, 116.

Orozco, F., & Paulina, G. (09 de 2021). *repositorio.espe.edu.ec*. Obtenido de http://repositorio.espe.edu.ec/bitstream/21000/26482/1/T-ESPE-050862.pdf

Perez, L. (22 de 2 de 2018). IDENTIFICACIÓN DEL ESTADO DE MADUREZ Y DISEÑO DE CONTROLES PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO TIC DE ESTRATEGIAS DE LA INFORMACIÓN EN EL PROCESO TIC DE ESTRATEGIAS DE LA INFORMACIÓN EN EL PROCESO. Santiago de Cali, Cai, Colombia.

Reyes, P. E., Narvaez, C. I., Erazo, J. C., & Giler, L. V. (2020). Configuración del impuesto a la patente municipal con base al ingreso de las actividades económicas. Caso: GAD Municipal de Pucará - Ecuador. *Espacios*, 197-2011.

Secaira, J. M., Ocampo, R. D., Mera, E. Z., & Kovalenko, I. E. (2020). El sistema de gestión de seguridad de la información bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior (Ecuador). *evista científico - educacional de la provincia Granma.*, 546-559.

e-ISSN: 2588-1000

Pro Sciences

Revista de Producción, Ciencias e Investigación

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado enla familia de normas ISO/IEC 27000. *Risti*, 16.

Cañar, 13 de octubre 2023

Asunto: Embargo Temporal del Trabajo de Titulación

Señor,
Ing. Leopoldo Pauta Ayabaca
DECANO DE LA UNIDAD ACADÉMICA DE ADMINISTRACIÓN DE INFROMATICA, CIENCIAS DE LACOMPUTACION, E ENOVACCION TECNOLÓGICA
Cañar.

De mi consideración:

Señor Decano, CLAUDIO XAVIER ZHAO YUQUIPA , como autora del Trabajo de Titulación "ANÁLISIS DEL NIVEL DE CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LOS GAD'S CANTONALES CAÑAR, EL TAMBO Y SUSCAL." y CRISTHIAN HUMBERTO FLORES URGILES, como director de la misma, solicitamos a usted y por su digno intermedio a Biblioteca y al responsable del repositorio institucional, el EMBARGO TEMPORAL del mismo, por un lapso de 6 meses, con la finalidad de evaluar su contenido con fines de: evaluación de artículo científico para publicación en revista indexada. Entiendo que luego de vencido este período automáticamente la obra será puesta a disposición del público bajo las normas de gestión de la Universidad.

Por la atención que sepa dar al presente, nos suscribimos de usted muy agradecidos.

Atentamente,

CLAUDIO XAVIER ZHAO YUQUIPA
CI:0302602222
Autor

C.C.: Biblioteca.