



UNIVERSIDAD INTERNACIONAL SEK
FACULTAD DE ARQUITECTURA E INGENIERÍAS

Trabajo de fin de carrera titulado:

**“DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL
ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN DE LA COOPERATIVA DE
AHORRO Y CRÉDITO CHIBULEO LTDA., BASADO EN LA NORMA ISO/IEC
27002:2013”**

Realizado por:

Julio Cesar Pilla Yanzapanta

Director del proyecto:

Msc. Christian David Pazmiño Flores

Como requisito para la obtención del título de:

**MÁSTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN
SEGURIDAD EN REDES Y COMUNICACIÓN**

Quito, 2019

DECLARACIÓN JURAMENTADA

Yo, JULIO CESAR PILLA YANZAPANTA, con cedula de identidad 1804273090, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente

JULIO CESAR PILLA YANZAPANTA

C.C.: 1804273090

DECLARACIÓN DEL DIRECTOR DE TESIS

Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.

Christian David Pazmiño Flores

Magister en Gerencia de Sistemas y Tecnologías de la Información

CC: 1719252049

LOS PROFESORES INFORMANTES

Los Profesores informantes:

Ing. Luis Fabian Hurtado Vargas

Ing. Diego Fernando Riofrio Luzcando

Después de revisar el trabajo presentado lo han calificado
como apto para su defensa oral ante el tribunal examinador

Ing. Luis Fabian Hurtado Vargas

Ing. Diego Fernando Riofrío Luzcando

Quito, septiembre de 2019

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

Julio César Pilla Yanzapanta

CC: 1804273090

AGRADECIMIENTOS

A Dios por darme la sabiduría y mantenerme con vida para poder cumplir mis objetivos, a mis padres que me han apoyado siempre.

A la Cooperativa de Ahorro y Crédito Chibuleo Ltda., y a su gerente Rodrigo Llambo quien me permitió realizar la investigación y la propuesta.

A la Universidad Internacional SEK, al personal docente y autoridades de la Maestría en Tecnologías de la Información, por su responsabilidad, profesionalismo y compromiso en todo el proceso de formación educativa y personal, desde el inicio hasta la finalización de la carrera.

Al Ingeniero Christian Pazmiño por su gentil y valioso aporte para el desarrollo del presente proyecto.

DEDICATORIA

El presente trabajo de investigación está dedicado a mis padres Margarita e Hislayo, quienes, con su ejemplo de perseverancia, lucha constante de superación y buenos ejemplos han sido el pilar fundamental para cumplir una nueva etapa de mi vida profesional.

A Isabel, mi compañera de vida, quien, gracias a su comprensión, amor y con su ejemplo de superación me ha brindado la fuerza necesaria para continuar cumpliendo objetivos.

A mis todos mis hermanos y familiares que me han brindado su voto de confianza en cada paso que doy, gracias a su cariño me han hecho sentir que tengo una gran familia.

RESUMEN

En la actualidad, la información es uno de los activos más importantes en las organizaciones, la misma puede ser vulnerada por grupos delictivos, generando pérdidas invaluable. Un informe de la ITU (International Communication Union, por sus siglas en inglés) sitúa al Ecuador en el puesto 14 de los países de Latinoamérica y en el 98 a nivel mundial, en lo que respecta a políticas de ciberseguridad (ITU, 2019). Este ranking, evidencia que en el país es necesario continuar trabajando en el diseño e implementación de políticas de seguridad de la información en aras de prevenir ataques, los cuales pueden perjudicar a toda la estructura institucional: directivos, empleados, clientes y proveedores.

Dada esta problemática, el presente proyecto tiene como objetivo el diseño de una política de seguridad de la información para el área de Tecnología de la Información (TI) de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., basado en la norma ISO/IEC 27002:2013. Esta propuesta tiene con la finalidad mitigar posibles vulnerabilidades en los sistemas de información, estableciendo dominios, objetivos y controles para la gestión de la seguridad de la información. Previo al desarrollo de la misma, se realizó un análisis inicial del estado de la seguridad de la información del área de TI, a través de reuniones con distintos involucrados del departamento. Posteriormente, los resultados se sintetizaron en una matriz de riesgos de Deloitte (2015) y del Banco de España (2012), donde se detallan los activos de información y los riesgos a evaluar. Luego de realizado este diagnóstico, se llevo a cabo un análisis de la norma internacional ISO 27002:2013, para identificar controles aplicables y así poder mitigar los eventos de alto riesgo; y como último paso, se diseñó la política de seguridad de información para el área de Tecnología de Información.

Finalmente, se recomienda que esta política sea aprobada por el Consejo de Administración, dando paso a su posterior implementación y difusión a todos los empleados de la Cooperativa.

Palabras clave: Seguridad de la información, Norma ISO/IEC 27002:2013, Cooperativa de Ahorro y Crédito Chibuleo, política de seguridad de la información.

ABSTRACT

Currently, information is one of the most important assets in organizations, it can be violated by criminal groups, generating invaluable losses. A report from the ITU (International Communication Union) places Ecuador in 14th place in Latin America and 98 worldwide, in terms of cybersecurity policies (ITU, 2019). This ranking shows that in the country it is necessary to continue working on the design and implementation of information security policies in order to prevent attacks, which can harm the entire institutional structure: managers, employees, customers and suppliers.

With this background, this project aims to design an information security policy for the Information Technology (IT) area of the “Cooperativa de Ahorro y Crédito Chibuleo Ltd.”, based on ISO / IEC 27002: 2013, This proposal aims to mitigate possible vulnerabilities in information systems, establishing domains, objectives and controls for information security management.

Previously to the development of the same, an initial analysis of the state of information security in the IT area was carried out, through meetings with different stakeholders of the department. Subsequently, the results were synthesized in a Deloitte risk matrix (2015) and Spanish Bank (2012), where the information assets and the risks to be evaluated are detailed. After this diagnosis was made, an analysis of the international standard ISO 27002: 2013 was carried out, to identify applicable controls and thus be able to mitigate high-risk events; and as a last step, the information security policy was designed for the Information Technology area. Finally, it is recommended that this policy be approved by the Board of Directors, giving way to its subsequent implementation and dissemination to all employees of the Cooperativa Chibuleo.

Keywords: Information Security, ISO/IEC 27002:2013 Standard, “Cooperativa de Ahorro y Crédito Chibuleo”, Information Security Policy.

ÍNDICE DE CONTENIDOS

DECLARACIÓN JURAMENTADA	I
DECLARACIÓN DEL DIRECTOR DE TESIS	II
LOS PROFESORES INFORMANTES.....	III
DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE	IV
AGRADECIMIENTOS	V
DEDICATORIA	VI
RESUMEN	VII
ABSTRACT.....	VIII
ÍNDICE DE CONTENIDOS	IX
ÍNDICE DE FIGURAS.....	XIII
ÍNDICE DE TABLAS	XIV
CAPÍTULO I	1
INTRODUCCIÓN	1
1.1. EL PROBLEMA DE INVESTIGACIÓN.....	1
1.1.1. Planteamiento del problema.	1
1.1.2. Diagnóstico.....	3
1.2. PRONOSTICO.....	5
1.2.1. Control del Pronóstico.	5
1.2.2. Formulación del problema.	5
1.3. OBJETIVOS.....	6
1.3.1. Objetivo General.	6
1.3.2. Objetivos específicos.	6

1.4.	JUSTIFICACIÓN	6
1.5.	ESTADO DEL ARTE	7
CAPITULO II.....		8
MARCO TEÓRICO.....		8
2.1.	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	8
2.2.	USO DEL SGSI	10
2.2.1.	Beneficios.	10
2.3.	ISO/IEC 27001:2013	11
2.4.	ISO / EC 27002:2013	12
2.5.	CONTROLES NORMA ISO/IEC 27002:2013	13
2.6.	NORMA INTERNACIONAL ISO/IEC 27005	23
2.7.	POLÍTICAS DE SEGURIDAD	25
CAPÍTULO III.....		27
DIAGNÓSTICO SITUACIÓN.....		27
3.1.	COOPERATIVA DE AHORRO Y CRÉDITO	27
3.1.1.	Reseña Histórica	27
3.1.2.	Razón Social.	28
3.1.3.	Misión	28
3.1.4.	Visión	28
3.1.5.	Fundamentación legal	28
3.1.6.	Valores.	29
3.1.7.	Organigrama Estructural de la Empresa.	30
3.1.8.	Análisis FODA	31
3.1.9.	Análisis situacional del área de Tecnología de la Cooperativa de Ahorro y Crédito Chibuleo Ltda.	32

3.2.	ANÁLISIS Y VALORACION DE RIESGOS.....	35
3.2.1.	Selección y Análisis de las operaciones críticas.	35
3.2.2.	Aplicaciones y servicios informáticos de Tecnología.	35
3.2.3.	Principales servicios.....	36
3.2.4.	Validación de la criticidad por proceso.....	37
3.2.5.	Criticidad del riesgo.....	37
3.2.6.	Determinar las vulnerabilidades y amenazas a los activos de información.....	52
3.3.	VALORACION DE RIESGOS DE ACTIVOS DE INFORMACIÓN	66
3.3.1.	Metodología para Valoración de Riesgos.....	67
3.3.2.	Evaluación de los eventos de riesgos y calificaciones	73
3.3.3.	Aplicación de controles ISO/IEC 27002:2013.....	80
CAPÍTULO IV.....		92
DESARROLLO DE LA PROPUESTA.....		92
4.1.	ANÁLISIS	92
4.2.	INTRODUCCIÓN	92
4.3.	OBJETIVO	93
4.4.	ALCANCE.....	93
4.5.	DEFINICIONES	94
4.6.	POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN	95
SECCIÓN I: DIRECTRICES DE LA DIRECCIÓN EN SEGURIDAD DE LA INFORMACIÓN.....		95
SECCIÓN II: ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.....		97
SECCIÓN III: SEGURIDAD LIGADA A LOS RECURSOS HUMANOS		98
SECCIÓN IV: GESTIÓN DE ACTIVOS.....		100

SECCIÓN V: CONTROL DE ACCESO.....	102
SECCIÓN VI: SEGURIDAD FÍSICA Y DEL ENTORNO.....	106
SECCIÓN VII: SEGURIDAD DE OPERACIONES	109
SECCIÓN VII: SEGURIDAD EN LAS TELECOMUNICACIONES	111
SECCIÓN IX: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.....	112
SECCIÓN X: RELACIONES CON SUMINISTRADORES.....	113
SECCIÓN XI: GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	114
SECCIÓN XII: ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.....	114
RESPONSABILIDADES	115
CONTROL Y CUMPLIMIENTO.....	115
CAPÍTULO V.....	116
CONCLUSIONES Y RECOMENDACIONES.....	116
6.1. CONCLUSIONES.....	116
6.2. RECOMENDACIONES.....	117
BIBLIOGRAFÍA:	118
ANEXOS	122

ÍNDICE DE FIGURAS

Figura 1 Gráfico de un SGSI	9
Figura 2 Uso del Sistema de gestión de seguridad de la información	10
Figura 3 <i>Organigrama</i>	30
Figura 4 Riesgo del Área de tecnología de la información.....	79

ÍNDICE DE TABLAS

Tabla 1. Dominios, objetivos de control, controles	13
Tabla 2 Análisis FODA	31
Tabla 3. Criterios de valoración de activos.....	39
Tabla 4 Análisis de impacto en áreas de la Cooperativa de Ahorro y Crédito Chibuleo.....	40
Tabla 5 Procesos del área de Tecnología de Información.....	42
Tabla 6. Recursos tecnológicos que ofrece sistemas (activos).....	42
Tabla 7. Valoración de activos.....	46
Tabla 8. Amenazas y vulnerabilidades de información	52
Tabla 9. Niveles de Probabilidad	67
Tabla 10 Niveles de Severidad o Impacto	68
Tabla 11 Descripción de los Riesgos – Medición.....	69
Tabla 12. Umbrales de Riesgo	71
Tabla 13. Matriz de eventos de riesgo	73
Tabla 14. Aplicación de controles ISO/IEC 27002:2013, con la finalidad de reducir el riesgo	80

CAPÍTULO I

INTRODUCCIÓN

1.1. EL PROBLEMA DE INVESTIGACIÓN

1.1.1. Planteamiento del problema

En la actualidad, las empresas y organizaciones utilizan las Tecnologías de la Información y Comunicación (TIC) en casi todos los procesos internos y externos, con la finalidad de que éstos sean ágiles y adaptados a las necesidades de sus públicos. No obstante, la implementación de estas tecnologías, trae mejoras, también puede conllevar riesgos en lo referente a la seguridad de la información. Las instituciones sean públicas, privadas u ONG's, tienen información confidencial como bases de datos de clientes, proveedores, contratos, etc. (Cevallos, 2019).

La consultora internacional Deloitte realizó el estudio “Seguridad de la Información – Ecuador 2017” (2017), cuyo documento presenta las principales tendencias y retos a los que se enfrentan las empresas que operan en el país en relación a la seguridad de la información. En el análisis, se recoge la información de más de 50 compañías nacionales y extranjeras pertenecientes a distintos sectores económicos. Entre las conclusiones más destacadas, se reveló un panorama poco maduro en cuanto a seguridad de la información, debido a que las empresas aún no consideran este insumo como un elemento prioritario dentro de sus planes estratégicos.

Además, el informe señala que sólo un 79% de las empresas participantes tienen un responsable de seguridad de la información, mientras que un 21% no lo tiene (Deloitte, 2017). Por ello, el estudio recomienda a las empresas contar con personas encargadas de las distintas

taresas: gobierno, monitoreo y cumplimiento de la seguridad de la información; y también sensibilización y respuesta ante incidentes.

Estos datos sugieren que en el Ecuador la cultura en cuanto a seguridad de la información todavía es escasa, ya que no las organizaciones aún no son conscientes de los riesgos existentes frente a un ataque informático, pese a que el estudio de Deloitte (2017) confirma que la mitad de las empresas participantes han experimentado un incidente de seguridad interna o externa, incentivando de esta forma a destinar recursos humanos, económicos y tecnológicos para gestionar correctamente la información que poseen.

En lo que respecta a los factores de riesgo, en el ámbito externo, destacan los software maliciosos instalados por los propios usuarios, mientras que en el ámbito interno, se presentan fallas en la gestión de usuarios y el acceso a los sistemas informáticos que tiene la compañía, exponiendo la información empresarial a robos y/o pérdida de datos (Deloitte, 2017)

En función de lo expuesto anteriormente, surge la necesidad de diseñar una política de seguridad de la información para el área de TI de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., que ayude a proteger la información confidencial, este proceso se realizará utilizando la norma ISO/IEC 27002:2013. Córdova (2015) argumenta que este marco de referencia permite implementar buenas prácticas y prevenir ataques informáticos internos y externos.

Como contexto, la Cooperativa de Ahorro y Crédito Chibuleo Ltda., cuenta con un oficial de seguridad de la información, pero con funciones compartidas, debido a que no existe un departamento o un área en la cual pueda desarrollar sus actividades de mejor manera. La Cooperativa aún no asigna un presupuesto para la puesta en marcha de dichos procesos, por lo tanto dificulta el cumplimiento de las normas de seguridad de información, en el presente año se prevé implementar un departamento de seguridad integral, donde se tomarán en cuenta varias aristas sobre la seguridad y tendrá bajo su nivel jerárquico la seguridad física, electrónica y de la información.

Las funciones de estos niveles son los siguientes: seguridad física y electrónica son los encargados cumplir las normativas de la Superintendencia de Economía Popular y Solidaria, mediante, a través de una matriz de seguimiento, cumplimiento y responsables de las actividades. El producto final es la certificación del Ministerio del Interior donde se avala que

la institución es una cooperativa con los niveles de seguridad óptimos de una institución financiera.

En tanto que, el responsable de seguridad de información es el encargado de clasificar la información que posee la cooperativa sea esta física y lógica, siempre cumpliendo los principios de seguridad como son: confidencialidad, integridad y disponibilidad de información. Para el cumplimiento de la política de seguridad de información se realizará una matriz de seguimiento donde figuren los dominios de la norma ISO 27002:2013, que serán monitorizadas a través de auditorias anuales de un sistema de gestión de seguridad de la información.

1.1.2. Diagnóstico

La Cooperativa de Ahorro y Crédito Chibuleo Ltda., es una entidad financiera que tiene como objetivo brindar servicios financieros a los sectores no atendidos por la banca tradicional, especialmente del sector indígena, se creó hace 16 años en Tungurahua con la visión de contribuir con el mejoramiento socioeconómico de los socios (Cooperativa de Ahorro y Crédito Chibuleo, sf.).

Entre las funciones de la Cooperativa se encuentran la intermediación financiera y también de administración en: Captaciones, Créditos, Atención al Cliente, Tesorería, Contabilidad, Tecnología de la Información y Seguridad Física. Todas éstas recopilan información crítica y confidencial, la misma que está administrada por el área de Tecnología de Información, que además se encarga de la Administración de los servicios externos y complementarios, como brindar acceso a los proveedores a la red interna.

La información detallada en el párrafo anterior se obtuvo mediante la observación directa y una reunión realizada con jefe de tecnología, el coordinador de desarrollo y un técnico de infraestructura del área de TI de la organización, en la cual se determinó los activos de información que posee el área de tecnología (Anexo 6). A raíz de esas reuniones se pudo evidenciar los siguientes inconvenientes:

- Carencia de documentación sobre la asignación de funciones en el área de TI, la poca información existente acerca de este tema no está parametrizada, es decir, se crea bajo un criterio subjetivo y empírico de los integrantes del equipo.

- Los usuarios cuando están fuera del escritorio físico no bloquean las pantallas y esto conlleva a que otras persona accedan a las computadoras sin ningún control.
- Existen usuarios que realizan cambios de contraseñas de sus máquinas sin niveles de seguridad como utilizar letras, número y caracteres especiales.
- No existe historial de cambios de contraseñas de los equipos y sistemas informáticos.
- Los equipos no tienen actualizados los antivirus sin actualizar y son propensos a recibir ataques de usuarios internos / externos.
- Los puertos USB de las computadoras se encuentran activos en todas las área, la conexión de este dispositivo puede provocar que el equipo se infecte de un virus.
- Los usuarios no utilizan los correos institucionales para enviar información sensible entre colaboradores de la institución.
- No existen contratos de confidencialidad y de protección de datos que garanticen el resguardo y correcto uso de la información de la cooperativa.
- No existen documentos correspondientes a manuales de: programación, mesa de ayuda, uso de correos electrónicos, manuales de usuarios, manejo de claves de Tecnología de Información.
- Cuando existen errores de ejecución en el CORE financiero Financial 2.0 las únicas personas que pueden realizar correcciones son dos personas y no existen manuales.
- El área de Tecnología no cuenta con un manual actualizado, y el que posee no tiene marcos de referencia internacionales tales como COBIT, ITIL, ISO que ayuden a precautelar la información de la Cooperativa.

1.2. PRONOSTICO

El área de Tecnología de Información de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., es una de las áreas más importante de la institución, siendo un pilar fundamental en el cumplimiento de los objetivos estratégicos propuestos por la alta gerencia.

El área de tecnología de información no cuenta con una política de seguridad de la información, por lo tanto, se evidencian fallos en lo referente al almacenamiento físico y digital de los datos que posee la Cooperativa, esto trae consigo riesgos informáticos que pueden afectar a la operatividad y productividad de la institución.

El área de Tecnología no cuenta con procedimientos para el control de acceso a la información, como consecuencia se realizan ingresos no autorizados a los datos que tiene el área, lo que puede ocasionar una filtración de la información confidencial.

1.2.1. Control del Pronóstico

Al realizar un análisis al área de Tecnología de Información de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., se determinó que la institución no tiene un control de seguridad de información que ayude a mitigar posible riesgos relacionadas al correcto uso y manejo de los datos que almacena. Este proyecto plantea elaborar una política de seguridad de información, basada en la norma internacional ISO/EC 27002:2013, mediante la aplicación de los dominios y controles para definir buenas prácticas de seguridad de la información.

1.2.2. Formulación del problema

El área de Tecnología de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., reúne todos los componentes técnicos de la institución y aloja el sistema transaccional, además es donde se almacena la base de datos de socios y clientes. Sin embargo, no tienen procesos definidos para manipular la información, se han registrado inconvenientes, comprometiendo la integridad, confidencialidad y disponibilidad de los datos.

1.3. OBJETIVOS

1.3.1. Objetivo General

- Diseñar una política de seguridad de la información para el área de Tecnología de Información (TI) de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., en base a la norma ISO/IEC 27002:2013, que garantice la confidencialidad, integridad y disponibilidad de los datos de la organización.

1.3.2. Objetivos específicos

- Realizar una matriz de riesgo, mediante la recolección de datos sobre el estado actual del área de TI, para el diagnóstico de amenazas, vulnerabilidades y riesgos relacionados a la manipulación de información en la Cooperativa.
- Identificar los principales eventos de la matriz de riesgos previamente elaborada, gestionando dichos riesgos mediante los controles de la norma ISO/IEC 27002:2013.
- Definir los riesgos altos del área de TI para la revisión de los controles de la norma internacional ISO/IEC 27002:2013, además de la mitigación de los riesgos obtenidos de la matriz.

1.4.JUSTIFICACIÓN

En los últimos años, las tecnologías de la información han penetrado en los distintos sectores productivos: banca, telecomunicaciones, gran consumo, etc. Estas soluciones, buscan agilizar procedimientos generando confianza y compromiso en sus clientes, proveedores y empleados.

La Cooperativa de Ahorro y Crédito Chibuleo Ltda., no se ha alejado de esta tendencia en lo que respecta al uso de las nuevas tecnologías. Sin embargo, la institución no ha desarrollado protocolos de actuación ante posibles riesgos y vulnerabilidades. Cabe destacar que, una buena política de seguridad de la información debe mantener la confidencialidad, integridad y disponibilidad de los datos, mermando los posibles riesgos a ataques internos y externos, que pongan en evidencia errores de manejo de información por parte de la entidad.

El objetivo de diseñar una política de seguridad de información para el área de tecnología de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., es mantener un documento actualizado y efectivo que contemple normas internacionales de seguridad de información. Para ello, la norma ISO/IEC 27002:2013, es una de las opciones que mejor se adaptan a las necesidades de la Cooperativa, ya que mediante sus dominios y controles se puede establecer un adecuado monitoreo de los incidentes de seguridad que ocurren dentro de la institución.

Gracias al análisis de la norma internacional ISO/IEC 27002:2013, se pueden implementar controles de seguridad de la información y poder mitigar los eventos de riesgos que mantiene el área de tecnología de información, además se puede establecer buenas prácticas de seguridad informática en toda la institución y la concientización de los empleados.

1.5. ESTADO DEL ARTE

Actualmente, existen varios estudios relacionados sobre el tema a nivel nacional e internacional. Cevallos (2019) diseñó una política de seguridad de la información para el área de TI del Instituto Tecnológico Superior Central Técnico, mediante la aplicación de la norma de seguridad ISO/IEC 27002: 2013.

Asimismo, Contero (2019), en el marco de su tesis de maestría en la UISEK realizó el diseño de una política de seguridad de la información, usando la norma ISO 27002:2013 para el sistema de botones de seguridad del Ministerio del Interior.

En Colombia, Barreto (2014) realizó un caso de estudio sobre un Plan de Recuperación de Desastres (DRP) en una empresa de tecnología, para ello, el autor se plantea redactar los eventos de riesgo y tomar conciencia de que estos existen, utilizó la metodología Magerit, para caracterizar, seleccionar, gestionar y monitorizar los riesgos.

Gualpa (2017) en su tesis de maestría, realizó un plan de seguridad informática basado en la ISO 27002, para el control de accesos indebidos a la red de la Uniandes (sede Puyo), donde se detallan los controles de accesos a las áreas catalogadas críticas, lo que da una visión mucho más amplia de lo que se debe implementar, así como de las capacitaciones a llevar adelante con las personas responsables de las áreas involucradas.

CAPITULO II

MARCO TEÓRICO

2.1. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Sistema de Gestión de Seguridad de la Información (SGSI)¹, tiene los lineamientos bases para la implementación, seguimiento y mejora continua del sistema de gestión de la información, mediante los cuales garantiza la preservación de la confidencialidad, la integridad y la disponibilidad de la información, con una buena aplicación de los procesos en los sistemas de información, a través del levantamiento, seguimiento y mejora continua de los eventos de riesgos (ISO 27000,sf.). Además, el SGSI ayuda a mejorar los niveles de competitividad y rentabilidad de la organización para lograr los objetivos institucionales.

La norma internacional ISO 27001:2013, lanzada en octubre del 2005, es la que establece las pautas y requisitos para implementar, mantener y mejorar un SGSI. También, puede ser utilizada para evaluar las capacidades de la organización en la implementación de estrategias de seguridad de la información. Asimismo, permite adoptar un criterio de aceptación con clientes internos o externos.

El SGSI ayuda a cumplir requisitos para la evaluación, seguimiento y tratamiento de los riesgos de seguridad de información en función a las necesidades de la institución, los requerimientos de la norma son genéricos, de tal manera que se pueden implementar en cualquier tipo de organización sin importar su tamaño. (ISO 27000, sf.)

¹ En el ANEXO 7 se puede encontrar un glosario con Conceptos básicos de Seguridad de la Información dentro del área de tecnología

A continuación, se analiza el modelo del SGSI:

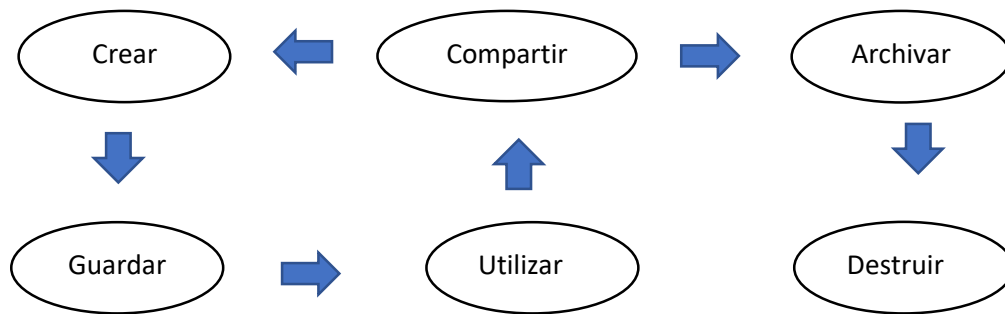


Figura 1 Gráfico de un SGSI

Fuente: ISO 27000 (sf). Recuperado de: <http://www.iso27000.es/sgsi.html>

UNE-EN (2017) categoriza a las siguientes normas dentro de las ISO 27000:

ISO/IEC 27000 Introducción y Vocabulario

ISO/IEC 27001 Requerimientos

ISO/IEC 27002 Código de buenas prácticas para sistemas de gestión de seguridad.

ISO/IEC 27003 Guía de Implementación

ISO/IEC 27004 Métricas y Mediciones

ISO/IEC 27005 Gestión del Riesgos de seguridad de la información

ISO/IEC 27006 Requerimientos para organizaciones que proveen auditorías y certificaciones

ISO/IEC 27007 Directrices de auditoría para SGSI

ISO/IEC 27008 Directrices de auditoría para controles del SGSI

ISO/IEC 27010 Directrices de seguridad para las comunicaciones entre organizaciones.

ISO/IEC 27011 Directrices de seguridad para organizaciones de telecomunicaciones

ISO/IEC 27013 Directrices para la integración de ISO 27001 e ISO 20000-1

ISO/IEC 27014 Gobierno de la seguridad de información

ISO/IEC 27015 Directrices para servicios financieros

2.2. USO DEL SGSI

El uso del SGSI es un proceso que cumple distintos ciclos y etapas, las cuales sirven para mantener los niveles de competitividad, rentabilidad y reputación corporativa. El uso de estas estrategias genera beneficios a mediano y largo plazo (ISO, 2017).

2.2.1. Beneficios

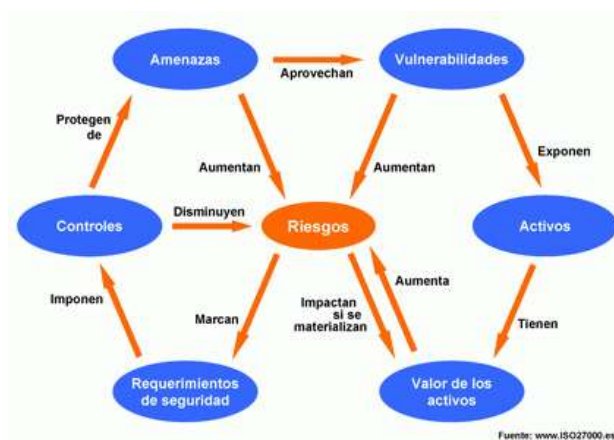


Figura 2 Uso del Sistema de gestión de seguridad de la información

Fuente: ISO 27000 (sf). Recuperado de:
<http://www.iso27000.es/sgsi.html>

A continuación, se describen algunos beneficios de la norma internacional relacionada con el uso del SGSI:

- Establece las generalidades para la administración de seguridad de la información.
- Mitiga el riesgo de pérdida, robo y corrupción de los archivos de información.
- Mejora en los controles de acceso a la información.
- Monitoreo: los controles aplicados para el control de los activos de información son revisados periódicamente.

- Aumenta la confianza entre los cliente y socios de la institución, debido a los criterios de confidencialidad que se aplican a sus datos.
- A través de las auditorías externas se puede identificar debilidades sobre la seguridad y por medio de las observaciones se puede seguir con la mejora continua.
- Tiene la posibilidad de integrar varios sistemas de gestión como son las normas internacionales (ISO 9001, ISO 14001, OHSAS 18001).
- Ayuda a que las operaciones continúen en desarrollo en caso de incidentes de seguridad de información.
- Mejora la imagen y reputación corporativa frente a la competencia local y nacional.
- El cumplimiento de los estándares de seguridad de la información le puede otorgar a la empresa la certificación ISO.
- Mejora los flujos de comunicación, en miras de que el personal interno sea conocedor de la política de seguridad de la información y pueda actuar correctamente en caso de incidentes.

Existen varias formas de realizar el robo de la información por medio de virus, hackers, y también por ataques de denegación de servicios, los cuales son peligrosos para toda la información que los sistemas informáticos proveen a las áreas de la cooperativa.

Castro (2014) señala que un SGSI es flexible y debe adaptarse a las mejoras en función de las necesidades de la organización, afirma que debe ser rmonitorizado constantemente.

2.3. ISO/IEC 27001:2013

2.3.1. Generalidades de la Norma

Es la encargada de proporcionar los requisitos para establecer un sistema de gestión de seguridad de la información (SGSI) dentro de una organización sin importar su tamaño, es aplicable para pequeñas y grandes empresas.

Siguiendo a la ISO 27001, se establece que el SGSI es la forma de preservar la confidencialidad, integridad y disponibilidad de la información, además de garantizar que todos los sistemas implicados tengan un tratamiento seguro dentro de la organización (IsoTools, 2018).

Paltán (2017) en su investigación acerca de seguridad de la información coincide con que el principal objetivo de este tipo de estrategias se concentra en el correcto uso de los datos, siempre tomando precauciones para evitar daños que puedan ocasionar crisis internas o externas.

De igual manera, Córdoba (2015) afirma que las empresas y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas externas, que aprovechan cualquier vulnerabilidad existente, y pueden acceder a los activos críticos de información. Las empresas también enfrentan diversas formas de fraude, espionaje, sabotaje o vandalismo dentro de la institución.

El SGSI es aplicable para todas las empresas, sin importar el giro del negocio, es el encargado de mantener la información a buen recaudo y disponible cuando se la requiera.

2.4. ISO / EC 27002:2013

Los controles de la ISO 27002 son los que ayudan a mantener las medidas relacionadas a seguridad de la información. Esta norma fue publicada originalmente como un cambio de nombre de la 17799 ISO. En general, describe potenciales controles y mecanismos, que pueden ser implementados siguiendo las directrices de la norma ISO 27001 (Torres, 2012, p.6).

Torres (2012) reseña los principales lineamientos para crear, mantener y gestionar un sistema de gestión de seguridad de la información de la organización, señala lo siguiente:

Los controles reales que figuran en la norma tienen por objeto atender las necesidades específicas identificadas por medio de una evaluación de riesgo formal. La norma también tiene por objeto proporcionar una guía para el desarrollo de controles de seguridad de la organización y las prácticas eficaces de gestión de la seguridad y para ayudar a construir la confianza en las actividades interinstitucionales (p.9)

La norma ISO 27002:2013 es la encargada de aplicar controles de seguridad de la información, y la ISO/IEC 27001 trata sobre la gestión de seguridad de la información, ambas están enfocadas a todo tipo de organizaciones sean (públicas y privadas), tamaños (multinacionales o nacionales, microempresas, finanzas) (Nieto, 2015)

2.5.CONTROLES NORMA ISO/IEC 27002:2013

A continuación, se definen los dominios, objetivos de control y controles de la norma que se utiliza para el análisis y el desarrollo de la política de seguridad, y se detallan los 14 dominios, 35 objetivos de control y 114 controles.

Tabla 1. Dominios, objetivos de control, controles

5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
5.1. Directrices de gestión de la seguridad de la información.
Objetivo: “Proporcionar orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativa pertinentes”. (UNE-EN, 2017, p.20)
5.1.1. Políticas de la seguridad de la información
5.1.2. Revisión de las políticas para la seguridad de la información.
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.
6.1. Organización interna
Objetivo: “Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización”. (UNE-EN, 2017, p.20)
6.1.1. Roles y responsabilidades de la información.
6.1.2. Segregación de tareas.
6.1.3. Contacto con las autoridades

<p>6.1.4. Contactos con grupos de interés especial</p> <p>6.1.5. Seguridad de información en la gestión de proyectos</p>
<p>6.2 Dispositivos para la móviles y teletrabajo.</p>
<p>Objetivo: “Garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles”. (UNE-EN, 2017, p.21)</p>
<p>6.2.1. Políticas de uso de dispositivos para movilidad</p> <p>6.2.2. Teletrabajo</p>
<p>7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.</p>
<p>7.1. Antes del empleo</p>
<p>Objetivo: Los empleados y contratistas deben tener claro sus responsabilidades y funciones (SGSI, 2017b)</p>
<p>7.1.1. Investigación de antecedentes.</p> <p>7.1.2. Términos y condiciones del empleo.</p>
<p>7.2 Durante el empleo</p>
<p>Objetivo: “Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad de la información”. (UNE-EN, 2017, p. 21)</p>
<p>7.2.1. Responsabilidades de gestión.</p> <p>7.2.2. Concienciación, educación y capacitación en seguridad de la información.</p> <p>7.2.3. Proceso disciplinario.</p>
<p>7.3 Finalización del empleo o cambio en el puesto de trabajo</p>
<p>Objetivo: “Proteger los intereses de la organización aunque se ejecute un proceso de cambio o la finalización del empleo”. (UNE-EN, 2017, p. 22)</p>
<p>7.3.1. Responsabilidades ante la finalización o cambio.</p>
<p>8. GESTIÓN DE ACTIVOS.</p>

8.1. Responsabilidad sobre los activos.

Objetivo: “Identificar los activos de la organización y definir las responsabilidades de protección adecuadas”. (UNE-EN, 2017, p. 22)

8.1.1. Inventario de activos.

8.1.2. Propiedad de los activos.

8.1.3. Uso aceptable de los activos.

8.1.4. Devolución de activos.

8.2. Clasificación de la información.

Objetivo: “Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización”. (UNE-EN, 2017, p. 22)

8.2.1. Directrices de clasificación de la información.

8.2.2. Etiquetado y manipulación de la información.

8.2.3. Manipulación de archivos de la información.

8.3. Manejo de los soportes de almacenamiento.

Objetivo: “Evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en soportes”. (UNE-EN, 2017, p. 23)

8.3.1. Gestión de soportes extraíbles.

8.3.2. Eliminación de soportes.

8.3.3. Soportes físicos en tránsito.

9. CONTROL DE ACCESO.

9.1 Requisitos de negocio para el control de acceso.

Objetivo: “Limitar el acceso a los recursos de tratamiento de la información y a la información”. (UNE-EN, 2017, p. 23)

9.1.1. Política de control de acceso

9.1.2. Control de acceso las redes y servicios asociados.

9.2. Gestión de acceso de usuarios.

Objetivo: “Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios”. (UNE-EN, 2017, p. 23)

9.2.1. Gestión de altas y bajas en el registro de usuarios.

9.2.2. Gestión de los derechos de acceso asignados a usuarios.

9.2.3. Gestión de los derechos de acceso con privilegios especiales.

9.2.4. Gestión de información confidencial de autenticación de usuarios.

9.2.5. Revisión de los derechos de acceso de los usuarios.

9.2.6. Retirada o adaptación de los derechos de acceso.

9.3. Responsabilidad del usuario.

Objetivo: “Para que los usuarios se hagan responsables de salvaguardar su información de autenticación”. (UNE-EN, 2017, p. 24)

9.3.1. Uso de información confidencial o para la autenticación.

9.4. Control de acceso a sistemas y aplicaciones.

Objetivo: “Prevenir el acceso no autorizado a los sistemas y aplicaciones”. (UNE-EN, 2017, p. 24)

9.4.1. Restricción del acceso a la información

9.4.2. Procedimientos seguros de inicio de sesión.

9.4.3. Gestión de contraseñas de usuarios.

9.4.4. Uso de utilidades con privilegios del sistema

9.4.5. Control de acceso al código fuente de los programas.

10. CRIPTOGRAFÍA.

10.1. Controles criptográficos.

Objetivo: “Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información”. (UNE-EN, 2017, p. 24)

<p>10.1.1. Políticas de uso de los controles criptográficos.</p> <p>10.1.2. Gestión de claves.</p>
<p>11. SEGURIDAD FÍSICA Y DEL ENTORNO.</p>
<p>11.1. Áreas seguras.</p>
<p>Objetivo: “Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información”. (UNE-EN, 2017, p. 25)</p>
<p>11.1.1. Perímetros de seguridad física.</p> <p>11.1.2. Controles físicos de entrada.</p> <p>11.1.3. Seguridad de oficinas, despacho y recursos.</p> <p>11.1.4. Protección contra las amenazas externas y ambientales.</p> <p>11.1.5. El trabajo en áreas seguras.</p> <p>11.1.6. Áreas de descarga y descarga.</p>
<p>11.2. Seguridad de los equipos.</p>
<p>Objetivo: “Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización”. (UNE-EN, 2017, p. 25)</p>
<p>11.2.1. Emplazamiento y protección de equipos.</p> <p>11.2.2. Instalaciones de suministro.</p> <p>11.2.3. Seguridad del cableado.</p> <p>11.2.4. Mantenimiento de los equipos.</p> <p>11.2.5. Salida de activos fuera de las dependencias de la empresa.</p> <p>11.2.6. Seguridad de los equipos y activos fuera de las instalaciones.</p> <p>11.2.7. Reutilización o retirada segura de los dispositivos de almacenamiento.</p> <p>11.2.8. Equipos informáticos de uso desatendidos.</p> <p>11.2.9 Política de puesto de trabajo despejado y pantalla limpia.</p>

12. SEGURIDAD DE LAS OPERACIONES.
12.1. Responsabilidades y procedimientos de operación.
Objetivo: “Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información”. (UNE-EN, 2017, p. 27)
<p>12.1.1. Documentación de procedimientos operacionales.</p> <p>12.1.2. Gestión de cambios.</p> <p>12.1.3. Gestión de capacidades.</p> <p>12.1.4. Separación de los recursos de desarrollo, prueba y operación.</p>
12.2. Protección contra código malicioso.
Objetivo: “Asegurar que los recursos de tratamiento de información y la información estén protegidos contra el malware”. (UNE-EN, 2017, p. 27)
12.2.1. Controles contra el código malicioso.
12.3. Copias de seguridad.
Objetivo: “Evitar la pérdida de datos”. (UNE-EN, 2017, p. 27)
12.3.1 Copias de seguridad de la información
12.4. Registros y supervisión.
Objetivo: “Registrar eventos y generar evidencias”. (UNE-EN, 2017, p. 27)
<p>12.4.1. Registro de eventos.</p> <p>12.4.2. Protección de la información de registro.</p> <p>12.4.3. Registro de administración y operación.</p> <p>12.4.4. Sincronización del reloj.</p>
12.5. Control del software en explotación.
Objetivos: “Asegurar la integridad del software en explotación”. (UNE-EN, 2017, p. 27)
12.5.1. Instalación del software en explotación

12.6. Gestión de la vulnerabilidad técnica
Objetivo: “Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas”. (UNE-EN, 2017, p. 28)
<p>12.6.1. Gestión de las vulnerabilidades técnicas.</p> <p>12.6.2. Restricción en la instalación de software.</p>
12.7. Consideraciones sobre la auditoria de sistemas de información.
Objetivo: “Minimizar el impacto de las actividades de auditoría en los sistemas operativos”. (UNE-EN, 2017, p. 28)
12.7.1 Controles de auditoría de sistemas de información
13. SEGURIDAD DE LAS COMUNICACIONES.
13.1. Gestión de la seguridad de las redes
Objetivo: “Asegurar la protección de la información en las redes”. (UNE-EN, 2017, p. 28)
<p>13.1.1. Controles de red.</p> <p>13.1.2. Mecanismos de seguridad asociado a servicios en red.</p> <p>13.1.3. Segregación en redes.</p>
13.2 Intercambio de información
Objetivo: “Mantener segura la información que se transfiere dentro y fuera de una organización”. (UNE-EN, 2017, p. 28)
<p>13.2.1. Políticas y procedimientos de intercambio de información.</p> <p>13.2.2. Acuerdos de intercambio de información.</p> <p>13.2.3. Mensajería electrónica.</p> <p>13.2.4. Acuerdos de confidencialidad o no revelación.</p>
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

14.1. Requisitos de seguridad en los sistemas de información.

Objetivo: “Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas”.
(UNE-EN, 2017, p. 29)

14.1.1. Análisis y especificación de los requisitos de seguridad.

14.1.2. Seguridad de las comunicaciones en servicios accesibles por redes públicas.

14.1.3. Protección de las transacciones por redes telemáticas.

14.2. Seguridad en el desarrollo y en los procesos de soporte.

Objetivo: “Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de los sistemas de información”. (UNE-EN, 2017, p. 29)

14.2.1. Políticas de desarrollo seguro de software.

14.2.2. Procedimientos de control de cambios en los sistemas.

14.2.3. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.

14.2.4. Restricciones a los cambios en los paquetes de software.

14.2.5. Uso de principios de ingeniería de sistemas seguros

14.2.6. Seguridad en entornos de desarrollo.

14.2.7. Externalización del desarrollo del software

14.2.8. Pruebas de funcionalidad durante el desarrollo de los sistemas.

14.2.9. Pruebas de aceptación de sistemas.

14.3. Datos de prueba.

Objetivo: “Asegurar la protección de los datos de prueba”. (UNE-EN, 2017, p. 30)

14.3.1. Protección de los datos de prueba.

15. RELACIÓN CON PROVEEDORES.

15.1. Seguridad con las relaciones con proveedores.

Objetivo: “Asegurar la protección de los activos que sean accesibles a proveedores”.

(UNE-EN, 2017, p. 30)

15.1.1. Política de seguridad de la información en las relaciones con los proveedores

15.1.2. Requisitos de seguridad de contratos con terceros

15.1.3. Cadena de suministro de tecnología de la información y de las comunicaciones

15.2. Gestión de la prestación de servicios por suministradores.

Objetivo: “Mantener un nivel acordado de seguridad y de provisión de servicios en línea mediante acuerdos con proveedores”. (UNE-EN, 2017, p. 31)

15.2.1. Supervisión y revisión de los servicios prestados por terceros.

15.2.2. Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

16.1 Gestión de incidentes de seguridad de la información y mejoras

Objetivo: “Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades”. (UNE-EN, 2017, p. 31)

16.1.1. Responsabilidades y procedimientos.

16.1.2. Notificación de los eventos de seguridad de la información.

16.1.3. Notificación de puntos débiles de la seguridad.

16.1.4. Valoración de eventos de seguridad de la información y toma de decisiones.

16.1.5. Respuesta a incidentes de seguridad de la información.

16.1.6. Aprendizaje de los incidentes de seguridad de la información.

16.1.7. Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

17.1. Continuidad de la seguridad de la información.

Objetivo: “La continuidad de la seguridad de la información debe formar parte de los sistemas de gestión para la correcta evolución del negocio”. (UNE-EN, 2017, p. 32)

17.1.1. Planificación de la continuidad de la seguridad de la información

17.1.2. Implementar la continuidad de la seguridad de la información

17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información

17.2 Redundancia

Objetivo: “Asegurar la disponibilidad de los recursos de tratamiento de la información”. (UNE-EN, 2017, p. 32)

17.2.1 Disponibilidad de los recursos de tratamiento de la información

18. CUMPLIMIENTO.

18.1. Cumplimiento de los requisitos legales y contractuales.

Objetivo: “Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad”. (UNE-EN, 2017, p. 32)

18.1.1. Identificación de la legislación aplicable y de los requisitos contractuales.

18.1.2. Derechos de propiedad intelectual (DPI).

18.1.3. Protección de los registros de la organización.

18.1.4. Protección y privacidad de la información de carácter personal.

18.1.5. Regulación de los controles criptográficos.

18.2 Revisión de la seguridad de la información

Objetivo: “Garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización”. (UNE-EN, 2017, p. 33)

18.2.1. Revisión independiente de la seguridad de la información.

18.2.2. Cumplimiento de las políticas y normas de seguridad.

18.2.3. Comprobación del cumplimiento técnico.

Fuente: UNE-EN ISO/IEC 27001:2017 (2017). Tecnología de la información, Técnicas de seguridad Sistemas de Gestión de la Seguridad de la Información, Requisitos (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015).

2.6. NORMA INTERNACIONAL ISO/IEC 27005

Esta norma internacional es la que permite la implementación y gestión de riesgos de seguridad informática.

El portal web especializado SGSI (2017a) informa que la norma ISO 27005 reemplaza a la norma ISO13335-2 Gestión de Seguridad de la Información y la tecnología de las comunicaciones. Se publicó en junio de 2008, y su última versión mejorada es de 2011. Esta norma define al riesgo como una amenaza que puede causar daños relacionados con el uso, la propiedad, la operación o la adopción de tecnologías en la empresa. Es por ello que se recomienda el desarrollo de procedimientos para la gestión de estos riesgos, los cuales deben ser sistemáticos, estructurados y rigurosos.

2.6.1. Gestión de Riesgos en Tecnologías de la Información con ISO 27005

La implementación de un Sistema de Gestión de Seguridad de Información (SGSI) y la ayuda de la norma internacional ISO 27005 de gestión de riesgos de seguridad informática, detallan los pasos necesarios para realizar el análisis, planificación, ejecución y control para el seguimiento de las políticas de seguridad de información implementada en cualquier institución. Mantener actualizado el SGSI indica que las organizaciones tienen un enfoque claro de la necesidad de llevar adelante una correcta gestión de estos datos (SGSI, 2017a).

2.6.2. Identificación de riesgo

La identificación del riesgo se hace con base en causas identificadas para los procesos, las mismas que pueden ser internas o externas, según lo que haya identificado la entidad a través del contexto estratégico.

2.6.3. Evaluación del riesgo

Es el proceso en el que se evalúa el cumplimiento de la implementación del Sistema de Gestión de Seguridad de Información y sus requerimientos.

El principal objetivo de evaluación de riesgos es identificar y valorar cada uno de los riesgos encontrados, además ayuda a determinar el costo económico de cada activo de información y la importancia que tiene cada uno de estos en la institución. Durante esta fase se toma en cuenta la probabilidad de repetitividad del riesgo, este proceso se realiza mediante reuniones con los encargados del área, responsables de las decisiones tomadas y de las actividades llevadas a cabo en la organización. Otro factor importante son los clientes internos o externos, que ayudan a establecer los niveles de riesgo de una institución.

2.6.4. Tratamiento del Riesgo

Luego de la evaluación es necesario pasar a la acción mediante una gestión ordenada y procedimental. De tal forma, que se aplican controles para reducir, optimizar, transferir o contener dicho riesgo.

Paltán (2017) señala, que el tratamiento del riesgo es el proceso de selección e implementación de medidas de seguridad para corregir y mitigar los riesgos, con miras de no afectar a la productividad, además de “reducir estos riesgos con la menor inversión posible” (p.68).

2.7. POLÍTICAS DE SEGURIDAD

Las políticas de seguridad informática son una herramienta utilizada en las empresas para generar conciencia en los usuarios sobre la importancia y resguardo de datos confidenciales y sensibles, que están relacionados con los procesos de la institución (Escudero, sf., párr.5).

Una política de seguridad es una vía de comunicación que auna las partes interesadas en una empresa, ya que se establece una filosofía o protocolos de actuación, y se detalla todo lo que se desea proteger y los controles necesarios para mantener la disponibilidad, integridad y confidencialidad de los datos (Escudero, sf.)

Para Escudero (sf.) una política de seguridad de información debe establecer los siguientes puntos:

- Cumplimiento de todos los criterios de seguridad de la institución.
- Tener objetivos claros de los dominios y aplicar los controles de manera eficiente para proteger los niveles físicos, humanos y lógicos.
- Designación de responsabilidades al personal de tecnología de información y servicios similares.
- Definición de los requerimientos mínimos en torno a la seguridad de la información, en las cuales se incluyen estrategias para la mejora continua y la continuidad del negocio.
- Establecimiento de las reglas de sanciones en caso de incumplimiento a la política.
- Determinación de responsabilidades a los usuarios internos y externos, con controles de accesos necesarios para precautelar la información.

Las políticas de seguridad de la información debe tener una redacción sencilla y fácil de leer, con expresiones claras para el usuario, con el objetivo de hacerlo entendible a los involucrados. Además, “debe actualizarse de manera periódica cada vez que se realicen cambios institucionales” (Escudero,sf.)

Asimismo, Escudero (sf.) afirma que los parámetros para establecer políticas de seguridad son las siguientes:

- Analizar los riesgos de informática, software, hardware, usuarios y clientes internos/externos.
- Realizar reuniones con las áreas de la institución y sus responsables
- Involucrar a todo el personal que interviene dentro de la institución para el desarrollo de la política.
- Identificar a los encargados de los procesos de cada área de la institución.
- Revisar periódicamente los procedimientos y operaciones de la empresa.
- Analizar continuamente todos los procesos y procedimientos de las áreas de la institución.
- Detallar el alcance que tendrá la política de seguridad de información.

Es importante que, las políticas de seguridad sean puestas en práctica por parte de los colaboradores y usuarios internos/externos, estas políticas deben integrarse en el modelo de negocio de la empresa y debe calar en sus públicos (Escudero,sf.)

Es necesario que esta política sea consensuada con las distintas instancias administrativas y directivas de la institución, con la finalidad de que sea efectiva y adaptada a las necesidades internas y externas. Además, debe ser difundida entre todos los colaboradores y demás personas involucradas. Finalmente, debe estar disponible para consulta, informando que es prohibida su difusión y comercialización a personas no relacionadas con la entidad.

CAPÍTULO III

DIAGNÓSTICO SITUACIÓN

3.1. COOPERATIVA DE AHORRO Y CRÉDITO

La cooperativa de Ahorro y Crédito Chibuleo Ltda., es una Institución que se dedica a la intermediación financiera desde el año 2003, la oficina matriz fue creada en Ambato el 27 de enero del mismo año, en la actualidad cuenta con 13 agencias u oficinas ubicadas en: Machachi, Latacunga, Quito, Sangolquí, Salcedo, Riobamba, Mercado Mayorista de la ciudad de Ambato, Pujili, Otavalo, Ibarra, Tulcán, Cayambe y Pelileo. La Cooperativa celebró su primera década en el 2013 en su edificio ecológico en la ciudad de Ambato. En promedio, tiene más de 120.000 socios activos a quienes brinda distintos servicios, cuentas de ahorro, créditos e inversiones (Cooperativa de Ahorro y Crédito Chibuleo, sf.)

3.1.1. Reseña Histórica

La Cooperativa de Ahorro y Crédito Chibuleo Limitada, es una de las instituciones financieras de referencia en el centro del Ecuador y su principal finalidad es promover el desarrollo de la economía, atendiendo a los sectores más rezagados de la banca tradicional. En 2014, 11 años después de su fundación, la Cooperativa Chibuleo representa el sueño de toda institución puesto que había experimentado un crecimiento significativo, contribuyendo a la par al desarrollo socioeconómico de la ciudadanía.

La Cooperativa de Ahorro y Crédito Chibuleo Ltda. nace el 17 de Enero de 2003, fruto de un inspirador y 27 jóvenes no mayores de 20 años, aquellos que, no teniendo nada, juntaron sus ideas y pensamientos en la búsqueda de un firme rumbo que aliviará sus penumbras y

tormentos en difíciles momentos en que se veían rodeados las clases menos privilegiadas de nuestro país. Con el paso de los años la Cooperativa de Ahorro y Crédito Chibuleo está escribiendo una historia de éxito... ha logrado posicionarse en el sistema financiero como una cooperativa de demostrada capacidad de crecimiento e innovadora, que trabaja por un futuro mejor para nuestra gente, con más de 100 mil socios, 13 oficinas: Machachi, Latacunga, Quito, Sangolquí, Salcedo, Riobamba, Mercado Mayorista de la ciudad de Ambato, Pujili, Otavalo, Ibarra, Tulcán, Cayambe, Pelileo y su principal en Ambato con un edificio propio de última generación.

(...) Este sitio de honor se ha obtenido gracias al respaldo que hemos recibido de todos nuestros socios que con gran orgullo, lealtad y confianza continúan apoyando esta empresa cooperativa (Cooperativa de Ahorro y Crédito Chibuleo, sf., párr.1-2)

3.1.2. Razón Social

COOPERATIVA DE AHORRO Y CRÉDITO CHIBULEO LTDA.

3.1.3. Misión

En Ecuador estamos construyendo historias de éxito, a través de la inclusión financiera.

3.1.4. Visión

Ser referente para las futuras generaciones, consolidando nuestro liderazgo a través de la innovación.

3.1.5. Fundamentación legal

A continuación, se describe la parte legal para la creación de la institución este dato fue tomado de la investigación de Elsa Toaquiza (2012):

La Cooperativa de Ahorro y Crédito Chibuleo Ltda. es una entidad financiera sin fines de lucro, controlada por la Subdirección de Cooperativas Central Departamento Jurídico, se constituyó mediante Acuerdo Ministerial 003-SDR CC 2003 del Ministerio de Bienestar Social e inscrita en el Registro General de Cooperativas con el Numero de Orden 6384 de 27 de enero de enero del 2003 (...) Su estructura interna y administrativa se fundamenta en los instrumentos legales como; Leyes y Reglamento General de las

Cooperativas, Estatutos, Manuales Instructivos, la ley de Régimen Tributario Interno y el Código del Trabajo (p.48).

3.1.6. Valores

- Lealtad
- Respeto
- Integridad
- Confianza
- Puntualidad
- Innovación

3.1.8. Análisis FODA

Tabla 2 Análisis FODA

FORTALEZAS	DEBILIDADES
Calificación de Riesgo	Deficiencia en la comunicación
Personal joven y comprometido	Deficiencia en atención al cliente interno y externo
Desarrollo Tecnológico	Alta rotación del personal
Imagen institucional	Gestión de seguridad integral
Indicadores Financieros adecuados	Remuneración inferior al mercado
Innovación	Falta de difusión del plan de capacitación
	Procesos de inducción deficiente

OPORTUNIDADES	AMENAZAS
Avance tecnológico	Inestabilidad en el entorno económico y político.
Normativas legales: trato diferenciado a las cooperativas de ahorro y crédito	Competencia
Las absorciones por fusiones, temas de expansión	Cierre de instituciones financieras.
Líneas de fondeos internos y externos	Desastres naturales
Remesas del exterior	Robo de información

Fuente: Cooperativa de Ahorro y Crédito Chibuleo Ltda., y Jefe Financiero.

3.1.9. Análisis situacional del área de Tecnología de la Cooperativa de Ahorro y Crédito Chibuleo Ltda.

En este apartado se desarrolla un análisis sobre los activos de información más relevantes que posee el área de tecnología de la información, así como su aporte en los procesos que realiza la institución junto a las áreas críticas que van a intervenir en Plan de continuidad del Negocio y en la creación de las Políticas de Seguridad de la Información de la Cooperativa.

Los activos que se detallan más adelante se obtuvieron a través de una reunión con los siguientes involucrados: jefe de tecnología, analista de sistemas, técnico de infraestructura, analista de riesgo, y el oficial de Seguridad de Información.

A continuación, se detallan todos los activos de Tecnología de Información que ofrece el área de TI a la Cooperativa:

Administración de la Base de Datos

La administración de datos consiste en la generación, administración y control de la información, para la realización de reportes que solicitan las distintas áreas y jefaturas de la institución. Cabe señalar que, la gestión de almacenamiento de base es donde se realiza un control adecuado de los respaldos de información diarios, que provee el área de TI y que a su vez son utilizados por los sistemas informáticos. También se realiza la administración y control de la réplica en línea, la misma que mantiene respalda y segura la información (Ortega, 2014, p.19)

Existen procesos de restauración de los datos para los diferentes sistemas informáticos, los cuales están alojados en los servidores de pruebas o de producción cuando lo amerite, también se realizan mantenimientos periódicos del log de motor de base de datos, se monitorea el uso de memorias RAM que utiliza el gestor de base de datos, y por último se actualiza el programa de base de datos a una nueva versión o parches de seguridad -en caso de ser necesarios- para evitar fallas de seguridad en el software gestor de datos.

Gestión del área de Tecnología

Para la correcta gestión del área de TI, debido a su importancia dentro de la empresa, es necesaria la contratación de un gerente de tecnología, que realice la planificación interna y externa del personal. Otro recurso humano valioso es el responsable del desarrollo de nuevas funcionalidades en el Core Financiero, ya que es el encargado de brindar soporte a los usuarios finales dentro de la cooperativa.

Administración de infraestructura

La infraestructura concentra toda la parte física como servidores, ups, sistemas de aire acondicionado, extintores, conexiones de la red interna y externa, para lo cual se han definido las siguientes actividades dentro del data Center: gestión y administración del sitio alterno, gestión del centro de datos principal, proceso de hardening a servidores antes de salir a producción, mantenimientos de las telecomunicaciones, gestión de los UPS y respaldos de energía para el centro de datos principal y alterno; y por último la administración, configuración y estructuración del cableado dentro de la institución y las agencias. (Paltán, 2017, p. 31)

Gestión de telecomunicaciones

Son las actividades relacionadas a la administración de los servicios de telecomunicaciones como: redes cableadas, antenas de radio frecuencia, routers, firewall, switches y ISP, cuentan con procesos definidos para cada dispositivo y sus respectivas herramientas de monitoreo. Contribuye a la rentabilidad del negocio con clientes internos y externos (Burgos, 2014, p.37).

Soporte Técnico

Consiste en la asistencia que brinda el área de TI para que clientes internos o externos puedan hacer uso de los productos o servicios, realiza funciones específicas, como: respaldos de información de los equipos de los colaboradores, gestión del licenciamiento para las estaciones de servicios, servidores y la gestión de la mesa de ayuda (Mera, 2014, p.61).

Seguridad de información

En la actualidad, los datos y la información se han convertido en los activos más valiosos dentro de las organizaciones, esta información puede ser pública o privada, y la falta de una política de seguridad puede hacerla vulnerable a ataques internos o externos.

Gualpa (2017) manifiesta que la seguridad de la información debe contemplar tres principios: integridad, disponibilidad y confidencialidad de los datos. En su investigación, el área de tecnología era la encargada de mantener segura esta información tomando medidas como la gestión de la seguridad perimetral Firewall, gestión de contraseñas de usuario y acceso a áreas restringidas, con políticas de seguridad de información; y por ultimo un plan de recuperación de tecnología de la información (p.38).

Mantenimiento Correctivo y Perfectivo de Software

Son los desarrollos solicitados por las áreas de la cooperativa, mediante la implementación de formatos de requerimiento y formatos de proyectos de desarrollo para nuevas funcionalidades que se puedan implementar en el Core financiero. También concentra a los sistemas informáticos que provee el área de Tecnología a toda la cooperativa, para la cual se realizan las siguientes actividades: análisis e implementación de requerimientos perfectivos y correctivos de software, desarrollo del requerimiento, administración y control del cambio. Finalmente la debida certificación de los desarrollos antes de poner a producción. (Cevallos, 2019, p. 34)

Contratación de servicios

Este proceso es uno de los más importantes dentro del área, mediante el análisis de proformas y su posterior aprobación se realiza el/los proceso/s de contratación de servicios externos /internos (Kowask, Alcántara, Motta, & Boca, 2014).

Personal

Los profesionales que colaboran dentro del área de Tecnología de Información son los siguientes:

- Jefe de sistemas
- Analista de Sistemas
- Programadores
- Soporte Técnico
- Help Desk

3.2. ANALISIS Y VALORACION DE RIESGOS

3.2.1. Selección y Análisis de las operaciones críticas

El objetivo de realizar el análisis y la selección es determinar las tareas, procesos y procedimientos e infraestructura que utilizan los activos críticos que tiene el área de tecnología de información.

3.2.2. Aplicaciones y servicios informáticos de Tecnología

Los principales servicios y aplicaciones utilizados por la cooperativa son los siguientes:

- Sistemas
- Financial 2.0 (Core financiero principal)
- Coonecta (Switch de cajero automático)
- Aplicativos APP
- Eset End Point Security (administrador de seguridad-antivirus)
- Intranet institucional, TFS (servidor de código fuente)
- Creditreport o ServiPagos (externos)
- SPI-Remesas (externos)

3.2.3. Principales servicios

Entre los servicios tecnológicos que el área de Tecnología ofrece a sus usuarios para la operación del negocio de la Cooperativa tenemos la siguiente clasificación:

Servicios Windows

- Antivirus
- Servidor de email interno y externo
- Herramientas office

Gestor de Base de datos

- Gestor de base SQL Server 2014
- Sistema Operativo, Servidores pruebas y de producción
- Sistema Operativo de equipos personales y laptops
- Backup de la Información de equipos críticos
- Publicaciones y fuentes Financial 2.0.

Respaldo y almacenamiento de información

- Respaldos de la Base SQL desde Financial 2.0 (SQL server).
- Respaldos de las publicaciones del Sistema Financial 2.0 puestas a producción.
- Respaldos completos de los servidores de producción, dominio y de los equipos de comunicación.

Otros

- Red interna de datos.
- Red privada con el BCE a través de Telconet.
- Red privada con Coonecta.

3.2.4. Validación de la criticidad por proceso

Un proceso es considerado crítico cuando afecta a la continuidad del negocio y a las operaciones de la cooperativa. También, cuando se presentan fallas o una inadecuada ejecución de los procesos, estas eventualidad pueden tener un alto impacto en la institución según el área y la criticidad. Están basados en función a los sistemas de información detallados a continuación: aplicaciones, hardware, software y sistemas adicionales que utilizan las áreas de la cooperativa.

En la cooperativa existe el área de riesgo que realizó la metodología de riesgo operacional, el documento fue elaborado por Klever Pilamunga e Isaac Maliza en el año 2018 y contiene lo siguiente:

Impacto alto: Se considera impacto alto cuando ante una eventualidad se encuentran inhabilitadas las operaciones de la Cooperativa, sin permitir que los usuarios internos y externos puedan realizar de manera normal sus funciones.

Impacto medio: Se considera que una actividad crítica tiene un impacto medio cuando la falla de ésta ocasiona una interrupción en las operaciones de la Cooperativa por un tiempo mínimo de tolerancia.

Impacto bajo: se considera que una actividad crítica tiene un impacto bajo, cuando la falla de ésta no tiene un impacto en la continuidad de las operaciones de la Cooperativa

A continuación, se enumeran los procesos que son parte del Core del negocio y la evaluación de su grado de importancia en función a la magnitud del impacto (Pilamunga & Maliza, 2018).

Criticidad del riesgo

En la publicación web de la empresa ISOTools sobre la norma ISO 27001, señala que, la criticidad del riesgo es una evaluación de las consecuencias potenciales sobre un evento, este tipo de riesgos se clasifica en aceptable o residual.

Riesgo aceptable. No se trata de eliminar totalmente el riesgo, ya que muchas veces no es posible, y tampoco resultaría rentable, se trata de minimizar al máximo las consecuencias, con

la finalidad de realizar una gestión sobre las mismas, sin que perjudique a los distintos niveles de la empresa: económico, logístico, reputacional, etc. (ISOTools, 2019, párr. 11)

Riesgo residual. Es aquel que subsiste luego de haber implementado los controles necesarios, es decir posterior a la puesta en marcha de una estrategia de SGSI. (ISOTools, 2019, párr. 12)

A continuación, se detallan los principios de Sistema de Gestión de Seguridad de Información, insumo que ayudará al levantamiento de datos de los activos de información del área de tecnología. Para ello, se ha tomado como ejemplo el texto de Amutio y González (2012) donde muestran el uso de la metodología Magerit.

Confidencialidad. Que la información restringida dentro de la organización sea accesible únicamente a las personas que cuenten con los permisos necesarios.

“¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?”.
(Amutio & González, 2012, p.15)

Integridad. Que la información este completa y no se haya realizado modificaciones sin autorización.

¿Qué importancia tendría que los datos fueran modificados fuera de control? (Amutio & González, 2012, p.15)

Disponibilidad. Que los datos se encuentren accesibles y utilizables cuando los usuarios lo requieren.

¿Qué importancia tendría que el activo no estuviera disponible? (Amutio & González, 2012, p.15)

Criterio de valoración

Para la valoración de activos este trabajo de titulación utilizará una combinación de una escala cuantitativa y cualitativa, donde los criterios van desde un nivel 0 a un nivel 5. Siendo 0 considerado como un nivel despreciable, y 5 una escala alta para la organización. Esta propuesta se basa en la desarrollada por Amutio & González, 2012, que establecieron un criterio del 0 al 10, siendo 0 despreciable y 10 extremo. En la siguiente Tabla (3) se puede

observar con mayor claridad los criterios de valoración de activos que serán usados para esta propuesta.

Tabla 3. Criterios de valoración de activos

Descripción	Valor	Confidencialidad	Integridad	Disponibilidad
Extremo	5	<i>“¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?”.</i> (Amutio & González, 2012, p.15)	<i>¿Qué importancia tendría que los datos fueran modificados fuera de control?</i> (Amutio & González, 2012, p.15)	<i>¿Qué importancia tendría que el activo no estuviera disponible?</i> (Amutio & González, 2012, p.15)
Muy alto	4			
Alto	3			
Medio	2			
Bajo	1			
Depreciable	0			

Fuente: Adaptación propia del texto de Amutio & González (2012, p.19)

Para un correcto análisis de los elementos de riesgo que forman parte de la institución se analizan los equipos informáticos y la información confidencial, para ello, se requiere describir los recursos informáticos tales como: equipamiento software y hardware; herramientas y sistemas externos; y el Core financiero. El análisis se detalla en las siguientes tablas:

Tabla 4 Análisis de impacto en áreas de la Cooperativa de Ahorro y Crédito Chibuleo

Código	Operaciones Críticas	Objetivos de las operaciones	Prioridad
GN-CAP	Captaciones	Negociación de las condiciones de la póliza Creación, aprobación y activación de la póliza Cancelación o renovación de las pólizas	Medio
GN-CRE	Créditos	Concesión del crédito Creación del crédito Análisis del crédito Aprobación del crédito Legalización del crédito Desembolso del crédito Recuperación del crédito. Constitución de hipotecas y prendas Levantamiento de hipotecas y prendas Castigo de créditos	Medio
GN-ATC	Atención al Cliente	Creación, activación y cierre de cuentas de ahorro y aportes. Actualización de datos de socios y clientes. Emisión de certificados. Atención Reclamos. Administración de tarjetas de débito. Reposición de libretas de ahorro. Envío de estructuras a los organismos de control.	Medio
GA-TES	Tesorería	Administración de cajero automático. Transferencias de fondos. Transacciones bancarias e inversiones. Envío de estructuras a los organismos de control.	Alta

		<p>Control y manejo de la bóveda.</p> <p>Apertura y cierre de ventanillas.</p> <p>Transacciones de depósitos y retiros.</p> <p>Pagos de servicios de terceros.</p> <p>Envío y pago de remesas.</p> <p>Pagos de préstamos.</p> <p>Entrega de préstamos.</p> <p>Actualización de libretas.</p> <p>Ingreso, órdenes.</p>	
GA-CON	Contabilidad	<p>Adquisiciones o contrataciones de bienes y servicios.</p> <p>Venta de bienes muebles o inmuebles.</p> <p>Gestión activos fijos.</p>	Medio
SA-SFM	Seguridad Física y Mantenimiento	<p>Cancelación de operaciones crediticias.</p> <p>Reembolso cronológico socios/clientes afectados.</p> <p>Comunicación interna sobre base de listas negativas.</p> <p>Controles para prevenir lavado de activos.</p> <p>Transmisión de información operaciones inusuales.</p>	Medio
GT-TIN	Gestión de Tecnología de Información	<p>Administración de los motores de Base de Datos</p> <p>Administración de área de Tecnología</p> <p>Administración de Infraestructura</p> <p>Gestión de Telecomunicaciones</p> <p>Soporte Técnico</p> <p>Seguridad Informática</p> <p>Mantenimiento Correctivo y Perfectivo de Software</p> <p>Contratación de Servicios</p>	Alto

Fuente: Elaboración propia

Tabla 5 Procesos del área de Tecnología de Información

MACROPROCESO	PROCESO	SUBPROCESO	CÓDIGO
Gestión de Tecnología de Información	Tecnología de Información	Administración de los motores de Base de Datos	GT-TIN-ABD
		Administración de área de Tecnología	GT-TIN-GTI
		Administración de Infraestructura	GT-TIN-AIN
		Gestión de Telecomunicaciones	GT-TIN-TEL
		Soporte Técnico	GT-TIN-STE
		Seguridad Informática	GT-TIN-SIN
		Mantenimiento Correctivo y Perfectivo de Software	GT-TIN-MCP
		Contratación de Servicios	GT-TIN-CSE

Fuente: Elaborado por el autor con el apoyo de un analista de riesgos de la Cooperativa Chibuleo

Tabla 6. Recursos tecnológicos que ofrece sistemas (activos)

CODIGO PROCESO	CODIGO ACTIVO TI	ACTIVO
GT-TIN-ABD	GT-TIN-ABD-01	Reportes
	GT-TIN-ABD-02	Generación de datos para estructuras
	GT-TIN-ABD-03	Almacenamiento y entrega de información a los sistemas existentes
	GT-TIN-ABD-04	Respaldos de información

	GT-TIN-ABD-05	Restauración de información
	GT-TIN-ABD-06	Mantenimiento a las BBDD existentes.
	GT-TIN-ABD-07	Seguridad en las BBDD
	GT-TIN-ABD-08	Ambiente de pruebas
	GT-TIN-ABD-09	Otros (link Server, Exportación, importación)
GT-TIN-AIN	GT-TIN-AIN-01	Acceso a la Red
	GT-TIN-AIN-02	Autenticación a la red, mediante AD
	GT-TIN-AIN-03	Asignación de equipamiento
	GT-TIN-AIN-04	Telefonía IP
	GT-TIN-AIN-05	Correo Electrónicos
	GT-TIN-AIN-06	Mensajería Instantánea
	GT-TIN-AIN-07	Accesos a Internet
	GT-TIN-AIN-08	Accesos a servicios externos
	GT-TIN-AIN-09	Segmentación de la red (VLAN's,DMZ, Firewall)
	GT-TIN-AIN-10	Implementación de servidores
	GT-TIN-AIN-11	Administración de espacio físico en el Data Center
	GT-TIN-AIN-12	Instalación SO
	GT-TIN-AIN-13	Hardening
	GT-TIN-AIN-14	Administración Centro de Datos
GT-TIN-CS	GT-TIN-CS-01	Elaboración del presupuesto anual de sistemas
	GT-TIN-CS-02	Análisis de proveedores
	GT-TIN-CS-03	Administración de adquisición y contratos externos
	GT-TIN-CS-04	Análisis de Cotización
	GT-TIN-CS-05	Control de Presupuesto asignado a TI

GT-TIN-GTE	GT-TIN-GTE-01	Interconexión de oficinas con Matriz
	GT-TIN-GTE-02	Calidad de servicios de las conexiones
	GT-TIN-GTE-03	Transparencia en la interconexión
	GT-TIN-GTE-04	Monitoreo de la red
	GT-TIN-GTE-05	Actualización firmware
	GT-TIN-GTE-06	Alta disponibilidad
	GT-TIN-GTE-07	Mantenimiento preventivo y correctivo
GT-TIN-MCP	GT-TIN-MCP-01	Adecuación de módulos
	GT-TIN-MCP-02	Implementación de módulos
	GT-TIN-MCP-03	Corrección de módulos
	GT-TIN-MCP-04	Versionamiento de sistemas existentes
	GT-TIN-MCP-05	Parametrización de sistemas existentes
	GT-TIN-MCP-06	Procesos Batch
	GT-TIN-MCP-07	Ambiente de pruebas (publicación, pruebas, certificación, capacitación)
	GT-TIN-MCP-08	Publicaciones de software existente
	GT-TIN-MCP-09	Respaldos de los sistemas existentes de software
	GT-TIN-MCP-10	Sistema Financiamiento 2.0
GT-TIN-SIN	GT-TIN-SIN-01	Cambio de Claves de usuarios directorio activo
	GT-TIN-SIN-02	Control de acceso al Data Center, Sistemas y Sala de control de las oficinas
	GT-TIN-SIN-03	Cambio de claves de accesos a Wifi
	GT-TIN-SIN-04	Administración de respaldos de información de todos los sistemas informáticos

	GT-TIN-SIN-05	Mantener la información confiable, Intgra, Disponible
GT-TIN-STE	GT-TIN-STE-01	Soporte técnico Help Desk
	GT-TIN-STE-02	Mantenimiento correctivo de equipamiento de infraestructura
	GT-TIN-STE-03	Soporte segundo nivel (Personalizado con usuarios)
	GT-TIN-STE-04	Soporte Tercer nivel (externos, coordinación)

Fuente: Elaboración propia

En la siguiente tabla se realizará la respectiva valoración de los activos de tecnología de información, tomando en cuenta los criterios de Disponibilidad, Confidencialidad e Integridad.

Tabla 7. Valoración de activos

CODIGO	RECURSOS	Disponibilidad	Confidencialidad	Integridad	Promedio	Valoración
GT-TIN-ABD-01	Reportes	5	5	5	5	Extremo
GT-TIN-ABD-02	Generación de datos para estructuras	5	5	5	5	Extremo
GT-TIN-ABD-03	Almacenamiento y entrega de información a los sistemas existentes	5	5	5	5	Extremo
GT-TIN-ABD-04	Respaldos de información	5	5	5	5	Extremo
GT-TIN-ABD-05	Restauración de información	5	5	5	5	Extremo
GT-TIN-ABD-06	Mantenimiento a las bases de datos existentes	5	5	5	5	Extremo
GT-TIN-ABD-07	Seguridad en las bases de datos	5	5	5	5	Extremo
GT-TIN-ABD-08	Ambiente de pruebas	5	5	5	5	Extremo
GT-TIN-ABD-09	Otros (link Server, Exportación, importación)	3	3	3	3	Alto

GT-TIN-AIN-01	Acceso a la Red	5	5	5	5	Extremo
GT-TIN-AIN-02	Autenticación a la red, mediante Directorio Activo	3	3	3	3	Alto
GT-TIN-AIN-03	Asignación de equipamiento	1	1	1	1	Bajo
GT-TIN-AIN-04	Telefonía IP	5	5	5	5	Extremo
GT-TIN-AIN-05	Correo Electrónicos	5	5	5	5	Extremo
GT-TIN-AIN-06	Mensajería Instantánea	1	1	1	1	Bajo
GT-TIN-AIN-07	Accesos a Internet	5	5	5	5	Extremo
GT-TIN-AIN-08	Accesos a servicios externos	5	5	5	5	Extremo
GT-TIN-AIN-09	Segmentación de la red (VLAN's,DMZ, Firewall)	5	5	5	5	Extremo
GT-TIN-AIN-10	Implementación de servidores	5	5	5	5	Extremo
GT-TIN-AIN-11	Administración de espacio físico en el Data Center	5	5	5	5	Extremo
GT-TIN-AIN-12	Instalación sistemas operativos	5	5	5	5	Extremo
GT-TIN-AIN-13	Hardening	5	5	5	5	Extremo

GT-TIN-AIN-14	Administración Centro de Datos	5	5	5	5	Extremo
GT-TIN-CS-01	Elaboración del presupuesto anual de sistemas	5	5	5	5	Extremo
GT-TIN-CS-02	Análisis de proveedores	5	5	5	5	Extremo
GT-TIN-CS-03	Administración de adquisición y contratos externos	5	5	5	5	Extremo
GT-TIN-CS-04	Análisis de cotización	5	5	5	5	Extremo
GT-TIN-CS-05	Control de presupuesto asignado a tecnología e información	5	5	5	5	Extremo
GT-TIN-GTE-01	Interconexión de oficinas con Matriz	5	5	5	5	Extremo
GT-TIN-GTE-02	Calidad de servicios de las conexiones	5	5	5	5	Extremo
GT-TIN-GTE-03	Transparencia en la interconexión	4	4	4	4	Muy Alto
GT-TIN-GTE-04	Monitoreo de la red	3	3	3	3	Alto
GT-TIN-GTE-05	Actualización firmware de los sistemas operativos	3	3	3	3	Alto

GT-TIN-GTE-06	Alta disponibilidad	5	5	5	5	Extremo
GT-TIN-GTE-07	Mantenimiento preventivo y correctivo	5	5	5	5	Extremo
GT-TIN-MCP-01	Adecuación de módulos	3	3	3	3	Alto
GT-TIN-MCP-02	Implementación de módulos	3	3	3	3	Alto
GT-TIN-MCP-03	Corrección de módulos	3	3	3	3	Alto
GT-TIN-MCP-04	Versionamiento de sistemas existentes	2	2	2	2	Medio
GT-TIN-MCP-05	Parametrización de sistemas existentes	5	5	5	5	Extremo
GT-TIN-MCP-06	Procesos Batch cierre fin de día del core	5	5	5	5	Extremo
GT-TIN-MCP-07	Ambiente de pruebas (publicación, pruebas, certificación, capacitación)	3	3	3	3	Alto
GT-TIN-MCP-08	Publicaciones de software existentes	3	3	3	3	Alto

GT-TIN-MCP-09	Respaldos de los sistemas existentes de software.	3	3	3	3	Alto
GT-TIN-MCP-10	Sistema Financial 2.0	5	5	5	5	Extremo
GT-TIN-SIN-01	Cambio de Claves de usuarios directorio Activo	1	1	1	1	Bajo
GT-TIN-SIN-02	Control de acceso al Data Center, Sistemas y Sala de control de las oficinas	5	5	5	5	Extremo
GT-TIN-SIN-03	Cambio de claves de accesos a Wifi	2	2	2	2	Medio
GT-TIN-SIN-04	Administración de respaldos de información de todos los sistemas informáticos	5	5	5	5	Extremo
GT-TIN-SIN-05	Mantener la información confiable, integra y disponible	5	5	5	5	Extremo
GT-TIN-STE-01	Soporte técnico Help Desk	5	5	5	5	Extremo

GT-TIN-STE-02	Mantenimiento correctivo de equipamiento de infraestructura	3	3	3	3	Alto
GT-TIN-STE-03	Soporte segundo nivel (Personalizado con usuarios)	2	2	2	2	Medio
GT-TIN-STE-04	Soporte Tercer nivel (externos, coordinación)	1	1	1	1	Bajo

Fuente: Realizado por el Investigador y el jefe de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Chibuleo

Ltda.

3.2.5. Determinar las vulnerabilidades y amenazas a los activos de información

En la presente tabla se mostrará las amenazas y vulnerabilidades que tiene o que se considera en cada activo de información.

Tabla 8. Amenazas y vulnerabilidades de información

Activo	Causa riesgo o amenaza	Vulnerabilidad
Administración	Incendio	No existe un manual de tecnologías
Centro de Datos	Inundación	de la información
	Terremoto	Falta un protocolo de procesos de
	Erupción volcánica	tecnología de información
	Sabotaje	Inadecuado instructivo de procesos
	Corto circuito	de tecnología de información
		Falta un protocolo de procesos de administración de infraestructura
Administración de servidores	No enciende el equipo servidor	No existe un manual de tecnologías
	Daños en los componentes de hardware del servidor (Disco, Memoria, Tarjeta de red, Fuentes, etc.)	de la información
	Cortes de energía eléctrica, variaciones de voltaje y suministros eléctricos, descarga de UPS	Falta un protocolo de procesos de tecnología de información
	Discos de almacenamiento llenos sin espacio	No existe instructivo de encendido y apagado de servidores
		Falta de un Cronograma de mantenimiento de Servidores Físicos y virtuales

Límite de vida útil (equipos obsoletos)	No existe un procedimiento de
Robo de equipos informáticos y archivos	administración de respaldos de sistemas operativos
Caída imprevista del sistema operativo	No existe un procedimiento para
El sistema operativo no arranca	adquisiciones inmediatas
No se carga los servicios del sistema operativo	Falta de un Manual de configuración de antivirus
Configuraciones erróneas	Instructivo incompleto de correo electrónico
No se tiene acceso a la consola de administración	
Abuso de puertos para el soporte remoto.	
Aplicación de seguridad y actualizaciones no autorizadas	
Daño a la información	
Robo de información	
Mal funcionamiento servicios	
Reinicio del equipo	
Mantenimiento a las bases de datos existentes, Seguridad en las BBDD	
No sube la base de datos	No existe manual de tecnología de información
No responde la base de datos	
No hay espacio en el disco duro	Falta un protocolo de procesos de tecnología de información
No se dispone de contraseña de administración	No existe un Instructivo de

	Mala configuración de tareas programadas	respaldo de base de datos
	Seguridad de base de datos deficiente	No existe un Procedimiento de administración de respaldos de los sistemas operativos
	Acceso sin autorización a base de datos (insert, delete, update)	No existe un Manual de seguridad para la base de datos
	Robo de la información de datos.	
Sistema	No se ejecuta la aplicación	No existe un manual de tecnología de información
Finacial 2.0	Configuración inadecuada	Falta un protocolo de procesos de tecnología de información
	Información no integra	No existe un Instructivo de configuración de Finacial
	Sin permisos de ejecución	No existe un Procedimiento de administración de respaldos de Sistemas operativos
	No sube los servicios del sistema WEB	Falta de un Manual de configuración de antivirus
	No se cargan los archivos dll de la aplicación	Instructivo incompleto de correos electrónicos
	No se tiene acceso a los archivos ejecutables de Finacial	No existe un instructivo para el encendido y apagado para servidores
	Daño o caída del servidor de reportes	
	Uso indebido del sistema Finacial	
	Acceso sin autorización a la base de datos (borrado, modificaciones, inserciones, etc.)	
	Daños en tarjeta de red	

	IP sin definir	Falta de procesos de administración
	Acceso no autorizado a la red	de infraestructura
	Daños en el cable físico de red	No existe un Procedimiento para
	Sin acceso por el Switch	adquisiciones inmediatas
	Integridad de la información	No existe un Instructivo de
	Robo de información	configuración de los sistemas de
	Funcionamiento inestable de los servicios	administración y comunicación internos
	Acceso no autorizado	
Alta disponibilidad (Sistema operativo que soporta el servidor espejo)	No enciende el equipo servidor	No existe un manual de tecnología de información
	Daños en los componentes de hardware del equipo servidor (daño en disco, memoria, tarjeta de red)	Falta un protocolo de procesos de tecnología de información
	Daños del UPS	Falta protocolo de procesos de administración de infraestructura
	Discos de almacenamiento llenos sin espacio	No existe instructivo para el encendido y apagado para servidores
	Caída imprevista del sistema operativo	
	El sistema operativo no arranca	No existe un Procedimiento para adquisiciones inmediatas
	No se carga los servicios del sistema operativo	Inadecuado instructivo de procesos de tecnología de información
	Configuraciones erróneas	
	No se tiene acceso a la consola de administración	No existe un Instructivo de

	Aplicación de parches de seguridad y actualizaciones no autorizadas.	configuración de los sistemas de administración y comunicación internos
	Daño a la información	
	Robo de información	No existe un Procedimiento de administración de respaldos de sistema operativo
	Mal funcionamiento de los servicios	
	Reinicio del equipo	Falta de un Manual de configuración de antivirus
Reportes, Generación de datos para estructuras, Almacenamiento y entrega de información a los sistemas existentes, Respaldos de información, Restauración de información	No sube la base de datos	No existe un manual de tecnología de información
	No responde la base de datos	
	No hay espacio disco duro	Falta un protocolo de procesos de tecnología de información
	No se tiene acceso a la consola administración	No existe un Instructivo de respaldo de base de datos
	No se dispone de contraseñas de administración	Falta de procesos de administración de infraestructura
	No existe sincronización con la base de datos principal	No existe un Procedimiento de administración de respaldos de sistemas operativos

Accesos a servicios externos. (Sistema operativo del equipo servidor de cajero automático /cajero automático)	No enciende el equipo servidor	No existe un manual de tecnología de información
	Daños en los componentes de hardware del equipo servidor (error en disco, memoria, tarjeta de red)	Falta un protocolo de procesos de tecnología de información
	Daños del UPS	Falta de protocolo de procesos de administración de infraestructura
	Virus informático	No existe un instructivo para el encendido y apagado para servidores
	Discos de almacenamiento llenos sin espacio	Falta de un Manual de configuración de antivirus
Accesos a servicios externos. (Sistema operativo del equipo servidor de cajero automático /cajero automático)	Caída imprevista del sistema operativo	No existe un manual de tecnología de información
	El sistema operativo no arranca	Falta un protocolo de procesos de tecnología de información
	No se carga los servicios del sistema operativo	Falta de protocolo de procesos de administración de infraestructura
	Servicios caídos	No existe un instructivo para el encendido y apagado para servidores
	Configuraciones erróneas	Actualizaciones de parches de seguridad, actualización no autorizada

	Daño a la información	Falta de un Manual de
	Robo de información	configuración de antivirus
	Mal funcionamiento de los servicios	Instructivo incompleto de correos
	Reinicio del equipo	electronicos
Equipo servidor	No enciende el equipo servidor	No existe un manual de tecnología
antivirus	Daños en los componentes de hardware del equipo servidor (error en disco, memoria, tarjeta de red)	de información Falta un protocolo de procesos de tecnología de información
	Daños del UPS	Inadecuado instructivo de procesos de tecnología de información
	Discos de almacenamiento llenos sin espacio	Falta de procesos de administración de infraestructura No existe un instructivo para el encendido y apagado para servidores Falta de un Cronograma de mantenimiento de Servidores Físicos y virtuales
Procesos Batch	Caída imprevista del sistema operativo	No existe un manual de tecnología de información
	El sistema operativo no arranca	
	No se carga los servicios de Financial	Falta un protocolo de procesos de tecnología de información
	Servicios caídos	
	Configuraciones erróneas	

	No se tiene acceso a Financial	Inadecuado instructivo de procesos
	no se ejecuta los respaldos desde el Sistema	de tecnología de información
	Cambio de fecha incorrecto	No existe un Instructivo de respaldo de base de datos
	Sin conexión a la Base de datos	No existe un Instructivo de configuración de Financial
	Actualizaciones de parches de seguridad, actualización sin autorización	
Parametrización de sistemas existentes	Usuarios sin roles específicos	No existe un manual de tecnología de información
	Las aplicaciones no funcionan como es debido	Inadecuado instructivo de procesos de tecnología de información
	Acceso no autorizado	No existe un Proceso de administración de cambios (parámetros)
	Mal funcionamiento de los procesos	
	Carga operativa	
	Clientes inconformes	
	Mala contabilización	
Telefonía IP	No enciende el equipo servidor. Daños en los componentes de hardware del equipo servidor (error en disco, memoria y tarjeta de red)	Falta de un Manual de tecnología de información
Correo Electrónicos		Inadecuado instructivo de procesos de tecnología de información
Accesos a Internet (hardware)	Daños del UPS	Falta de protocolo de procesos de administración de infraestructura
	Daños en los discos de almacenamiento	

		No existe instructivo para el encendido y apagado para servidores
		Falta de un Cronograma de mantenimiento de Servidores Físicos y virtuales
Telefonía IP	Caída imprevista del sistema operativo.	No existe un manual de tecnología de información
Correo Electrónicos	El sistema operativo no arranca	Inadecuado instructivo de procesos de tecnología de información
Accesos a internet (software)	No se carga los servicios del sistema operativo	No existe un Instructivo de configuración de los sistemas de administración y comunicación internos
	Servicios caídos	No existe instructivo para el encendido y apagado para servidores
	Configuraciones erróneas	Falta de un Cronograma de mantenimiento de Servidores Físicos y virtuales
	No se tiene acceso a la consola de administración	
	Aplicación de parches de seguridad y actualizaciones no autorizadas	
	Daño a la información	
	Robo de información	
	Mal funcionamiento servicio	
	Reinicio del equipo	

Segmentación de la red (VLAN's, DMZ, Firewall)	Daños en los equipos de comunicación: Routers, switch, antenas	Falta de protocolo de procesos de administración de infraestructura
	Error en el software de acceso a Internet	No existe un Instructivo de configuración de los sistemas de administración y comunicación internos
	Mala parametrización del firewall	Falta de un Cronograma de mantenimiento de Servidores Físicos y virtuales
	Segmentación de la red	No existe un Procedimiento para adquisiciones inmediatas
	Perdida de comunicación con proveedores y organismos de control	
Administración de adquisición y contratos externos	Daño físico de la unidad de servidores	No existe un manual de tecnología de información
	Compras de urgencia	No existe un Procedimiento para adquisiciones inmediatas
	Robo	
Análisis de Cotización	Errores en las funciones	
	Servicios externos no funcionan	
Interconexión de oficinas con Matriz (Switch Mikrotik)	Daño	No existe un manual de tecnología de información
	Dispositivo no responde.	
Matriz (Switch Mikrotik)	Conectores dañados	Falta de protocolo de procesos de tecnología de información
	Puerto dañado	Falta de procesos de administración de infraestructura
	Pérdida de energía	
	Configuración deficiente	

	Sin acceso a la consola de administración	No existe un Instructivo de configuración de los sistemas de administración y comunicación internos No existe un Procedimiento para adquisiciones inmediatas
Interconexión de oficinas con Matriz (Canal de datos de todas las agencias con Telconet)	Caídas Error de configuración Señal defectuosa Pérdida de comunicación con el proveedor	No existe un manual de tecnología de información No existe un Proceso de administración de infraestructura No existe un Instructivo de configuración de los sistemas de administración y comunicación internos No existe un Procedimiento para adquisiciones inmediatas
Interconexión de oficinas con Matriz (Canal Datos Radio Enlaces Agencias)	Caídas Configuración inadecuada Señal defectuosa Daño en las antenas Pérdida de energía	No existe un manual de tecnología de información Falta de protocolo de procesos de administración de infraestructura No existe Contratos de Calidad de servicio con proveedores

Acceso a la Red (Red Datos)	Dispositivo de tarjeta de red	No existe un manual de tecnología de información
	IP mal asignadas	Falta de protocolo de procesos de administración de infraestructura
	Corte en cable de red	No existe un Instructivo de configuración de los sistemas de administración y comunicación internos
	Diseño en el swicth	No existe iun Procedimiento para adquisiciones inmediatas
	Daño en el punto de red	No existe un <i>Service Level Agreement (SLA)</i>
Señal defectuosa		
Calidad de servicios de las conexiones	Sin acceso al servicio	No existe un manual de tecnología de información
	Pérdida de las credenciales de acceso	Falta de protocolo de procesos de tecnología de información
	Pérdida de comunicación	No existe un Instructivo de configuración de los sistemas de administración y comunicación internos
		No existe Contratos de Calidad de servicio con proveedores

Soporte técnico Help Desk (Computador / Laptop / Impresora)	No arranca sistema operativo	No existe un manual de tecnología
	Error en la ejecución de procesos	de información
	Mal uso	Falta de protocolo de procesos de
	Equipos desprotegidos	tecnología de información
	Daño a la información	Inadecuado instructivo de procesos
	Robo de información	de tecnología de información
Mal funcionamiento de los aplicativos	Falta de un Cronograma de	
Reinicio del equipo	mantenimiento de estaciones de	
	trabajo	
	No existe un instructivo de	
	mantenimiento de estaciones de	
	trabajo	
	Falta de un Manual de	
	configuración de antivirus	
	Instructivo incompleto de correos	
	electrónicos	
Mantenimiento correctivo de equipamiento de infraestructura (Aire Acondicionado)	Daño	No existe un manual de tecnología
	No enfría	de información
		Falta de protocolo de procesos de
	administración de infraestructura	

Mantenimiento correctivo de equipamiento de infraestructura (UPS)	Daño Sin batería Equipo no se activa automáticamente Sobrecarga operativa	No existe un manual de tecnología de información Falta de protocolo de procesos de administración de infraestructura
Mantenimiento correctivo de equipamiento de infraestructura (Planta Eléctrica)	Daño Sin combustible Equipo no se activa automáticamente Equipos sin operatividad	No existe un manual de tecnología de información Falta de protocolo de procesos de administración de infraestructura
Mantenimiento correctivo de equipamiento de infraestructura (Red eléctrica para equipos de cómputo)	Daños Apagones Variaciones eléctricas	No existe un manual de tecnología de información Falta de protocolo de procesos de administración de infraestructura
Sistema Swicth Entura – Xtream Web	No se tiene conexión con el proveedor Desconfiguración de los componentes	No existe un manual de tecnología de información Falta de protocolo de procesos de administración de infraestructura

Mantener la información confiable, Intgra, Disponible	Lugar de almacenamiento inadecuado	No existe un manual de tecnología de información
	Datos inadecuados	
	Información Corrupta	Falta de protocolo de procesos de tecnología de información
		No existe un Instructivo de respaldo de base de datos
Respaldos de los sistemas existentes de software	El disco culmino su vida útil	No existe un manual de tecnología de información
	Daño en el almacenamiento	
	Sin espacio	Falta de protocolo de procesos de administración de infraestructura
	Daño en las unidades de almacenamiento	No existe un Instructivo de configuración de los sistemas de administración y comunicación internos
	Daño en sistema operativo	
	No tiene conexión con la red	No existe un Procedimiento de administración de respaldos de sistemas operativos

Fuente: Elaborado por el investigador y el Jefe de Tecnología de información.

3.3. VALORACION DE RIESGOS DE ACTIVOS DE INFORMACIÓN

3.3.1. Metodología para Valoración de Riesgos

Un riesgo se mide por el impacto que pueda causar dentro y fuera de las organizaciones, y por la probabilidad de que un evento no esperado ocurra. Para realizar la valoración de riesgos de los activos críticos de tecnología de información que fueron definidos para el plan de contingencia del área de tecnología, se aplicará la metodología de matriz de riesgos de cinco columnas, tanto para la probabilidad, como para el impacto.

El producto entre probabilidad e impacto determinará el nivel de riesgo del evento de contingencia que se valore y que afecte al activo de tecnología de información (Burgos, 2014; Pilamunga & Maliza, 2018)

A continuación, se describen los valores para la probabilidad, y para el impacto definidos en la metodología de riesgo operacional elaborado por Klever Pilamunga y Isaac Maliza en el año 2018:

Probabilidad: Se refiere a la medida “criterios de frecuencia” que permite estimar la repetición del evento de riesgo de contingencia en tres categorías, cada una de ellas con su calificación como consta en la siguiente tabla:

Tabla 9. Niveles de Probabilidad

PROBABILIDAD	PESO	DESCRIPCION
MUY BAJA	1	El evento puede ocurrir en algún momento y es probable que suceda (1 – 2 veces mes)
BAJA	2	El evento puede ocurrir ocasionalmente (3- 4 veces mes)
MEDIA	3	El evento puede ocurrir esporádicamente en algunas ocasiones (5 -6 veces mes)

ALTA	4	El evento probablemente ocurrirá en varias ocasiones (7 -8 veces mes)
EXTREMA	5	El evento muy probablemente ocurrirá de forma continua (Más de 8 veces me)

Fuente: Pilamunga & Maliza (2018, p.13)

Riesgos Impacto: Se refiere a la medida “criterios de consecuencias” por la materialización del riesgo, la cual permite calificar la gravedad de la pérdida, se mide este impacto en función de pérdidas económicas (Cevallos, 2019).

Tabla 10 Niveles de Severidad o Impacto

IMPACTO	PESO	DESCRIPCION
MUY BAJO	1	Hay daños menores, la pérdida económica es menor. Menor de \$350.
BAJO	2	Los daños se pueden solucionar de manera inmediata. Pérdidas económicas medias. De \$350 a \$3.500
MEDIO	3	Daños considerables, la reparación lleva tiempo. Pérdidas económicas importantes. De \$3.500 a \$8.750

ALTO	4	Los daños no se pueden solucionar con personal interno y se requiere de externos. Pérdidas económicas muy importantes. De \$8.750 a \$17.500
EXTREMO	5	Daños fuertes que permiten la pérdida de las operaciones parciales o totales. Pérdidas económicas muy altas. Superior a \$17.500.

Fuente: Pilamunga & Maliza (2018)

Tabla 11 Descripción de los Riesgos – Medición

PROBABILIDAD	IMPACTO	NIVEL DE RIESGO		COLOR
Muy Baja	Muy Bajo	Bajo	1	Green
Muy Baja	Bajo	Bajo	1	
Muy Baja	Medio	Bajo	1	
Muy Baja	Alto	Medio	2	Yellow
Muy Baja	Extremo	Alto	3	Orange
Baja	Muy Bajo	Bajo	1	Green
Baja	Bajo	Medio	2	Yellow
Baja	Medio	Medio	2	Yellow
Baja	Alto	Alto	3	Orange

Baja	Extremo	Alto	3	
Media	Muy Bajo	Bajo	1	
Media	Bajo	Medio	2	
Media	Medio	Alto	3	
Media	Alto	Alto	3	
Media	Extremo	Crítico	4	
Alta	Muy Bajo	Medio	2	
Alta	Bajo	Alto	3	
Alta	Medio	Alto	3	
Alta	Alto	Crítico	4	
Alta	Extremo	Crítico	4	
Extrema	Muy Bajo	Alto	3	
Extrema	Bajo	Alto	3	
Extrema	Medio	Crítico	4	
Extrema	Alto	Crítico	4	
Extrema	Extremo	Crítico	4	

Fuente: Pilamunga & Maliza (2018)

La metodología de riesgo operacional, de la cooperativa brinda pautas claras del proceso de interpretación de riesgo, la cual fue elaborada por Klever Pilamunga y Isaac Maliza en el año 2018:

El cálculo del Nivel de Riesgo se establecerá de forma individual para cada riesgo y se obtendrá de la multiplicación de la probabilidad e impacto, bajo la siguiente formula.

$$Rin_i = Pin_i \times In_i$$

Donde:

Rin_i : Riesgo Inherente

Pin_i : Probabilidad de Ocurrencia de un evento, sin considerar las acciones y controles mitigantes

In_i : Impacto de un evento, sin considerar las acciones y controles mitigantes

Por lo tanto, el Nivel de riesgo será categorizado en función a las siguientes escalas y conforme se muestra:

Tabla 12. Umbrales de Riesgo

Umbrales	RIESGO
$0 \geq Rin_i \leq 3$	BAJO
$3 > Rin_i \leq 6$	MEDIO
$6 > Rin_i \leq 12$	ALTO
$12 > Rin_i \leq 20$	CRÍTICO

Fuente: Pilamunga & Maliza (2018)

Matriz de Riesgo del área de Tecnología de la Información

Mediante la siguiente matriz se detalla y se muestra el riesgo que tiene la institución en el área de sistemas.

3.3.2. Evaluación de los eventos de riesgos y calificaciones

Tabla 13. Matriz de eventos de riesgo

DOMINIO/ PROCESO	LÍDER PROCESO	CÓDIGO DEL ACTIVO	RIESGO EVALUADO	CRITICIDAD	VULNERABILIDAD	IMPACTO	VOTO / CARGOS			
							Integrantes del proceso	Calificac ión Funciona rio Nro. 1 (Cargo)	Calificac ión Funciona rio Nro. 2 (Cargo)	Calificac ión Funciona rio Nro. 3 (Cargo)
Administración de Base de Datos	TI	GT-TIN- DBA-001	Generación de Datos para reporte	Medio	2,0	2,7	VOTO IMPACTO	3,0	2,0	3,0
							VOTO	2,0	2,0	2,0
							VULNERABILIDAD			
Administración de Base de Datos	TI	GT-TIN- DBA-002	Gestión del almacenamiento de las bases de datos	Alto	3,0	5,0	VOTO IMPACTO	5,0	5,0	5,0
							VOTO	3,0	3,0	3,0
							VULNERABILIDAD			
Administración de Base de Datos	TI	GT-TIN- DBA-003	Administración de réplica en línea	Alto	3,7	5,0	VOTO IMPACTO	5,0	5,0	5,0
							VOTO	4,0	3,0	4,0
							VULNERABILIDAD			
	TI			Alto	3,7	4,3	VOTO IMPACTO	4,0	4,0	5,0

Administración de Base de Datos		GT-TIN-DBA-004	Proceso de restauración de base de datos				VOTO	4,0	4,0	3,0
							VULNERABILIDAD			
Administración de Base de Datos	TI	GT-TIN-DBA-005	Almacenamiento y vaciado de Logs	Medio	1,7	3,0	VOTO IMPACTO	3,0	3,0	3,0
							VOTO	2,0	1,0	2,0
							VULNERABILIDAD			
Administración de Base de Datos	TI	GT-TIN-DBA-006	Gestión de uso de memoria RAM para motor de base de datos	Medio	5,0	2,7	VOTO IMPACTO	3,0	2,0	3,0
							VOTO	5,0	5,0	5,0
							VULNERABILIDAD			
Administración de Base de Datos	TI	GT-TIN-DBA-007	Actualización del motor de base de datos	Medio	3,0	3,0	VOTO IMPACTO	3,0	3,0	3,0
							VOTO	3,0	3,0	3,0
							VULNERABILIDAD			
Gestión del área de TI	TI	GT-TIN-GTI-001	Planificación Interna de TI para desarrollar o dar soporte a la entidad	Alto	5,0	4,3	VOTO IMPACTO	5,0	4,0	4,0
							VOTO	5,0	5,0	5,0
							VULNERABILIDAD			
Administración de Infraestructura	TI	GT-TIN-AIN-001	Gestión de la data center alternativo	Alto	4,0	4,3	VOTO IMPACTO	4,0	4,0	5,0
							VOTO	4,0	4,0	4,0
							VULNERABILIDAD			

Administración de Infraestructura	TI	GT-TIN- AIN-002	Gestión de la data center principal	Alto	4,0	5,0	VOTO IMPACTO	5,0	5,0	5,0		
								VOTO	4,0	4,0	4,0	
								VULNERABILIDAD				
Administración de Infraestructura	TI	GT-TIN- AIN-003	Proceso de Harding a servidores	Alto	4,3	4,7	VOTO IMPACTO	5,0	4,0	5,0		
								VOTO	5,0	5,0	3,0	
								VULNERABILIDAD				
Administración de Infraestructura	TI	GT-TIN- AIN-004	mantenimiento de telecomunicación	Alto	4,0	4,0	VOTO IMPACTO	4,0	4,0	4,0		
								VOTO	4,0	4,0	4,0	
								VULNERABILIDAD				
Administración de Infraestructura	TI	GT-TIN- AIN-005	Gestión para el mantenimiento de respaldo de energía eléctrica	Medio	3,0	4,0	VOTO IMPACTO	3,0	5,0	4,0		
								VOTO	3,0	3,0	3,0	
								VULNERABILIDAD				
Administración de Infraestructura	TI	GT-TIN- AIN-006	Administración del cableado estructural	Medio	3,0	2,3	VOTO IMPACTO	2,0	2,0	3,0		
								VOTO	2,0	4,0	3,0	
								VULNERABILIDAD				
Gestión de Telecomunicaciones	TI	GT-TIN- TEL-001	Interrupción de Comunicaciones Interna y/o Externa	Alto	3,7	4,3	VOTO IMPACTO	4,0	5,0	4,0		
								VOTO	3,0	4,0	4,0	
								VULNERABILIDAD				

Gestión de Telecomunicaciones	TI	GT-TIN-TEL-002	Monitoreo de Servicios Locales de TI	Medio	3,7	3,3	VOTO IMPACTO	4,0	3,0	3,0
							VOTO	3,0	4,0	4,0
							VULNERABILIDAD			
Soporte Técnico	TI	GT-TIN-STE-001	Respaldo de información de los equipos de colaboradores	Medio	3,0	3,3	VOTO IMPACTO	3,0	4,0	3,0
							VOTO	3,0	3,0	3,0
							VULNERABILIDAD			
Soporte Técnico	TI	GT-TIN-STE-002	Gestión de licenciamiento para PC y servidores	Medio	3,0	2,7	VOTO IMPACTO	2,0	3,0	3,0
							VOTO	3,0	3,0	3,0
							VULNERABILIDAD			
Soporte Técnico	TI	GT-TIN-STE-003	Gestión de estaciones de trabajo	Medio	3,7	3,3	VOTO IMPACTO	3,0	4,0	3,0
							VOTO	3,0	4,0	4,0
							VULNERABILIDAD			
Soporte Técnico	TI	GT-TIN-STE-004	Administración de incidentes de TI (Helpdesk)	Medio	3,3	2,7	VOTO IMPACTO	3,0	3,0	2,0
							VOTO	3,0	4,0	3,0
							VULNERABILIDAD			
Seguridad Informática	TI	GT-TIN-SIN-001	Gestión de la seguridad perimetral	Medio	3,0	4,3	VOTO IMPACTO	4,0	5,0	4,0
							VOTO	3,0	2,0	4,0
							VULNERABILIDAD			
	TI			Alto	4,3	4,0	VOTO IMPACTO	3,0	4,0	5,0

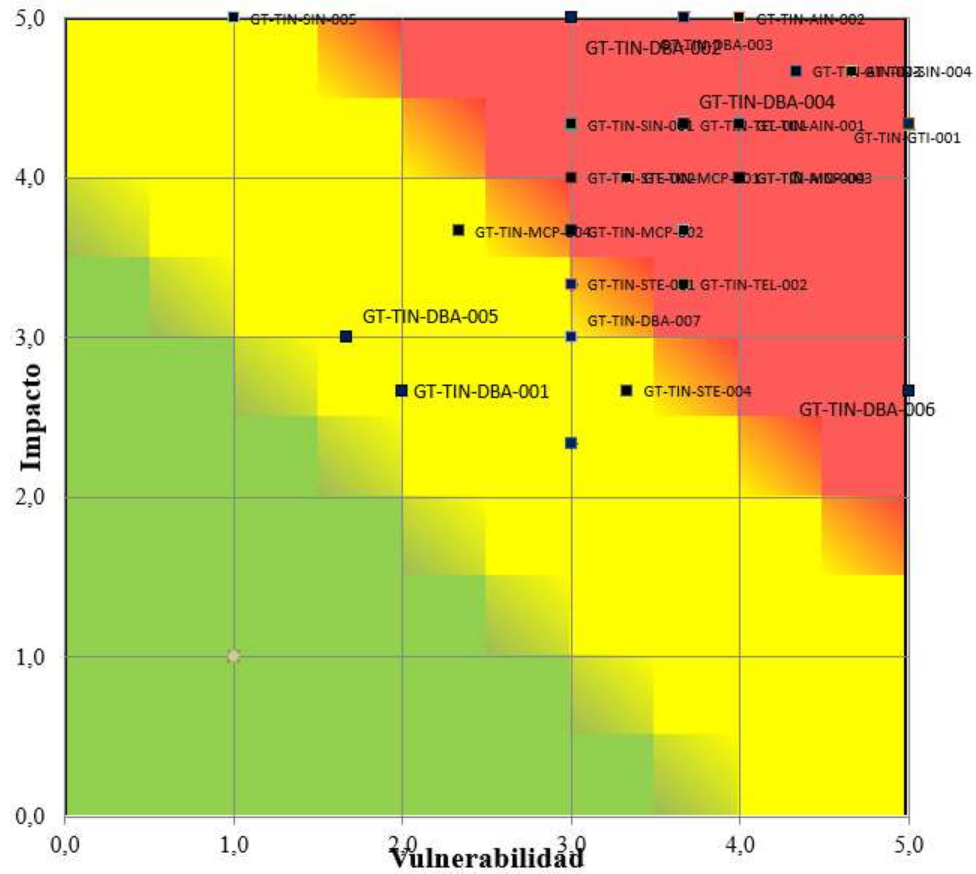
Seguridad		GT-TIN-	Gestión de usuarios y				VOTO	3,0	5,0	5,0
Informática		SIN-002	contraseñas				VULNERABILIDAD			
Seguridad	TI	GT-TIN-	Mantener la	Medio	3,7	3,7	VOTO IMPACTO	2,0	4,0	5,0
Informática		SIN-003	confidencialidad, integridad y disponibilidad de la información de la Cooperativa				VOTO	3,0	4,0	4,0
							VULNERABILIDAD			
Seguridad	TI	GT-TIN-	Difusión de las políticas	Alto	4,7	4,7	VOTO IMPACTO	4,0	5,0	5,0
Informática		SIN-004	seguridad informática				VOTO	5,0	5,0	4,0
							VULNERABILIDAD			
Seguridad	TI	GT-TIN-	Plan de Recuperación de	Alto	5,0	5,0	VOTO IMPACTO	5,0	5,0	5,0
Informática		SIN-005	Tecnología de la Información en caso de desastres				VOTO	5,0	5,0	5,0
							VULNERABILIDAD			
Mantenimiento	TI	GT-TIN-	Requerimiento perfecto	Medio	3,3	4,0	VOTO IMPACTO	4,0	4,0	4,0
Correctivo y		MCP-001	y correctivo de Software				VOTO	3,0	4,0	3,0
Perfectivo de							VULNERABILIDAD			
Software										
	TI		Desarrollo de software	Medio	3,0	3,7	VOTO IMPACTO	4,0	3,0	4,0

Mantenimiento		GT-TIN-					VOTO	3,0	3,0	3,0
Correctivo y		MCP-002					VULNERABILIDAD			
Perfectivo de										
Software										
Mantenimiento	TI	GT-TIN-	Administración de	Alto	4,0	4,0	VOTO IMPACTO	4,0	4,0	4,0
Correctivo y		MCP-003	control de cambio, QA, y				VOTO	4,0	4,0	4,0
Perfectivo de			certificación de sistemas				VULNERABILIDAD			
Software			informáticos							
Mantenimiento	TI	GT-TIN-	Puesta a producción de	Medio	2,3	3,7	VOTO IMPACTO	4,0	4,0	3,0
Correctivo y		MCP-004	software				VOTO	2,0	2,0	3,0
Perfectivo de							VULNERABILIDAD			
Software										
Contratación	TI	GT-TIN-	Condiciones en los	Alto	3,7	4,3	VOTO IMPACTO	4,0	4,0	5,0
de Servicios		CSE-001	Contratos de Servicios				VOTO	3,0	4,0	4,0
			Tecnológicos				VULNERABILIDAD			

Fuente: Elaborado por el investigador y el área de riesgo de la Cooperativa de Ahorro y Crédito Chibuleo Ltda en base a la matriz de Deloitte (2015) y del Banco de España (2012).

Vulnerabilidad, impacto del área de Tecnología de Información

Figura 4 Riesgo del Área de tecnología de la información



Fuente: Elaborado por el investigador y el área de riesgo de la Cooperativa de Ahorro y Crédito Chibuleo Ltda.

3.3.3. Aplicación de controles ISO/IEC 27002:2013

Tabla 14. Aplicación de controles ISO/IEC 27002:2013, con la finalidad de reducir el riesgo

DOMINIO/ PROCESO	LÍDER PROCESO	CÓDIGO DEL EVENTO	RIESGO EVALUADO	CRITICIDAD	CONTROLES ISO/EC 27002:2013
Administración de Base de Datos	SISTEMAS	GT-TIN-DBA- 001	Generación de Datos para reporte	Medio	“5.1.1 Políticas para la seguridad de la información 6.1.2 Segregación de tareas” (ISO Controles, 2013)
	SISTEMAS	GT-TIN-DBA- 002	Gestión del almacenamiento de las bases de datos	Alto	“5.1.1 Políticas para la seguridad de la información 8.2.3 Manipulado de la información

SISTEMAS	GT-TIN-DBA-003	Administración de réplica en línea	Alto	17.1.1 Planificación de la continuidad de la seguridad de la información”. (ISO Controles, 2013)
SISTEMAS	GT-TIN-DBA-004	Proceso de restauración de base de datos	Alto	“12.3.1 Copias de seguridad de la información”. (ISO Controles, 2013)
SISTEMAS	GT-TIN-DBA-005	Almacenamiento y vaciado de Logs	Medio	“12.3.1 Copias de seguridad de la información”. (ISO Controles, 2013)
SISTEMAS	GT-TIN-DBA-006	Gestión de uso de memoria RAM para motor de base de datos	Medio	“11.2.4 Mantenimiento de los equipos”. (ISO Controles, 2013)
SISTEMAS	GT-TIN-DBA-007	Actualización del motor de base de datos	Medio	“11.2.4 Mantenimiento de los equipos”. (ISO Controles, 2013)

Gestión del área de TI	SISTEMAS	GT-TIN-GTI-001	Planificación Interna de TI para desarrollar o dar soporte a la entidad	Alto	<p>“6.1.1 Asignación de responsabilidades para la seguridad de la información.</p> <p>6.1.2 Segregación de tareas.</p> <p>7.2.1 Responsabilidades de gestión”. (ISO Controles, 2013)</p>
Administración de Infraestructura	SISTEMAS	GT-TIN-AIN-001	Gestión de data center alternativo	Alto	<p>“9.1.1 Política de control de accesos.</p> <p>11.2.4 Mantenimiento de los equipos.</p> <p>11.1.4 Protección contra las amenazas externas y ambientales.</p> <p>13.1.1 Controles de red.</p> <p>13.1.2 Mecanismos de seguridad asociados a servicios en red.</p> <p>13.1.3 Segregación de redes.</p> <p>17.1.3 Verificación, revisión y evaluación de la continuidad de la</p>

					seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información” (ISO Controles, 2013)
Administración de Infraestructura	SISTEMAS	GT-TIN-AIN-002	Gestión de data center principal	Alto	“9.1.1 Política de control de accesos. 11.2.4 Mantenimiento de los equipos. 11.1.4 Protección contra las amenazas externas y ambientales. 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.1.3 Segregación de redes. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad

					de la información.”. (ISO Controles, 2013)
Administración de Infraestructura	SISTEMAS	GT-TIN-AIN-003	Proceso de Harding a servidores	Alto	<p>“11.2.1 Emplazamiento y protección de equipos.</p> <p>11.2.2 Instalaciones de suministro.</p> <p>12.6.1 Gestión de las vulnerabilidades técnicas.”. (ISO Controles, 2013)</p>
Administración de Infraestructura	SISTEMAS	GT-TIN-AIN-004	Mantenimiento de telecomunicaciones	Alto	<p>“8.1.1 Inventario de activos.</p> <p>11.2.4 Mantenimiento de los equipos.</p> <p>12.1.1 Documentación de procedimientos de operación.</p> <p>13.1.2 Mecanismos de seguridad asociados a servicios en red.”. (ISO Controles, 2013)</p>
Administración de Infraestructura	SISTEMAS	GT-TIN-AIN-005	Gestión para el mantenimiento del	Medio	“11.2.2 Instalaciones de suministro.” (ISO Controles, 2013)

			respaldo de energía eléctrica		
Administración de Infraestructura	SISTEMAS	GT-TIN-AIN-006	Administración del cableado estructural	Medio	“9.1.2 Control de acceso a las redes y servicios asociados. 13.1.1 Controles de red. 13.1.3 Segregación de redes.”. (ISO Controles, 2013)
Gestión de Telecomunicaciones	SISTEMAS	GT-TIN-TEL-001	Interrupción de Comunicaciones Interna y/o Externa	Alto	“13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.2.2 Acuerdos de intercambio. 13.2.4 Acuerdos de confidencialidad y secreto.”. (ISO Controles, 2013)
Gestión de Telecomunicaciones	SISTEMAS	GT-TIN-TEL-002	Monitoreo de Servicios Locales de TI	Medio	“12.4.3 Registros de actividad del administrador y operador del sistema. 9.1.2 Control de acceso a las redes y

					servicios asociados.”. (ISO Controles, 2013)
Soporte Técnico	SISTEMAS	GT-TIN-STE-001	Respaldo de información de los equipos de colaboradores	Medio	<p>“12.3.1 Copias de seguridad de la información.</p> <p>11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.”. (ISO Controles, 2013)</p>
Soporte Técnico	SISTEMAS	GT-TIN-STE-002	Gestión de licenciamiento para PC y servidores	Medio	<p>“12.5.1 Instalación del software en sistemas en producción.</p> <p>9.4.4 Uso de herramientas de administración de sistemas.”. (ISO Controles, 2013)</p>
Soporte Técnico	SISTEMAS	GT-TIN-STE-003	Gestión de estaciones de trabajo	Medio	<p>“11.2.1 Emplazamiento y protección de equipos.</p> <p>11.2.8 Equipo informático de usuario</p>

					desatendido. 11.2.4 Mantenimiento de los equipos.
Soporte Técnico	SISTEMAS	GT-TIN-STE-004	Administración de incidentes de TI (Help desk)	Medio	16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones. 16.1.5 Respuesta a los incidentes de seguridad.”. (ISO Controles, 2013)
Seguridad Informática	SISTEMAS	GT-TIN-SIN-001	Gestión de la seguridad perimetral	Medio	“5.1.1 Conjunto de políticas para la seguridad de la información. 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.1.3 Segregación de redes.”. (ISO Controles, 2013)
	SISTEMAS			Alto	

Seguridad		GT-TIN-SIN-	Gestión de	Alto	“9.1.1 Política de control de accesos.
Informática		002	usuarios y contraseñas		9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso”. (ISO Controles, 2013)
Seguridad	SISTEMAS	GT-TIN-SIN-	Confidencialidad,	Medio	“5.1.1 Conjunto de políticas para la
Informática		003	integridad y disponibilidad de la información		seguridad de la información.”. (ISO Controles, 2013)
	SISTEMAS			Alto	

Seguridad Informática		GT-TIN-SIN-004	Difusión de las políticas seguridad informática		“6.1.1 Asignación de responsabilidades para la seguridad de la información.”. (ISO Controles, 2013)
Seguridad Informática	SISTEMAS	GT-TIN-SIN-005	Plan de Recuperación de Tecnología de la Información en caso de desastres	Alto	“17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.”. (ISO Controles, 2013)
Mantenimiento Correctivo y	SISTEMAS	GT-TIN-MCP-001	Requerimiento perfectivo y	Medio	“14.1.1 Análisis y especificación de los requisitos de seguridad.

Perfectivo de Software			correctivo de Software		14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas. 14.1.3 Protección de las transacciones por redes telemáticas.”. (ISO Controles, 2013)
Mantenimiento Correctivo y Perfectivo de Software	SISTEMAS	GT-TIN-MCP-002	Desarrollo de software	Medio	“14.2.1 Política de desarrollo seguro de software. 14.2.6 Seguridad en entornos de desarrollo.”. (ISO Controles, 2013)
Mantenimiento Correctivo y Perfectivo de Software	SISTEMAS	GT-TIN-MCP-003	Administración de control de cambio, QA, y certificación de sistemas informáticos.	Alto	“14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.”. (ISO Controles, 2013)
	SISTEMAS			Medio	

Mantenimiento Correctivo y Perfectivo de Software		GT-TIN-MCP-004	Puesta a producción de software		“14.2.9 Pruebas de aceptación.”. (ISO Controles, 2013)
Contratación de Servicios	SISTEMAS	GT-TIN-CSE-001	Condiciones en los Contratos de Servicios Tecnológicos	Alto	“15.1.1 Política de seguridad de la información para suministradores. 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores. 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.” (ISO Controles, 2013)

Fuente: Elaboración propia e ISO Controles (2013)

CAPÍTULO IV

DESARROLLO DE LA PROPUESTA

4.1. ANÁLISIS

Luego de un análisis exhaustivo de los riesgos a los que se enfrenta el área de tecnología de Información de la Cooperativa de Ahorro y Crédito Chibuleo Ltda, se determinó que los controles detallados anteriormente son los más adecuados para mitigarlos. Este diagnóstico fue el punto de partida para el desarrollo de una política de seguridad de información, que logre fortalecer el área de Tecnología de información con la finalidad de precautelar los datos de la institución.

4.2. INTRODUCCIÓN

La información es el activo más importante que tienen las instituciones financieras, por lo tanto existen amenazas internas / externas, que pueden acceder ilegalmente a los datos que las organizaciones recaban a diario. Existen distintos tipos de amenazas, como aquellas relacionadas con el entorno: erupciones volcánicas, terremotos, inundaciones, etc., y a amenazas relacionadas al factor humano: ambiente laboral, estabilidad, infraestructura, fallos en el software, etc.

Uno de los principales retos para disminuir los riesgos en una institución es desarrollar un plan de contingencias y continuidad del área de tecnología, que establezca políticas de respaldo de información y diseñe modelos de recuperación de desastres, junto con un plan de continuidad del negocio.

El departamento de Tecnología de Información de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., ha elaborado un plan de contingencia para la recuperación de desastres, donde describe las tareas y actividades primordiales, con el fin de mantener los servicios tecnológicos disponibles y que cumplan con los requerimientos del negocio. Este plan, permite continuar sus procesos operativos en caso de interrupciones, las cuales pueden acaecer por la presencia de desastres naturales o eventos fortuitos que provoquen fallas e interrupción en el funcionamiento del hardware y software implementados en el centro de datos.

El diseño de una política de seguridad para el área de Tecnología de la Informaciones de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., basado en la Norma de seguridad ISO/IEC 27002:2013, permitirá contar con una metodología internacional para la seguridad de la información, que ayude a mantener la confidencialidad, integridad y disponibilidad de los datos.

4.3. OBJETIVO

Diseñar una política de seguridad de información para el área de tecnología de información de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., apoyado en la norma internacional ISO/IEC 27002:2013 mediante la aplicación de los controles de seguridad y mantener la confidencialidad, integridad y disponibilidad de los datos que posee la institución.

4.4. ALCANCE

En el presente documento se establecen políticas de seguridad de información para el área de tecnología de la Cooperativa de Ahorro y Crédito Chibuleo Ltda.. Además, se definen los controles necesarios para el cumplimiento de medidas de seguridad mínimas, en miras de resguardar los datos de la institución con un correcto planeamiento, preparación, entrenamiento, ejecución y difusión de esta política.

4.5. DEFINICIONES

Disponibilidad: La información debe estar disponible en el momento y formato que se requieran, así como los recursos necesarios para mitigar cualquier amenaza (Vasquez, 2017, p. 117)

Tecnología de Información: Según la resolución de la Superintendencia de Economía Popular y Solidaria (SEPS-IGT-IR-IGJ-2018-0279, 2018, p.6), son las herramientas y métodos utilizados para la administración de la información e incluye hardware, software, sistemas operativos, redes, etc.

Proceso crítico: “Es indispensable para la continuidad del negocio y las operaciones de una institución, y cuya falta de identificación o aplicación deficiente puede generar un impacto financiero negativo”. (SEPS-IGT-IR-IGJ-2018-0279, 2018, p. 5)

Información crítica: “Es la información considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones”. (SEPS-IGT-IR-IGJ-2018-0279, 2018, p.5)

Control de Acceso: Es la autorización o restricción de acceso a un sistema determinado, en función de los requisitos planteados.

Ataque: Es una ofensiva que busca destruir, deteriorar o alterar una persona, bien o servicio. En el caso de los sistemas informáticos, es el ingresar a un sistema de manera fraudulenta para alterar o robar información importante en la entidad.

Parte Interesada: Persona o institución que puede afectar o es afectada por una decisión o actividad.

Plan de continuidad: “Conjunto de procedimientos alternativos para el funcionamiento normal de los procesos críticos y de aquellos definidos por la entidad que permitan su operatividad, a fin de minimizar el impacto operativo y financiero que pueda ocasionar cualquier evento inesperado específico”. (SEPS-IGT-IR-IGJ-2018-0279, 2018, p. 5)

Maliciosos-Externos: Acceso de cualquier persona a las instalaciones de la Institución, que tengan como intención robar, perder, dañar o alterar los equipos informáticos y la información.

Maliciosos-Internos: Cualquier persona/organismo interno que pretenda utilizar los recursos disponibles en perjuicio de la institución con la que colabora.

No maliciosos: Cuando los datos no están completos o se encuentran con errores.

Administración de la información: “Es el proceso mediante el cual se captura, procesa, almacena y transmite información por cualquier medio”. (SEPS-IGT-IR-IGJ-2018-0279, 2018)

Aplicación informática: “Son los procedimientos programados a través de alguna herramienta tecnológica” (SEPS-IGT-IR-IGJ-2018-0279, 2018).

Evento de riesgo operativo: “Es el incidente o hecho que se ha presentado o puede presentarse que puede derivar en pérdidas financieras o de información, suspensión de operaciones para la entidad, originadas por fallas o insuficiencias en los factores de riesgo operativo”. (SEPS-IGT-IR-IGJ-2018-0279, 2018).

Factores de riesgo operativo: “Son las fuentes generadoras de riesgos operativos tales como: personas, procesos, tecnología de la información y eventos externos” (SEPS-IGT-IR-IGJ-2018-0279, 2018)

Impacto: “Es la afectación financiera que podría tener la entidad, en el caso de que ocurra un evento de riesgo”. (SEPS-IGT-IR-IGJ-2018-0279, 2018)

4.6. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

SECCIÓN I: DIRECTRICES DE LA DIRECCIÓN EN SEGURIDAD DE LA INFORMACIÓN

Art. 1 Conjunto de políticas para la seguridad de la información. - El Jefe de Tecnología de Información deberá aprobar un documento formal donde conste acuerdos de confidencialidad

y no divulgación, la misma que será publicado y comunicado a los empleados y proveedores de la Cooperativa de Ahorro y Crédito Chibuleo Ltda. Anexo (1) Acuerdo de confidencialidad.

Art. 2 Revisión de las políticas de seguridad de la información. - La política de seguridad de información debe ser revisada, documentada, actualizada y socializada de forma permanente como establece la norma de referencia o cada vez que ocurran cambios importantes, mediante la presente política se podrá evitar el acceso no autorizado de usuarios internos / externos.

SECCIÓN II: ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

A. ORGANIZACIÓN INTERNA

Art. 3 Asignación de responsabilidades para la seguridad de la información. - El jefe de tecnología de información puede delegar funciones sobre seguridad de la información, a uno o varios integrantes del área.

Art. 4 Segregación de funciones

1. El jefe de tecnología de información deberá asignar un responsable de cada una de las actividades que tiene el área de Tecnología de la Información, con el objetivo de mantener un control adecuado de los activos de información y poder evitar accesos no autorizados.
2. El área de Tecnología deberá implementar controles de monitoreo para las actividades realizadas por todo el personal de TI, con el fin de revisar el cumplimiento de las mismas.

B. DISPOSITIVOS PARA MOVILIDAD Y TELETRABAJO

Art. 5 Política de uso de dispositivos para movilidad. - El área de Tecnología con la ayuda del oficial de seguridad deberá definir unas reglas de autenticación entre el dispositivo y la red de la institución, mediante la cual se puede realizar el intercambio de información con dispositivos autorizados.

SECCIÓN III: SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

A. ANTES DE LA CONTRATACIÓN

Art. 6 Investigación de antecedentes. – Los candidatos seleccionados a ser parte de la institución, deberán pasar por un proceso de investigación de antecedentes que será realizado por el área de Talento Humano, con el fin de mitigar riesgos en lo referente al uso de información.

Art. 7 Términos y condiciones de contratación. – Los empleados deben firmar un compromiso de confidencialidad y resguardo de la información, este procedimiento lo llevarán adelante el jefe del área junto con el jefe de Talento Humano.

B. DURANTE LA CONTRATACIÓN

Art. 8 Responsabilidades de gestión. - El jefe de Tecnología desde el día que ingresa hasta el día que se desvincula de la institución, deberá asignar responsabilidades definidas para una mejor administración de los activos de información.

Art. 9 Concienciación, educación y capacitación en seguridad de la información

1. La Cooperativa de Ahorro y Crédito Chibuleo Ltda., mediante el área de Tecnología deberá realizar capacitaciones periódicas sobre las políticas de seguridad de la información, mediante, con el fin de concientizar a los colaboradores sobre la criticidad de la información.
2. La Cooperativa de Ahorro y Crédito Chibuleo Ltda., mediante el área de Tecnología deberá realizar capacitaciones semestrales a los usuarios sobre el uso y manejo de las aplicaciones que provee el área de TI a las demás. Estas capacitaciones tienen que realizarse en un ambiente de pruebas para evitar el riesgo de error humano.

Art. 10 Procesos disciplinarios

1. El jefe de Tecnología de información designará a los usuarios que dominen el tema de seguridad de la información para realizar las capacitaciones en cada área de la institución.
2. Es responsabilidad de los usuarios de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., asistir a las capacitaciones de forma semestral y también acatar las disposiciones expuestas en cada una de ellas.

C. CESE O CAMBIO DE LOS PUESTOS DE TRABAJO

Art. 11 Cese o cambio de puesto de trabajo.

1. El área de Talento Humanos de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., deberá comunicar de forma inmediata la renuncia o desvinculación de un empleado de la institución al área de Tecnología, para que este pueda dar de baja al usuario de los sistemas informáticos. Los usuarios que no se ciñan a esta política serán responsables de las acciones que se generen al no cumplir con el proceso adecuado.
2. El área de Talento Humano de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., deberá notificar de forma inmediata el inicio y fin del periodo de vacaciones de los empleados, para que el área de TI pueda inhabilitar o habilitar a los usuarios en las fechas indicadas. Los usuarios que no se ciñan a esta política serán responsables de las acciones que se generen al no cumplir con el proceso adecuado.
3. El área de tecnología de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., debe informar al empleado de las obligaciones y responsabilidades en seguridad de la información que tiene durante el proceso de cambio de puesto de trabajo en la Institución.
4. Los empleados del área de TI que se desvinculen laboralmente de la institución deberán entregar los insumos que les fueron proporcionados en las mismas condiciones que los recibieron. Este proceso se realiza para el control de inventarios de la institución.

SECCIÓN IV: GESTIÓN DE ACTIVOS

A. RESPONSABILIDAD SOBRE LOS ACTIVOS

Art. 12 Inventario de activos. - La Cooperativa de Ahorro y Crédito Chibuleo Ltda., debe mantener un inventario de todos los activos de información, y los responsables de los procesos deben clasificar la información dependiendo de su valor, sensibilidad, riesgo de pérdida y requerimientos legales de retención.

Art. 13 Uso aceptable de los activos. - Los responsables de cada proceso, independientemente del área donde se encuentren, deben clasificar la información. Los controles deben ser realizados desde la creación, almacenamiento o destrucción de la información.

Art. 14 Devolución de activos. - Los empleados o usuarios externos deben devolver a la organización todos los activos que se encuentren a su cargo al terminar la relación laboral o de prestación de servicio. Debe quedar como constancia un acta de dicha devolución firmada por ambas partes.

B. CLASIFICACIÓN DE LA INFORMACIÓN

Art. 15 Clasificación de la información. - El responsable de seguridad de información deberá realizar una correcta clasificación de la información dependiendo de su criticidad e importancia para la organización.

Art. 16 Manipulación de activos. - Cada jefe de área debe realizar el proceso de clasificación de información, haciendo un inventario de la información utilizada por su área, debe especificar lo siguiente:

- Nombre la información
- Procesos en los que se usa
- Formato en el que se encuentra
- Nivel de sensibilidad
- Correcta codificación

En los casos en que la misma información esté clasificada por diferentes áreas en niveles de sensibilidad diferentes, el responsable de Seguridad de la Información determinará el valor y el nivel de clasificación para dicha información.

Art. 17 Gestión de soportes extraíbles. - No está permitida la conexión a la red de la Entidad de equipos portátiles, notebooks, computadores, dispositivos móviles o cualquier otro artefacto de uso personal de los funcionarios, sin la debida autorización del responsable de Seguridad de la Información.

Art. 18 Eliminación de soportes. - La entidad, establece la siguiente política en materia de respaldo y borrado seguro de la información:

1. Permanentemente se debe efectuar copia de respaldo de toda la información considerada confidencial o sensible y que se encuentre contenida en los equipos de la Entidad. En especial se debe asegurar el respaldo de información al finalizar el vínculo laboral del funcionario o contractual del proveedor, quien generó, editó y manejó previamente dicha información. Se debe seguir el mismo procedimiento al dar de baja un activo tecnológico (por pérdida, daño, devolución, enajenación o donación, entre otros).
2. Se deben adoptar procedimientos para la aplicación de técnicas de borrado seguro de información, mediante herramientas o procesos manuales y/o automáticos que permitan eliminar toda la información contenida en el equipo o dispositivo asignado a un funcionario o proveedor cuando sea necesario, ya sea por su desvinculación o por la baja del activo tecnológico.
3. Los procedimientos establecidos en esta política se deben aplicar a todo dispositivo de almacenamiento que contenga información confidencial o sensible para la Entidad, como discos duros, dispositivos removibles, tabletas, equipos móviles, entre otros.
4. Está prohibida la reutilización y/o reasignación de equipos o dispositivos a otros funcionarios o terceros que contenga información sensible de la Entidad sin que la respectiva área de Tecnología haya aplicado previamente los procedimientos de back-up y de borrado seguro de información.

Art. 19 Soportes físicos en tránsito. – El Jefe de Tecnología junto con el responsable de procesos deberán crear un procedimiento para el transporte seguro de medios físicos que contengan información como: Discos Duros, Unidades extraíbles, portátiles y otros dispositivos de la institución, cifrando la información.

SECCIÓN V: CONTROL DE ACCESO

A. REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO

Art. 20 Políticas de control de acceso.

1. El jefe del área de tecnología deberá proporcionar a los colaboradores los manuales de usuario para el correcto uso y manejo de los sistemas que provee el área de Tecnología hacia el resto de las áreas.
2. Obligar a que los empleados cambien sus claves temporales en su primer acceso al sistema asignado.
3. No mostrar las contraseñas en pantalla cuando el usuario está ingresando a los sistemas.
4. Utilizar contraseñas seguras, para lo cual se debe cumplir los siguientes requisitos:
 - La contraseña debe tener mínimo de 8 caracteres y máxima de 16 carácter.
 - Usar mínimo una letra mayúscula
 - Usar mínimo una letra minúscula
 - Utilizar mínimo un carácter especial
 - Utilizar mínimo un número
 - La contraseña debe tener una vigencia, y luego se debe cambiar por una nueva, mantener un histórico de 5 contraseñas anteriores, las cuales no podrán ser utilizadas.
 - No usar contraseñas que contengan relación con el usuario, nombres, apellidos, fechas de nacimiento, fechas de matrimonio, etc.

Art. 21 Control de acceso a las redes y servicios asociados. - El acceso a la red de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., debe ser otorgado solo a usuarios autorizados, debidamente asignado todos los roles y perfiles a los diferentes sistemas informáticos, en

coordinación con el área de Talento Humano, jefes de área, responsable de seguridad de información y el jefe de Tecnología de Información.

B. GESTIÓN DE ACCESO DE USUARIOS

Art. 22 Gestión de altas/bajas en el registro de usuarios.

1. El jefe de Talento Humanos de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., deberá informar al responsable de Seguridad de la Información, y éste a su vez enviará su aprobación al área de Tecnología junto con la nómina del nuevo personal y sus respectivos “Check List” de vinculación (Anexo 2) para que el área de Tecnología asigne los roles y perfiles en los sistemas informáticos.
2. El jefe de Talento Humanos de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., deberá informar de forma inmediata al responsable de seguridad de la información la baja de algún empleado para su proceso de inactivación de usuarios de los diferentes sistemas de información, la cual será procesada por el área de Tecnología de información.

Art. 23 Gestión de los derechos de acceso asignado a usuarios. - El responsable de seguridad de información deberá mantener y establecer mecanismos de accesos físicos y lógicos para los usuarios que acceden a los sistemas informáticos.

Art. 24 Gestión de los derechos a accesos con privilegios especiales. - La asignación de privilegios a usuarios en los sistemas informáticos se los realizará previa autorización del jefe de Tecnología en conjunto con el responsable de información, con un documento firmado o un correo de autorización.

Art. 25 Revisión de los derechos de acceso de los usuarios. - El jefe de Tecnología junto con el responsable de seguridad de información deberán revisar los accesos de los usuarios a cada rol y a los accesos que mantienen dentro de los sistemas de informáticos, en periodos definidos.

Art. 26 Retirada o adaptación de los derechos de acceso. - El área de Tecnología deberá revocar de manera inmediata los privilegios de los usuarios que cambiaron de puesto, con sus

respectivas tareas, del mismo modo también revocar los accesos a usuarios que fueron autorizados por la gerencia.

C. RESPONSABILIDADES DE USUARIO

Art. 27 Uso de la información confidencial para la autenticación.

1. El usuario es responsable directo de su estación de trabajo y es su responsabilidad bloquear la cuenta de usuario de su equipo de cómputo cuando no esté presente en su lugar de trabajo.
2. Ningún usuario deberá acceder a las aplicaciones informáticas de la cooperativa, utilizando la cuenta de otro usuario.
3. Es responsabilidad de los usuarios el uso que realicen en las cuentas de acceso y contraseñas que fueron otorgadas a los sistemas informáticos de la Cooperativa y equipos de cómputo.
4. Los usuarios son los responsables de todas las actividades y procesos realizados con sus cuentas de acceso y claves.
5. Las contraseñas de acceso a las cuentas de usuarios no deben ser almacenados en dispositivos que no estén cifrados, almacenados o escritos en lugares de fácil acceso como en cuadernos, escritorio o pegados en la pantalla.
6. Los usuarios deben informar de manera inmediata al área de Tecnología de información sobre daños, fallas o amenazas detectadas en las aplicaciones informáticas.
7. El área de Tecnología no es responsable del mal uso que se le dé a las cuentas de correos electrónicos, otorgada a usuarios cuando inician su relación laboral con la institución.
8. La cuenta del correo electrónico de los usuarios que terminen su relación laboral con la empresa debe ser desactivada de forma inmediata.

D. CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

Art. 28 Restricción del acceso a la información. - El jefe de Tecnología junto con el responsable de seguridad de la información, deberán restringir el acceso a los sistemas de información, y tener acceso únicamente a la información que le concierne para cumplir con las actividades encomendadas por el cargo.

Art. 29 Procedimientos seguros de inicio de sesión. - Todos los dispositivos de cómputo, que tengan acceso a los sistemas de información, bases de datos, reportes deben contar con mecanismos de autenticación y privilegios de usuarios apropiados, dependiendo el tipo de información que está manipulando el usuario final.

Art. 30 Sistema de gestión de contraseñas.

1. Todas las contraseñas por defecto de servidores, bases de datos, sistemas informáticos, aplicaciones, Routers, Switch, Acces Point debes cambiarse antes de sacarlos a producción.
2. El área de Tecnología de Información será quien genere un usuario y una contraseña a los usuarios de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., el primer inicio lo realizarán con las credenciales entregadas, luego los usuarios deberán cambiar esta contraseña para acceder a sus servicios.
3. Los usuarios podrán realizar cambios de su contraseña cuando crean necesarios o cuando el encargado de seguridad de información exija hacerlo.

Art. 31 Control de acceso al código fuente de los programas. - El jefe de tecnología de información mediante correo electrónico solicitará el acceso a las fuentes del sistema financiero a usuarios internos o externos con sus respectivos permisos de lectura, escritura, ejecución etc., y la persona que ejecutará es el analista de sistemas.

SECCIÓN VI: SEGURIDAD FÍSICA Y DEL ENTORNO

A. ÁREAS SEGURAS

Art 32. Controles físicos de entrada

1. Todos los lugares que son identificados como áreas restringidas y tengan información sensible para la institución, deben ser protegidos contra accesos no autorizados, utilizando medios y procedimientos tecnológicos o registro de ingresos en formatos definidos por las áreas.
2. Todos los usuarios que tengan acceso a los sitios donde se encuentran los sistemas de información deben llevar obligatoriamente visible su credencial.
3. Los usuarios que ingresen a áreas restringidas deben registrarse de forma obligatoria el ingreso, detalle de la visita y hora de salida.

Art. 33 Seguridad de las oficinas, despachos y recursos. - Los ingresos y egresos de personal a las instalaciones de la Cooperativa de Ahorro y Crédito Ltda., deben ser registrados, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.

- a) Los funcionarios deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la Entidad; en caso de pérdida del identificación o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.
- b) Pedir autorización al encargado de seguridad de información para el ingreso a áreas restringidas.

Art. 34 Protección contra las amenazas internas / externas

1. Los empleados de la institución no deben consumir líquidos y alimentos dentro de los centros de cómputo o áreas restringidas de la institución.
2. El personal de limpieza, al igual que otros empleados de la entidad, deben recibir capacitaciones sobre seguridad de la información, debido a que por su actividad tienen

acceso a los distintos equipos informáticos. La capacitación debe ser coordinada entre el departamento de Talento Humano y el área de TI, con el fin de prevenir la fuga de información.

3. El personal de limpieza de la Institución tiene prohibido el ingreso de maletas o material que no sea el relacionado a sus funciones.
4. El piso de los ambientes que son asignados para los equipos de procesamiento de información no debe ser de material combustible.
5. La Cooperativa de Ahorro y Crédito Chibuleo Ltda., debe contar extintores de incendios en aquellos ambientes que cuenten con equipos de procesamiento de información, deben tener la capacidad de mitigar el fuego generado o bien por equipos eléctricos o papel.
6. Los suministros como papelería, deben almacenarse a una distancia considerable de los equipos de procesamiento y almacenamiento de información, para evitar daños que afecte a los mismos.

B. SEGURIDAD DE LOS EQUIPOS

Art. 35 Instalaciones de suministros. - Todos los equipos que proveen de información a la institución como centros de datos, equipos del área de sistemas deben tener ininterrumpida la energía eléctrica.

Art. 36 Seguridad del Cableado

1. El técnico de infraestructuras debe realizar mantenimientos periódicos del cableado estructurado de la institución, para prevenir daños ambientales e interceptación de datos.
2. El cableado estructurado debe estar claramente codificado, permitiendo identificar la estructura de conexión entre sitios de la institución.

Art. 37 Mantenimiento de los equipos

1. El jefe de Tecnología junto con el técnico de soporte de infraestructura deben realizar planificaciones anuales de mantenimiento de equipos de cómputo en toda la institución, los cuales deben ser en horarios que no afecte el correcto funcionamiento del personal operativo.

2. El jefe de tecnología junto con el técnico de infraestructura deberán llevar registros de mantenimiento preventivo y correctivo de los equipos de cómputo.
3. Los usuarios que hayan recibido mantenimiento en sus equipos deben ser informados previamente por el jefe de tecnología junto con el técnico de infraestructura.

Art. 38 Seguridad de los equipos fuera de la institución. - El responsable de seguridad de la información debería suministrar seguridad para los equipos fuera de las oficinas, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.

Se recomienda tener en cuenta las siguientes directrices para la protección del equipo fuera de las instalaciones:

- a) El equipo y los medios llevados fuera de las instalaciones deben contar con un cifrado de los discos duros. El responsable no deberían descuidarlos en sitios públicos, los computadores portátiles se deben llevar como equipaje de mano y camuflado, cuando sea posible, durante los viajes;
- b) Se deberían observar en todo momento las instrucciones del fabricante para la protección del equipo, por ejemplo, protección contra la exposición a campos electromagnéticos fuertes;
- c) Se recomienda determinar controles para el trabajo que se realiza en casa mediante una evaluación de riesgos y controles adecuados que se aplican de forma idónea, por ejemplo, gabinetes de archivos con seguro, política de escritorio despejado, controles de acceso a los computadores y comunicaciones seguras con la oficina.
- d) Se debería establecer la cobertura adecuada del seguro para proteger el equipo fuera de las instalaciones.

Art. 39 Políticas de puestos de trabajo y bloqueo de pantalla.

1. Cuando el usuario requiera ausentarse de su puesto de trabajo debe bloquear el acceso a su equipo de cómputo, con un protector de pantalla y contraseñas seguras como lo menciona en el **Art. 24.**

2. Los usuarios de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., tiene totalmente prohibido mover, instalar, reubicar los equipos y retirar los sellos de seguridad de los aparatos de cómputo.
3. Al terminar su jornada laboral, el usuario es responsable de apagar sus equipos informáticos, para evitar el acceso de terceros.

SECCIÓN VII: SEGURIDAD DE OPERACIONES

A. COPIAS DE SEGURIDAD

Art. 40 Separación del entorno de desarrollo, pruebas y producción. - El jefe de Tecnología deberá separar los ambientes de desarrollo, pruebas y producción para poder realizar pruebas y evitar riesgos de accesos no autorizados a los sistemas de producción.

B. PROTECCIÓN CONTRA EL SOFTWARE MALICIOSOS

Art. 41 Control contra el código malicioso. - Todas las computadoras, portátiles, tabletas y teléfonos móviles que son propiedad de la institución deben tener instalado un antivirus actualizado.

C. COPIAS DE SEGURIDAD

Art. 42 Copias de Seguridad de la Información. - El jefe de tecnología de información debe contar con un proceso de copias de seguridad de los sistemas informáticos y mantener un control de accesos restringidos solo al personal autorizado.

D. REGISTRO DE ACTIVIDAD Y SUPERVISIÓN

Art. 43 Protección de los registros de información. - El jefe de tecnología de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., definirá la periodicidad de generar copias de seguridad de los sistemas de información de la institución.

1. Las copias de seguridad de la información deben ser resguardadas en unidades de almacenamiento en discos duros extraíbles en buen estado.

2. Cuando las unidades de almacenamiento extraíbles se encuentren en mal estado, se debe realizar un proceso de eliminación de información de forma segura, y posteriormente dar de baja de los activos.
3. Se debe enviar a bóveda, específicamente al área de cajas, una copia de seguridad de la información de los sistemas informáticos, con el fin de mantener un respaldo de información fuera del área de tecnología.
4. El jefe de tecnología debe enviar una copia de información semanal a otro lugar fuera de la institución.

Art. 44 Registro de actividad del administrador y operador del sistema. - El jefe de tecnología junto con el oficial de seguridad de información, deben revisar los logs de auditoría de los administradores y operadores de los sistemas informáticos, con el fin de identificar brechas de seguridad y revisar sus actividades dentro del sistema.

E. CONTROL DEL SOFTWARE EN EXPLOTACIÓN

Art. 45 Instalación de software en producción. - El jefe de tecnología designará al responsable para la instalación de los sistemas informáticos en la institución con las siguientes recomendaciones:

- a) Realizar procedimientos de instalación para cada aplicativo.
- b) Verificación: contar con los contactos de los soportes de sistemas de terceros.
- c) Se asegurará del correcto funcionamiento y actualización.

F. GESTIÓN DE LA VULNERABILIDAD TÉCNICA

Art. 46 Restricción en la instalación del software. - La instalación de software en las computadoras de la institución, son funciones exclusivas del área de tecnología con el personal de soporte y se deben tomar las siguientes observaciones:

- a) Se debe mantener una lista actualizada del software autorizado para la instalación.
- b) De forma permanente, el área de tecnología junto con el responsable de seguridad de información deberá revisar el software instalado en cada estación de trabajo.

- c) El uso de otros programas no autorizados dentro de la institución será considerado como una falta a la política de seguridad de información.

SECCIÓN VII: SEGURIDAD EN LAS TELECOMUNICACIONES

A. GESTIÓN EN LA SEGURIDAD EN LAS REDES

Art. 47 Control de red

1. El área de tecnología de información de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., es el encargado de administrar y permitir el acceso a los usuarios que necesiten ingresar a la red, siempre que estos equipos sean autorizados por el encargado de la seguridad de la información y sean utilizados para fines laborales.
2. Los usuarios que fueron autorizados por la persona encargada de la seguridad de la información deberán acercarse con sus equipos al área de Tecnología para su registro de MAC, y su asignación de una IP estática.
3. El área de tecnología de información de la institución deberá implementar herramientas de gestión y monitoreo permanente de la red de datos de toda la Cooperativa de Ahorro y Crédito Chibuleo Ltda.
4. El control de acceso a la red de datos de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., se realizará cuando se detecte que el usuario está navegando en páginas con contenido pornográfico, comunidades de hackers y/o realizando acceso no autorizado a datos restringidos de la institución.

Art. 48 Mecanismos de seguridad asociados a servicios en red.

1. El jefe de tecnología deberá incluir acuerdos de niveles de servicios cuando se requiera contratar servicios de terceros.
2. El jefe de tecnología mantendrá una bitácora de respaldos de las configuraciones de routers, firewall, switch de core y otros dispositivos de red, de manera mensuales o cada vez que se realicen cambios significativos.

Art. 49 Segmentación de redes. - El área de tecnología de información deberá mantener la red de datos segmentada dependiendo de los grupos de trabajo, dominios, ubicación geográfica y red de enlaces.

B. INTERCAMBIO DE INFORMACIÓN CON PARTES EXTERNAS.

Art. 50 Acuerdos de confidencialidad y secreto. - El área legal junto con el jefe de tecnología deberá establecer cláusulas en los contratos, como: acuerdos de confidencialidad, de intercambio de información y no divulgación, para poder evitar cualquier incidente relacionado con la seguridad de la información.

SECCIÓN IX: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

A. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Art. 51 Análisis y especificaciones de los requisitos de seguridad. - El jefe de tecnología junto con el responsable de seguridad deberá implementar controles de seguridad antes, durante y después de la implementación o mantenimiento de los sistemas de informáticos.

B. SEGURIDAD EN EL DESARROLLO Y EN LOS PROCESOS DE SOPORTE

Art. 52 Políticas de desarrollo seguro de software. - El área de tecnología de información velará por el desarrollo de los sistemas informáticos internos o externos, para que cumplan con los requisitos de seguridad, y buenas prácticas en desarrollo como las que se describen a continuación:

- a) Metodología para realizar pruebas de certificación y seguridad al software desarrollado.
- b) El área de Tecnología será la única autorizada para realizar copias de seguridad de los códigos fuentes.
- c) Se deben tener ambientes de desarrollo, certificación y control de las versiones para la posterior actualización en producción.

Art. 53 Procedimientos de control de cambios en los sistemas. - Los cambios en los sistemas informáticos de la institución desarrolladas por el área de tecnología de información deben ser

ingresados bajo requerimientos formales, estos pueden ser correos electrónicos, actas de reuniones de levantamiento de requerimientos, y actas de certificación.

Art. 54 Seguridad en entornos de desarrollo.

1. El área de tecnología deberá crear ambientes de desarrollo, en la cual el personal de desarrollo será restringido el acceso a los sistemas de producción.
2. El administrador de la base de datos deberá generar roles de acceso a los desarrolladores.

Art. 55 Pruebas de aceptación.

1. El área de desarrollo de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., deberá poner en pruebas los desarrollos nuevos, y el área que lo pidió, deberá certificar con un documento formal, para el sustento de las partes se debe levantar un acta de certificación.
2. El área de seguridad de información verificará que el desarrollo realizado sea seguro y dará el visto bueno y puesta en producción.

SECCIÓN X: RELACIONES CON SUMINISTRADORES

A. SEGURIDAD DE INFORMACIÓN EN LAS RELACIONES DE SUMINISTRADORES

Art. 56 Políticas de seguridad de la información para suministradores. - La Cooperativa de Ahorro y Crédito Chibuleo Ltda., deberá establecer mecanismos de control en sus relaciones con externos (proveedores, convenios, y otros) con el objeto de asegurar la información que están compartiendo entre las partes.

Art. 57 Tratamiento del riesgo dentro de acuerdos de suministradores. - El área de tecnología, legal y seguridad de la información deberán establecer un modelo de acuerdos de confidencialidad y niveles de servicios entre las partes, dicho modelo de acuerdos debe ser difundido a todas las áreas que realizan adquisiciones o contratos.

SECCIÓN XI: GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

A. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS.

Art. 58 Notificación de puntos de la seguridad. - Todos los empleados de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., de manera obligatoria deberán reportar algún evento de seguridad de la información, que observe en su puesto de trabajo o áreas visitadas, y debe informar fallas en los sistemas informáticos.

Art. 59 Respuesta a incidentes de seguridad de la información. - EL jefe de seguridad de información deberá designar una persona que se encargue de investigar adecuadamente los incidentes de seguridad reportados por todo el personal de la institución, y su respectiva solución a los mismos.

SECCIÓN XII: ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

A. CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN.

Art. 60 Planificación de la continuidad de la seguridad de la información. - Desarrollar, documentar e implementar procesos de continuidad del negocio, para reducir los niveles de riesgo, así como la interrupciones de operaciones de los sistemas informáticos; sea por desastres naturales o fallos de seguridad, aplicando controles preventivos y correctivos de recuperación.

Art. 61 Implantación de la continuidad de la seguridad de la información. - La Cooperativa de Ahorro y Crédito Chibuleo Ltda., proporcionará los recursos suficientes para la implementación del plan de recuperación de desastres, para obtener una respuesta efectiva e inmediata del funcionamiento de la organización en caso de eventos catastróficos que se presenten en la institución.

Art. 62 Verificación, revisión y evaluación de la continuidad de la seguridad de información. - El comité de simulacros, junto con el área de seguridad de la información, deben

asegurarse de la ejecución de pruebas periódicas del plan de recuperación de desastres de la institución.

RESPONSABILIDADES

Art. 63 Del Consejo de Administración

Aprobar las políticas y procedimientos contenidos en el presente manual, en donde se establece claramente los lineamientos de servicios y atención basados en calidad y la satisfacción del cliente.

Art. 64 Del Gerente

Implementar en la Cooperativa, las políticas, principios y procesos básicos del área de seguridad de la información contenidos en la presente Norma.

CONTROL Y CUMPLIMIENTO

Art. 65 Del Auditor Interno

Verificar el cumplimiento del manual de políticas y procedimientos de seguridad de la información de la cooperativa, además, informará al Consejo de Vigilancia sobre las medidas correctivas señaladas en los casos de debilidades.

Art. 66 Cumplimiento

Corresponde a los involucrados del área de seguridad de la información el cumplimiento del presente manual de políticas y procedimientos descritos en la presente Norma.

El presente reglamento entrará en vigor una vez aprobado por el Consejo de Administración.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

A través del diagnóstico y de una revisión profunda de la norma internacional ISO/IEC 27002:2013 se diseñó una política de seguridad de la información para el área de TI de la Cooperativa de Ahorro y Crédito Chibuleo Ltda. En la propuesta se tomó en cuenta tres aspectos fundamentales: la confidencialidad, integridad y disponibilidad de los datos que posee la institución. En base estos elementos se realizó un análisis actual de las medidas de seguridad que el área de tecnología ha implementado, además de plasmar en una matriz los incidentes de seguridad.

En base a los incidentes de seguridad, se desarrolló una matriz de riesgo, basada en Deloitte (2015) y el Banco de España (2012), en la que se identificó las principales amenazas, eventos de riesgo y vulnerabilidades que tienen los activos de información dentro del área de Tecnología (Tabla 13).

Con la matriz de riesgo completa, se realizó una valoración de los activos de información, además de una reunión con el jefe de tecnología, el analista de riesgos y el oficial de seguridad de la información, quienes con criterios ponderaron los eventos y calificaron la vulnerabilidad y ocurrencia, los informantes identificaron los eventos críticos de seguridad de información que tiene el área de Tecnología.

Para mitigar los eventos críticos de seguridad de información del área de tecnología, es necesario realizar un análisis a la norma ISO/IEC 27002:2013, identificando los controles adecuados para reducir dichas incidencias relacionadas a la seguridad de la información.

En esta investigación el área de Tecnología de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., obtuvo una política de seguridad de información basado en los controles de la norma ISO 27002:2013, la cual contiene lineamientos y controles de seguridad de información que deben cumplir todas las áreas de la cooperativa.

6.2. RECOMENDACIONES

Se recomienda que la Política de Seguridad de Información que se realizó en la presente investigación, sea puesta a trámite ante el Comité de Administración Integral de Riesgos (CAIR) de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., para su posterior aprobación por parte del Consejo de Administración.

Realizar un seguimiento y actualización anual de la política de seguridad de información, con la finalidad de mantener la confidencialidad, integridad y disponibilidad de la información dentro de la organización.

Una vez aprobada la política se sugiere realizar la difusión dentro del área de Tecnología y de la Cooperativa, con el objetivo de mantener informada a la plantilla, y así puedan adoptar buenas prácticas de seguridad. De igual forma, es recomendable involucrar en esta política a proveedores, ya que también pueden tener acceso a información sensible.

Se recomienda al área de TI implementar todos los controles de la norma ISO/IEC 2700:2013 debido a que es la que mejor se adapta a las necesidades de la institución.

BIBLIOGRAFÍA

- Amutio, M., & González, J. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos*. Madrid: Ministerio de Hacienda y Administraciones Públicas. Recuperado de: <https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html>
- Banco de España (2012). *Guía para la elaboración de la matriz de riesgos*. Recuperado de: https://www.bde.es/f/webbde/INF/MenuVertical/Supervision/transparencia/ficheros/Guia_para_la_elaboracion_de_la_matriz_de_riesgos_ESP.PDF
- Barreto, J. H. (2014). *Caso de estudio DRP en la empresa JB Security* (Tesis de pregrado, Universidad Piloto de Colombia).
- Burgos, J.E. (2014). *Elaboración del plan de gestión de riesgos de las tecnologías de la información para Roche Ecuador s.a. en la ciudad de Quito, provincia de Pichincha, para el año 2014*. (Tesis de Maestría, UDLA).
- Castro, C. (2014). *Elaboración de un sistema de gestión de seguridad de la información SGSI para la empresa radical CIA. Ltda., en la ciudad de Quito para el Año 2014*. (Tesis de Maestría, UDLA).
- Cevallos, H. Y. (2019). *Diseño de una política de seguridad de la información para el área de TICS del Instituto Tecnológico Superior Central Técnico, basado en la norma de seguridad ISO/IEC 27002: 2013*. (Tesis de Maestría, UISEK).
- Contero, W. (2019). *Diseño de una política de seguridad de la información basada en la norma ISO 27002:2013, para el sistema de botones de seguridad del Ministerio del Interior*. (Tesis de Maestría, UISEK).
- Cooperativa de Ahorro y Crédito Chibuleo (sf.). *Historia*. Recuperado de: <http://www.chibuleo.com/index.php/historia/>

- Córdoba, A. (2015). Diseño e implementación de un GCSI para el área de informática de la curaduría urbana segunda de pasto bajo la norma ISO/IEC 27001. (Tesis de pregrado, Universidad Nacional Abierta y Distancia “UNAD”).
- Deloitte (2015). *COSO Evaluación de Riesgos. Enterprise Risk Services*. Recuperado de: <https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/Evaluacion-Riesgos-COSO.pdf>
- Deloitte Ecuador (2017). *Seguridad de la Información en Ecuador 2017*. Recuperado de: <https://www2.deloitte.com/content/dam/Deloitte/ec/Documents/deloitte-analytics/Estudios/SeguridadInformacion2017.pdf>
- Escudero, J. (sf.). *IEDGE - Políticas de Seguridad Informática*. Recuperado de: <https://www.iedge.eu/juan-manuel-escudero-politicas-de-seguridad-informatica>
- Gualpa, L. (2017). *Plan de seguridad informática basada en la norma ISO 27002 para el control de accesos indebidos a la red de Uniandes Puyo*. (Tesis de Maestría, Universidad Regional Autónoma de los Andes)
- International Communication Union (2019). *Global Cybersecurity Index (GCI) 2018*. Recuperado de: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
- ISO 27000 (sf.) *¿Qué es un SGSI*. Recuperado de: <http://www.iso27000.es/sgsi.html>
- ISO 27000 (sf.). *Sistema de Gestión de la Seguridad de la Información*. Recuperado de: http://www.iso27000.es/download/doc_sgsi_all.pdf
- ISO Controles (2013). *ControlesISO27002-2013*. Recuperado de: <http://iso27000.es/download/ControlesISO27002-2013.pdf>
- ISOTools (2018, marzo, 05) *Norma ISO/IEC 27000 Aspectos clave de su diseño e implantación, Calidad y Excelencia*. Recuperado de: <https://www.isotools.org/2018/03/05/la-norma-iso-iec-27000-va-a-ser-revisada/>

ISOTools (2019, junio, 06). *Análisis y evaluación de riesgos en ISO 27000*. Recuperado de: <https://www.pmg-ssi.com/2019/06/analisis-y-evaluacion-de-riesgos-en-iso-27001-amenazas-consecuencias-y-criticidad/>

Kowask, E., Alcántara, F., Motta, A., & Boca, J. (2014). *Gestión del riesgo de las TI NTC 27005*. Colombia: RENATA - Escuela Superior de Redes – ESR Colombia.

Mera, A. (2014). *Diseño del modelo de gestión de seguridad de la información del sistema ERP de EP Petroecuador de acuerdo a norma ISO/IEC 27002 y COBIT 5*. (Tesis de Maestría, Universidad de las Fuerzas Armadas ESPE. Sede Sangolquí).

Nieto, B. V. (2015). *Análisis y evaluación para el diseño de un plan de recuperación ante desastres (DRP) aplicado en un centro de datos para empresas municipales basado en la norma ISO/IEC 24762: 2008*. (Tesis de pregrado, Universidad Politécnica Salesiana-Guayaquil).

Ortega, I.P. (2014). *Los sistemas de información gerencial y el esquema de la base de datos en la asociación mutualista Ambato*. (Tesis de Maestría, Universidad Técnica de Ambato).

Paltán, A. (2017). *Evaluación de riesgos y desarrollo de un plan de recuperación ante desastres informáticos aplicado al Centro de Datos y Comunicaciones de la UPSE*. (Tesis de pregrado, Universidad Estatal Península de Santa Elena).

Pilamunga, K. & Maliza, I. (2018). *Metodología - Riesgo Operativo*. Ambato.

SEPS-IGT-IR-IGJ-2018-0279 (2018). Resolución Superintendencia de Economía Popular y Solidaria No. SEPS-IGT-IR-ICJ-2018-0279. Ecuador.

SGSI (2017, enero, 05). *ISO 27005: ¿Cómo identificar los riesgos?* Blog de ISOTools Excellence. Recuperado de: <https://www.pmg-ssi.com/2017/01/iso-27005-como-identificar-los-riesgos/>

SGSI (2017, agosto, 17). *¿Cómo se encuentra ligada la Seguridad de Información con Recursos Humanos?*. Blog de ISOTools Excellence. Recuperado de: <https://www.pmg-ssi.com/2017/08/seguridad-de-la-informacion-recursos-humanos/>

Toaquiza, E. (2012). *Análisis a los riesgos crediticios en la Cooperativa de Ahorro y Crédito Chibuleo Ltda. agencia Latacunga, ubicada en la parroquia la matriz cantón Latacunga al periodo del 01 de enero al 30 de diciembre del 2012.* (Tesis de pregrado, Universidad Técnica de Cotopaxi).

Torres, E. (2012). *Políticas de Seguridad de la Información basado en la Norma ISO/IEC 27002:2013 para la dirección de tecnología de información y comunicación de la Universidad Técnica de Ambato.* (Tesis de pregrado, Universidad Técnica de Ambato).

UNE-EN ISO/IEC 27001:2017 (2017). *Tecnología de la información, Técnicas de seguridad Sistemas de Gestión de la Seguridad de la Información, Requisitos (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015).* AENOR.

Vásquez, W. (2017). *Propuesta de un método para elaborar un plan de recuperación de desastres (DRP) en el Área de tecnología de la información para Cooperativas de Ahorro y Crédito del Ecuador.* (Tesis de Maestría, Universidad Politécnica del Chimborazo, ESPOCH).

ANEXOS

ANEXO 1: ACUERDO DE CONFIDENCIALIDAD

ACUERDO DE CONFIDENCIALIDAD

COMPARECIENTES: Comparecen a la celebración del presente acuerdo de confidencialidad, la Cooperativa Ahorro y Crédito CHIBULEO Ltda., representada por RODRIGO LLAMBO, en calidad de "empleador", a quien en adelante y para efectos del acuerdo se le denominará LA COOPERATIVA; y, por otra parte el/la señor(a), el Sr. MARCO VINICIO CAIZA TELENCHANA, portador de la cédula de ciudadanía N° 1803978368 a quien en adelante y para efectos del acuerdo se le denominará "trabajador", conforme los documentos habilitantes que se agregan.

Los comparecientes son ecuatorianos, domiciliados en la ciudad de AMBATO, Provincia de TUNGURAHUA, legalmente capaces y hábiles para contratar y obligarse.

En virtud de lo expuesto, los comparecientes en forma libre y voluntaria, por los derechos que representan, acuerdan en suscribir el presente ACUERDO DE CONFIDENCIALIDAD, contenido en las siguientes cláusulas:

PRIMERA. - ANTECEDENTES:

Como antecedentes de este acuerdo citamos lo siguiente:

- a) La Cooperativa de Ahorro y Crédito CHIBULEO Ltda., es una Institución Financiera legalmente constituida en el Ecuador, según consta del Acuerdo Ministerial, y regulada por la Superintendencia de Economía Popular y Solidaria, RUC Número 1891710328001, con su matriz en la ciudad de Ambato, con domicilio en la provincia de Tungurahua, cantón Ambato, parroquia Matriz, calle Espejo número 12-78 y Av. 12 de noviembre, teléfono 032422526, 033700190.
- b) El/la trabajadora(a), fue legalmente contratado por la Cooperativa de Ahorro y Crédito Chibuleo Ltda.
- c) Que, el artículo 445 del Código Orgánico Monetario y Financiero, establece 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 la Economía Popular y Solidaria, con el objeto de realizar actividades de intermediación financiera.
- d) Que, el artículo 272 del Código Orgánico Monetario y Financiero. - Sanción por divulgación de información. Las personas naturales o jurídicas que divulguen, en todo o en parte, información sometida a sigilo o reserva, serán sancionadas con una multa de veinte y cinco salarios básicos unificados sin perjuicio de la responsabilidad penal que corresponda.
- e) Que el artículo 352 del Código Orgánico Monetario y Financiero. - Protección de la información. Los datos de carácter personal de los usuarios del sistema financiero nacional que reposan en las entidades de dicho sistema y su acceso están protegidos. Y solo podrán ser entregados a su titular o a quien éste autorice o por disposición de este Código.
- f) Que, el artículo 353 del Código Orgánico Monetario y Financiero. - Sigilo y reserva. Los depósitos y demás captaciones de cualquier naturaleza que reciban las entidades del sistema financiero nacional están sujetos a sigilo, por lo cual no se podrá proporcionar información alguna relativa a dichas operaciones, sino a su titular o a quien haya sido expresamente autorizado por él o a quien lo represente legalmente.
- g) Que, artículo 354 del Código Orgánico Monetario y Financiero. - Excepciones. No se aplican las disposiciones del artículo precedente para la entrega de la siguiente información que se solicite a los organismos de control o a las entidades del Sistema Financiero Nacional:

1. Los antecedentes relativos a operaciones efectuadas por quienes sean parte o sean investigados en causas que se encuentren bajo el conocimiento de un juez o de la Fiscalía General del Estado;

2. Los datos del titular de cuentas corrientes cerradas por giro de cheques sin provisión de fondos, requeridos por el tenedor legítimo de los cheques;

3. Cualquier información requerida por los organismos de control y el Servicio de Rentas Internas, en el ámbito de su competencia;

4. La información que requiera la Junta de Política y Regulación Monetaria y Financiera, la cual deberá ser canalizada a través del organismo de control;

5. La información que deben entregar los organismos de control para dar a conocer al público la situación patrimonial y financiera de las entidades financieras;

6. Los informes requeridos a los organismos de control, en el ámbito de su competencia, por gobiernos o por autoridades competentes de los países con los que el Ecuador mantenga convenios recíprocos y legítimamente celebrados para combatir la delincuencia, en los términos de dichos convenios;

7. Las informaciones financieras que constituyan intercambio con autoridades de control bancario, financiero y tributario de otros países, siempre que existan convenios recíprocos, vigentes y legítimamente celebrados; y,

8. Los demás que establezca la ley.

h) Que, artículo 179 del Código Orgánico Integral Penal. - Revelación de secreto. La persona que teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año.

i) Que, artículo 322 del Código Orgánico Integral Penal. - Pánico Financiero. La persona que divulgue noticias falsas que causen alarma en la población y provoquen el retiro masivo de los depósitos de cualquier institución del sistema financiero y las de la economía popular y solidaria que realicen intermediación financiera, que pongan en peligro la estabilidad o provoquen el cierre definitivo de la institución, será sancionado con pena preventiva de libertad de cinco a siete años de prisión.

SEGUNDA. - DEFINICIONES:

Información Confidencial. - Por efectos de este acuerdo se entiende por información confidencial, todos los hechos o antecedentes que no han sido divulgados al público de manera oficial por parte la Cooperativa de Ahorro y Crédito Chibuleo Ltda.

a. Información relacionada con productos software o hardware en general de propiedad de la Cooperativa de Ahorro y Crédito Chibuleo Ltda.

b. Información de las bases de datos de la Cooperativa de Ahorro y Crédito Chibuleo Ltda.

c. Planes de trabajo, planes estratégicos, planes operativos, planes y estrategias de negocio, procesos; y, normativa interna, considerada como confidencial según lo determinado por el Comité de Seguridad de la Información.

TERCERA. - OBJETO:

El presente Acuerdo tiene como objeto establecer la obligación de las partes de mantener en forma reservada y confidencial toda la información considerada como confidencial la que haya y tenga acceso EL/LA TRABAJADOR (A), dentro de sus actividades en la Cooperativa.

CUARTA. - CONFIDENCIALIDAD:

Por la naturaleza de la información y riesgos por la mala utilización y/o divulgación de la misma implican para la COOPERATIVA DE AHORRO Y CRÉDITO CHIBULEO LTDA., EL/LA TRABAJADOR(A) se obliga a mantener en forma estrictamente reservada y confidencial toda la información considerada como confidencial a la que tenga acceso en función de sus actividades; por tal motivo EL/LA TRABAJADOR(A) se obliga a abstenerse divulgar y/o publicar por cualquier medio, oral o escrito y en general, aprovecharse de ella de cualquier otra forma que atente a los intereses de la Cooperativa de Ahorro y Crédito Chibuleo Ltda. Por lo tanto, no podrá ser divulgada información a terceros sin previo consentimiento por escrito de la entidad propietaria de dicha información que es la Cooperativa de Ahorro y Crédito Chibuleo, excepto a aquellas que sean consideradas como información pública.

QUINTA. - PROPIEDAD INTELECTUAL:

La Cooperativa de Ahorro y Crédito Chibuleo Ltda., adicional a las marcas, logotipos, tipos de productos, es propietaria de todos los derechos detallados en el presente acuerdo de confidencialidad que no sean de carácter público, por lo que se prohíbe su reproducción, siendo manejados como confidencial a menos que la Cooperativa expresamente manifieste lo contrario.

SEXTA. - RESPONSABILIDADES:

Es responsabilidad de las partes mantener un adecuado nivel de comunicación y cumplir con los términos respecto de reserva y sigilo de información y en estricto cumplimiento al presente acuerdo. En el caso de que EL/LA TRABAJADOR(A) entregue a terceros la información materia de este acuerdo, será directamente responsable frente a la Cooperativa de Ahorro y Crédito Chibuleo por el mal uso y/o divulgación de la información proporcionada o a la cual tenga acceso. En el caso de que un EL/LA TRABAJADOR(A) entregue información confidencial de su responsabilidad a otro TRABAJADOR(A) de la institución mantendrá su responsabilidad del buen y mal uso de la información confidencial.

SÉPTIMA. - SANCIONES:

Toda infracción, violación o inobservancia de las estipulaciones y obligaciones contenidas en el presente Acuerdo de confidencialidad de información debidamente comprobado, dará lugar a que la cooperativa inicie acciones de carácter legal y que EL/LA TRABAJADOR(A) asuma las responsabilidades pertinentes.

OCTAVA. - VIGENCIA:

Las obligaciones asumidas en el presente documento se mantendrán en vigencia durante toda la relación laboral y durante dos años posterior a su desvinculación.

NOVENA. - CONTROVERSIAS:

En caso de surgir entre las partes cualquier controversia en relación con este contrato, inclusive las relacionadas con su interpretación, cumplimiento, validez o terminación, así como cualquier controversia que se produzca respecto a cualquier obligación, será resuelta directa y amistosamente entre las partes. En caso de no poder solucionar el diferendo por esta vía, las partes renuncian fuero y domicilio y concurrirán ante un mediador del Centro de Arbitraje y Mediación de la Cámara de Comercio de la ciudad de Ambato. En el evento que el referido procedimiento concluya por imposibilidad de lograrlo, las partes se someten a la resolución de un Tribunal de Arbitraje que se sujetará a lo dispuesto en la Ley de Arbitraje y Mediación, en el Reglamento del Centro de Arbitraje y Mediación de la Cámara de Comercio de Ambato, el Arbitraje será en derecho.

DÉCIMA. - ACEPTACION:

Para constancia de lo estipulado, las partes se afirman y ratifican en el contenido íntegro del presente instrumento en virtud de lo cual suscriben en unidad de acto en la ciudad de Ambato a los 1 de Junio del 2019.



Ing. RODRIGO LLAMBO

GERENTE


Sr. MARCO VINICIO CAIZA
TELENCHANA

TRABAJADOR

ANEXO 2: CHECK LIST DE VINCULACIÓN

		Código: GTH-REG-013	
		Fecha de implementación: 07-May-2014	
		Última aprobación: 07-May-2014	
		Revisión: 00	
CHECK LIST PARA VINCULACIÓN DE PERSONAL			
Elaborado por: Karina Ortiz		Revisado por: Merli Salazar	
Aprobado por: Rodrigo Uamba			
PERSONAL <input checked="" type="radio"/> Fijo <input type="radio"/> Eventual <input type="radio"/> Pasante			
DATOS INFORMATIVOS:			
Nombres Completos: TICHE ANDAGANA ABEL ISAIAS		Teléfono: 099578835	
Dirección: CHIBULEO SAN FRANCISCO BARRIO TOTORA		No. C.I.: 1805002944	
Carga: ASESOR DE CRÉDITO		Fecha Nacimiento: 14/08/1990	
Jefe inmediato superior: BLANCA CHACA		Departamento: Créditos	
Fecha de ingreso como usuario: MARZO 01, 2019		Estado Civil: Soltero	
ACTIVIDADES QUE DEBEN EJECUTARSE POR ÁREA:			
SISTEMAS / SEGURIDAD			
1	Asignación del usuario en el Sistema Financiero/ Custodio de Bóveda	FECHA DE SOLICITUD	RESPONSABLE
			Danián Ufag
2	Creación de dirección de correo interno		Danián Ufag
3	Acceso a navegación en Internet (restricciones)		N/A
4	Configuración de usuario en Active Directory		Danián Ufag
5	Spark		Danián Ufag
6	Asignación de extensión y teléfono		Danián Ufag
7	Credireport (Crédito)		N/A
8	Mesa de Ayuda		Danián Ufag
JEFES DE ÁREA, JEFE DE AREA O AGENCIA			
		FECHA DE SOLICITUD	RESPONSABLE
1	Equipo de computo		AIDA BARRONUEVO
2	Impresora		AIDA BARRONUEVO
3	Solicitud de todos los recursos para desempeño del cargo / Activos fijos (realización de acta entrega - recepción, entregar a GTH).		AIDA BARRONUEVO
4	Autorización para llamadas a celular		AIDA BARRONUEVO
5	Entrenamiento al Puesto		AIDA BARRONUEVO
6	Usuario y Clave Red Fajito		N/A
7	Clave Money Gram (Atención al Cliente)		N/A
8	Otros:		
GESTIÓN DEL TALENTO HUMANO			
		FECHA DE SOLICITUD	RESPONSABLE
1	Requisición de personal		Talento Humano
2	Llenar oferta de trabajo		Talento Humano
3	Realizar inducción general		Talento Humano
4	Comunicar del ingreso, a todo el personal, vía email.		Talento Humano
5	Recepción de documentos para carpeta personal		Talento Humano
6	Ingreso al IESS		Talento Humano
7	Elaboración y legalización del contrato en el MRL		Talento Humano
8	Entrega de tarjeta de identificación		Talento Humano
9	Registro en el reloj para control de ingresos		Talento Humano
10	Apertura de Cuenta de ahorros		Talento Humano
11	Entrega de uniforme		Talento Humano
12	Seguimiento del Entrenamiento al Puesto		Talento Humano
13	Evaluación Período de Prueba (70 días)		Talento Humano
14	Evaluación antes de que cumpla el año		Talento Humano
15	Consulta del Buró de Crédito		Talento Humano

Elaborado por:
GESTIÓN DEL TALENTO HUMANO

Revisado por:
TICHE ANDAGANA ABEL ISAIAS

ANEXO 3: CONTROLES ISO/IEC 27002:2013

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.

- 5.1 Directrices de la Dirección en seguridad de la información.
 - 5.1.1 Conjunto de políticas para la seguridad de la información.
 - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.

- 6.1 Organización interna.
 - 6.1.1 Asignación de responsabilidades para la segur. de la información.
 - 6.1.2 Segregación de tareas.
 - 6.1.3 Contacto con las autoridades.
 - 6.1.4 Contacto con grupos de interés especial.
 - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
 - 6.2.1 Política de uso de dispositivos para movilidad.
 - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

- 7.1 Antes de la contratación.
 - 7.1.1 Investigación de antecedentes.
 - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
 - 7.2.1 Responsabilidades de gestión.
 - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
 - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
 - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.

- 8.1 Responsabilidad sobre los activos.
 - 8.1.1 Inventario de activos.
 - 8.1.2 Propiedad de los activos.
 - 8.1.3 Uso aceptable de los activos.
 - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
 - 8.2.1 Directrices de clasificación.
 - 8.2.2 Etiquetado y manipulado de la información.
 - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
 - 8.3.1 Gestión de soportes extraíbles.
 - 8.3.2 Eliminación de soportes.
 - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.

- 9.1 Requisitos de negocio para el control de accesos.
 - 9.1.1 Política de control de accesos.
 - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
 - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
 - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
 - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
 - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
 - 9.2.5 Revisión de los derechos de acceso de los usuarios.
 - 9.2.6 Retirada o adaptación de los derechos de acceso.
- 9.3 Responsabilidades del usuario.
 - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
 - 9.4.1 Restricción del acceso a la información.
 - 9.4.2 Procedimientos seguros de inicio de sesión.
 - 9.4.3 Gestión de contraseñas de usuario.
 - 9.4.4 Uso de herramientas de administración de sistemas.
 - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.

- 10.1 Controles criptográficos.
 - 10.1.1 Política de uso de los controles criptográficos.
 - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.

- 11.1 Áreas seguras.
 - 11.1.1 Perímetro de seguridad física.
 - 11.1.2 Controles físicos de entrada.
 - 11.1.3 Seguridad de oficinas, despachos y recursos.
 - 11.1.4 Protección contra las amenazas externas y ambientales.
 - 11.1.5 El trabajo en áreas seguras.
 - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
 - 11.2.1 Emplazamiento y protección de equipos.
 - 11.2.2 Instalaciones de suministro.
 - 11.2.3 Seguridad del cableado.
 - 11.2.4 Mantenimiento de los equipos.
 - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
 - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
 - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
 - 11.2.8 Equipo informático de usuario desatendido.
 - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.

- 12.1 Responsabilidades y procedimientos de operación.
 - 12.1.1 Documentación de procedimientos de operación.
 - 12.1.2 Gestión de cambios.
 - 12.1.3 Gestión de capacidades.
 - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
 - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
 - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
 - 12.4.1 Registro y gestión de eventos de actividad.
 - 12.4.2 Protección de los registros de información.
 - 12.4.3 Registros de actividad del administrador y operador del sistema.
 - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
 - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
 - 12.6.1 Gestión de las vulnerabilidades técnicas.
 - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
 - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.

- 13.1 Gestión de la seguridad en las redes.
 - 13.1.1 Controles de red.
 - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
 - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
 - 13.2.1 Políticas y procedimientos de intercambio de información.
 - 13.2.2 Acuerdos de intercambio.
 - 13.2.3 Mensajería electrónica.
 - 13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:



14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

- 14.1 Requisitos de seguridad de los sistemas de información.
 - 14.1.1 Análisis y especificación de los requisitos de seguridad.
 - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
 - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
 - 14.2.1 Política de desarrollo seguro de software.
 - 14.2.2 Procedimientos de control de cambios en los sistemas.
 - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
 - 14.2.4 Restricciones a los cambios en los paquetes de software.
 - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
 - 14.2.6 Seguridad en entornos de desarrollo.
 - 14.2.7 Externalización del desarrollo de software.
 - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
 - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
 - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.

- 15.1 Seguridad de la información en las relaciones con suministradores.
 - 15.1.1 Política de seguridad de la información para suministradores.
 - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
 - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
 - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
 - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
 - 16.1.1 Responsabilidades y procedimientos.
 - 16.1.2 Notificación de los eventos de seguridad de la información.
 - 16.1.3 Notificación de puntos débiles de la seguridad.
 - 16.1.4 Valgración de eventos de seguridad de la información y toma de decisiones.
- 16.1.5 Respuesta a los incidentes de seguridad.
- 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
- 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

- 17.1 Continuidad de la seguridad de la información.
 - 17.1.1 Planificación de la continuidad de la seguridad de la información.
 - 17.1.2 Implantación de la continuidad de la seguridad de la información.
 - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
 - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.

- 18.1 Cumplimiento de los requisitos legales y contractuales.
 - 18.1.1 Identificación de la legislación aplicable.
 - 18.1.2 Derechos de propiedad intelectual (DPI).
 - 18.1.3 Protección de los registros de la organización.
 - 18.1.4 Protección de datos y privacidad de la información personal.
 - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
 - 18.2.1 Revisión independiente de la seguridad de la información.
 - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
 - 18.2.3 Comprobación del cumplimiento.

ANEXO 4. MEMORANDO DE ACEPTACIÓN DEL COMITÉ INTEGRAL DE RIESGOS DE LA COOPERATIVA

yo CEO en ti... 

MEMORANDO N° CCBL- CAIR-007-2019

DE: Oswaldo de la Cruz
PRESIDENTE DE CAIR

PARA: Señores:
CONSEJO DE ADMINISTRACION
Rodrigo Llamba
GERENTE

CCO: Juan José Tiche
Jefe de Crédito
Byron Albán
Auditor Interno
Trinidad Baltazar
Responsable de Calidad y Procesos
Cesar Pilla
Oficial de Seguridad de la Información

ASUNTO: Resolución - Reunión ordinaria del CAIR No. 07.

FECHA: 16 de julio del 2019

Por medio de la presente me permito informar que en Reunión Ordinaria del Comité de Administración Integral de Riesgos (CAIR) realizada con fecha martes 16 de julio 2019 se tomaron las siguientes resoluciones:

No.	Resolución	Responsable de Ejecución
01	Conocer y aprobar el informe de la Unidad de Riesgos con Corte al 30 de junio 2019.	CAIR
02	Presentar al Consejo de Administración el Informe del Comité de Administración Integral de Riesgos con corte al 30 de junio 2019.	CAIR
03	Conocer y aprobar el informe de cobranzas presentado por el Coordinador de Cobranzas con datos cortados al 30 de junio de 2019.	CAIR
04	Conocer y aprobar el informe de calificación de Activos de Riesgo presentado por a la Unidad de Riesgos mediante MEMORANDO N.º CCBL-UR-021-2019 emitido con fecha 12 de julio 2019.	CAIR
05	Proponer y recomendar al Consejo de Administración la aprobación del Informe de Calificación de Activos de Riesgo presentado por a la Unidad de Riesgos mediante MEMORANDO N.º CCBL-UR-021-2019 emitido con fecha 12 de julio 2019.	Consejo de Administración
06	Proponer y recomendar al Consejo de Administración la aprobación del Reglamento de Seguridad de la Información presentado por el Ing. Cesar Pilla Oficial de Seguridad de la Información, mediante	Consejo de Administración

www.chibuleo.com

	Memorando No. 005-CCBL-CGO-2019, del 16 de julio de 2019.	
07	Solicitar a Talento Humano, se incluya en el Reglamento Interno de Trabajo lo establecido en la cláusula 7 sobre seguridad ligada a los recursos humanos señalados en el Reglamento de Seguridad de la Información.	Talento-Humano

Particular que pongo en conocimiento, me suscribo:

Atentamente,










Oswaldo de la Cruz
PRESIDENTE DEL CAIR

ANEXO 5. REGISTRO DE ASISTENCIA AL COMITÉ CAIR.

REGISTRO DE ASISTENCIA

REUNIÓN - ORDINARIA DEL COMITE CAIR

Fecha: 16/07/2019

NOMBRE	CEDULA	CARGO	PARA CONSTANCIA FIRMAN	HORA
Kleber Plannoy	1804507037	R. Riesgo		15:00
Sara Mendi	1804507038	As. Riesgo		15:00
Ezequiel Nuyra	1500976116	Asistente de Administración		15:00
Verónica Amador	0104332315	Asistente de Cuentas		15:00
Carlos Baltazar	1802175287	Pres. de Credito		15:00
Caro Pilo	1304022080	CISO		15:00
Verónica Amador	1107460499	Tesoro		15:00

FIRMA: Responsable

ANEXO 6. ACTA DE REUNIÓN LEVANTAMIENTO DE ACTIVOS DE INFORMACIÓN

ACTA DE LEVANTAMIENTO DE RECURSOS Y SERVICIOS

Proyecto	Investigación
Responsable del proyecto	César Pilla
Responsable del área	Darwin Uñog
Fecha	08/04/2019
Macroproceso	Gestión de Tecnología de la Información
Proceso	Tecnología de la Información
Código	GT-TIN-MCP

Alcance	Obtener todos los recursos que ofrece el departamento de TI a las áreas y departamentos de la COOPERATIVA DE AHORRO Y CRÉDITO CHIBULEO LTDA.
Objetivo Principal	Determinar los recursos que ofrece el subproceso "Mantenimiento correctivo y perfectivo de software".
Objetivos específicos	<ul style="list-style-type: none"> • Obtener los recursos por departamentos o áreas. • Definir las prioridades de recursos por departamentos y áreas.

Proceso

CODIGO PROCESO	CODIGO ACTIVO	ACTIVO
GT-TIN-ABD	GT-TIN-ABD-01	Reportes
	GT-TIN-ABD-02	Generación de datos para estructuras
	GT-TIN-ABD-03	Almacenamiento y entrega de información a los sistemas existentes
	GT-TIN-ABD-04	Respaldos de información
	GT-TIN-ABD-05	Restauración de información
	GT-TIN-ABD-06	Mantenimiento a las BDD existentes.
	GT-TIN-ABD-07	Seguridad en las BDD
	GT-TIN-ABD-08	Ambiente de pruebas
	GT-TIN-ABD-09	Otros (link Servar, Exportación, importación)
GT-TIN-ADN	GT-TIN-ADN-01	Acceso a la Red
	GT-TIN-ADN-02	Autenticación a la red, mediante AD
	GT-TIN-ADN-03	Asignación de equipamiento
	GT-TIN-ADN-04	Telefonia IP
	GT-TIN-ADN-05	Correo Electrónicos
	GT-TIN-ADN-06	Mensajería Instantánea
	GT-TIN-ADN-07	Accesos a internet
	GT-TIN-ADN-08	Accesos a servicios externos.

	GT-TIN-ADN-09	Segmentación de la red (VLAN's,DMZ, Firewall)
	GT-TIN-ADN-10	implementación de servidores
	GT-TIN-ADN-11	Administración de espacio físico en el Data Center
	GT-TIN-ADN-12	Instalación SO
	GT-TIN-ADN-13	Hardening
	GT-TIN-ADN-14	Administración Centro de Datos
GT-TIN-CS	GT-TIN-CS-01	Elaborar el presupuesto anual de sistemas
	GT-TIN-CS-02	Análisis de proveedores
	GT-TIN-CS-03	Administración de adquisición y contratos externos
	GT-TIN-CS-04	Análisis de Cotización
	GT-TIN-CS-05	Control de Presupuesto asignado a TI
GT-TIN-GTE	GT-TIN-GTE-01	Interconexión de oficinas con Matriz
	GT-TIN-GTE-02	Calidad de servicios de las conexiones
	GT-TIN-GTE-03	Transparencia en la interconexión
	GT-TIN-GTE-04	Monitoreo de la red
	GT-TIN-GTE-05	Actualización firmwares
	GT-TIN-GTE-06	Alta disponibilidad
	GT-TIN-GTE-07	Mantenimiento preventivo y correctivo
GT-TIN-MCP	GT-TIN-MCP-01	Adecuación de módulos
	GT-TIN-MCP-02	Implementación de módulos
	GT-TIN-MCP-03	Corrección de módulos
	GT-TIN-MCP-04	Versionamiento de sistemas existentes
	GT-TIN-MCP-05	Parametrización de sistemas existentes
	GT-TIN-MCP-06	Procesos Batch
	GT-TIN-MCP-07	Ambiente de pruebas (publicación, pruebas, certificación, capacitación)
	GT-TIN-MCP-08	Publicaciones de software existen.
	GT-TIN-MCP-09	Respaldos de los sistemas existentes de software.
	GT-TIN-MCP-10	Sistema Financial 2.0
GT-TIN-SIN	GT-TIN-SIN-01	Cambio de Claves de usuarios directorio activo
	GT-TIN-SIN-02	Control de acceso al Data Center, Sistemas y Sala de control de las oficinas
	GT-TIN-SIN-03	Cambio de claves de accesos a Wifi

	GT-TIN-SDN-04	Administración de respaldos de información de todos los sistemas informáticos
	GT-TIN-SDN-05	Mantener la información confiable, Integra, Disponible
GT-TIN-STE	GT-TIN-STE-01	Soporte técnico Help Desk
	GT-TIN-STE-02	Mantenimiento correctivo de equipamiento de infraestructura
	GT-TIN-STE-03	Soporte segundo nivel (Personalizado con usuarios)
	GT-TIN-STE-04	Soporte Tercer nivel (externos, coordinación)

Firman para constancia

Aprobado por: César Pilla
Cargo: Investigado

Aprobado por: Darwin Uñog
Cargo: jefe de Tecnología

Aprobado por: Vicente Vásquez
Cargo: Técnico de infraestructura

Aprobado por: Javier Jerez
Cargo: Coordinador de desarrollo

ANEXO 7: CONCEPTOS BÁSICOS DE SEGURIDAD DE LA INFORMACIÓN DENTRO DEL ÁREA DE TECNOLOGÍA

Efectividad. - La información debe ser real, y necesaria para el desarrollo de las actividades dentro de la institución, siendo oportuna, real, sólida y viable.

Integridad. – esta información debe estar indemne, exacta y completa.

Disponibilidad. – Es un principio para que la información esté disponible cuando se lo necesite, para actividades importantes o para cuando los entes control lo soliciten.

Activo de Información. - El activo de información de una empresa se los puede catalogar de la siguiente manera débito al nivel de información que mantenemos dentro de la institución, la cuales se describe a continuación:

Información – Electrónico / Digital. – Para el almacenamiento de información como base de dato, hojas de caculos, documentos procesadores de texto entre otros.

Información Físico. – Reportes, contratos, propuestas, títulos de valores.

Hardware. – Elementos físicos que soportan los procesos, equipos de comunicación, servidores, medios de almacenamiento.

Software. – Contribuye al procesamiento de datos, Aplicaciones, sistemas operativos, Software de servicios / mantenimiento y administración.

Personas. – Participantes de las operaciones de la empresa, responsable de activos, administrador, operador, usuarios.

Sitio. – Lugares que son parte del alcance/ Operación de la empresa. Edificio, oficinas, bodega, data center, bóvedas.

Entidades externas. – Proveedores, subcontratistas y fabricantes.

Servicios Esenciales. – Son los que apoyan la operación de la infraestructura y operación de la empresa. Energía, climatización, combustible, agua.