Artículo de Investigación

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

Guamán, Antonio; Cárdenas Muñoz, Jorge Vinicio

Antonio Guamán
laguamanz29@est.ucacue.edu.ec
Universidad Católica de Cuenca extensión Cañar

Jorge Vinicio Cárdenas Muñoz
jvcardenasm@ucacue.edu.ec
Universidad Católica de Cuenca extensión Cañar

Pro Sciences: Revista de Producción, Ciencias e Investigación
CIDEPRO, Ecuador
e-ISSN: 2588-1000
Periodicidad: Trimestral
Vol. 6, No. 43, 2022
editor@journalprosciences.com

Recepción: 14 Marzo 2022
Aprobación: 30 Abril 2022

DOI: https://doi.org/10.29018/issn.2588-1000vol6iss43.2022pp127-138

Cómo citar: Guamán, A., & Cárdenas Muñoz, J. V. (2022). Cumplimiento de las políticas de seguridad de información en las cooperativas de ahorro y crédito del cantón Cañar. Pro Sciences: Revista De Producción, Ciencias E Investigación, 6(43), 127-138. https://doi.org/10.29018/issn.2588-1000vol6iss43.2022pp127-138

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, las 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 establecidos 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).

Desarrollo

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 ya que amas de 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. La familia ISO 27000

"Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI y establece una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora". (Juncos & Vera, pág. 24).

2.2.1. 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).

2.2.1.1. Evolución de la norma ISO/IEC 27001: 2013

"La norma ISO/IEC 27001: 2013 es el único estándar certificable, aceptado internacionalmente de manera global para la gestión de seguridad de la información, esta norma es aplicable para todo tipo de organización sin importar el tamaño" (Ing. Mantilla, 2019).

Con el pasar de los años esta norma ha evolucionado considerablemente, inicia con la primera versión en el año 1995 con el nombre BS 7799-1(Norma británica), llegando a su última versión en la actualidad como ISO/IEC 27001:2013(Norma internacional certificable).

2.2.1.2. Componentes básicos de la norma ISO/IEC 27001:2013

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 por: los autores

2.2.2. 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 por: los autores
Fuente: (iso27000., 2012)

2.2.3. Ciclo de Deming (PDCA[1] o PHVA[2])

La norma ISO/IEC 27001: 2013 determina que para gestionar los riesgos se debe aplicar el ciclo Deming (Plan, Do, Check, Act)**,** donde la empresa establece las políticas de seguridad, en el cual se determine los procesos, procedimientos que deben cumplir los funcionarios de una empresa, con el fin de proteger la información de cada uno de ellos manejan y son responsables. Cabe recalcar que el SGSI debe contar con un seguimiento para verificar si las medidas tomadas están siendo efectivo, es decir, llevar a cabo una auditoría para manejar y mejorar el SGSI. (Sanchez, 2014)

2.3. 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).

2.3.1. Cooperativas de Ahorro y Crédito en el Ecuador

El sistema financiero está regulado por cuatro cuerpos legales: Constitución de la República del Ecuador, Código Orgánico Monetario Financiero (COMYF), la Ley Orgánica de Instituciones del Sistema Financiero; y la Ley Orgánica de Economía Popular y Solidaria (LOEPS). Así mismo los organismos de control son la Superintendencia de Bancos; y la Superintendencia de Economía Popular y Solidaria.

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.

Las cooperativas constituyen un sujeto jurídico diferenciado del conjunto de sociedades mercantiles, que presentan rasgos sustantivos derivados, entre otros, de la existencia de una regulación legal propia, con una larga tradición y; en las variadas circunstancias políticas, económicas y sociales han tenido que hacer frente demostrado su capacidad generadora de bienestar y riqueza para sus socios, constituyéndose las cooperativas en el motor de la vida económica y social en numerosos territorios y el principal instrumento empresarial al servicio de sus habitantes (Cardenas Muñoz y otros, 2021).

Según el COMYF en su artículo 445 indica que las cooperativas de ahorro y crédito son organizaciones formadas por personas naturales o jurídicas que se unen voluntariamente bajo los principios establecidos en la Ley Orgánica de Economía Popular y Solidaria (LOEPS), con el objetivo de realizar actividades de intermediación financiera y de responsabilidad social con sus socios (Asamblea Nacional Republica del Ecuador , 2014, pág. 72).

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).

[1] Plan, Do, Check, Act (Ciclo de mejora continua)

[2] Planificar, Hacer, Verificar y Actuar

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 2.

Tabla 2. 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 Economía 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 Economía 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 estructuró con los 14 dominios principales, 35 objetivos de control y 114 controles, de acuerdo a la norma ISO/IEC 27001: 2013. 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 3), análisis que permitió la selección de las políticas que se requieren implementar en las cooperativas para mejorar la seguridad de la información.

Tabla 3. Porcentajes de madurez para medir el cumplimento de los dominios ISO 27002

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

Elaborado por: los autores
Fuente: (Pérez, 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 madures es administrado y optimizado el riesgo es pasable, y se hallan examinados en la entidad.
- Medio: Si el nivel de madures es repetible y definido el riesgo es tolerable.
- Alto: Si el nivel de madures es inexistente e inicial el riesgo es inadmisible, solicita la ejecución contigua de controles.

Resultados

En el dominio políticas 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 auditoría 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.

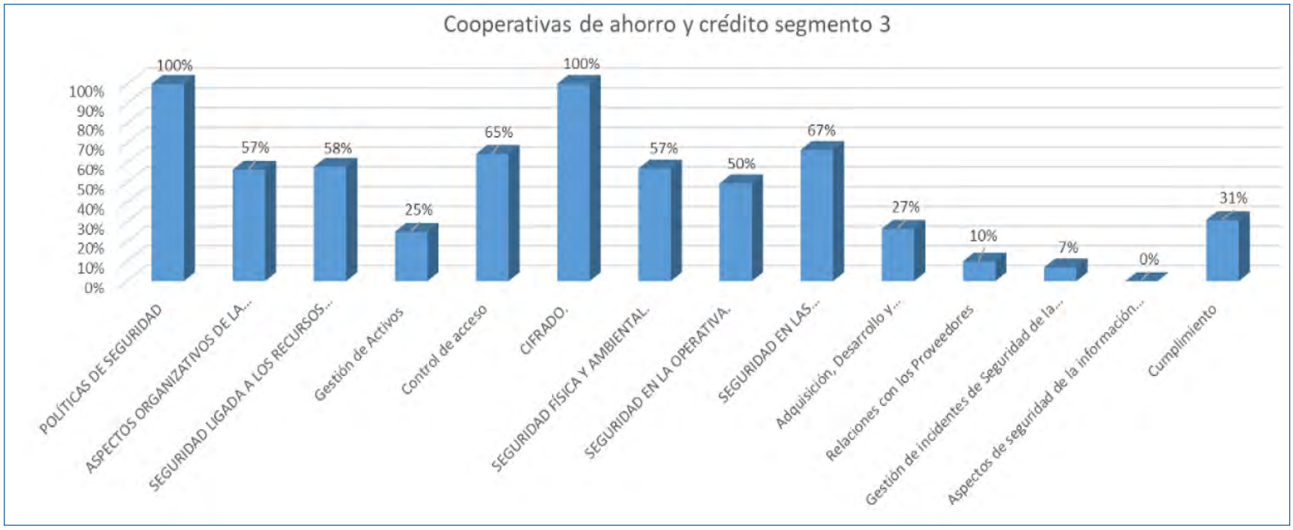

Figura 2. Nivel de Porcentaje en cuanto al cumplimiento de los dominios de seguridad de la información
Elaborado por: los autores

Los resultados expuestos en párrafos anteriores se obtuvieron de la tabla Nº 4.

Tabla 4. 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	Medio
Seguridad en la operativa	50%	100%	Repetible	
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	

Elaborado por: los autores
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%) se encuentran 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) están 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 ISO/IEC 27001: 2013, es un instrumento muy lucrativo que ayuda a identificar los aspectos que se deben tener en cuenta por las entidades financieras para instituir un modelo de seguridad de la información y estructura un adecuado SGSI.

El diagnóstico realizado a las cooperativas de ahorro y crédito segmento 3 del Cantón Cañar permite conocer la situación real frente a lo requerido por la normativa, siendo el principal problema que las políticas de seguridad de la información no se implementan en su totalidad.

Referencias Bibliográficas

- 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
- 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 Muñoz, 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
- Ing. 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 Moreno, 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 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 GESTIÓN 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 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
- Yanzapanta, J.C. (01 de 01 de 2019). *repositorio.uisek.edu.ec.* Recuperado el 08 de 07 de 2021, de https://repositorio.uisek.edu.ec/bitstream/123456789/3601/1/DISE%c3%91O%20DE%20UNA%20POL%c3%8dTICA%20DE%20SEGURIDAD%20DE%20LA%20INFORMACI%c3%93N%20PARA%20EL%20%c3%81REA%20DE%20TECNOLOG%c3%8dA%20DE%20LA%20INFORMACI%c3%93.pdf