UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS

CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE INFORMACIÓN EN LAS COOPERATIVAS DE AHORRO Y CRÉDITO DEL CANTÓN CAÑAR

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

AUTOR: LUIS ANTONIO GUAMÁN ZARUMA

DIRECTOR: ECO. JORGE VINICIO CÁRDENAS MUÑOZ

CAÑAR - ECUADOR

2022

DIOS, PATRIA, CULTURA Y DESARROLLO

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS

CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE INFORMACIÓN EN LAS COOPERATIVAS DE AHORRO Y CRÉDITO DEL CANTÓN CAÑAR

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

AUTOR: LUIS ANTONIO GUAMÁN ZARUMA

DIRECTOR: ECO. JORGE VINICIO CÁRDENAS MUÑOZ

CAÑAR - ECUADOR

2022

DIOS, PATRIA, CULTURA Y DESARROLLO

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Luis Antonio Guamán Zaruma portador de la cédula de ciudadanía Nº**0302389929**. Declaro ser el autor de la obra: "Cumplimiento de las Políticas de Seguridad de Información en las Cooperativas de Ahorro y Crédito del Cantón Cañar**"**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, 20 de abril de 2022

F: .....

Luis Antonio Guamán Zaruma

C.I. 0302389929

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por el Est. Luis Antonio Guamán Zaruma, bajo mi supervisión.

Eco. Jorge Vinicio Cárdenas Muñoz

DIRECTOR DEL TRABAJO DE TITULACIÓN UNIVERSIDAD CATÓLICA DE CUENCA CAMPUS CAÑAR

CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE INFORMACIÓN EN LAS COOPERATIVAS DE AHORRO Y CRÉDITO DEL CANTÓN CAÑAR

COMPLIANCE WITH INFORMATION SECURITY POLICIES IN THE CANTON CAÑAR SAVINGS AND CREDIT COOPERATIVES

RESUMEN

El estudio tiene como fin determinar el grado de cumplimiento de las políticas de seguridad de la información en las cooperativas de ahorro y crédito del Cantón Cañar segmento 3, la metodología utilizada tiene un enfoque cuantitativo de carácter descriptivo y explicativo, se usa la norma ISO 27001:2013 y la guía de buenas prácticas ISO 27002 con el fin de evaluar cada uno de sus dominios y objetivos de control. El sustento teórico se lo realiza analizando documentos que explican sobre el Sistema de Gestión de Seguridad de la Información (SGSI), ISO 27000, Ley Orgánica de Economía Popular y Solidaria (LOEPS) y la normativa que emiten los organismos de control referente a la seguridad de los sistemas de información. Para determinar la situación actual de las cooperativas se aplicó una encuesta a los responsables del departamento de tecnologías de la información para valorar cada uno de los dominios. Los resultados indican que existen dos dominios con riesgo bajo, seis dominios tienen riesgo medio y seis dominios con riesgo alto.

Palabras Clave: seguridad, normas ISO, dominios, riesgo.

Abstract

This study aims at determining the compliance degree of the information security policies at the savings and credit cooperatives section 3 in the Canar Canton, the methodology used has a quantitative approach of descriptive and explanatory nature, the ISO 27001:2013 standard and the ISO 27002 good practice guide were used to evaluate each of its domains and control objectives. Theoretical support is carried out by analyzing documents that explain the Information Security Management System (ISMS), ISO 27000, Popular and Solidarity Economy Organic Law (PSEOL), and the regulations issued by control agencies regarding the information systems security. To determine the current situation of the organizations, a survey was directed to the information technology department heads to evaluate each of the domains. It was proved in the results that there are two areas with low risk, six with medium risk and six with high risk.

***Keywords**:* security, iso standards, areas, risk

INTRODUCCIÓN

Con el avance de la tecnología muchas de las empresas y organizaciones han reformado su práctica, la comunicación entre los empleados, la rapidez y eficacia con la que desarrollan cualquier actividad ayuda a dar solución a los problemas que se presentan a través de sistemas innovadores que son flexibles a las necesidades de cada una de ellas.

Hoy en día la información que manejan las Cooperativas de Ahorro y Crédito son reconocidos como activos sumamente importantes ya que ayuda en gran medida a la toma de decisiones, razón por la cual debe existir un mayor conocimiento de la seguridad de la información y redes de datos.

Por ende, es necesario que toda entidad financiera tenga establecido los controles de seguridad en base a sus requerimientos, que permita asegurar constantemente la confidencialidad integridad y disponibilidad de la información.

Una adecuada gestión de la seguridad de la información permite a las entidades llevar un control del cumplimiento de sus obligaciones y regulaciones, generando confianza en sus clientes al garantizar la seguridad para proteger su información y realizar eficientemente las distintas actividades administrativas y financieras de la empresa.

Es importante indicar que la información en las organizaciones puede ser manipulada por las personas que no están autorizadas, por esta razón se considera necesario implementar políticas de seguridad de la información.

Las cooperativas de ahorro y crédito tienen talento humano, tecnologías e infraestructura necesarias, pero no cuentan con la normativa para tratar la seguridad de información, para lo cual es importante conocer el rango de cumplimiento que tienen las cooperativas respecto a la aplicación del SGSI (norma ISO/IEC 27001: 2013).

MARCO TEÓRICO

1. Sistema de gestión de Seguridad de la Información (SGSI)

Un SGSI consiste en el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales. Es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos comerciales y/o de servicio (Porras, 2019).

El uso de sistemas de gestión de seguridad de la información implica una serie de pasos o etapas, destinados a mantener el nivel de competencia, rentabilidad y reputación de una empresa.

Es importante tener un SGSI debido a que ayuda a establecer políticas, analiza el riesgo y valora las diferentes amenazas, por ello trae consigo grandes beneficios, algunos de ellos se mencionan a continuación: "Estructura e inversiones adecuadas y costos correctos, control y calificación de activos, dirección de operaciones y comunicaciones, políticas de seguridad. Evaluación de riesgos Internos y a terceros" (Torres, 2020), reduce la probabilidad y el impacto de los incidentes de seguridad, direcciones de plan de Contingencia (ISO 27000, 2019).

2. Estándares asociados a la seguridad de la Información

2.1. La seguridad de la información y el gobierno corporativo

En la seguridad de la información es importante enfocar el gobierno corporativo es decir cómo se gobierna, gestiona y controla una empresa. El gobierno corporativo "actúa como una serie de interacciones entre la dirección de la compañía, su consejo de administración y otros grupos de interés social, proporciona la estructura que permite establecer los objetivos, determinando los medios para alcanzar y como supervisar el cumplimiento" (Muñoz C. , 2013, pág. 20).

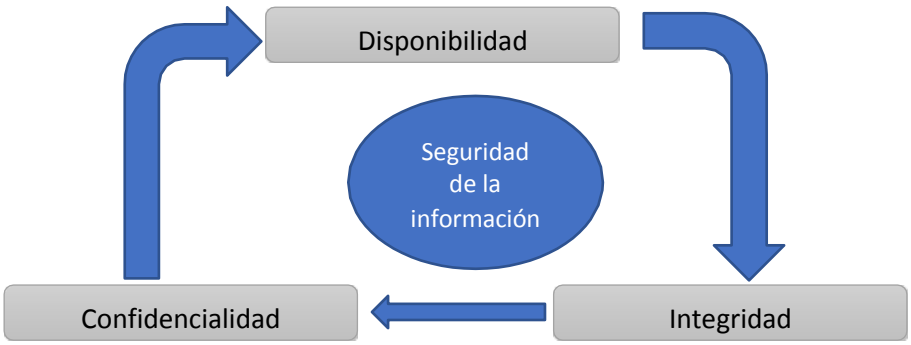
2.2. Estándar de seguridad de la Información – ISO/IEC 27001: 2013

Un SGSI no solo requiere de su implementación sino también de un mantenimiento y mejora de las medidas de seguridad, es por ello que la norma ISO 27001 otorga una solución

continua con la evaluación de los riesgos de los activos de información y con un objetivo de protección y defensa de los mismos (Torres, 2020, pág. 13).

Un SGSI, según la norma ISO/IEC 27001: 2013, busca la preservación de los tres apoyos fundamentales de la seguridad de la información: Confidencialidad, integridad y disponibilidad, las cuales son importantes para garantizar el debido resguardo y protección de la información.

Figura 1: Pilares básicos de la seguridad de la información.



Elaborado: Autor

2.3. Guía de buenas prácticas - ISO/IEC 27002

Según Moscaiza (2018) esta norma define los "objetivos y recomendaciones en materia de seguridad de la información y se anticipa a las preocupaciones globales de las organizaciones, contiene 35 objetivos de control y 114 controles agrupados en 14 dominios" (pág. 74).

Tabla 1: Estructura del estándar ISO 2002 (Dominios y controles).

Estructura de la norma		
Dominio		**Control**
1	Políticas de seguridad de la información	Dirección de la gestión de la seguridad de la información
2	Organización de la seguridad de la información	Organización interna. Dispositivos móviles y teletrabajo.
3	Seguridad de los recursos humanos	Previo a la contratación. Durante el empleo Terminación y cambio de empleo

4	Gestión de activos	Responsabilidades por los activos
		Clasificación de la información
		Manejo de los medios de almacenamiento
5	Control de acceso	Requerimientos de negocio del control de accesos
		Gestión de acceso de usuarios
		Responsabilidades de los usuarios
		Control de acceso de sistemas y aplicaciones.
6	Criptografía	Controles criptográficos
7	Seguridad física y ambiental	Áreas seguras
		Seguridad del equipamiento
8	Seguridad de las operaciones	Procedimientos y responsabilidades operacionales.
		Protección contra el malware
		Respaldo
		Registro de monitoreo
		Control del software operativo
		Gestión de las vulnerabilidades técnicas
		Consideraciones de la auditoria de sistemas de información.
9	Seguridad de las comunicaciones	Gestión de la seguridad de redes
		Transferencia de información
10	Adquisición, desarrollo y mantenimiento de sistemas	Requerimientos de seguridad de los sistemas de información
		Seguridad en los procesos de desarrollo y soporte
		Pruebas de datos.
11	Relaciones con proveedores	Seguridad de la información en las relaciones con proveedores
		Gestión de entrega de servicios de proveedores
12	Gestión de incidentes de seguridad de la información	Gestión de incidentes y mejoras de la seguridad de la información

13	Aspectos de la seguridad de la información en la gestión de continuidad de negocios	Continuidad de seguridad de la información Redundancias
14	Cumplimiento	Compromiso con los requerimientos legales y contractuales. Revisiones de la seguridad de la información

Elaborado: Autor

Fuente: *(iso27000., 2012).*

2.4. Políticas de seguridad de la información

Las políticas deben considerar los procesos, la gestión de los activos, el personal, seguridad operativa, física y ambiental, telecomunicaciones, proveedores, pero sobre todo la gestión de la información que es lo que se va a salvaguardar y para ello se recomienda hacerlo mediante un análisis con la ISO 27001:2013 (Morales, 2019).

3. Cooperativas de Ahorro y Crédito en el Ecuador

Las instituciones que cuentan con mayor cobertura en el sistema financiero ecuatoriano son los Bancos privados y las Cooperativas de Ahorro y Crédito (COACs) y, razón por la cual este estudio se focalizará en estos dos sectores.

Las COACs surgen como un movimiento de Economía Popular y Solidaria o Economía Social que propende el desarrollo y crecimiento de un territorio en base a la generación de empleo, distribución equitativa de excedentes, que, a decir de Castelló & Trías (2015) combina rentabilidad, inclusión social y gestión democrática.

La LOEPS en su artículo 21 define al sector cooperativo como sociedades de personas que se han unido en forma voluntaria para satisfacer sus necesidades económicas, sociales y culturales en común, mediante una empresa de propiedad conjunta y de gestión democrática, con responsabilidad jurídica de derecho privado e interés social (Superintendencia de Economía Popular y Solidaria, 2018).

Las cooperativas de ahorro y crédito en el Ecuador están clasificadas en cinco segmentos de acuerdo al valor de sus activos conforme se establece en la siguiente Tabla 1.

Tabla 1

Segmentos de las cooperativas de ahorro y crédito

Segmento	Activos
Segmento 1	Mayor a 80.000.000,00
Segmento 2	Mayor a 20.000.000,00 hasta 80.000.000,00
Segmento 3	Mayor a 5.000.000,00 hasta 20.000.000,00
Segmento 4	Mayor a 1.000.000,00 hasta 5.000.000,00
Segmento 5	Hasta un 1.000.000,00 Cajas de ahorro, bancos comunales y cajas comunales

Nota. Elaborado a partir de las normas para la segmentación de las entidades del sector financiero popular y solidario (2020).

La Superintendencia de Economía Popular y Solidaria (SEPS), ha emitido las resoluciones:

No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103 norma de control de las seguridades en el uso de transferencias electrónicas tiene por objeto "instituir los niveles de salvaguardia en las transferencias electrónicas realizadas mediante mensajes o instrucciones telefónicas, celulares desde un ordenador conectado a la red de comunicación a otro ordenador, mediante el uso de cualquier terminal" (Superintendencia de Economia Popular y Solidaria, 2017).

No. SEPS-IGT-IR-IGJ-2018-021 Norma respecto al control de la seguridad física y electrónica cuyo objeto es tomar las "medidas de seguridad física y electrónica de las entidades, que admitan precautelar la seguridad de sus empleados, socios, clientes y bienes, así como para el resguardo de trasporte de efectivo y valores" (Superintendencia de Economia Popular y Solidaria, 2018).

METODOLOGÍA

El enfoque de la investigación es de carácter cuantitativo por cuanto se recogerá información y datos referentes a los controles de la norma ISO/IEC 27001: 2013 aplicada en las cooperativas de ahorro y crédito segmento tres del Cantón Cañar, el nivel de investigación de tipo descriptivo ya que tiene como objetivo evaluar las características de una población o situación particular, en este caso se evalúa la gestión de la seguridad de la información en las cooperativas de ahorro y crédito de la ciudad de Cañar que pertenecen al segmento tres a través de la aplicación de la norma ISO/IEC 27002 (Muñoz & Vasques, 2017).

El levantamiento de información se realiza a través de la aplicación de una encuesta que se estructuro con los 14 dominios principales, 35 objetivos de control y 114 controles, de acuerdo a la norma ISO/IEC 27002. Los resultados de ponderación se obtienen en base a los resultados de cada control, objetivo de control y de cada dominio.

Para priorizar que dominios de la norma son los que más requieren atención o son considerados de gran importancia en la seguridad de la información, se procedió con la categorización de los dominios de acuerdo a los porcentajes de cumplimiento, para lo cual se utilizó la siguiente tabla de criterios (ver tabla 1), análisis que permitió la selección de las políticas que se requieren implementar en las cooperativas para mejorar la seguridad de la información.

Tabla 2: Porcentajes de Madurez para medir el cumplimento de los dominios ISO 27002.

Riesgo	Nivel de Madures	Límite Inferior	Limite Superior
Bajo	Optimizado	91%	100%
	Administrado	71%	90%
Medio	Definido	61%	70%
	Repetible	40%	60%
Alto	Inicial	16%	39%
	Inexistente	0%	15%

Elaborado: Propio;

Fuente: (Perez, 2018)

Niveles de Madurez

Nivel 0 – Inexistente: La empresa no admite que hay un problema que necesita solución.

Nivel 1 – Inicial: La empresa reconoce la existencia del problema que requiere solución necesaria, pero no cuentan con proceso estándar que les permita solucionar el inconveniente de manera completa

Nivel 2 - Repetible: La empresa cuenta con procedimientos documentados, pero no tiene establecido un plan de formación.

Nivel 3 – Definido: Los procedimientos son estandarizados, documentados y socializados, sin embargo, la decisión de usarlos o no es de cada individuo, siendo poco probable que se detecte extravíos.

Nivel 4 – Administrados: Es posible monitorear y evaluar el cumplimiento de los procesos y tomar medidas en caso de que no funcionen de manera eficiente.

Nivel 5 – Optimizado: Los procesos tecnológicos trabajan en la automatización de las actividades, por lo que, los problemas son mínimos y estas no afectan al rendimiento de la empresa.

Riesgo

Bajo: Si el nivel de madurez es administrado y optimizado el riesgo es pasable, y se hallan examinados en la entidad.

Medio: Si el nivel de madurez es repetible y definido el riesgo es tolerable.

Alto: Si el nivel de madurez es inexistente e inicial el riesgo es inadmisible, solicita la ejecución contigua de controles.

RESULTADOS

En el dominio político de seguridad se obtiene un 100% de cumplimiento, las cooperativas de ahorro y crédito del cantón Cañar encuestadas mencionan que cuentan con documentación de seguridad y las mismas son revisadas por la alta gerencia.

En el dominio aspectos organizativos de la seguridad de la información se obtiene un nivel de cumplimiento es de un 57%, debido a que no cuentan con acuerdos entre instituciones que les brinde servicios de seguridad.

En el dominio seguridad ligada a los recursos humanos, se obtuvo un promedio de un 58% de cumplimiento ya que las cooperativas de ahorro y crédito no cuenta con políticas en la que establezca los términos y condiciones de contratación, en caso de cambio o abandono de puesto de trabajo, no cuentan con normas que instituya la devolución del equipamiento y la eliminación de los derechos de accesos a los sistemas informáticos que les haya sido asignados.

En el dominio Gestión de activos se obtiene un promedio del 25%, esto debido a que no cuentan con documentación en el que se especifique el inventario de activos, los propietarios de los mismos y en caso de existir devolución que activos han sido devueltos.

Por otra parte, el dominio control de acceso tiene un promedio del 65%, de acuerdo a la encuesta aplicada, se llegó a determinar que ambas cooperativas de ahorro y crédito cumple con la mayoría de los controles que brinda este domino, es decir, que se hallan determinados las políticas para la gestión de redes, servicios, usuarios y contraseñas.

En el domino cifrado el nivel de cumplimiento por parte de las cooperativas de ahorro y crédito es del 100%, el acceso a las instalaciones o el acceso a cualquier sistema de información lo realizan mediante claves, por lo que llevan a cabo la gestión de claves.

Para el dominio seguridad física y ambiental el resultado es del 57%, ya que, no cumplen con todos los controles como: control físico de entrada, áreas de acceso público, carga y descarga, movimiento de activos fuera de la dependencia de la organización, seguridad de los unidades y activos fuera de las infraestructuras.

En la seguridad de las telecomunicaciones tiene un nivel de cumplimiento del 67%, ya que no cuentan con políticas o normas para intercambio de información, no se firma un acuerdo de confidencialidad entre el personal que laboran en la entidad, no se realiza una revisión técnica de las aplicaciones después de cambio en la plataforma entre otras.

En el dominio seguridad en la operativa se obtiene un promedio del 50%, dado que cumplen con la mayoría de los objetivos de control, cuentan con restricciones a la hora de realizar un a instalación de software, se realizan auditoria cada cierto tiempo a los sistemas de información, así como también se otorga responsabilidades y protección de las operaciones.

En el dominio Adquisición, desarrollo y mantenimiento del sistema se obtiene un `porcentaje del 27%, no cuentan con los requisitos para la protección de los sistemas de información, de la misma manera no disponen de políticas de seguridad en el proceso de desarrollo y soporte de sistema.

En el dominio relaciones con los proveedores se obtiene un resultado del 10%, siendo el porcentaje preocupante a diferencia de los demás dominios ya mencionados, las cooperativas de ahorro y crédito no disponen de políticas de seguridad de la información en relación con los proveedores, es decir, que no se mantiene la integridad al momento de requerir servicios por terceros.

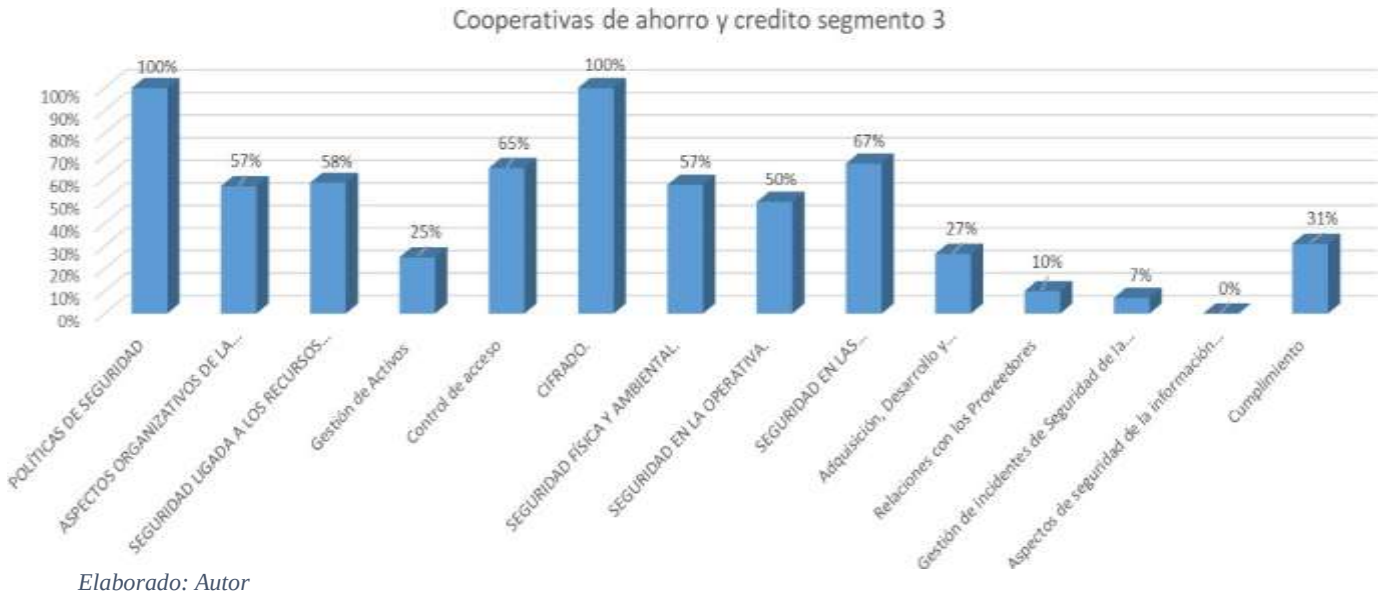
En lo que corresponde al dominio gestión de incidentes de seguridad de la Información, existe un nivel de cumplimiento bajo de las cooperativas de ahorro y crédito, con un promedio del 7%, siendo uno de los dominios más importantes y más críticos a la vez, ya que, al no contar con procedimientos documentados, se vuelve difícil la comunicación, gestión y evaluación de los acontecimientos de seguridad de la información de forma inmediata.

Aspectos de seguridad de la información de la gestión de continuidad del negocio se obtiene como resultado 0% de cumplimiento, ya que las cooperativas de ahorro y crédito segmento 3 no cuentan con un plan de continuidad de negocio, el cual permite actuar de manera óptima ante la presencia de un incidente de seguridad.

En el dominio cumplimiento, se obtiene un porcentaje del 31%, debido a que las Cooperativas de ahorro y Crédito no cumplen a su totalidad con los requisitos legales y contractuales, políticas y normas de seguridad.

A continuación, se muestra una representación gráfica de los resultados obtenidos en base a cada dominio de la ISO/IEC 27001: 2013.

Figura 2: Nivel de Porcentaje en cuanto al cumplimiento de los dominios de seguridad de la información:



Elaborado: Autor

Los resultados expuestos en párrafos anteriores se obtuvieron de la tabla Nº3.

Tabla 3. Matriz de nivel de Madurez y Riesgo.

Dominios ISO 27001	**% de Madurez**	**Meta**	**Nivel de Madurez**	**Riesgo**
Políticas de seguridad de la información	100%	100%	Optimizado	Bajo
Aspectos Organizativos de la Seguridad de la Información	57%	100%	Repetible	Medio
Seguridad en los Recursos Humanos	58%	100%	Repetible	
Gestión de Activos	25%	100%	Inicial	Alto
Control de acceso	65%	100%	Definido	Medio
Cifrado	100%	100%	Optimizado	Bajo
Seguridad Física y Ambiental	57%	100%	Repetible	

Seguridad en la operativa	50%	100%	Repetible	Medio
Seguridad en las telecomunicaciones	67%	100%	Definido	
Adquisición, desarrollo y mantenimiento de sistemas	27%	100%	Inicial	Alto
Relaciones con los proveedores	10%	100%	Inexistentes	
Gestión de incidentes de seguridad de la información	7%	100%	Inexistente	
Aspectos de seguridad de la información de la Gestión de continuidad de Negocio.	0%	100%	Inexistente	
Cumplimiento	31%	100%	Inicial	

Nota: Elaboración propia

Fuente: *(iso27000., 2012)*

DISCUSIÓN

Teniendo en cuenta que los dominios y controles de la norma ISO/IEC 27001:2013 están encaminados a resguardar la seguridad de las personas, de las instalaciones física y lógica, de los patrimonios tecnológicos y por ende de la información, garantiza el cumplimiento de la normativa vigente conexo con la seguridad de la información y en base a los resultados encontrados se realiza un análisis de los niveles de Madurez de cada uno de los dominios.

Nivel Inexistente (menor o igual a 39%) encontramos los dominios:

- Gestión de activos.
- Adquisición y mantenimiento de sistemas.
- Relación con los proveedores.
- Gestión de incidentes de seguridad de la información.
- Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio.
- Cumplimiento.

Lo cual constituye un riesgo ALTO para estas entidades, debido al abandono de estos controles que componen un nivel bajo de resguardo y el incumplimiento de las normativas vigentes relacionados con la seguridad de la información.

Nivel Definido (Mayor a 39 y menor a 70) tenemos a los dominios:

- Aspectos organizativos de la seguridad de la información.
- Seguridad en los recursos humanos.
- Control de acceso, seguridad física y ambiental.
- Seguridad en la operativa, seguridad en las telecomunicaciones.

Cuyo cumplimiento por parte de las cooperativas de ahorro y crédito segmento 3 implica un riesgo MEDIO, ya que existen controles que no se encuentran debidamente implementados y documentados.

Nivel Optimizado (Mayor a 70%), corresponde a los siguientes dominios.

- Políticas de seguridad de la información.

- Cifrado.

Siendo un riesgo BAJO para las entidades financieras, ya que los controles se encuentran efectuados, son positivos y por lo tanto avalan la debida protección de sus activos de información, manteniendo la confidencialidad, disponibilidad e integridad de los mismos.

CONCLUSIONES

La norma ISO27001:2013 recoge todos los requisitos con los que debe contar una organización para establecer un SGSI, una de ellas es la de contar con políticas de seguridad de la información, teniendo en cuenta que este sistema de gestión de seguridad se complementa con las buenas prácticas o controles establecidas por la norma ISO 27002, se realizó una evaluación de cumplimiento de las políticas en base a los dominios y controles definidos por la ISO 27002 a las diferentes Cooperativas de Ahorro y crédito segmento 3 del Cantón Cañar.

El diagnóstico realizado a las cooperativas de ahorro y crédito segmento 3, permitió consolidar la situación real en contraste a los dominios establecidos por la ISO 27001, en lo que se pudo verificar que uno de los problemas principales en las entidades financieras es la ausencia de controles de seguridad de la información establecidas por la ISO 27002.

En cuanto a la matriz realizada para determinar el nivel de madurez, se pudo constatar que existen 6 dominios de la norma que se encuentra en un nivel de bajo cumplimiento siendo estas: Gestión de activos, Adquisición y mantenimiento de sistemas, Relación con los proveedores, Gestión de incidentes de seguridad de la información, Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio, Cumplimiento, estos a su vez se encuentra en un nivel de riesgo alto, para las entidades financieras, debido a que los controles establecidos en estos dominios ayudan a conocer el manejo adecuado de los activos de información de forma que estén menos expuestas a riesgos de seguridad y si estos se presenta saber la manera en que se deben proceder para minimizar los riesgos.

Referencias

Alvarado, C. (2021). *https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas.* Obtenido de Sistema de gestion de la seguridad: Que es y sus estapas: https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas

Alvarado, L. A. (01 de 06 de 2018). *repositorio.uees.edu.ec.* Recuperado el 08 de 07 de 2021, de http://repositorio.uees.edu.ec/bitstream/123456789/3059/1/PACHECO%20ALVARADO%20LUIS%20ANGEL.pdf

Asamblea Nacional Republica del Ecuador . (12 de 9 de 2014). *pge.gob.ec.* Obtenido de pge.gob.ec: http://www.pge.gob.ec/documents/Transparencia/antilavado/REGISTROOFICIAL332.pdf

Aucapiña., T. V. (01 de 06 de 2012). *repositorio.uta.edu.ec.* Recuperado el 01 de 01 de 2021, de https://repositorio.uta.edu.ec/bitstream/123456789/2361/1/Tesis_t715si.pdf

Cardenas M, J., Treviño Saldivar, E., Cuadrado Sanchez, G., & Ordoñez Parra, J. (2021). Análisis comparativo entre cooperativas de ahorro y crédito y bancos en el Ecuador. *Socialium*, 159-184. Obtenido de http://www.aeca1.org/pub/on_line/comunicaciones_xvicongresoaeca/cd/169i.pdf

Cooperativa Policia Nacional. (01 de 01 de 2013). *cpn.fin.ec.* Obtenido de cpn.fin.ec: https://cpn.fin.ec/frontend/web/pdf/REGLAMENTO%20INTERNO%20CPN%20.pdf

Espinoza, M. A. (01 de 01 de 2018). *dspace.espoch.edu.ec.* Recuperado el 08 de 07 de 2021, de http://dspace.espoch.edu.ec/bitstream/123456789/8880/1/82T00864.pdf

Mantilla, A. (01 de 06 de 2019). *bibdigital.epn.edu.ec.* Recuperado el 01 de 01 de 2021, de https://bibdigital.epn.edu.ec/bitstream/15000/8103/4/CD-2254.pdf

ISO 27000. (01 de 01 de 2019). *iso27000.es*. (iSO 27000) Recuperado el 10 de 06 de 2021, de https://www.iso27000.es/iso27000.html

iso27000. (01 de 01 de 2012). *iso27000.es.* Recuperado el 08 de 07 de 2021, de https://www.iso27000.es/iso27000.html

Juncos, N., & Vera, E. (s.f.). *repositorio.uade.edu.* Obtenido de repositorio.uade.edu: https://repositorio.uade.edu.ar/xmlui/bitstream/handle/123456789/2491/Juncos.pdf?isAllowed=y&sequence=1

La Comision de legislacion y codificacion . (29 de 8 de 2001). *inclusion.* Obtenido de inclusion: https://www.inclusion.gob.ec/wp-content/uploads/downloads/2012/07/LEY_DE_COOPERATIVAS.pdf

LOEPS. (2018). *LEY ORGANICA DE ECONOMIA POPULAR Y SOLIDARIA.* QUITO.

Medina Tapia, M. A. (01 de 07 de 2015). *repositorio.espe.edu.ec.* Recuperado el 08 de 07 de 2021, de http://repositorio.espe.edu.ec/jspui/bitstream/21000/10889/1/T-ESPE-049202.pdf

Morales, L. (01 de 01 de 2019). *repositorio.uta.edu.ec.* Recuperado el 10 de 06 de 2021, de https://repositorio.uta.edu.ec/bitstream/123456789/29216/1/Tesis_%20t1537msi.pdf

Moscaiza, O. (01 de 01 de 2018). *repositorioacademico.upc.edu.pe.* Recuperado el 10 de 06 de 2021, de https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/623063/MOSCAIZA_MO.pdf?sequence=5&isAllowed=y

Muñoz, C. (01 de 01 de 2013). *repositorio.uasb.edu.ec.* Obtenido de repositorio.uasb.edu.ec: https://repositorio.uasb.edu.ec/bitstream/10644/3762/1/T1316-MBA-Mu%C3%B1oz-Dise%C3%B1o.pdf

Muñoz, J., & Vasques, D. (15 de 8 de 2017). *publicaciones.ucuenca.edu.ec.* Obtenido de publicaciones.ucuenca.edu.ec: https://publicaciones.ucuenca.edu.ec

Parra M, D. A. (01 de 01 de 2012). *repository.unimilitar.edu.co.* Recuperado el 11 de 06 de 2021, de https://repository.unimilitar.edu.co/bitstream/handle/10654/6821/ParraMorenoDuverAugusto2012.pdf?sequence=2&isAllowed=y

Parra, H., Contreras, J., Diaz, D., & Lopez, E. (2016). Recuperado el 20 de 06 de 2021, de Diseño de las politicas de seguridad de la informacion de la empresa comunitaria de aceueducto de rio de oro, Cesar EMCAR: http://repositorio.ufpso.edu.co/bitstream/123456789/2860/1/26550.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. Santiago de Cali, Cai, Colombia.

Porras, M. (01 de 01 de 2019). *repositorio.upla.edu.pe.* Obtenido de repositorio.upla.edu.pe: https://repositorio.upla.edu.pe/bitstream/handle/20.500.12848/2604/T037_45702501_T.pdf?isAllowed=y&sequence=1

Reglamento a la Ley Organica de Economia Popular y Solidaria. (4 de 8 de 2020). *sep.* Obtenido de seps: https://www.seps.gob.ec/documents/20181/25522/REGLAMENTO%20GENERAL%20DE%20LA%20LEY%20ORGANICA%20DE%20ECONOMIA%20POPULAR%20Y%20SOLIDARIA%20agosto2020.pdf/66c4825b-cf79-4aa1-b995-1739be63bee3

Sanchez, S. (01 de 10 de 2014). *repository.unimilitar.edu.co.* Recuperado el 08 de 07 de 2021, de https://repository.unimilitar.edu.co/bitstream/handle/10654/12262/IMPORTANCIA%20DE%20IMPLEMENTAR%20EL%20SGSI%20EN%20UNA%20EMPRESA%20CERTIFICADA%20BASC.pdf;jsessionid=4F1B85E8E597B059C1C5FB32A478CC17?sequence=1

Silva, C. A. (01 de 01 de 2015). Diseño de un sistema de gestion de seguridad de la informacion para una entidad financiera de segundo piso. Colombia.

Superintendencia de Economia popular y solidaria. (2013). *Boletin Trimestral I.* Quito.

Superintendencia de Economia Popular y Solidaria. (23 de 11 de 2017). *seps.gob.ec*. Obtenido de seps.gob.ec: https://www.seps.gob.ec/wp-content/uploads/Resolucion-No.-SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103.pdf

Superintendencia de Economia Popular y Solidaria. (13 de 07 de 2018). *seps.gob.ec.* Obtenido de seps.gob.ec: https://www.seps.gob.ec/wp-content/uploads/SEPS-IGT-IR-IGJ-2018-021.pdf

Superintendencia de Economía Popular y Solidaria. (01 de 01 de 2018). *seps.gob.ec.* Obtenido de seps.gob.ec: https://www.seps.gob.ec/rendicion-de-cuentas?rendicion-de-cuentas-2018

Superintendencia de Economía Popular y Solidaria. (01 de 01 de 2019). *seps.gob.ec*. (SEPS) Recuperado el 10 de 06 de 2021, de https://www.seps.gob.ec/interna?-que-es-la-seps-

Torres, C. (01 de 01 de 2020). *repositorio.uta.edu.ec.* Recuperado el 10 de 06 de 2021, de https://repositorio.uta.edu.ec/bitstream/123456789/30690/3/Tesis_t1657si.pdf

Anexo 1: Ante Proyecto

Trabajo de Titulación

Tema:

Cumplimiento de las políticas de seguridad de información en las Cooperativas de Ahorro y Crédito del cantón Cañar

Unidad Académica:

Tecnologías de la Información y la Comunicación

Carrera:

Ingeniera de Sistemas

Alumno:

Luis Antonio Guamán Zaruma

Tutor:

Eco. Jorge Vinicio Cárdenas Muñoz

Abril – Agosto-2021

Universidad Católica de Cuenca

Cañar, 22 de febrero de 2021

Ingeniero

Leopoldo Pauta Ayabaca, Msc.

DECANO DE LA UNIDAD ACADÉMICA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Ciudad.

Yo, **LUIS ANTONIO GUAMAN ZARUMA**, con número de identificación **030238992-9**, alumno de la carrera de Ingeniería de Sistemas, solicito por su intermedio a Consejo Directivo la aprobación del tema de tesis **"CUMPLIMIENTO DE LAS POLITICAS DE SEGURIDAD DE INFORMACION EN LAS COOPERATIVAS DE AHORRO Y CREDITO DEL CANTON CAÑAR",** proponiendo como tutor de esta al Eco. Jorge Vinicio Cárdenas Muñoz, el tema propuesto está considerado su desarrollo en décimo ciclo, ya que estaré matriculado en la Unidad de Titulación.

Por la atención que Ud. y el Honorable Consejo Directivo le brinden a la presente, anticipo mis sentimientos de consideración y estima para cada uno de Uds.

Atentamente;

_____

Sr. LUIS ANTONIO GUAMAN ZARUMA

Estudiante de Ingeniería de Sistemas, extensión Cañar

CI: 030238992-9

Anexo: Formato del Anteproyecto.

A. TÍTULO
Cumplimiento de las políticas de seguridad de información en las Cooperativas de Ahorro y Crédito del cantón Cañar.

B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN			
Línea		**Sublinea**	
Energía eléctrica y tecnologías de la información para la innovación y el desarrollo sostenible.	**Ciencia de los ordenadores, Analítica de datos y Algoritmos computacionales**	Analítica de Datos	
		Ingeniería de Software	
		Algoritmos computacionales	
		Inteligencia de negocios	
		Gobierno de TI	
		Auditoria y Seguridad Informática	**X**
		Simulación	

C. PLANTEAMIENTO DEL PROBLEMA
La información es uno de los recursos importantes en las organizaciones, pues de ella depende no solo la base del negocio, sino el logro de los objetivos a mediano o largo plazo, debido a que la información permite la toma de decisiones. Esta es una de las razones por las cuales, actualmente todas las empresas deberían realizar una apropiada gestión de riesgos, permitiéndoles de esa forma conocer las vulnerabilidades que poseen, las amenazas a las que se encuentran expuestas y el tamaño del riesgo que tendrían de no realizar control alguno. En la actualidad, las Cooperativas utilizan la tecnología de información y comunicación (TIC) en la mayoría de los procesos internos y externos, con el objetivo de que estos sean agiles y adaptados a las necesidades de los socios. No obstante, la implementación de estas tecnologías, trae mejoras, como también puede ocasionar riesgos a la información que manejan cada una de las instituciones financieras.

La Cooperativas de Ahorro y Crédito son entidades financieras, por ello se encuentra regulada por la Superintendencia de Economía Popular y Solidaria (SEPS), entidad técnica encargada de supervisar y controlar las organizaciones del sector económico popular y solidario del país, buscando su desarrollo, estabilidad, solidez y correcto funcionamiento en el sector financiero, así como asegurar el bienestar de los usuarios para que de esta forma exista confianza en la comunidad en general.

El 23 de noviembre de 2017 se publicó la Resolución No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103, en la cual se dispuso que el sistema financiero económico popular y solidario debe incrementar los niveles de seguridad en los canales electrónicos, mejorar los controles de gestión de la infraestructura de tecnología de la información y la gestión del riesgo operativo.

Con lo expuesto en párrafos anteriores se plantea realizar la presente investigación para analizar el cumplimiento de las políticas de seguridad de la información en las Cooperativas de Ahorro y crédito segmento tres en el cantón Cañar.

D. OBJETIVO GENERAL

Analizar el cumplimiento de las políticas de seguridad de información en las Cooperativas de Ahorro y Crédito del cantón Cañar.

E. OBJETIVOS ESPECÍFICOS

1. Revisión bibliográfica relacionado con la investigación que se va a realizar.

2. Realizar el levantamiento y análisis de información para determinar el diagnóstico de la situación actual de la seguridad de la información del departamento de TIC de las Cooperativas de Ahorro y Crédito del cantón Cañar, acorde al marco de trabajo de la norma ISO/IEC 27001:2013, y la guía de buenas prácticas ISO 27002

y la normativa vigente establecida por la SEPS y la junta de política y regulación monetaria, así como la normativa y procesos internos propios de las Cooperativas.

3. Elaborar un artículo científico de la investigación realizada.

F. JUSTIFICACIÓN

Actualmente, Las organizaciones empresariales soportan su actividad de negocio en tecnologías de la información y de la comunicación, por lo que necesita dotar a sus sistemas e infraestructuras informáticas en red de las políticas y medidas de protección que garanticen el desarrollo y sostenibilidad de su actividad de negocio. [1]

Un estándar o norma es un documento de aplicación voluntaria que tiene especificaciones técnicas basadas en los resultados de la experiencia y desarrollo tecnológico. [2]

El objetivo de las normas o estándares es ayudar a las organizaciones a minimizar los riesgos y conservar los pilares de la seguridad de la información.

La presente investigación se realiza para analizar el nivel de cumplimiento de las políticas de seguridad de la información las mismas que ayudan a prevenir los riesgos a las que puedan estar expuestas los sistemas de información de las diferentes Cooperativas de Ahorro y Crédito del cantón Cañar.

G. ALCANCE

El alcance de la presente investigación tiene como finalidad analizar el cumplimiento de políticas de seguridad de las Cooperativas de Ahorro y Crédito del segmento 3 y que tienen su matriz en el cantón Cañar.

H. CONCEPTOS RELACIONADOS

Sistema de información (SI)

Es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para conseguir sus objetivos. [3]

Ataque Informáticos

El principal objetivo de la seguridad informática es proteger la información. La información tiene un gran valor, ya que el acceso a ella por parte de una persona no autorizada puede hacer daños tanto en el ámbito laboral como en el personal, pues podría acceder a información confidencial de la empresa o a archivos personales [4]

Políticas de seguridad

Recoge las directrices u objetos de una organización con respecto a la seguridad de la información. Forma parte de su política general y, por tanto, ha de ser aprobada por la dirección. El objetivo principal de la redacción de una política de seguridad es la de conciencia a todo el personal de una organización, y en particular al involucrado directamente con el sistema de la información, en la necesidad de conocer que principios rigen la seguridad de la entidad y cuáles son las normas para conseguir los objetivos de seguridad planificados [3]

Norma ISO/IEC 27001

ISO/IEC 27001, en su apartado 0.3 Compatibilidad con otros sistemas de gestión, asegura que esta norma internacional sigue las pautas marcadas en las normas ISO 9001:2000 e ISO 14001:2014 para asegurar una implementación integrada y consistente con las mencionadas normas de gestión. Esta norma internacional está diseñada para posibilitar a una organización el adaptar su SGSI a los requisitos de los sistemas de gestión [5]

ISO 27002

El estándar ISO/IEC 27002 fue creado con el objetivo de proporcionar la debida información a los responsables de la implementación de seguridad de la información. Es considerado como una

buena práctica para el desarrollar y mantener normas de seguridad en una organización y así mejorar la confidencialidad de la seguridad de la información. En él se define las estrategias de 114 controles de seguridad organizados bajo 14 dominio. [6]

I. TRABAJOS RELACIONADOS

Existen distintos autores que han desarrollado investigaciones sobre el tema, cuyos resultados han generado una guía de las mejores prácticas a tomarse a consideración. A continuación, se describe algunas de ellas:

Un estudio similar realizado en la Universidad Técnica de Ambato en la Facultad de Ingeniería en Sistema Electrónica e Industrial, proyecto de investigación, presentado previo a la obtención del título de Ingeniero en sistemas Computacionales e Informáticos, realizado por Torres Núñez Elizabeth Magdalena que lleva como título "POLÍTICAS DE SEGURIDAD DE LA INFORMACION BASADA EN LA NORMA ISO/ICE 27002:2013 PARA LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACION Y COMUNICACIÓN DE LA UNIVERSIDAD TÉCNICA DE AMBATO" que hace referencia a que todos los activos de información se encuentren protegidos se propone políticas de seguridad de la información basados en la norma ISO 27002 versión 2013, las mismas que permitirán proteger la información de accesos no autorizados, daños físicos o ambientales, y de plagios. [7]

Esta investigación servirá para conocer cuáles son los lineamientos basados en la norma ISO 27002 que se deberán de aplicar en una evaluación a las políticas de la seguridad de información.

De la misma manera un estudio realizado en la Universidad Politécnica Salesiana sede Guayaquil en la carrera de Ingeniería de Sistemas, Trabajo previo a la obtención del título de Ingeniero de sistemas realizado por Kelly Gabriela Bermúdez Molina, Edber Rafael Bailón Sánchez, con título de ANÁLISIS EN SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACION BASADO EN LA NORMA ISO/IEC 27001- SISTEMAS DE GESTIÓN DE SEGURIDAD DE

LA INFORMACION DIRIGIDO A UNA EMPRESA DE SERVICIOS FINANCIEROS. Que busca conocer las vulnerabilidades a las que están expuestas la información por la falta de aplicación de controles de seguridad. [8]

Este proyecto servirá como referencia para conocer cuáles son los controles de la norma ISO 27001 que se debería implementar en un manual de políticas de información.

J. METODOLOGÍA

El método a utilizar en el presente trabajo de investigación será descriptivo, en vista de que describirá la realidad presente de las cooperativas de ahorro y crédito referente al cumplimiento de políticas de seguridad de información. Para el cumplimiento de esta metodología se seguirá las siguientes etapas:

1. **Identificación y delimitación del problema**

En esta primera etapa de la investigación se identifica las distintas cooperativas de ahorro y crédito con la cual se va a trabajar, al personal y departamentos al cual se realizará las encuestas.

2. **Elaboración y construcción de los instrumentos**

Los instrumentos a utilizar son encuestas en base a las normas y estándares de políticas de seguridad de la información.

3. **Observación y registro de datos**

En esta etapa se va a realizar un análisis de datos en base a las encuestas aplicadas a las distintas cooperativas de Ahorro y crédito del cantón Cañar.

4. **Decodificación y categorización de la información**

Aquí los datos recopilados de las encuestas realizadas pasan a trascribirse en la matriz.

5. Análisis

Una vez que los datos han sido categorizados, procedemos a la interpretación de los mismo y su análisis con referencia a los objetivos ya antes mencionados.

K. CRONOGRAMA DE ACTIVIDADES																								
N°	ACTIVIDAD	MES I				MES II				MES III				IV				V				MEDIOS DE VERIFICACIÓN
		S 1	S 2	S 3	S 4	S 1	S 2	S 3	S 4	S1	S 2	S3	S 4	S 1	S 2	S 3	S 4	S 1	S 2	S 3	S4	
1	**Revisión bibliográfica relacionado con la investigación que se va a realizar.**																					
1.1	Revisar información científica relacionados al tema en la Bases de Datos de la Institución.																					Lista de documentos de investigación almacenados en la plataforma MENDELEY
2	**Realizar el levantamiento de información para determinar el diagnóstico de la situación actual de la seguridad de la información del departamento de TIC de las Cooperativas de Ahorro y Crédito del Cantón Cañar, acorde al marco de trabajo de la norma ISO/IEC 27001:2013, y la guía de buenas prácticas ISO 27002 y la normativa vigente establecida por la SEPS y la junta de política y regulación monetaria, así como la normativa y procesos internos propios de las cooperativas.**																					
2.1	Modelo de encuesta basado en las normas.																					Hojas de Excel
2.2	Permiso para admitir la aplicación de las encuestas.																					Oficios de Autorización de las cooperativas a las cuales se va aplicar.
2.3	Aplicación de la encuesta a los departamentos de TI.																					Hojas de Excel con sus respectivas respuestas.
2.4	Tabulación y Análisis de datos																					Documentación de resultados

3	**Elaborar un artículo científico de la investigación realizada.**																					
3.1	Construcción de un artículo científico																					Documentación
3.2	Elaboración de la introducción																					
3.3	Elaboración del estado del arte																					
3.4	Elaboración de la metodología																					
3.5	Elaboración de resultados																					
3.6	Elaboración de Discusión, conclusiones, referencias																					
3.7	Elaboración del resumen, Abstract																					Documentación del resumen.
3.8	Presentación del articulo																					Documento concluido

L. DECLARACIÓN FINAL
Los abajo firmantes declaramos bajo juramento que el proyecto descrito en este documento no ha sido presentado a otra institución nacional o internacional para su financiamiento, no causa perjuicio al ambiente, es de nuestra autoría y no transgrede norma ética alguna.

M. PARTICIPANTES	
DIRECTOR:	Eco. Jorge Vinicio Cárdenas Muñoz
ESTUDIANTE 1	Luis Antonio Guamán Zaruma

N. FIRMAS DE RESPONSABILIDAD	
Lugar:	
Fecha:	

Firmas:

Nombre:	Nombre: Luis Antonio Guamán Zaruma
CC:	C.C.:030238992-9
Director del Proyecto	**Estudiante / Egresado**

O. APROBACIÓN

Firmas:

Nombre:	Nombre:
CC:	C.C.:
Primer Par Revisor	**Segundo Par Revisor**

P. REFERENCIAS

[1] J. AREITIO BERTOLIN, Seguridad de la información. Redes, informática y sistemas de información, Madrid: Editorial Paraninfo, 2008.

[2] V. Rodrigo Raya, Gestión de Proyectos (GRADO SUPERIOR), Madrid: Grupo Editorial RA-MA, 2014.

[3] P. A. López, Seguridad Informatica, Editex, 2010.

[4] C. V. MIRANDA, Sistemas informáticos y redes locales, Madrid: Ediciones Paraninfo, S.A., 2005.

[5] A. L. Mesquia, A. Mas, E. Amengual y I. Cabestrero, «Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001,» *REICIS. Revista Española de Innovación, Calidad e Ingeniería del Software,* p. 11, 2010.

[6] ISOTools Excellence, «Norma ISO 27002: El dominio política de seguridad,» 3 agosto 2017. [En línea]. Available: https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/. [Último acceso: 01 marzo 2021].

[7] E. M. Torres Nuñez, «repo.uta.edu.ec,» julio 2015. [En línea]. Available: http://repo.uta.edu.ec/bitstream/123456789/13057/1/Tesis_t1030si.pdf.

[8] K. G. Bermudez Molina y E. R. Bailon Sanchez, «Analisis en seguridad informatica y seguridad de la informacion basado en la norma ISO/IEC 27001-Sistemas de gestion de seguridad de la informacion dirigido a una empresa de servicios financieros,» 01 marzo 2015. [En línea]. Available: https://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf.

[9] M. Campoverde-Molina y L. Valverde, «Accessibility analysis of the web portals of the educational institutions in Cuenca, Ecuador,» *Revista Cátedra,* vol. 2, nº 2, pp. 55-75, 2019.

[10] V. Simbaña-Gallardo y S. Luján-Mora, «Instructions about the manuscript structureof Revista Cátedra,» *Revista Cátedra,* vol. 1, nº 1, pp. 36-52, 2018.

[11] Universidad Católica de Cuenca, «Directrices para autores/as,» 2020. [En línea]. Available: https://killkana.ucacue.edu.ec/index.php/killkana_tecnico/about/submissions.

Articulo

INFORME DE ORIGINALIDAD

8%	7%	7%	4%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	aeca1.org Fuente de Internet	2%
2	repositorio.espe.edu.ec Fuente de Internet	1%
3	Submitted to Universidad Tecnológica Indoamerica Trabajo del estudiante	1%
4	www.circasia-quindio.gov.co Fuente de Internet	1%
5	www.icored.coop Fuente de Internet	1%
6	www.dspace.uce.edu.ec Fuente de Internet	1%
7	Submitted to Universidad Nacional de San Cristóbal de Huamanga Trabajo del estudiante	1%

AUTORIZACIÒN DE PUBLICACIÒN EN EL REPOSITORIO INSTITUCIONAL

Luis Antonio Guaman Zaruma portador(a) de la cédula de ciudadanía N.º 0302389929. En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación.

"Cumplimiento de las políticas de seguridad de información en las cooperativas de ahorro y crédito del cantón Cañar" de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales.

Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de este trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cañar, 30 de marzo del 2022

Luis Antonio Guaman Zaruma

0302389929