ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA DE AHORRO Y CRÉDITO KULLKI WASI.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

EDISON GERARDO GRANADA GUALOTUÑA
ferdu_pm001@hotmail.com

DIRECTOR: Ing. William Humberto Andrade Hinojosa, MSc.
william.andrade@epn.edu.ec

Quito, noviembre de 2018

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Edison Gerardo Granada Gualotuña, bajo mi supervisión.

MSc. William Humberto Andrade Hinojosa

DIRECTOR DE PROYECTO

DECLARACIÓN

Yo, Edison Gerardo Granada Gualotuña, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he 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 Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Edison Gerardo Granada Gualotuña

DEDICATORIA

A mi madre Rosita

A ti madrecita que siempre estuviste empujándome cuando quería botar la toalla, eres la única que creyó en mi incondicionalmente, a pesar de mis errores, mis malos momentos, las angustias y las malas decisiones siempre estás aquí para darme ánimos y apoyarme incondicionalmente. Por ti mi Rosita linda llegue hasta aquí y sé que me vas a seguir apoyando para más, porque sabes que puedo seguir haciendo más cosas grandes, no lo olvides esta meta cumplida es más tuya que mía, eres la súper mamá.

A ti padre Rodolfo

A pesar de las cosas que han pasado en nuestra vida no te juzgo padre ya que si no me hubieras enseñado desde pequeño ese bello oficio muchas de las cosas que tengo no existieran solo puedo decir pai.

A ti hermano Bladimir y cuñado Marco

Donde quieran que estén esta meta es para ustedes siempre tengo presente sus últimas palabras.

AGRADECIMIENTO

A ustedes padres por apoyarme en este largo camino, muchas de las cosas que pase en la universidad es gracias a su apoyo, que ayudaron a levantarme cada vez que caía y no quería pararme, sin ustedes esto no hubiese sido posible.

A todos los ingenieros que tuve a lo largo de la carrera, dejaron en mi un granito de arena tanto en lo profesional y como saber ser persona ante todas las cosas. Gracias Ing. Wiliam por haberme ayudado a dar este paso final en la carrera.

A ti Ennovi, como tú dices las personas se cruzan por algo en nuestras vidas y doy las gracias por ello, ya que en algunas veces me sentí derrotado y tú estabas ahí para darme palabras de aliento. Te agradezco por llegar a mi vida y darme este último empujo en esto, también por guiarme en esta etapa de verdad q naciste para ser profe.

A todos mis amig@s que fueron parte de esta etapa académica, gracias por permitirme vivir cosas buenas y cosas malas que son de las que uno aprende más. A todos los que fueron parte de ese gran equipo llamado QUITAPENAS, el futbol fue parte fundamental en mi vida estudiantil agradezco por permitirme jugar a su lado.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Actualmente, la Cooperativa de Ahorro y Crédito Kullki Wasi no cuenta con un plan de Gestión de la Seguridad de la Información, lo que ha provocado que no se lleve un manejo formal y seguro de la información sensible a la entidad. Por ello se plantea el presente proyecto de titulación, que consta de cuatro partes, las cuales se describen a continuación:

Parte Introducción: consta de seis secciones. En la primera sección se realiza el planteamiento del problema en cuanto a la gestión de la seguridad de la información, la segunda sección establece los objetivos del proyecto de titulación mismos que pretenden ayudar a la entidad en la mejora la Gestión de la Seguridad de la Información, la tercera sección define el alcance que tendrá el proyecto de titulación, en la cuarta sección se realiza el reconocimiento de la entidad partiendo del plan estratégico de la misma y con mayor detalle sobre el Departamento de Tecnología, la quinta sección está dedicada a la selección y justificación de la norma y estándar con los que se llevará a cabo el presente proyecto de titulación. Por último, la sexta sección en la que se realiza el diagnóstico de la situación actual de la entidad (apoyado en las herramientas MSAT y check list) en base a la norma NTE INEN-ISO/IEC 27001.

Parte Aplicación de la Metodología: esta parte está dividida en tres secciones dedicadas a la evaluación de los riesgos de la seguridad de la información. La primera sección trata sobre el plan de acción que se llevara para el análisis de riesgos, la segunda sección describe cada uno de los pasos a seguir según la NIST 800-30 y en la tercera sección se encuentra la ejecución del análisis de riesgos, donde con la ayuda de herramientas como Nessus, Nmap y el mismo check list se identifican las posibles amenazas y vulnerabilidades a los que están expuestos los activos críticos, obteniendo como resultado la matriz de riegos y con esto definir el plan de tratamiento y seleccionar los controles que propone la norma NTE INEN-ISO/27001 y tomando en cuenta los criterios de seguridad de la NIST 800-30 para finalmente mostrar los resultados obtenidos en el informe de valoración de riesgo.

Parte Resultados y Discusión: contiene las directrices que se deben llevar acabo para la implantación de los controles seleccionados y consta de cinco secciones. La primera sección muestra en que consiste un Sistema de Gestión de Seguridad

de la Información de acuerdo a la norma NTE INEN-ISO/27001, la segunda sección define el alcance y límites del plan del presente proyecto de titulación, en la tercera sección se muestran las fases que se deben cumplir para la elaboración del plan de Gestión de Seguridad de la Información con los entregables generados a lo largo de la elaboración de dicho plan y de acuerdo a lo que plantea la norma, en la cuarta sección se plantea una guía de implementación a llevarse a cabo si las autoridades de la entidad aceptan la ejecución del presente plan y finalmente en la sección cinco se realiza la aplicabilidad de la propuesta comparando el estado del cumplimiento actual con el estado del cumplimiento esperado.

Parte Conclusiones y Recomendaciones: contiene las conclusiones y recomendaciones obtenidas por el autor del proyecto, las cuales destacan los puntos más importantes que deben tomar en cuenta tanto a la entidad como los usuarios.

ABSTRACT

Nowadays, Cooperativa de Ahorro y Crédito Kullki Wasi doesn't have an Information Security Management plan, which has promoted an informal and not save management of the important information of the company. Hence, this project is posed, that consist in four parts which are described below:

Introduction part: consists in six sections. The first one sets the problem regarding the information security management, the second section sets the objective of the project which pretend to help the company to improve the information security management, the third section defines the scope of the project, in the fourth section a inspection of the company is made starting with its strategic plan and with more detail about the Technology Department, the fifth section is dedicated to the selections and justifying the policy and standard with which this project will be carry out. Finally, the sixth section makes a diagnosis on the current situation (supported by MSAT and check list tools) based on the NTE INEN-ISO/IEC 27001 standard.

Methodology application part: this part is divided into three sections dedicated to the evaluation of the security information risks. The first section is about the action plan to analyze risks, the second section describes each step followed according to NIST 800-30 and the third section presents the performance of the risk analysis, in which the possible threats and vulnerabilities that the critical assets are exposed to are identified, supported by tools such as Nessus Nmap and the check list, getting as a result the risk matrix and so the treatment plan and select the controls that the NTE INEN-ISO/27001 proposes and considering the NIST 800-30 security criteria to finally show results obtained in the risk assessment.

Results and discussion part: involves the guidelines that should be carried out to the implantation of the selected controls and consists in five sections. The first one shows what an Information Security Management System consists of according to the NTE INEN-ISO/27001 standard, the second section define the scope and limits of this project, in the third section, it is shown the phases that should be accomplished to make the Information Security Management plan with the deliverables done throughout the elaboration of the plan and according to what the standard sets, in the fourth section, it is set an implementation guide to be carried out if the company authorities accept the performance of the mentioned plan and finally, in the fifth section the applicability of the proposal is done by comparing the current accomplishment state with the expected.

Conclusions and recommendations part: consists in the conclusions and recommendations obtained by the author of the project, which emphasize the most important points that should be considered in the company and users as well

1 INTRODUCCIÓN

1.1 Planteamiento de Problema

La información es uno de los recursos importantes en las organizaciones, pues de ella depende no solo la base del negocio, sino el logro de los objetivos a mediano o largo plazo, debido a que la información permite la toma de decisiones. Esta es una de las razones por las cuales, actualmente todas las empresas deberían realizar una apropiada gestión de riesgos, permitiéndoles de esa forma conocer las vulnerabilidades que poseen, las amenazas a las que se encuentran expuestas y el tamaño del riesgo que tendrían de no realizar control alguno [1].

La Cooperativa de Ahorro y Crédito Kullki Wasi es una entidad financiera con 15 años en el Ecuador [2], por ello se encuentra regulada por la Superintendencia de Economía Popular y Solidaria (SEPS), entidad técnica encargada de supervisar y controlar las organizaciones del sector económico popular y solidario del país, buscando su desarrollo, estabilidad, solidez y correcto funcionamiento en el sector financiero, así como asegurar el bienestar de los usuarios para que de esta forma exista confianza en la comunidad en general [3]. El 23 de noviembre de 2017 se publicó la Resolución No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103, en la cual se dispuso que el sistema financiero económico popular y solidario debe incrementar los niveles de seguridad en los canales electrónicos, mejorar los controles de gestión de la infraestructura de tecnología de la información y la gestión del riesgo operativo [4], basado en la Resolución No.128-2015-F de la Junta de Política y Regulación Monetaria y Financiera misma que está enfocada en la Administración de Riesgos en las Cooperativas de Ahorro y Crédito y Cajas Centrales [5].

Actualmente la Cooperativa de Ahorro y Crédito Kullki Wasi posee deficiencia en cuanto al manejo interno de los activos de información, debido a que no cuenta con una guía para la gestión de la seguridad de la misma [6], generando por un lado el desconocimiento de los riesgos de la seguridad de la información y por otro el incumplimiento de la Resolución No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103 y la Resolución No. 128-2015-F, por ello, el presente trabajo de titulación propone "Diseñar un Plan de Gestión de Seguridad de la Información para el área de Tecnologías de la Información (TI) de la Cooperativa de Ahorro y

Crédito Kullki Wasi" basando en la serie de estándares ISO/IEC 27000, lo que le permitirá a la entidad tener definido políticas para que la seguridad de la información se gestione de mejor manera y dar una guía inicial para el cumplimiento las resoluciones emitidas.

1.2 Objetivos

1.2.1 Objetivo General

Diseñar un plan de gestión de seguridad de la información para el área de Tecnologías de la Información para la Cooperativa de Ahorro y Crédito Kullki Wasi.

1.2.2 Objetivos Específicos

- Analizar la situación actual de la seguridad de la información de la Cooperativa de Ahorro y Crédito Kullki Wasi.
- Seleccionar la metodología de evaluación y gestión de riegos que se adapte de mejor manera a la Cooperativa de Ahorro y Crédito Kullki Wasi.
- Identificar los activos críticos de información, sus amenazas y vulnerabilidades.
- Diseñar un plan de seguridad de la información para los activos críticos de la Cooperativa de Ahorro y Crédito Kullki Wasi.

1.3 Alcance

El objetivo inicial del presente proyecto de titulación permitirá conocer las deficiencias actuales sobre el nivel de seguridad de la información de la entidad basándose en entrevistas, evaluación de documentos y/o información proporcionada por la cooperativa para posteriormente, junto con la metodología, determinar los riesgos y el estado de la seguridad en relación a la norma NTE INEN-ISO/IEC 27001:2011, basándose en los resultados obtenidos se identificará los controles de seguridad apropiados acorde a las necesidades del negocio; para finalmente diseñar un plan de Sistema de Gestión de la Seguridad de la Información (SGSI) proponiendo una secuencia de actividades que podrían ser realizadas en la entidad el momento que dispongan de la implementación del mismo. Cabe mencionar que la implementación no será parte del presente proyecto de titulación.

1.4 Reconocimiento de la Entidad Financiera

La Cooperativa de Ahorro y Crédito Kullki Wasi, regulada por la Superintendencia de Economía Popular y Solidaria, fue creada en enero de 2003 mediante acuerdo ministerial número N° 6582 en la Provincia de Tungurahua. Instituida como una entidad financiera Indígena y privada que impulsa el desarrollo socio económico de la población rural y urbana marginal, especializada en microfinanzas, con domicilio matriz ubicado en la cuidad de Ambato (Juan B. Vela y Martínez, Esquina). Hoy cuenta con más de 60.000 socios [2].

1.4.1 Historia

En el año 2002 dirigentes de Chibuleo, Salasaca y Pilahuin (12 personas) se reúnen con la idea de conformar una cooperativa de ahorro y crédito a la que llamarían "Kullki Wasi", que en kichwa signfica la Casa de Dinero. Estos 12 socios deciden en primera instancia aportar $ 40,00 dólares cada uno para certificado de aportación, pero posteriormente se toma la resolución de que cada socio fundador deberá contribuir con $1000 dólares, monto que serviría para capitalizar a la cooperativa y servir a los socios ahorristas, a través del otorgamiento de créditos mejorando la calidad de vida de los asociados y la comunidad.

Aprobados los estatutos, el 13 de enero de 2003 se nombra al Lic. Juan Andagana Gerente General de la cooperativa quien, al no contar con ningún recurso económico ni mobiliario, realiza auto gestión para conseguir escritorios usados, hojas de papel boom, sillas y almuerzos a los colaboradores. Además, una de las medidas que se tomaron fue que los cuatro colaboradores principales ingresaran en calidad de trabajador sin bonificación, es decir no recibirían ni sueldo, ni alimentación por el lapso de un año.

En los primeros años, se otorgaron indistintamente créditos individuales de montos pequeños y sobre saldo de $50 hasta $1.000 dólares, con plazo máximo de 12 meses y un garante. Para el año 2007 el crecientito de la cooperativa se veía reflejado en los más de 4.000.000 dólares de la cartera de crédito de socios. Sin embargo, el incremento de Cooperativas de Ahorro y Crédito (COAC) del sector indígena en la ciudad de Ambato, dejo a la vista en los socios con crédito el sobreendeudamiento. En este mismo año, la cooperativa había logrado tener 4

diferentes agencias (Salcedo, Latacunga, Riobamba y Pillaro), cada una con su respectiva máquina a la que llamaban “servidor”, donde el jefe de agencia realizaba inicio y fin del día. En relación a la seguridad de la información, se llevaba a cabo un respaldo cada hora diariamente puesto que se administraba una base de datos propia para que cada fin de mes consolidara el balance. En cuanto a la comunicación para depósitos y retiros entre agencias se lo realizaba mediante llamadas telefónicas y registros en Excel para que al fin de mes las encargadas de bóveda realizaran la transferencia. Posteriormente la comunicación se realizaba vía modem para envió de información diaria.

La toma de decisiones estaba basada en una herramienta gerencial básica, desarrollada en Excel. Para el año 2011, en cumplimiento del plan estratégico, se inicia el plan de adecuación de plataforma tecnológica y desarrollo de productos financieros y no financieros. El plan de cambio de sistema de información fue prioritario, “Sistema Financial II” fue adquirido debido a que brinda seguridad, información en tiempo real, desarrolla reportes, y la contabilidad al día. Este plan de mejora permitió implantar el servicio de cajeros automáticos en todas las oficinas [7].

1.4.2 Plan Estratégico

1.4.2.1 Misión

“Impulsar el desarrollo socioeconómico de la comunidad, brindando productos financieros eficientes con responsabilidad social y transparencia” [2].

1.4.2.2 Visión

“Ser una cooperativa del segmento uno, rentable, sostenible y con enfoque intercultural, basado en valores de calidad y servicio” [2].

1.4.2.3 Valores

En la Cooperativa de Ahorro y Crédito Kullki Wasi se practica los siguientes valores:

- Transparencia
- Honestidad
- Compromiso

- Pasión
- Integridad
- Justicia
- Solidaridad
- Excelencia
- Respeto
- Responsabilidad Social
- Trabajo en Equipo [8].

1.4.2.4 Política

- Desarrollo integral del asociado
- Fomento de la economía solidaria.
- Identificación y apoyo constante a nuevos sectores empresariales emergentes.
- Desarrollo permanente de productos competitivos de calidad.
- Transparencia en la información de actividades desarrolladas por la Cooperativa [8].

1.4.2.5 Objetivos

Financieros

- Alcanzar una cartera en riesgo menor al 8% con una cobertura de provisiones mayor al 100%.
- Alcanzar una Rentabilidad sobre Activos mayor al 2%.

Clientes

- Incrementar las captaciones en al menos $ 6,5 millones a fin de ubicarse en el segmento 1
- Incrementar la satisfacción de los clientes, atendiendo sus requerimientos de crédito en menos de 3 días y resolviendo el 100% de las quejas en menos de 72 horas.

Procesos

- Fortalecer el sistema de control interno, con 100% de los procesos críticos levantados y controlados.

- Tecnología: Implementar servicios transaccionales online y garantizar continuidad de operaciones financieras de al menos el 98% en tiempo de servicio.

Aprendizaje y Conocimiento

- Fortalecer las competencias del personal: al menos el 50% del personal de apoyo tendrá título profesional de tercer nivel; 80% del personal de negocios tendrá título profesional al 2021 [8].

1.4.2.6 Servicios

La

Tabla 1.1 describe los servicios que la Cooperativa Kullki Wasi ofrece a la comunidad.

Tabla 1.1: Servicios que ofrece la Cooperativa de Ahorro y Crédito Kullki Wasi

Servicios financieros	
Ahorro a la Vista	Este servicio refleja el saldo proveniente de las transacciones realizadas, en realidad no es una forma de ahorro sino un sistema para mantener el dinero al cuidado de la cooperativa. El dinero está disponible tanto en ventanilla como en el servicio de cajeros automáticos.
Ahorro a Domicilio	Servicio 100% garantizado y seguro de la visita de un asesor hasta el lugar en el que se encuentre el socio de Ahorro a la Vista como una alternativa de depósito para aquellos socios que no pueden movilizarse a las diferentes agencias de la cooperativa.
Cuenta Amigo "La Hormiguita"	Se trata del servicio ahorro infantil, y es una cuenta de ahorros especial dirigida a los menores de edad.
Plan Ahorro Plus Familiar	“Mi Kullki Futuro” es un ahorro contractual periódico a corto y largo plazo mediante el ahorro programado. El tiempo definido para este servicio es por más de un año y el dinero e intereses estarán disponible luego de haber culminado el contrato. El interés es acumulativo al capital.
Inversión Plazo Fijo	Alternativa de inversión, donde el dinero trabaja por el socio y se puede realizar depósitos a corto, mediano y largo plazo.
Créditos	Se ofrece una variedad de créditos a los asociados, con una cantidad de dinero hasta un límite especificado y durante un período de tiempo determinado.

Seguro de Desgravamen con EQUIVIDA	Seguro que paga el valor inicial de la deuda pendiente a la fecha de fallecimiento del deudor o del cónyuge o en el caso de invalides de por vida. EQUIVIDA paga el préstamo a la cooperativa acreedor, evitando que la familia asuma la deuda.
Seguro Exequial	En el instante en el que el socio fallezca por cualquier causa este tipo de seguro pagara el valor de 1200.00.
Cajeros Automáticos	El dinero está disponible las 24 horas en los 365 días del año en todos los cajeros automáticos a nivel nacional y/o sistema de BAN RED.
Servicios Cooperativos	
Como un complemento la cooperativa de ahorro y crédito KULLKI WASI posee alianzas estratégicas con varias instituciones público, privadas y financieras facilitando a los socios servicios adicionales de cobro y pago para: SUPA, Bono de desarrollo humano, IESS, matriculación vehicular, planes celulares y recargas, servicios básicos, impuestos, western union y catálogos.	

Fuente: Elaborado por el autor en base a información del documento Catálogo de Servicios.

1.4.3 Estructura organizacional de la Institución Financiera

1.4.3.1 Organigrama

La Cooperativa de Ahorro y Crédito Kullki Wasi se encuentra estructurada por ocho niveles jerárquicos. El Departamento de Tecnología (TIC) se encuentra en el nivel jerárquico de Departamentos de Apoyo y Gestión, tal como se muestra en la *Figura 1.1*

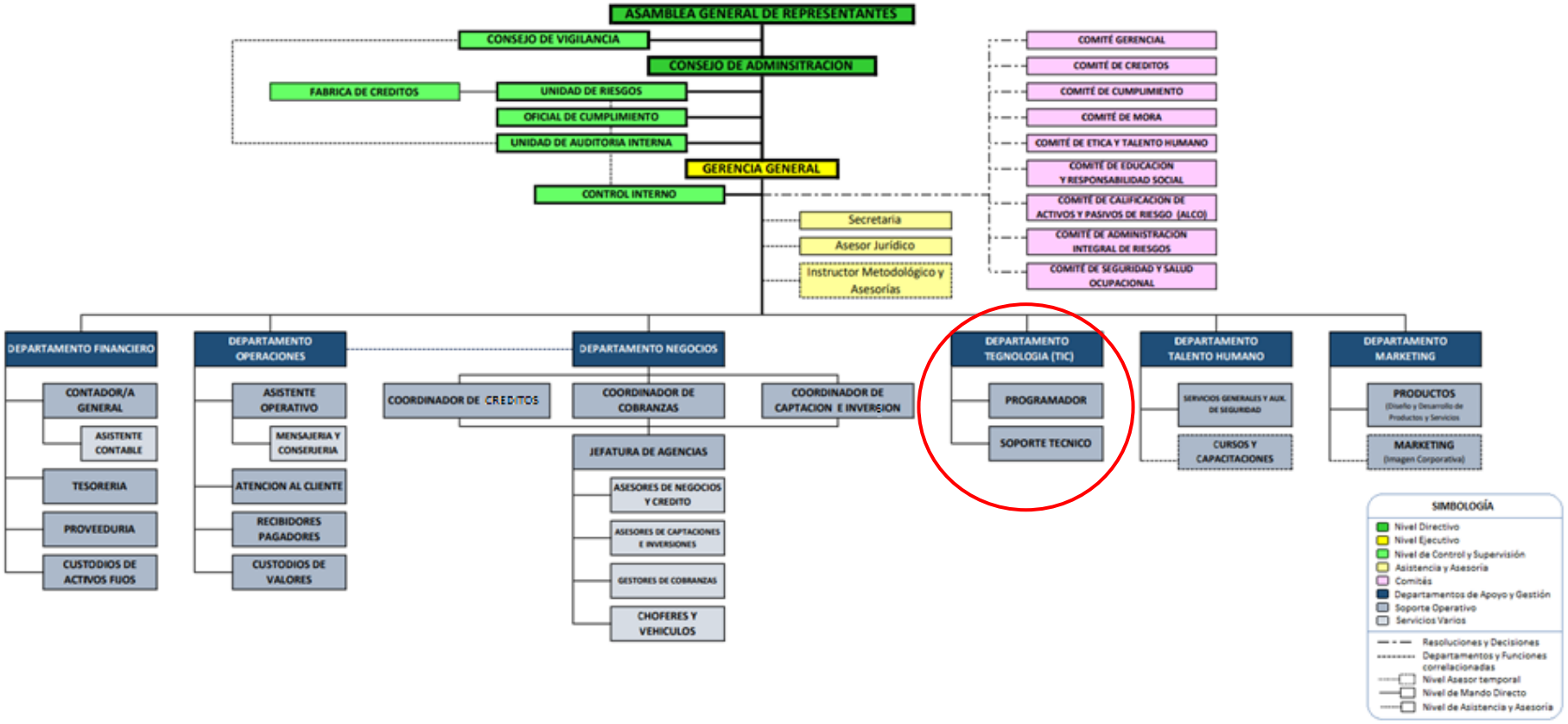

Figura 1.1: Organigrama de la Cooperativa de Ahorro y Crédito Kullki Wasi.

Fuente: Cooperativa de Ahorro y Crédito Kullki Wasi-Organigrama

1.4.4 Departamento de Tecnología (TIC)

Encargado de brindar un óptimo servicio de Tecnologías de Información y Telecomunicaciones, resguardando y gestionando eficientemente la plataforma tecnológica de la entidad financiera para satisfacer las necesidades de los usuarios y expectativas del negocio.

1.4.4.1 Plan Estratégico del departamento

1.4.4.1.1 Misión

Implementar y mantener servicios de Tecnología de Información adecuados, innovadores, seguros y eficientes, que faciliten la toma de decisiones de los diferentes procesos corporativos, permitiendo el cumplimiento de los objetivos de negocio de la Cooperativa, basados en buenas prácticas de calidad, compromiso, responsabilidad y confidencialidad.

1.4.4.1.2 Visión

Ser un área estratégica de apoyo a todos los procesos de la cooperativa enfocada en servicios y soluciones de excelencia para los usuarios, con tecnología de vanguardia.

1.4.4.1.3 Valores

El Departamento de Tecnología de la Cooperativa de Ahorro y Crédito Kullki Wasi practica los siguientes valores:

- Responsabilidad
- Honestidad
- Respeto
- Confidencialidad
- Compromiso
- Proactividad
- Vocación de servicio
- Trabajo en equipo

1.4.4.1.4 Responsabilidades

La *Tabla 1.2* que se muestra a continuación presenta las responsabilidades que tiene el departamento de tecnología ante el hardware y software.

Tabla 1.2: Responsabilidades del Departamento de Tecnología

Hardware	Software
Vigilar y llevar un inventario detallado de la infraestructura de Hardware acorde con las necesidades existentes.	Restringir el acceso a los equipos tecnológicos fuera de horario de trabajo, a aquellos usuarios que no cuenten con una autorización previa de su superior inmediato para laborar fuera de horario.
Ser el único responsable de hacer requerimientos de los activos informáticos que hayan sido proyectados, según las necesidades que se presenten en cada área de trabajo.	Llevar inventario del software (programas) instalados en la Cooperativa.
Determinar la vida útil de los equipos de informática, con la finalidad de optimizar su uso.	Velar porque todo el software instalado este legalmente licenciado.
Participar en los contratos de adquisición de bienes y/o servicios, donde se incluyan equipos informáticos, enlaces, o de soporte técnico referente a su área como parte integrante o complementaria de otros.	Custodiar y almacenar todos los programas informáticos de la Cooperativa.
Confirmar que los equipos de informática cumplan con las especificaciones técnicas indicadas en las solicitudes de compra, de no ser así se encargará de la devolución de los mismos.	Definir los discos de Red de todas las áreas, para poder fragmentar el acceso a la información y una mejor organización.
Realizar el mantenimiento técnico preventivo de todos los equipos informáticos.	Establecer configuraciones automatizadas para que los usuarios guarden toda su información en los discos de red y se puedan facilitar las copias de seguridad (backup).
Instalar los equipos tecnológicos.	Verificar los programas informáticos que sean instalados, con la finalidad de llevar un control de los mismos.
Evaluar el área física donde se instalará un nuevo equipo informático, confirmando que el área este óptima para la instalación de los mismos.	Instalar todas las aplicaciones de los equipos y programas informáticos utilizados por la Cooperativa.
Verificar que los equipos tecnológicos tengan: disponibilidad de energía eléctrica, cableado	

estructurado y mantengan las condiciones físicas aceptables y adecuada de temperatura, entre otros.
Presentar la proforma presupuestaria necesaria al Departamento Financiero en forma anua (hasta octubre de cada año).
Velar por el adecuado uso de las instalaciones eléctricas requerida para el funcionamiento de los equipos tecnológicos.
Verificar el inventario de l equipos, con la finalidad de llevar un control de estos.
Instruir al usuario sobre el uso y manejo adecuado de los equipos y programas informáticos instalados.
Verificar que los programas de computadoras suministren los manuales correspondientes al funcionamiento de los equipos o programas especializados.

Fuente: Elaborado por el autor en base a información del documento manual de tecnología de la información.

1.4.4.2 Estructura organizacional del departamento

La *Figura 1.2* muestra los dos niveles que constituyen el Departamento de Tecnología. El primer nivel está conformado por la administración del área, jefe del departamento, y el segundo nivel lo conforman dos programadores y un encargado de soporte técnico, responsables de la asistencia a los usuarios de la entidad financiera.

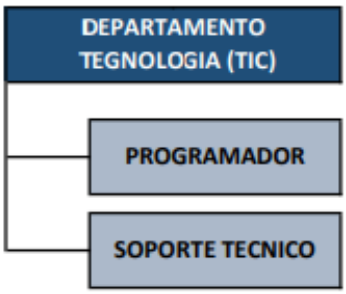

Figura 1.2: Organigrama Departamento de Tecnología (TIC).

Fuente: Cooperativa de Ahorro y Crédito Kullki Wasi-Organigrama

1.4.4.3 Recurso humano

La *Tabla 1.3* muestra el personal con el que cuenta actualmente el Departamento de Tecnología.

Tabla 1.3: Recurso humano del Departamento de Tecnología.

Nombre	Cargo	Funciones	Profesión
Franklin Ricardo Barrionuevo Caiza	Jefe de Sistemas	Responsable de la administración y el buen funcionamiento del Hardware, Software, Aplicaciones, Bases de Datos, Red, y Seguridad Informática dentro de la entidad.	Ingeniero de Sistemas
Víctor Alfonso Bombón Ramos	Programador	Mantenimiento y soporte a las aplicaciones de la entidad.	Ingeniero de Sistemas
José Antonio Caizabanda Jerez	Programador	Mantenimiento y soporte a las aplicaciones de la entidad.	Ingeniero de Sistemas
Geovanny Paul Ruiz Sánchez	Soporte Técnico	Mantenimiento de hardware y software de los equipos tecnológicos de la entidad.	Tecnólogo

Fuente: Elaborado por el autor en base a información proporciona por el Jefe del Departamento de Tecnología.

1.4.4.4 Componentes del Departamento de Tecnología

Actualmente, la cooperativa cuenta con 67 computadores y/o laptops distribuidas en todo el edificio matriz (8 pisos), que cuentan con garantías y sus respectivos seguros. En cuanto a los sistemas operativos instalados se tiene: Windows 7 Pro, Windows 8 Pro y Windows 10 Pro todos con sus respectivas licencias. La licencia de antivirus tiene una renovación cada 3 años siendo el proveedor la Compañía ESET.

1.4.4.4.1 Aplicaciones de Software

Las aplicaciones son programas desarrollados para solucionar y automatizar procesos específicos, a continuación, se presentan aquellos aplicativos que están alojados en los seis servidores a ser analizados

MicroScore

Es el aplicativo encargado de la evaluación crediticia, es decir, en base a variables de perfil, actividad productiva, capacidad de pago, comportamiento de pago entre otras variables determinadas por la entidad y conforme a las políticas y niveles de

riesgo asumidos se evalúa la criticidad del otorgamiento de un crédito; manejando la información de un posible sujeto de crédito.

Tabla 1.4: Características del servidor que aloja el MicroScore

	IP	Sistema Operativo	Características
MicroScore	192.168.X.X	Microsoft Windows Server 2012 Estándar	Máquina virtual Procesador: Intel Zeon 2.2GHz RAM: 16 GB 64 bits Disco: 299 GB

Fuente: Elaborado por el autor en base a información proporciona por el Jefe del Departamento de Tecnología.

Ventanillas Móviles

Web services de ventanillas móviles (de cara al Internet), es decir aloja todos aquellos servicios (depósitos de ahorro a la vista) que el asesor requiere al momento de trasladarse hasta el socio que no puede acercarse a alguna agencia de la entidad. En otras palabras, es el servicio que permite a los asesores llevar consigo el aplicativo tanto en los teléfonos celulares como el las tablets para poder brindar el servicio de “Ahorro a Domicilio”.

Tabla 1.5: Características del servidor que aloja las Ventanillas Móviles

	IP	Sistema Operativo	Características
Ventanillas Móviles	192.168.X.X	Microsoft Windows Server 2012 R2	Máquina virtual Procesador: Intel Zeon 2.40GHz RAM: 4 GB 64 bits Disco: 80 GB

Fuente: Elaborado por el autor en base a información proporciona por el Jefe del Departamento de Tecnología.

Cajeros Automáticos

Servicio de cajeros, mismo que realiza la generación de llaves y encriptación de tarjetas de débito. Permite el enlace con el switch “Conecte” para lograr la transacción de acuerdo a la solicitud del cliente.

Tabla 1.6: Características del servidor que aloja los Cajeros Automáticos

	IP	Sistema Operativo	Características
Cajeros Automáticos	192.168.X.X	Windows server 2008 R2	Procesador: Intel Core 2 Quad 2,66GHz RAM: 4 GB

		iPXE 1.0.0+ HCM	64bits Disco: 99.9 GB Sistema operativo. 198 GB Servicios de conecte

Fuente: Elaborado por el autor en base a información proporciona por el Jefe del Departamento de Tecnología.

Financiero

Aloja e integra todas las aplicaciones financieras que maneja la entidad, permitiendo el acceso a los servicios de Ahorro a la Vista, Cuenta amigo “La Hormiguita”, Plan Ahorro Plus Familiar, Inversión a Plazo Fijo, Créditos y Seguros.

Tabla 1.7: Características del servidor que aloja el Sistema Financiero

	IP	Sistema Operativo	Características
Aplicaciones	192.168.X.X	Microsoft Window Server 2008 R2	Procesador: IBM BLEI CENTER, ZEON 2.3 GHz RAM: 16 GB 64 bits Disco: 135 GB Sistema Operativo 558 GB Score financiero. 931GB Archivos.

Fuente: Elaborado por el autor en base a información proporciona por el Jefe del Departamento de Tecnología.

Cabe mencionar que el servidor que aloja las aplicaciones financieras también es utilizado para alojar el registro del biométrico, servicios de imágenes de conexión y el Excel financiero.

1.4.4.4.2 Servidores

Además de los servidores que alojan los aplicativos descritos anteriormente, el Departamento de Tecnología tiene a su responsabilidad los servidores que se encuentran en la *Tabla 1.8.*

Tabla 1.8: Inventario de servidores

No.	Servidor	IP	Función	Sistema Operativo	Características
1	Base de Datos	192.168.X.X	Almacenar toda la información del core del negocio	Microsoft Windows Server 2012 R2	Procesador: Intel Zeon 2.30 GHz 64 bits Discos: 558 GB Base de datos. 195BG Logs. 642GB Respaldos

					momentáneos backup. 558GB Guardar respaldos 182GB Sistema Operativo
2	Contingencia	192.168.X.X	Servidor donde se carga los respaldos de datos. Base de desarrollo	Microsoft Windows Server 2012 R2	Máquina virtual Procesador: Intel Zeon 2.2GHz RAM: 24GB 64 bits Disco: 699 GB Sistema operativo y base de datos

Fuente: Elaborado por el autor en base a información proporciona por el Jefe del Departamento de Tecnología.

1.4.4.4.3 Red

El departamento de Tecnología se encuentra en el tercer piso del edificio matriz. La *Figura 1.3* muestra la topología de red WAN y la *Figura 1.4* muestra la topología LAN de la entidad.

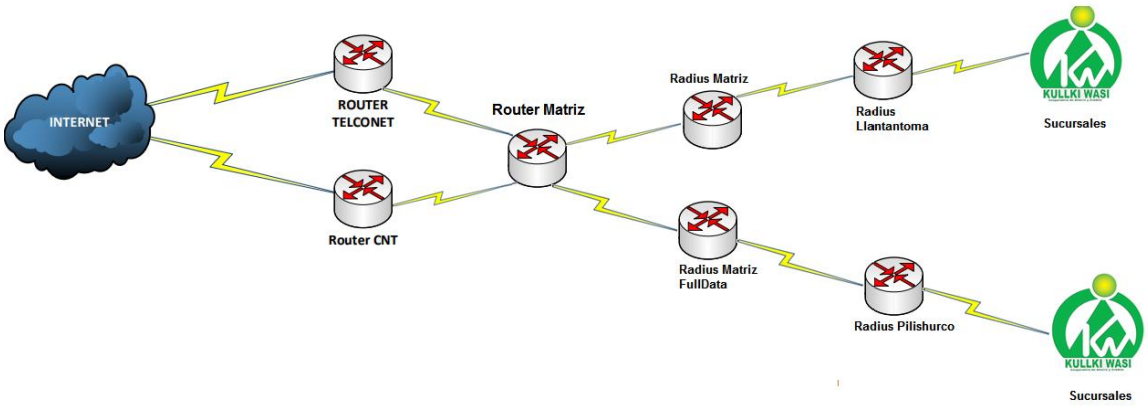

Figura 1.3: Red WAN de Cooperativa de Ahorro y Crédito Kullki Wasi

Fuente: Cooperativa de Ahorro y Crédito Kullki Wasi-Topología

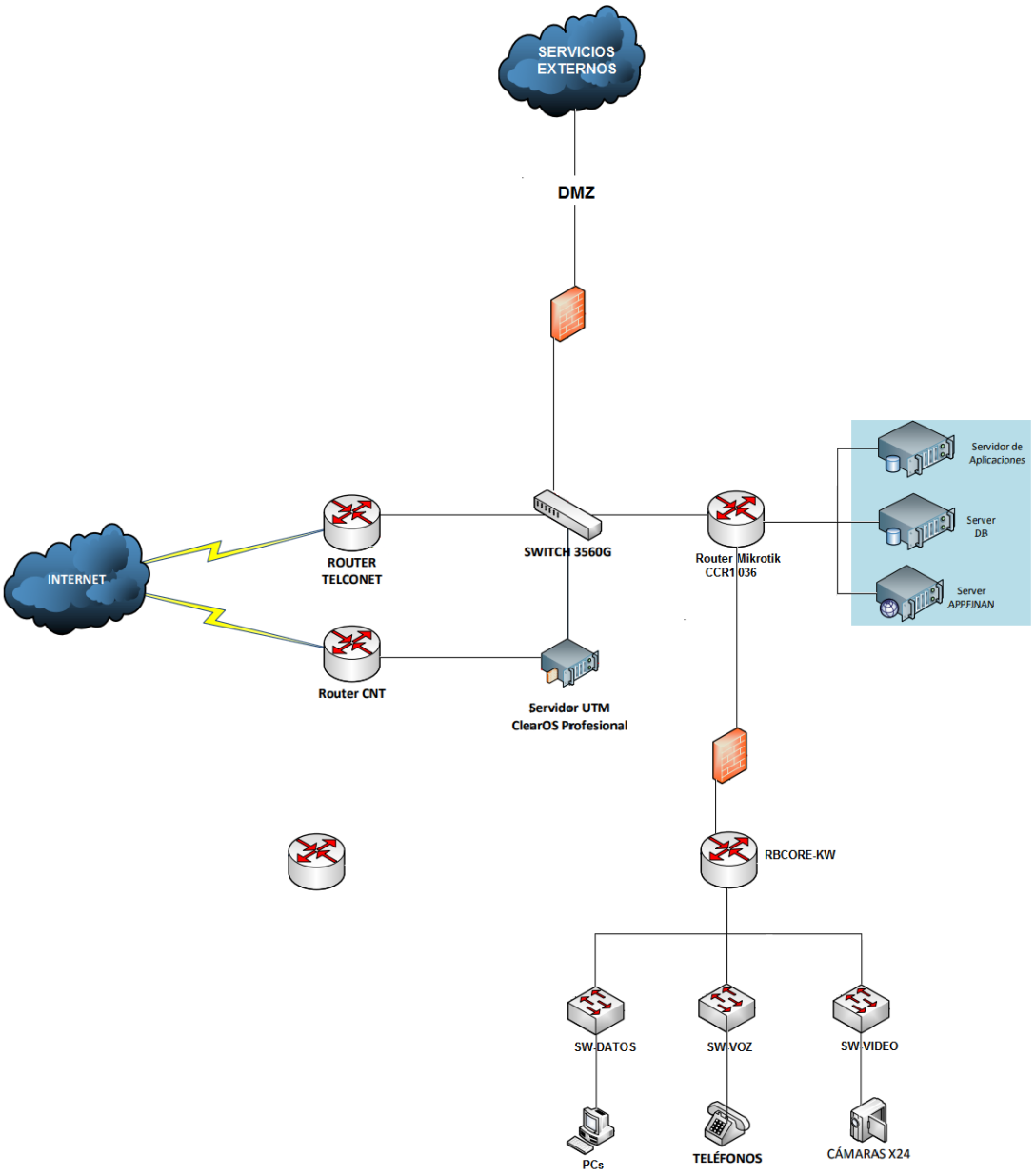

Figura 1.4: Red LAN de Cooperativa de Ahorro y Crédito Kullki Wasi

Fuente: Cooperativa de Ahorro y Crédito Kullki Wasi-Topología

La telefonía IP es manejada mediante central telefónica Cisco. Todos los usuarios poseen teléfono con excepción de los asesores comerciales quienes cuentan con una línea para cada grupo.

La seguridad de acceso a la red es controlada por un Gestor Unificador de amenazas (ClearOS Profesional) y Firewall.

Para el enlace de datos se cuenta con: antenas propias de16MB como enlace principal, fibra óptica de 5MB de Telconet como enlace secundario (oficinas tanto datos e Internet) y CNT como backup de conexión a Internet.

1.5 Selección de metodología y uso de estándar

La seguridad de la información hace referencia no solo a la seguridad técnica sino también a los riesgos del negocio, es decir la exposición a vulnerabilidades que determinan cuan segura es la información manejada. Realizar el análisis de los elementos (activos, amenazas, vulnerabilidades y controles existentes) que determinan los riesgos (físicos, operacionales, organizacionales y de TI) permiten conocer la importancia de la información y protegerla.

1.5.1 Metodologías para la evaluación y gestión de riesgos

Hablar de la seguridad de la información, hoy en día, es referirse a los riesgos a los que una entidad está expuesta. El establecer medidas para proteger la información puede resultar complejo ya que depende del nivel de su aplicación, por ello analizar los riesgos cumple un papel fundamental en este proceso. Llevar a cabo el análisis de riesgos permite conocer los factores de riesgos latentes que causan un impacto significativo dentro de una entidad, es decir permite establecer el nivel de riesgo y los controles y/o acciones a implementar en el Plan de Seguridad de la Información. La validez del proceso de análisis es en el tiempo que se lo efectúa debido a que las medidas que se puedan implantar pueden llegar a ser ineficientes con el transcurso del tiempo, ya que cada día existen nuevas amenazas lo que conlleva a nuevas ocurrencias de riesgo.

A continuación, se presenta una pequeña descripción de algunas de las metodologías que son utilizadas frecuentemente (RISK IT, MAGERIT, OCTAVE y NIST 800-30) para realizar el análisis de riesgos, proceso exigido dentro de la norma ISO 27001 en el marco de la implementación de los SGSI. La descripción más detallada de cada metodología se puede observar en el *ANEXO I - Selección de Metodología para el Análisis de Riesgos.*

1.5.1.1 *RISK IT*

Publicada por ISACA, diseñada y creada principalmente como un recurso educativo para los oficiales de información, la alta dirección y administración de TI. RISK IT está basada en los principios de gestión de los riesgos organizacionales, las normas y marcos como la norma ISO 31000 y provee información acerca de cómo aplicar estos principios a las TI, además de que considera la posibilidad de búsqueda de riesgos que podrían beneficiar a la organización, siempre que se encuentre el balance entre riesgo y costos [9].

1.5.1.2 MAGERIT

Publicada por el Consejo Superior de Administración Electrónica, es una metodología de análisis y gestión de riesgos de los Sistemas de Información diseñada para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, responde a lo que se denomina “Proceso de Gestión de los Riesgos” en otras palabras, esta metodología implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones sin olvidar los riesgos que provienen del uso de tecnologías de la información [10].

1.5.1.3 OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation, publicada por la Universidad Carnegie Mellon, es una metodología que estudia los riesgos en base a los objetivos de seguridad (Confidencialidad, Integridad y Disponibilidad), esta metodología comúnmente es utilizada por agencias gubernamentales. OCTAVE estudia la infraestructura de información y la manera en que esta es usada.

1.5.1.4 NIST 800-30

Risk Management Guide for Information Technology Systems, es una metodología que analiza y gestiona el riesgo de la seguridad de la información, proporciona las bases para el desarrollo de un programa de gestión de riesgos efectivo que contiene, definiciones, orientaciones prácticas necesarias para evaluar y mitigar los riesgos identificados dentro de los sistemas de TI [11].

1.5.1.5 Selección de metodología

Para la selección de la metodología se evaluaron las antes mencionadas, para conocer cuál de ellas alcanza mayor valoración respecto al análisis del riesgo, permitiendo seleccionarla para la realización del presente proyecto de titulación.

Para la identificación de las fortalezas de cada metodología se utilizó los elementos que se relacionan directamente con el Departamento de Tecnología (elementos de TI), dichos elementos son: Hardware, Software, Bases de Datos, Redes y Telecomunicaciones, Recurso Humano y Servicios, mismos que fueron calificados según el nivel de satisfacción en función a las actividades que deben ser llevadas a cabo para lograr el análisis y gestión de riesgos por metodología, permitiendo obtener resultados (de nivel de correspondencia) para compararlos y obtener la metodología con mayor valoración. La *Figura 1.5* que se presenta a continuación muestra los resultados de nivel de satisfacción alcanzado por cada metodología en relación a los elementos de TI. La asignación de los valores por actividad de cada metodología y la evaluación completa se puede observar en el *ANEXO I - Selección de Metodología para el Análisis de Riesgos.*

Metodología	ELEMENTOS DE TI					
	HARDWARE	SOFTWARE	BASES DE DATOS	REDES Y TELECOMUNICACIONES	RECURSO HUMANO	SERVICIOS
Octave	0,92	0,92	0,92	0,96	0,75	0,71
Risk IT	0,91	0,91	0,97	0,91	0,75	0,84
Magerit	0,93	0,93	0,93	0,93	0,84	0,98
Nist 800-30	0,97	0,97	1	0,97	0,81	0,92

Figura 1.5: Resultados de nivel de satisfacción alcanzado por cada metodología.

Fuente: Elaborada por el autor en base al ANEXO I - Selección de Metodología para el Análisis de Riesgos.

Para poder observar de mejor manera la metodología que posee mayor correspondencia con los elementos de TI a continuación se presenta la *Figura 1.6*.

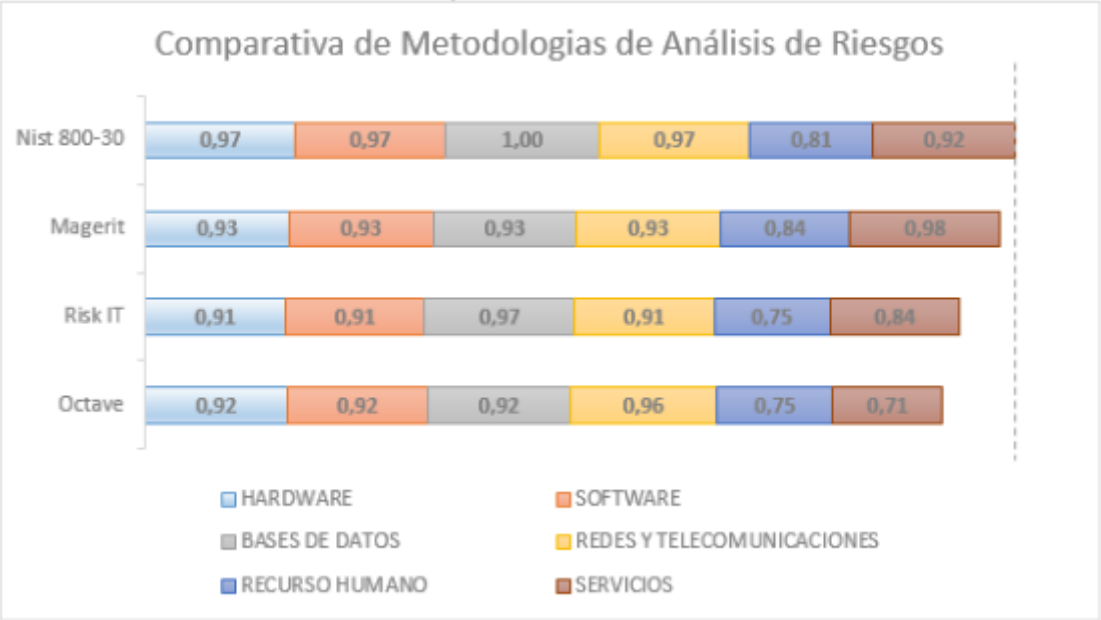

Figura 1.6: Escala de Medición de la Comparativa de Metodologías de Análisis de Riesgo.

Fuente: Elaborada por el autor en base al ANEXO I - Selección de Metodología para el Análisis de Riesgos.

Como se puede observar la metodología que alcanza mayor nivel de satisfacción es NIST 800-30 y esto se debe principalmente a que esta metodología permite determinar e identificar los componentes y recursos de TI para ejecutar el análisis de riesgo, por medio de entrevistas, visitas al sitio y uso de herramientas de mapeo de red. Así también se identifican las posibles fuentes de amenazas y vulnerabilidades en función al recurso humano, las motivaciones y acciones a tomar; todo esto adaptándose a cada organización. Así mismo la metodología NIST 800-30 define el análisis de impacto en función de los objetivos de seguridad (integridad, disponibilidad y confidencialidad) en relación a la comprobación de Requerimientos de Seguridad en todos los activos agrupadas en tres áreas (Administrativa, Operacional y Técnica), lo que hace que el nivel de satisfacción en correspondencia con los elementos de TI sea adecuado, alcanzando el mayor nivel por lo cual es la metodología seleccionada para el análisis de riesgos del presente trabajo de titulación.

1.5.2 Norma NTE INEN-ISO/IEC 27001:2011

La información es el activo más importante que posee una organización, mayormente hablando de una entidad financiera, por ello el resguardo y correcto manejo de esta es de suma importancia, debido a esto se puede afirmar que uno de los objetivos principales dentro de las organizaciones es la seguridad de la información fundamentado en una buena gestión mediante un sistema que tenga metodología y documentación basada en objetivos de seguridad y evaluación de riesgos, alineados con los objetivos del negocio. Para lograr lo dicho se utiliza estándares que se encuentran regulados por organizaciones especializas en el tema, estos estándares se denominan Norma ISO.

La norma NTE INEN-ISO/IEC 27001:2011 adopta un enfoque por proceso para crear, implementar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), siguiendo el modelo de proceso Planear-Hacer-Chequear-Actuar (PDCA de sus siglas en ingles), conjuntamente con la gestión de riesgo para los activos de información críticos de una organización [12]. Esta norma está orientada a todas las organizaciones (independientemente del tipo, tamaño o naturaleza) que estén interesada en certificarse en la misma, para ello la organización deberá cumplir con el sistema de gestión de seguridad de la información de acuerdo a la actividad económica que ésta desempeña y bajo el enfoque planteado por la NTE INEN-ISO/IEC 27001:2011.

El presente Plan de Gestión de Seguridad de la Información para la Cooperativa de Ahorro y Crédito Kullki Wasi estará basado en el estándar NTE INEN-ISO/IEC 27001:2011 debido a que todas sus actividades generadoras de valor son hechas mediantes procesos establecidos y evaluados por controles mismos que pueden ser mejorados al utilizar de forma correcta la norma en mención tal y como se encuentra establecido en Manual de Tecnología de la Información de la cooperativa.

1.6 Situación actual de la seguridad de la información

En el transcurso de esta sección se muestra la información obtenida en las visitas realizadas a la entidad financiera, entrevistas efectuadas al jefe del Departamento de Tecnología en la cuidad de Ambato, las misma que sirvieron para llenar la

evaluación que brindan las herramientas Microsoft Security Assessment Tool (MSAT) y Check List de Auditoria “Manejo de Seguridad de la Información”. Esta información permitirá conocer la situación actual y estado de cumplimiento basado en el estándar NTE INEN-ISO/IEC 27001 para conocer los problemas de la seguridad de la información que posee la entidad.

1.6.1 Análisis de la situación actual

Para el análisis de la situación actual de la entidad se utilizará la herramienta Microsoft Security Assessment Tool (MSAT), misma que permite a las organizaciones conocer la situación actual en la que se encuentra la seguridad de las tecnologías de la información. Esta herramienta gratuita ayuda a las organizaciones en la evaluación de las deficiencias del entorno de seguridad de TI, proporcionando una lista de problemas y una guía para minimizar el riesgo.

Las preguntas que maneja esta herramienta están relacionadas con la infraestructura, aplicaciones, operaciones y usuarios. Mismas que están basadas en las mejores prácticas y estándares como ISO 27001 y NIST-800.x, así como las recomendaciones y orientaciones normativas del Grupo Trustworthy Computing de Microsoft y otras fuentes externas de seguridad [13].

Una vez finalizado el cuestionario de MSAT se obtiene el perfil de riesgo para la empresa (BRP[1]) para cada área de análisis (AoAs[2]) y el índice de defensa en profundidad (DiDI[3]). La *Figura 1.7* muestra los resultados obtenidos tanto del BRP como del DiDI de acuerdo a las AoAs.

[1]BRP: medición del riesgo relacionado al modelo empresarial y al sector de la empresa

[2] AoAs: infraestructura, aplicaciones, operaciones y personal.

[3] DiDI: medición de las defensas de seguridad utilizadas en el personal, los procesos y la tecnología para ayudar a reducir los riesgos identificados en una empresa.

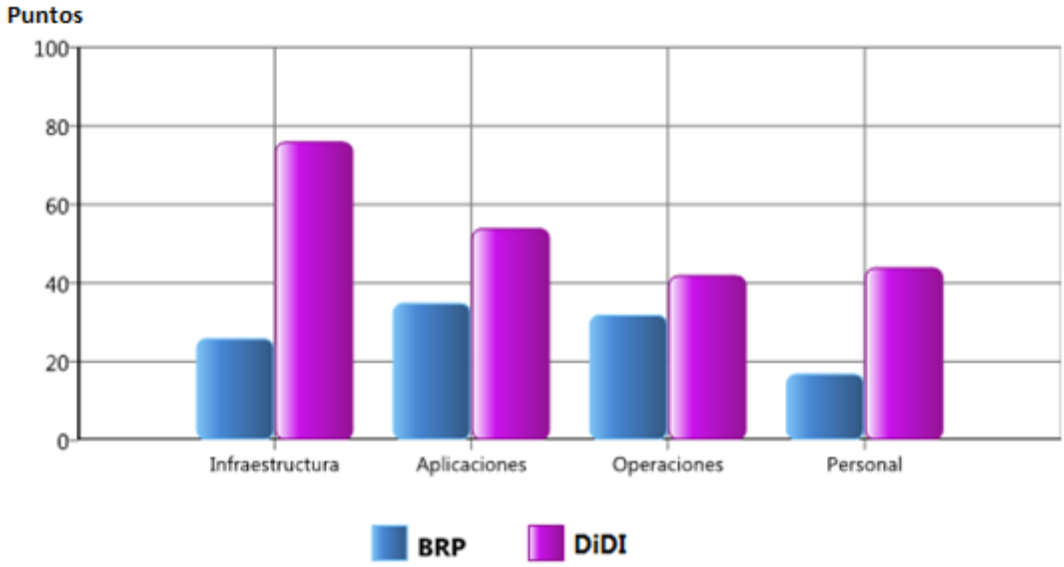

Figura 1.7: Resultados obtenidos de BRP y DiDI.

Fuente: Informe de la Herramienta MSAT (ANEXO II - Resultado de Medidas de Defensa MSAT).

Una puntuación alta en el BRP significa un aumento del posible riesgo al que está expuesta la organización según el área evaluada. Mientras que una puntuación alta en el DiDI significa un entorno donde se han tomado más medidas para implementar estrategias de defensa en profundidad según el área evaluada, sin embargo, no indica la eficacia general de la seguridad ni siquiera la cantidad de recursos para la misma, sino que cuantifica la estrategia global que se utiliza para defender el entorno. Cuando ambos valores son comparados se obtiene la distribución de defensa del riesgo. Una disparidad significativa entre el BRP y el DiDI indica que la estrategia de seguridad del negocio no es la adecuada produciendo un ambiente de vulnerabilidad dentro de este.

Por otro lado, la herramienta MSAT muestra la madurez de la seguridad que incluye controles físicos, técnicos, competencia técnica de los recursos informáticos, las directivas, los procesos y las prácticas sostenibles. Este nivel permite comparar las prácticas de seguridad que posee la entidad contra las mejores prácticas de la industria para que se pueda alinear las prácticas de seguridad con la realidad del negocio. Cada entidad debe esforzarse en alinear su nivel de madurez y estrategia de seguridad, en relación a los riesgos se su actividad comercial. Los posibles niveles de madurez son:

- **Básica:** algunas medidas eficaces de seguridad utilizadas como primer escudo protector; respuesta de operaciones e incidentes aún muy reactiva.

- **Estándar:** Capas múltiples de defensa utilizadas para respaldar una estrategia definida.
- **Optimizada:** Protección efectiva de los asuntos de forma correcta y garantía de la utilización del mantenimiento de las mejores prácticas recomendadas

La *Figura 1.8* muestra los resultados de distribución de defensa del riesgo y el nivel de madurez de la seguridad[4] del negocio.

Figura 1.8: Resultados de Distribución de defensa de riesgos y Madurez de la seguridad.
Fuente: Informe de la Herramienta MSAT (ANEXO II - Resultado de Medidas de Defensa MSAT).

El resultado mostrado como distribución de defensa de riesgos indica el balance entre los riesgos y las medidas para prevenirlos, por lo tanto, se puede observar que en el área de personal y de infraestructura se necesita una mejora considerable, en el área de aplicaciones una mejora leve y en el área de operaciones mantener las medidas que hasta el momento se han tomado, para que con ello el negocio logre un equilibrio. En cuanto a la madurez de la seguridad se observa que la protección actúa de forma correcta de acuerdo las mejores prácticas recomendadas

1.6.1.1 Resultados de las medidas de defensa

La *Figura 1.9* presenta los resultados obtenidos en base a las respuestas dadas por el jefe del Departamento de Tecnología para cada pregunta en las diferentes áreas de análisis provistas por la herramienta MSAT.

[4] Madurez de la seguridad: medición de la capacidad de la empresa para utilizar de forma eficaz las herramientas disponibles de forma que se cree un nivel de seguridad sostenible a lo largo de diversas disciplinas.

Infraestructura	
Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus - Equipos de escritorio	
Antivirus - Servidores	
Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	
Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas-Cuenta de administrador	
Directivas de contraseñas-Cuenta de usuario	
Directivas de contraseñas-Cuenta de acceso remoto	
Cuentas inactivas	
Gestión y control	
Informes sobre incidentes y respuesta	
Creación segura	
Seguridad física	
Aplicaciones	
Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicación y recuperación de datos	
Fabricante de software independiente (ISV)	
Desarrollado internamente	
Vulnerabilidades	
Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	
Almacenamiento y comunicaciones de datos	
Cifrado	
Cifrado - Algoritmo	

Operaciones	
Entorno	
Host de gestión	
Host de gestión-Servidores	
Host de gestión - Dispositivos de red	
Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	
Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	
Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	
Personal	
Requisitos y evaluaciones	
Requisitos de seguridad	
Evaluaciones de seguridad	
Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	
Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

Leyenda	
Cumple las mejores prácticas recomendadas	
Necesita mejorar	
Carencias severas	

Figura 1.9: Resultados de las medidas de defensa

Fuente: Informe de la Herramienta MSAT (ANEXO II - Resultado de Medidas de Defensa MSAT).

A continuación, se presenta un resumen de los resultados de las medidas de defensa por cada área de análisis. El informe completo de la evaluación de la herramienta MSAT se encuentra en el *ANEXO II - Resultado de Medidas de Defensa MSAT.*

Infraestructura

Esta área analiza el funcionamiento de la red, los procesos comerciales (internos externos) que debe favorecer, como se construye y utiliza los hosts, y la gestión y el almacenamiento efectivo de la red. Al diseñar una infraestructura que todos puedan comprender y seguir, la empresa podrá identificar las áreas de riesgo e idear métodos para acabar con las amenazas.

- El perímetro de red no cuenta únicamente con firewall (regularmente comprobado su funcionamiento) sino que se ha tomado precaución al crear segmentos DMZ con lo que se protege los recursos corporativos accesibles a través de Internet.
- Tanto los equipos de escritorio como los servidores cuentan con solución de antivirus.
- El acceso remoto utiliza VPN y autenticación multifactor, esta conexión solo puede realizarlo usuarios autorizados.
- Existe más de un segmento en la red.
- El sistema de detección de intrusiones está basado tanto en red (NIDS) como en host (HIDS).
- Existe la opción de conexión inalámbrica a la red con restricción por MAC.
- Para la autenticación en los dispositivos y hosts es necesario el uso de contraseñas complejas. Cada equipo utiliza protector de pantalla protegido por contraseña en el entorno.
- Se cuenta con un sistema de alarma de detección de intrusiones. Los servidores se encuentran en un armario cerrado. Los archivos confidenciales impresos se almacenan en armarios con llave.
- A los visitantes no se les entrega tarjeta de identificación sin embargo son registrados en recepción.

Aplicaciones

Esta área estudia las aplicaciones del entorno que son esenciales para la entidad, estas son valoradas desde el punto de vista de la seguridad y disponibilidad. También son examinadas las tecnologías utilizadas para aumentar el índice de defensa en profundas.

- Se realizan periódicamente pruebas de la recuperación de aplicaciones y datos.
- Las aplicaciones principales del entorno han sido desarrolladas por fabricantes independientes de software mismos que no suelen ofrecer revisiones ni actualizaciones de seguridad esto es efectuado por el equipo interno de desarrollo.
- Actualmente no se conoce vulnerabilidades para la seguridad en ninguna aplicación de entorno. En las aplicaciones principales se usa autenticación (se registran los intentos fallidos, pero no los correctos) con contraseñas complejas y controles de bloqueo de cuentas. Además, está limitado el acceso a datos y funciones confidenciales según el privilegio de la cuenta.
- Los datos de entrada de los usuarios finales y de las aplicaciones de cliente son validados.
- No se utiliza metodologías de desarrollo de seguridad de software para el desarrollo de código seguro.
- Los datos confidenciales en las aplicaciones principales del entorno son cifrados (algoritmo de hash MD5) antes de transmitirlos y cuando están almacenados.

Operaciones

Esta área valora las prácticas de funcionamiento y las normas que siguen la empresa para aumentar las estrategias de defensa en profundidad a fin de emplear más que meras defensas tecnológicas. Estudia las áreas relacionadas con la creación de datos en el entorno.

- No existe clasificación de la confidencialidad de la información.
- Existen procedimientos sobre los servicios y protocolos permitidos, pero no se encuentran formalmente documentados.

- Se regulan las cuentas de los usuarios dentro del entorno.
- Los diagramas lógicos de la red en el entorno son actualizados regularmente. No existen diagramas de la arquitectura, ni del flujo de datos de las aplicaciones.
- No se regulan, ni se revisan las actualizaciones en las aplicaciones.
- No existe gestión de cambios.
- Se realizan backup de acuerdo a la criticidad de la información. No existe copias de seguridad de los usuarios finales.
- No existen planes de recuperación ante desastres y continuidad del negocio.

Personal

Revisa los procesos de la empresa que regulan las directivas de seguridad corporativa, los procesos de recursos humanos, así como la formación y el grado de conocimiento de los empleados sobre la seguridad. También se centra en la seguridad en las operaciones diarias. Este apartado le ayuda a valorar como se mitigan los riesgos del área personal.

- No existe modelo para asignación de niveles de gravedad a cada componente del entorno informático.
- Las evaluaciones de seguridad son realizadas por el personal interno.
- La comprobación del historial personal únicamente se lo realiza a los empleados con cargos importantes o que controlen información confidencial.
- Existe un procedimiento formal para los empleados que dejan de formar parte de la entidad.
- Los acuerdos de nivel de servicio (SLA) están incluidos en los contratos con los proveedores de servicios subcontratados en estas se incluyen las especificaciones de seguridad.
- Los cursos de capacitación que el personal ha tenido no han incluido temas de prácticas de confidencialidad y/o seguridad informática. Las medidas de seguridad han sido divulgadas por parte del departamento de TI.

1.6.2 Estado de cumplimiento actual

Una vez que se ha completado el Check List, que contiene los 11 dominios del Anexo A de la norma NTE INEN-ISO/IEC 27001 con los objetivos de control y controles (ver *ANEXO III - Manejo de Seguridad de la Información NTE INEN-ISO-IEC 27001-2011 Auditoria Check List*) se tabularon los resultados de acuerdo a las respuestas proporcionadas por el Jefe del Departamento de TI, de manera que cuando un control se está cumpliendo correctamente se asigna el valor de "1" en la columna "Si Cumple", cuando el control se está cumpliendo pero no se tiene la debida documentación o hace falta alguna actividad para cumplirlo en su totalidad se asigna el valor de "1" en la columna "Cumple Parcialmente" y cuando el control no se lleva a cabo dentro de la entidad se asigna el valor de "1" en la columna "No cumple", para luego realizar una suma de los valores "1" por cada columna y así obtener los porcentajes de "Si cumple", "Cumple Parcialmente " y "No Cumple" para cada dominio. La *Figura 1.10* muestra un ejemplo de lo descrito anteriormente. Las tablas de valoración para el análisis de los porcentajes de todos los dominios se encuentran en el *ANEXO IV - Análisis del Estado de Cumplimiento Actual según la Norma NTE INEN-ISO-IEC 27001-2011.*

A.8 Seguridad ligada a los recursos humanos

		Si Cumple	Cumple Parcialmente	No Cumple
8.1	**Previo al empleo**			
8.1.1	Funciones y responsabilidades		1	
8.1.2	Investigación de antecedentes			1
8.1.3	Términos y condiciones de contratación	1		
8.2	**Durante el empleo**			
8.2.1	Responsabilidades de la dirección		1	
8.2.2	Concienciación, formación y capacitación en la seguridad de la información		1	
8.2.3	Proceso disciplinario			1
8.3	**Cese del empleo o cambio de puesto de trabajo**			
8.3.1	Responsabilidad del cese o cambio	1		
8.3.2	Devolución de activos		1	
8.3.3	Retirada de los derechos de acceso			1
		2	**4**	**3**

	Totales	Porcentajes
Si cumple	2	22%
Cumple Parcialmente	4	45%
No Cumple	3	33%

Figura 1.10: Ejemplo de Análisis del Estado de Cumplimiento Actual.

Fuente: Elaborado por el autor en base al ANEXO IV - Análisis del Estado de Cumplimiento Actual según la Norma NTE INEN-ISO-IEC 27001-2011

Tabulados los resultados y obteniendo los porcentajes de cumplimiento de todos los dominios, se elaboró la matriz de cumplimiento actual de acuerdo a la norma NTE INEN-ISO/IEC 27001, misma que se puede observar en la *Tabla 1.9*.

Tabla 1.9: Matriz de Estado de Cumplimiento Actual por Dominio.

Dominio	% Si Cumple	% Cumple Parcialmente	% No Cumple
A.5 Políticas de Seguridad	0%	50%	50%
A.6 Aspectos Organizativos de la Seguridad de la Información	36%	55%	9%
A.7 Gestión de Activos	40%	20%	40%
A.8 Seguridad ligada a los recursos humanos	22%	45%	33%
A. 9 Seguridad Física y Ambiental	62%	38%	0%
A.10 Gestión de Comunicaciones y Operaciones	34%	22%	44%
A.11 Control de Acceso	52%	28%	20%
A.12 Adquisición, Desarrollo y Mantenimiento de los Sistemas de información	56%	31%	13%
A.13 Gestión de Incidentes de Seguridad de la Información	20%	20%	60%
A.14 Gestión de la Continuidad del Negocio	0%	20%	80%
A.15 Cumplimiento	60%	0%	40%

Fuente: Elaborado por el autor en base al ANEXO IV - Análisis del Estado de Cumplimiento Actual según la Norma NTE INEN-ISO-IEC 27001-2011

Los porcentajes de la columna “% Si Cumple” corresponden a los objetivos de control que se cumplen en cada dominio, en otras palabras, son controles y/o procedimientos con los que la entidad cuenta. Los porcentajes de la columna “% Cumple Parcialmente” corresponden a los objetivos de control que se cumplen pero que no tienen una adecuada documentación o a su vez no cuentan con documentación. Finalmente, los porcentajes de la columna “% No Cumple” corresponden a los objetivos de control que actualmente no poseen control alguno.

A continuación, se describen los resultados obtenidos por cada dominio en relación al manejo de los objetivos de control dispuestos en la norma ISO/IEC 27001.

A.5 Políticas de Seguridad

Actualmente la entidad cuenta con el “Manual de Tecnología de la Información” dentro de este se define cierta política de seguridad únicamente como ítems mas no como documentos formales, en los que se detallen explícitamente dichas políticas, además no se realizan revisiones de los procedimientos descritos en el mencionado manual.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la *Figura 1.11*.

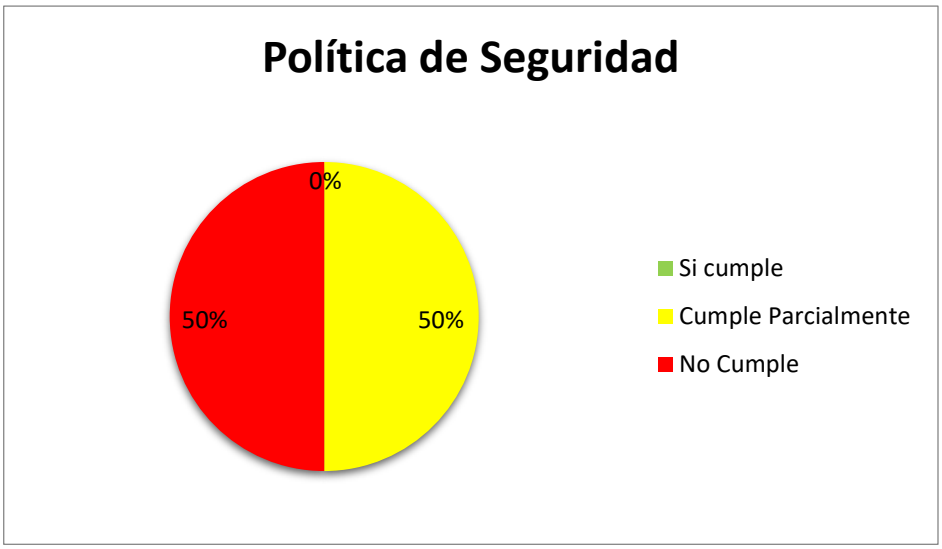

Figura 1.11: Porcentaje de cumplimiento del dominio Política de Seguridad.

Fuente: Elaborado por el autor.

A.6 Aspectos Organizativos de la Seguridad de la Información

Los altos directivos de la entidad se encuentran comprometidos con todo lo relacionado a la seguridad de la información, sin embargo, no existe un documento formal que lo sustente.

Los acuerdos de confidencialidad son firmados únicamente como parte del contrato de trabajo mas no como política de seguridad.

Al momento de contratar a terceros siempre se lo hace en base a contratos y firmas de acuerdos de confidencialidad.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la *Figura 1.12*.

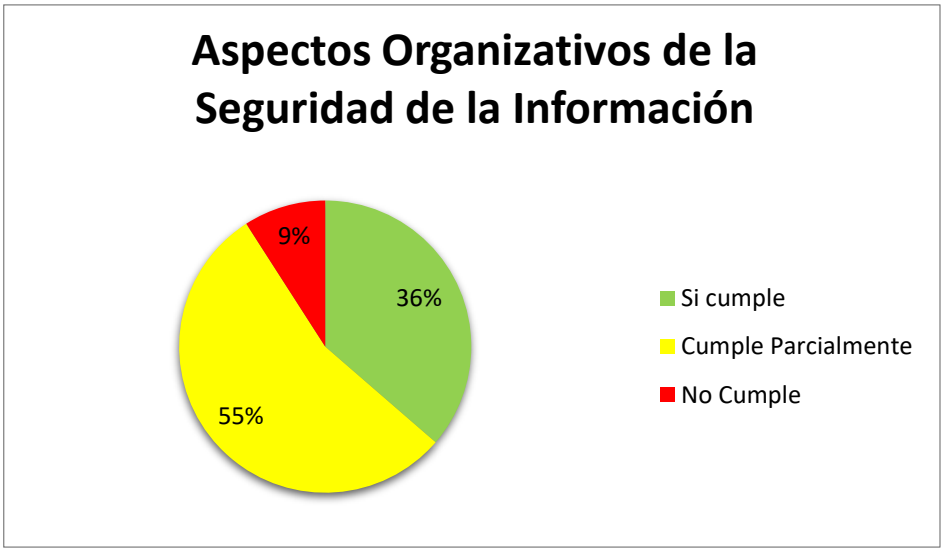

Figura 1.12: Porcentaje de cumplimiento del dominio Aspectos Organizativos de la Seguridad de la Información.

Fuente: Elaborado por el autor.

A.7 Gestión de Activos

Todos los bienes se encuentran bien identificados y el documento “inventario” es actualizado cada tres meses. Para cada bien existe su propietario y las debidas restricciones de acceso según el rol que posean, sin embargo, no existe las regulaciones necesarias para el uso aceptable de dichos activos.

No existen definidos procedimientos para etiquetado de la información, ni se tiene establecido el nivel de confidencialidad de la misma, además el manejo de esta se lo realiza de acuerdo al rol de usuario.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la *Figura 1.13*.

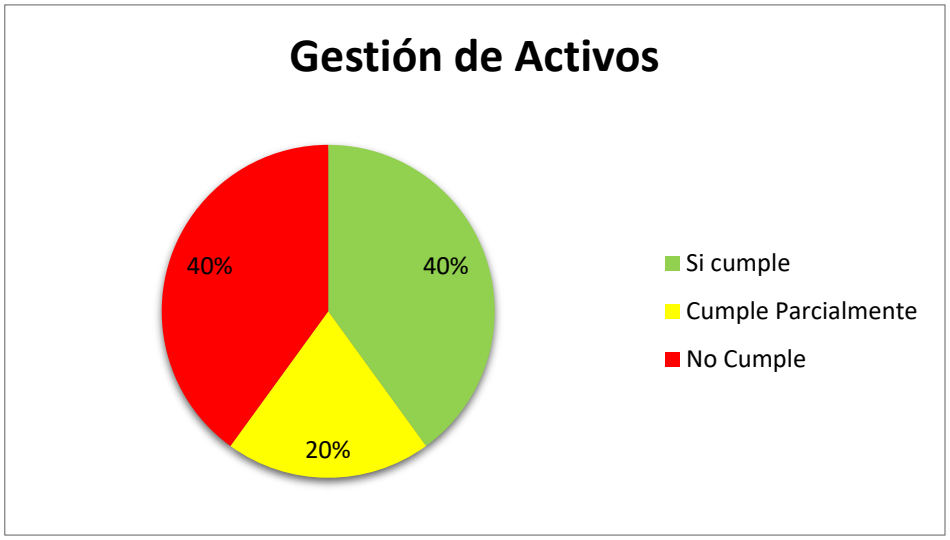

Figura 1.13: Porcentaje de cumplimiento del dominio Gestión de Activos

Fuente: Elaborado por el autor.

A.8 Seguridad ligada a los recursos humanos

El nuevo personal debe firmar el contrato laborar, mismo que contiene funciones, y responsabilidades, en este además esta detallado los acuerdos de confidencialidad. Al incorporarse a la entidad, se realiza una inducción sobre las actividades que tendrá a su cargo.

Uno de los mayores inconvenientes que se tiene cuando un empleado cesa sus funciones, es que talento humano no notifica al departamento de tecnología dicha salida por ello, aun cuando se tiene escrito en el manual la forma de devolución de activos y retirada de derechos de acceso, estos no se lo realizan en el momento adecuado.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la *Figura 1.14*.

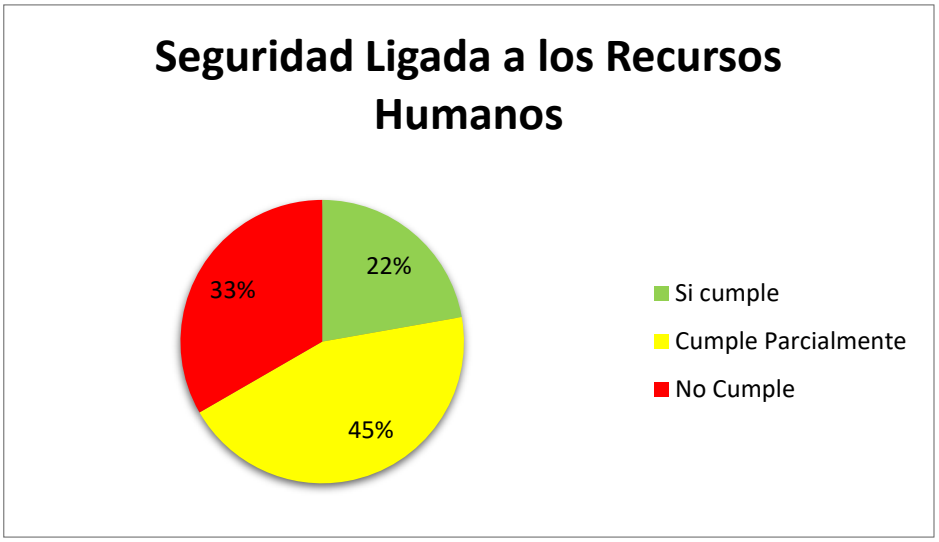

Figura 1.14: Porcentaje de cumplimiento del dominio Seguridad Ligada a los Recursos Humanos.

Fuente: Elaborado por el autor.

A. 9 Seguridad Física y Ambiental

En cuanto a la seguridad física, la entidad cuenta con accesos controlados mediante guardias de seguridad y recepcionista para el acceso al edificio, biométricos y tarjetas de acceso hacia las diferentes áreas de departamentos.
El área de servidores cuenta con puerta blindada, cerraduras reforzadas, accesos mediante biométrico y uso de tarjeta.

Todas las actividades dentro del edificio son monitoreadas mediante cámaras de seguridad y CCTV.

Todo el edificio cuenta con señal ética y rutas de evacuación definidas.

Todos los equipos tecnológicos cuentan con su respectivo seguro. Se realizan mantenimientos preventivos trimestralmente y correctivos cada que es necesario.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la *Figura 1.15*.

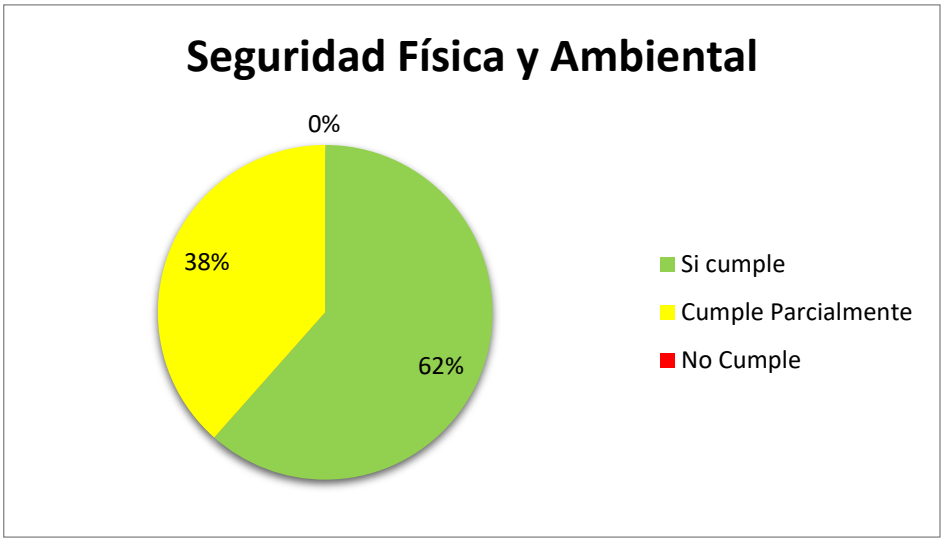

Figura 1.15: Porcentaje de cumplimiento del dominio Seguridad Física y Ambiental.

Fuente: Elaborado por el autor.

A.10 Gestión de Comunicaciones y Operaciones

Existen manuales que han sido elaborados por la necesidad o por pedidos momentáneos, es decir no se encuentran revisados y/o aprobados por alta gerencia.

Las tareas se encuentran segregadas por roles de usuarios. El ambiente de producción se encuentra separado al ambiente de pruebas.

Al tener mantenimientos trimestrales, la gestión de la capacidad en cuanto a disco, RAM y CPUs siempre tienen los criterios aceptables.

Aun cuando no se encuentra escrito la política de backups, si se realizan copias de seguridad de la información del CORE del negocio.

Existe el bloqueo del acceso al internet por medio del proxy y switch, además se manejan UTMs, firewall, antivirus y cifrados para todos los servicios de comercio electrónico.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la *Figura 1.16*.

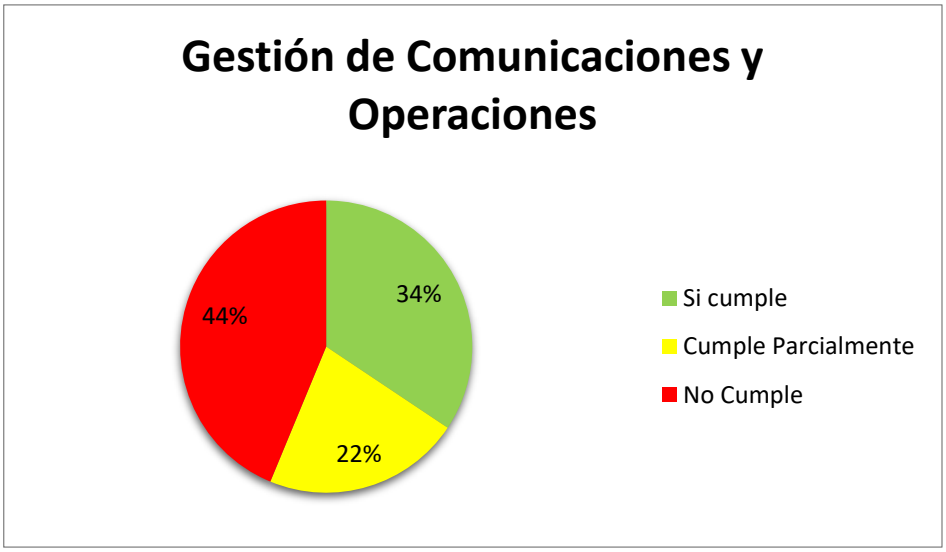

Figura 1.16: Porcentaje de cumplimiento del dominio Gestión de Comunicaciones y Operaciones.

Fuente: Elaborado por el autor.

A.11 Control de Acceso

El acceso a la información y aplicaciones depende del rol de usuario que el empleado posea. Para el ingreso tiene un máximo de intentos de contraseña de cinco oportunidades. Se tiene establecido la política de cambio de contraseñas sin embargo no existe el control periódico del cumplimiento de esta, es decir en el mayor de los casos la contraseña es la misma desde el inicio de sus funciones. La pantalla de logeo de las aplicaciones se deshabilita después de tres minutos de inactividad.

El acceso remoto únicamente tiene usuarios administradores y se utiliza VNC, VPNs, escritorios remotos y contraseñas.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la *Figura 1.17*.

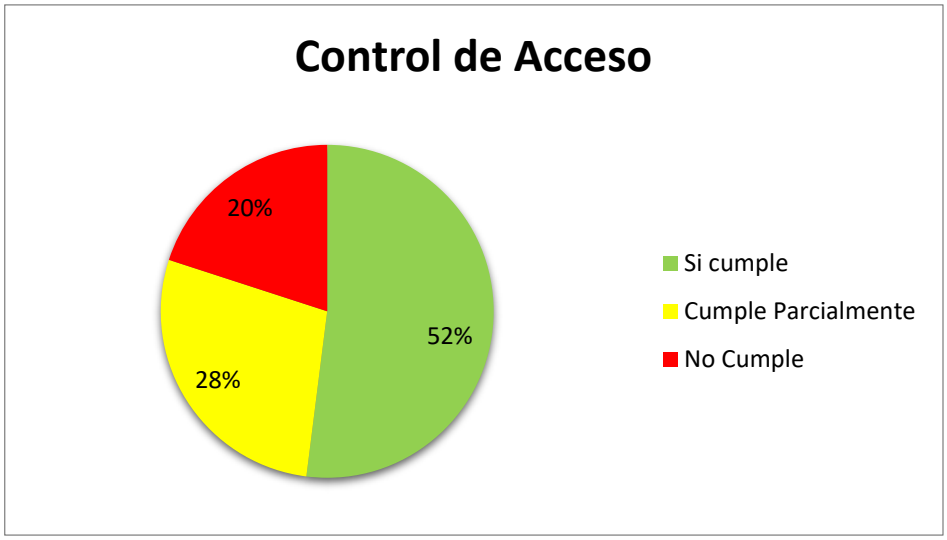

Figura 1.17: Porcentaje de cumplimiento del dominio Control de Acceso.

Fuente: Elaborado por el autor.

A.12 Adquisición, Desarrollo y Mantenimiento de los Sistemas de información

No se cuenta con el departamento de gestión de la seguridad de la información, actualmente se tiene como objetivo contratar un oficial de seguridad.

El ingreso de los datos en los aplicativos se realiza la validación correspondiente, en el caso de ingreso de datos incorrecto siempre existe el mensaje de error.

Para el control criptográfico se cuenta con un equipo dedicado al manejo de claves y encriptación de las mismas.

El control de desarrollo de software de terceros está a cargo del departamento de TI, sin embardo únicamente se firman los contratos mas no se realizan los controles en referencia a la fuga de información.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la *Figura 1.18*.

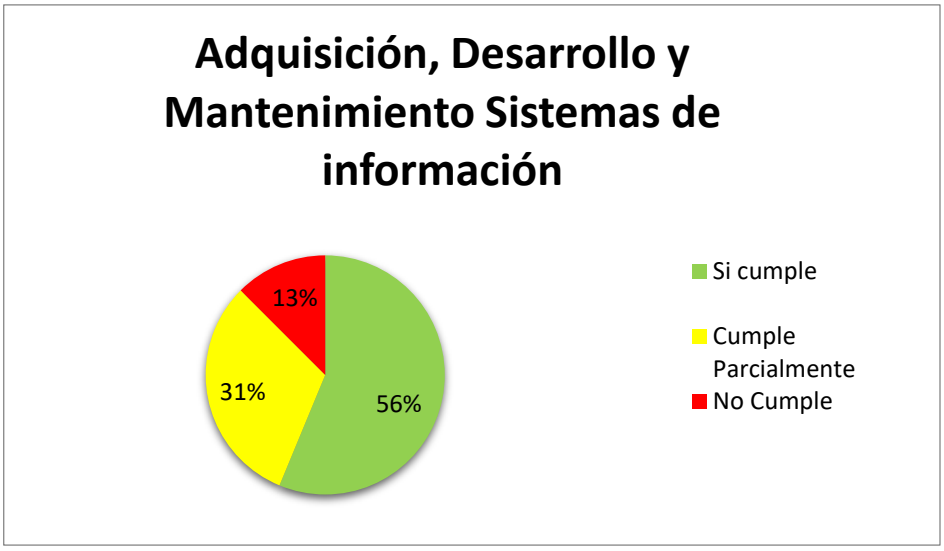

Figura 1.18: Porcentaje de cumplimiento del dominio Adquisición, Desarrollo y Mantenimiento de los Sistemas de información.

Fuente: Elaborado por el autor.

A.13 Gestión de Incidentes de Seguridad de la Información

No se tiene establecido la de gestión de incidentes. Los usuarios reportan al departamento de tecnología cuando existe una eventualidad por medio de un correo electrónico, dicho evento es tratado jerárquicamente pero no se lleva un control histórico.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la *Figura 1.19.*

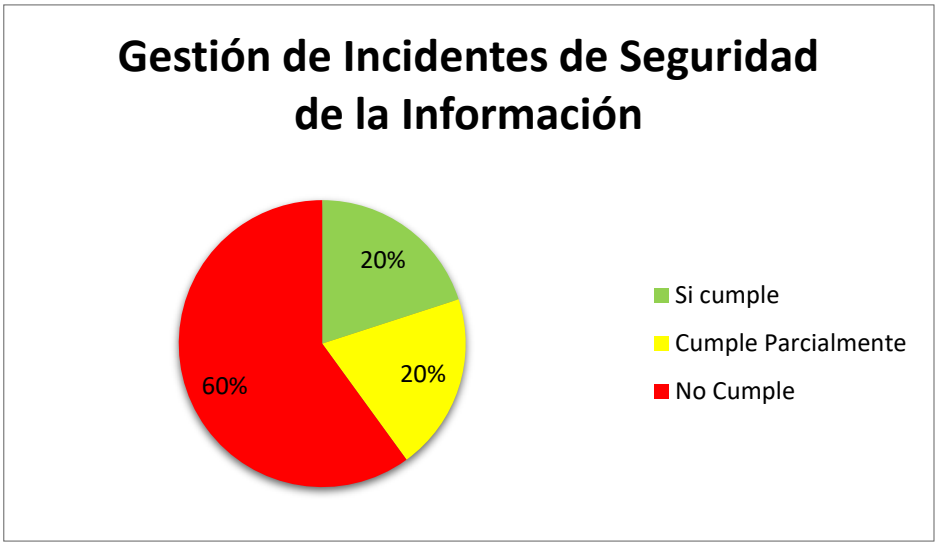

Figura 1.19: Porcentaje de cumplimiento del dominio Gestión de Incidentes de Seguridad de la Información.

Fuente: Elaborado por el autor.

A.14 Gestión de la Continuidad del Negocio

No existe un plan de continuidad del negocio ni con un plan de recuperación de desastres. Únicamente se cuenta con los backups realizados a diario para aquella información del CORE del negocio.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la *Figura 1.20*.

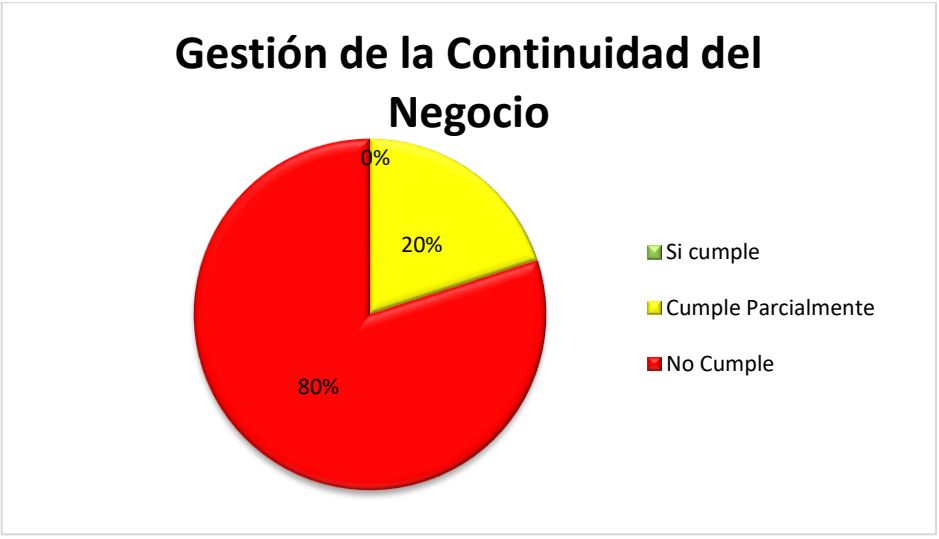

Figura 1.20: Porcentaje de cumplimiento del dominio Gestión de la Continuidad del Negocio.

Fuente: Elaborado por el autor.

A.15 Cumplimiento

Se cuenta con asistencia y asesoría jurídica para regular el cumplimiento de los parámetros legales exigidos por los entes reguladores.

En cuanto al departamento de tecnología no se han realizado auditorias en los últimos años ni se han dado los respectivos seguimientos.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la *Figura 1.21*.

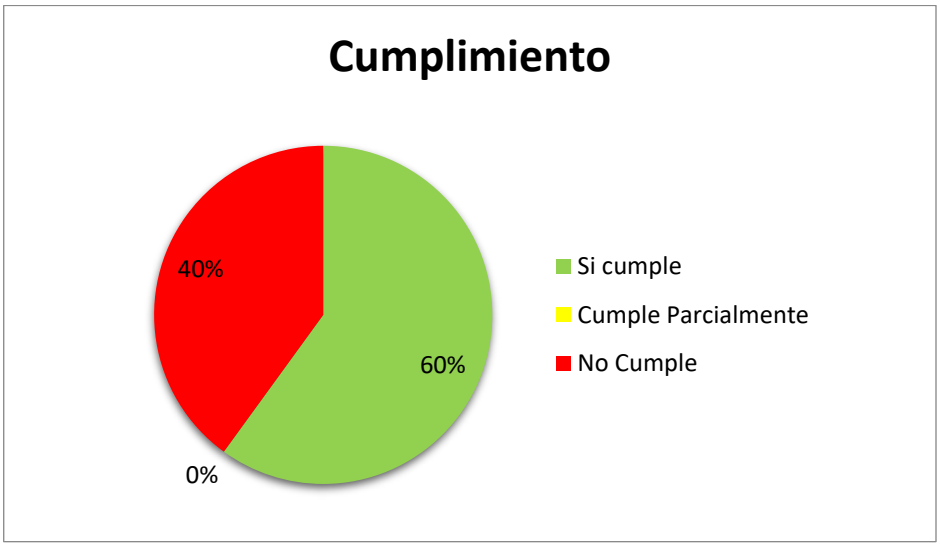

Figura 1.21: Porcentaje de cumplimiento del dominio Cumplimiento.

Fuente: Elaborado por el autor.

2 APLICACIÓN DE LA METODOLOGÍA

2.1 Análisis y evaluación de riesgos

Un análisis y evaluación de riesgos puede hacérselo de diversas formas y con diferentes grados de detalle, esto dependerá de la metodología utilizada y el valor que cada activo involucrado posee.

Esta sección está dedicada a realizar el análisis y evaluación de riesgos con el objetivo de determinar los componentes del sistema que requieren protección, identificando las vulnerabilidades que posee y las amenazas a las que está expuesto para valorar el riesgo existente. Con esta información la alta gerencia definirá el tratamiento de los riesgos encontrados (reducir, aceptar, evitar o transferir). Cabe mencionar que el análisis de riesgo es el punto central de la

definición de una estrategia de seguridad, este debe estar alineado con la visión de la entidad y su entorno operacional.

Acorde a la selección de la metodología, descrita en la sección 1.6.1 Metodologías para la evaluación y gestión de riesgos, se realizará el análisis y evaluación de riegos en base a la NIST SP 800-30, cuyo proceso se resume en la

Figura 2.1.

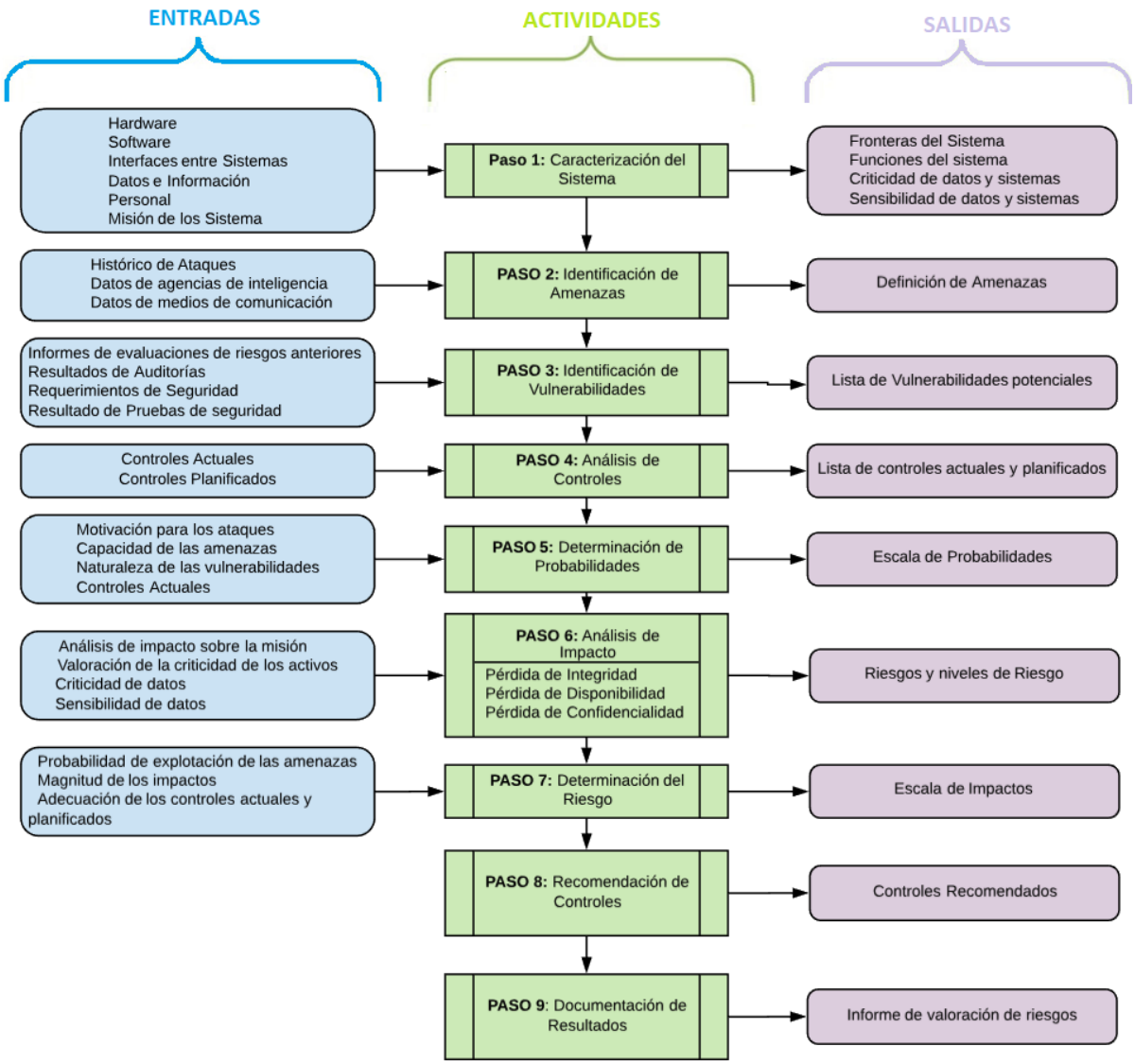

Figura 2.1: Proceso de análisis y evaluación de riesgos NIST SP 800-30

Fuente: Elaborado por el autor en base a la NIST SP 800-30.

2.2 Pasos para la evaluación de riesgos según la metodología NIST SP 800-30

A continuación, se explica cada uno de los 9 pasos que conforman el proceso de análisis y evaluación de riesgos de la NIST SP 800-30.

Paso 1: Caracterización del Sistema

Tiene como objetivo identificar, analizar y evaluar los recursos y la información necesaria para que los sistemas tecnológicos de la entidad funcionen correctamente, se establece el alcance de la evaluación del riesgo y los límites operacionales dando una mejor visión de la infraestructura tecnológica de la entidad financiera. Los activos a ser evaluados son:

- Hardware y Software
- Interfaces de sistemas
- Personas que manejan los sistemas
- Misión de los sistemas
- Datos e Información
- Topología de red actual

Paso 2: Identificación de Amenazas

El objetivo es identificar las posibles amenazas potenciales (naturales, humanas, técnicas y ambientales) que puedan dañar los activos (recursos, sistemas e información) o que interrumpan los objetivos del negocio de la entidad financiera, obteniendo un listado de aquellas amenazas que son aplicables al sistema que se está evaluando.

Paso 3: Identificación de Vulnerabilidades

En este paso se identifica las vulnerabilidades (debilidades o defectos) que tiene los activos o los controles del sistema y que podrían ser explotados por amenazas potenciales, permitiendo dañar al sistema de la entidad financiera.

Las vulnerabilidades pueden identificarse de forma manual ya sea a través del levantamiento de información (encuestas al personal o resultados anteriores) o de forma automatizada a través de alguna herramienta que determine los controles de seguridad existentes.

Paso 4: Análisis de Controles

Este paso permite efectuar un análisis en los controles existentes o previstos para su aplicación, con el fin de evitar que las amenazas potenciales se materialicen en el desarrollo de las actividades del sistema y de esta manera minimizar o eliminar la probabilidad de amenazas en la entidad financiera.

Paso 5: Determinación de Probabilidades

Tiene como objetivo determinar la probabilidad de que una vulnerabilidad sea ejercida por un evento de amenaza. La *Tabla 2.1* muestra en la columna "Valor Cualitativo" los tres valores posibles de nivel de probabilidad (Alto, Moderado y Bajo) y la columna "Descripción" describe cada nivel de probabilidad en relación a los factores que deben ser considerados (Fuente de amenaza, Naturaleza de la vulnerabilidad y Existencia y eficacia de los controles actuales), ambas columnas basadas en la Tabla 3-4 Definiciones de probabilidad de la sección 3.5 Paso 5: Determinación de Probabilidad (pág. 21) de la NIST 800-30. La columna "Valor Cuantitativo" por un lado muestra los valores (1.0, 0.5 y 0.1) que se le dan a cada nivel de probabilidad de amenaza, tal como lo asigna la NIST 800-30 en la Tabla 3-6 Matriz de nivel de riesgo (pág. 25), sin embargo, existe la posibilidad de que al momento de cuantificar la probabilidad de que una vulnerabilidad pueda materializarse se utilicen porcentajes en lugar de valores cualitativos, por ello el autor del presente proyecto de titulación conjuntamente con el jefe del Departamento de Tecnología de la entidad asignaron el rango de porcentaje(0-40%, 41-70% y 71-100%) para cada nivel de probabilidad, lo que facilitará las valoraciones el momento del análisis.

Tabla 2.1: Definición de la Probabilidad de ocurrencia de amenaza

Valor Cualitativo	Valor Cuantitativo	Descripción
Alto	1,0 (71-100) %	La amenaza es fuertemente motiva debido a que los controles para prevenir que se explote una vulnerabilidad son ineficientes.
Moderado	0,5 (41-70) %	La amenaza es motivada debido a que los controles podrían prevenir que se explote una vulnerabilidad.
Bajo	0,1 (0-40) %	La amenaza carece de motivación debido a que los controles impiden que se explote una vulnerabilidad de manera significativa.

Fuente: Elaborado por el autor en base a la NIST SP 800-30

Paso 6: Análisis de Impacto

El objetivo es la determinación del impacto resultante de que una amenaza se haya materializado debido a una vulnerabilidad. Esto se logra en base al nivel de protección requerido para mantener la disponibilidad, integridad y confidencialidad de la información. El sistema y los propietarios de información son los responsables de determinar el nivel de impacto, por ello es necesario que en este punto se realicen entrevistas a los dueños[5] de la información.

El impacto de un evento de seguridad, de acuerdo a lo expresado en la sección 3.6 Paso 6: Análisis de Impacto (pág. 22) de la NIST 800-30, dependerá de la pérdida o degradación de uno o la combinación de cualquiera de los tres objetivos de seguridad (disponibilidad, integridad y confidencialidad), por ello la *Tabla 2.2* muestra en la columna "Impacto" la descripción del impacto para cada objetivo de seguridad, la columna "Valor Cualitativo" la magnitud del impacto (Alto, Moderado y Bajo), y a su lado la columna "Valor Cuantitativo" es decir el valor numérico (3, 2 y 1) que se asignará para dicha magnitud, valores asignados por el autor del presente proyecto de titulación conjuntamente con el jefe del Departamento de Tecnología de la entidad para facilitar los cálculos puesto que la Valoración del Impacto estará dado por el promedio de los tres impactos.

Tabla 2.2: Definición del Impacto según la disponibilidad, integridad y confidencialidad

Valor Cualitativo	Valor cuantitativo	Impacto		
		Disponibilidad	Integridad	Confidencialidad
Alto	3	El impacto de la vulnerabilidad afecta severamente a la disponibilidad de la información.	El impacto de la vulnerabilidad afecta severamente a la integridad de la información.	El impacto de la vulnerabilidad afecta severamente a la confidencialidad de la información.
Moderado	2	El impacto de la vulnerabilidad afecta a la disponibilidad de la información.	El impacto de la vulnerabilidad afecta a la integridad de la información.	El impacto de la vulnerabilidad afecta a la confidencialidad de la información.
Bajo	1	El impacto de la vulnerabilidad no afecta	El impacto de la vulnerabilidad no afecta	El impacto de la vulnerabilidad no afecta

[5] Entiéndase dueño como la persona propietaria, responsable de la información dentro de la entidad financiera.

		a la disponibilidad de la información.	a la integridad de la información.	a la confidencialidad de la información.

Fuente: Elaborado por el autor en base a la NIST SP 800-30

El promedio de la magnitud del impacto en disponibilidad, integridad y confidencialidad da como resultado el valor del impacto total, mismo que será clasificado en función a lo descrito en la *Tabla 2.3*. La columna "Valor Cuantitativo" muestra el valor resultante de promedio (3, 2 y 1) de magnitudes de impacto y junto con este el valor (100, 50 y 10) que la NIST 800-30 en la Tabla 3-6 Matriz de nivel de riesgo (pág. 25) asigna a cada valor del impacto representado en la columna "Valor Cualitativo" (Alto, Moderado y Bajo). Finalmente, la columna "Descripción" describe cada nivel de impacto resultante.

Tabla 2.3: Valoración del impacto

Valor Cualitativo	Valor Cuantitativo		Descripción
Alto	3	100	La explotación de la vulnerabilidad puede provocar: • Pérdida altamente costosa de los activos críticos causando el incumplimiento significativo de la misión de la entidad. • Pérdidas humanadas o lesiones graves.
Moderado	2	50	La explotación de la vulnerabilidad puede provocar: • Perdida costosa de los activos críticos causando el incumplimiento de la misión de la entidad. • Lesiones humanas.
Bajo	1	10	La explotación de la vulnerabilidad puede provocar la pérdida de algunos activos afectando la misión de la entidad

Fuente: Elaborado por el autor en base a la NIST SP 800-30

Paso 7: Determinación del Riesgo

El propósito de este paso es la evaluación del nivel de riesgo de una amenaza para una vulnerabilidad en particular, es decir el producto entre la probabilidad de que un determinado origen de amenaza intente ejercitar una vulnerabilidad por la magnitud del impacto si una fuente de la amenaza con éxito explota una vulnerabilidad·

Para realizar dicho análisis es necesario el desarrollo de una matriz de nivel de riesgo. La *Tabla 2.4* que se presenta a continuación muestra dicha matriz de niveles de riesgo resultantes.

Tabla 2.4: Matriz de nivel de Riesgo

Probabilidad de ocurrencia de amenaza				
	Alto 1,0	Bajo 10 * 1,0 = 10	Moderado 50 * 1,0 = 50	Alto 100 * 1,0 = 100
	Moderado 0,5	Bajo 10 * 0,5 = 5	Moderado 50 * 0,5 = 25	Moderado 100 * 0,5 = 50
	Bajo 0,1	Bajo 10 * 0,1 = 1	Bajo 50 * 0,1 = 5	Bajo 100 * 0,1 = 10
		Bajo 10	Moderado 50	Alto 100
		Valoración del Impacto		

Fuente: Elaborado por el autor en base a la NIST SP 800-30(Tabla 3-6 Matriz de nivel de riesgo pág. 25)

Paso 8: Recomendación de Controles

Este paso tiene como objetivo determinar los posibles controles que podrían mitigar los riesgos identificados de manera que se logre reducir el nivel de riesgo hasta un nivel aceptable[6] para el sistema y sus datos.

Paso 9: Documentación de Resultados

Los resultados de la evaluación del riesgo deben documentarse en un informe oficial o en una reunión informativa, lo que ayudará a la alta gerencia de la entidad a la toma de decisiones sobre políticas, procedimientos, presupuestos y cambios operacionales y de gestión del sistema. Se debe recordar que este informe no presenta acusatorio sino un enfoque sistemático y analítico para evaluar el riesgo de manera que la alta dirección comprenda los riesgos y asigne recursos para reducir y corregir las posibles pérdidas.

2.3 Evaluación de riesgos según la metodología NIST SP 800-30

El objetivo de realizar una evaluación de riesgos es medir la consecuencia de los daños causados por una amenaza, las causas potenciales de los daños a la información, y qué hacer ante ello.

Para la presente evaluación se realizaron: entrevistas, revisión de documentación, levantamiento de información de la entidad, escaneo a la red (ver *ANEXO V* –

[6] Entiéndase "nivel aceptable del riesgo" al valor, que después del análisis, la entidad decide la no implementación de controles, es decir la entidad asume los daños provocados por la materialización del riesgo.

Escaneo de Vulnerabilidades con Nessus y Nmap), y evaluación de puntos débiles del entorno de seguridad de TI para los activos identificados como críticos (ver Documento - Aprobación por parte de la entidad.).

2.3.1 Caracterización del Sistema

La identificación, análisis y evaluación de la información y los recursos tecnológicos de la entidad se encuentra descrita en la sección *1.4 Reconocimiento de la Entidad Financiera.*

2.3.2 Identificación de Amenazas

Las amenazas son la causa potencial de que un incidente pueda ocasionar daños o comprometer el funcionamiento normal de los activos de la organización [14], las mismas deben ser identificadas a tiempo para evitar que ocurran y de llegar a ocurrir que el impacto no cause mayor daño.

La identificación de amenazas que podrían explotar las vulnerabilidades se realizó conjuntamente con el personal del Departamento de Tecnología de la entidad y fueron clasificadas de acuerdo a los tipos de amenazas más comunes: Amenazas Naturales, Amenazas Ambientales, Amenazas Humanas, Amenazas Técnicas y Amenazas Organizacionales, clasificación propuesta por la NIST 800-30 sección 3.2.1 Identificación de la fuente de amenaza (pág. 13). La *Tabla 2.5* muestra las amenazas identificadas de las visitas, entrevistas y conversaciones realizadas con el personal del Departamento de Tecnología de la entidad.

Tabla 2.5: Identificación de amenazas.

Tipo de amenaza	Origen de la Amenaza
Naturales	Inundaciones
	Fenómenos sísmicos
	Fenómenos volcánicos
	Tormentas eléctricas
Ambientales	Falta de energía eléctrica
	Contaminación
Humanas	Incumplimiento de las Políticas de Seguridad
	Crimen Computacional

	Usuarios y/o empleados internos descontentos, negligentes, deshonestos, cesados, etc.
	Divulgación de la información.
Técnicas	Sobrecalentamiento de equipos
	Manipulación del hardware y software
	Incumplimiento en el mantenimiento de los activos de información
Organizacionales	Falta o pérdida de personal
	Falta de capacitación al personal
	Falta e inadecuada documentación
	Falta o Insuficiente gestión de la seguridad de la información

Fuente: Elaborado por el autor.

2.3.3 Identificación de Vulnerabilidades

La vulnerabilidad es la debilidad que poseen los activos y que pueden ser aprovechadas por las amenazas [14]. Las vulnerabilidades están directamente relacionadas con las amenazas por ello para su identificación se apoyó en las visitas, entrevistas y revisión de documentos. A demás, se hizo el escaneo de vulnerabilidades, a cada uno de los servidores, con la herramienta Nessus y Nmap (ver ANEXO *V – Escaneo de Vulnerabilidades con Nessus y Nmap* y *ANEXO VI – Análisis de Vulnerabilidades*).

La *Tabla 2.6* que se presenta a continuación muestra las vulnerabilidades encontradas para cada fuente de amenaza.

Tabla 2.6: Identificación de vulnerabilidades.

Naturales	
Vulnerabilidad	**Amenaza**
No poseer un Plan de Recuperación de desastres.	Inundaciones
No poseer un Plan de Continuidad del Negocio.	Fenómenos sísmicos
No poseer un Plan de Recuperación de desastres.	
No se realizan periódicamente la validación del plan de evacuación.	
Falta de sociabilización del plan de evacuación.	
No se realizan periódicamente la validación del plan de evacuación.	Fenómenos volcánicos
No poseer un Plan de Recuperación de desastres.	
No poseer un Plan de Continuidad del Negocio.	
Falta de sociabilización del plan de evacuación.	
Falla de la planta de energía.	Tormentas eléctricas
Falla en los reguladores de voltaje.	

Falta de seguro en los equipos tecnológicos (que sobrepasan los 5 años de vida)	
Falla en los UPS	
Ambientales	
Vulnerabilidad	**Amenaza**
Falla en los UPS.	Falta de energía eléctrica
Falta de cometida eléctrica alterna	
Falta de plan de eliminación de equipos tecnológicos.	Contaminación
Humanas	
Vulnerabilidad	**Amenaza**
No existe política que exija documentar toda actividad realizada	Incumplimiento de las Políticas de Seguridad
No posee política de entrada, salida y transferencia de información	
No tienen una metodología para el ciclo de vida de desarrollo de sistemas	
No poseer un proceso de revisión de cuentas administrativas inactivas, de uso interno, de proveedores, usuario o acceso remoto.	
No poseer procedimientos de respuesta ante incidentes de manera formal	
El personal puede enviar cualquier documentación vía correo electrónico	
No poseer política de etiquetado de información	
Falla de control en accesos remotos	Crimen Computacional
Fuga de información a través del personal	Usuarios y/o empleados internos descontentos, negligentes, deshonestos, cesados, etc.
Desconocimiento y falta de sensibilización de los usuarios y de los responsables de la informática	
Falta de conciencia en la seguridad de la información por parte del personal de la entidad	
Falta de conciencia en la seguridad de la información por parte del personal de la entidad	Divulgación de la información.
Técnicas	
Vulnerabilidad	**Amenaza**
Falta de cumplimiento en cronogramas de mantenimiento	Sobrecalentamiento de equipos
Las configuraciones de algunos servicios no se realizan tomando en cuenta la seguridad de la información	Manipulación del hardware y software
No se autoriza, prueba y aprueba debidamente todo el hardware y software	
Debilidad en el diseño de los protocolos utilizados en la red	
No están identificadas las operaciones críticas y sus respaldos	Incumplimiento en el mantenimiento de los activos de información
Desactualización del software	
Organizacionales	
Vulnerabilidad	**Amenaza**
Falta de deshabilitación de cuentas de usuarios	Falta o pérdida de personal

El personal no ha recibido un adecuado entrenamiento para cumplir con sus responsabilidades de seguridad	Falta de capacitación al personal
Desconocimiento y falta de sensibilización de los usuarios y de los responsables de la informática	
Falta de conciencia en la seguridad de la información por parte del personal de la entidad	
No existe capacitación para los desarrolladores sobre seguridad	
Los controles son efectuados por la experiencia más que por una política o un procedimiento	
Falta de uso de estándares para la documentación	Falta e inadecuada documentación
No poseer documentación para la regulación de asignación de direcciones TCP/IP	
Falta de registro de actividades	
Las políticas de seguridad no se encuentran documentadas	
No tiene un plan de seguridad para la gestión de la información	
Inexistencia de un manual de políticas de seguridad de la información	
Falta de manuales de uso de herramientas	
Falta de asignación adecuada de responsabilidades en la seguridad de la información	Falta o Insuficiente gestión de la seguridad de la información
No se tiene designado formalmente a un "Responsable de Seguridad Informática"	
No tiene auditorias	
No se realizan pruebas de hackeo	
Servidores muestran versión del sistema operativo y direcciones IP	
Falta de monitorización que verifique que los controles se están realizando y que están cumpliendo el propósito para el cual fueron implementados	
Existe compartición de claves entre los usuarios	
Desconocimiento del estado actual de la seguridad de la información	
Habilitación de puertos USB	
Muestran dominios y grupos de trabajo	
No se revisan los controles de seguridad	

Fuente: Elaborado por el autor.

2.3.4 Análisis de Controles

Un control no es más que políticas, procedimientos y/o prácticas creadas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, en otras palabras, es la manera con que una entidad salvaguarda sus activos de información, modificando el nivel del riesgo [14].

Actualmente la cooperativa cuenta con los controles que se listan en la *Tabla 2.7*. Cabe mencionar que existen documentadas políticas que ayudarían a mitigar los

riesgos sin embargo estas no siempre se cumplen debido a que no existe el monitoreo y seguimiento adecuado del cumplimiento de las mismas. Así también, existen procedimientos que se llevan a cabo sin estar documentados formalmente, estas actividades de control de una u otra forma logran minimizar la probabilidad de que una amenaza ocurra. La identificación de dichos controles se basó en entrevistas, visitas, revisión de documentos y conversaciones realizadas al personal del Departamento de Tecnología.

Tabla 2.7: Controles existentes

Control existente	Observación
Sistemas contra Incendios	La entidad posee detectores de humo, extintores y la respectiva señalética en caso de una emergencia. Rutas de evacuación situadas en los puntos estratégicos.
Sistemas de enfriamiento	Todo el edificio posee aire acondicionado. El área de servidores tiene un sistema de enfriamiento propio.
Backups	Realización de backups de los seis servidores. Revisión de backups, pero sin documentación. Almacenamiento de backups fuera de la instalación matriz. Backups en sitio cerrado y a prueba de fuego. Pruebas periódicas de recuperación de aplicaciones y datos.
Sistema de Energía Alterna (UPS)	Mediante este control se garantiza el funcionamiento continuo de los servidores.
Planta de Energía	La planta de energía es activada en caso de la interrupción de la corriente primaria.
Seguridad Física	Se cuenta con guardias de seguridad en la entrada del edificio. Para el acceso del segundo piso en adelante, es necesario el registro y anuncio por medio de una secretaria. Cada área posee control de acceso mediante tarjetas o biométrico. El departamento de tecnologías y el área de servidores poseen puertas blindadas, acceso con biométrico y cerradura reforzada. Todo el edificio cuenta con Circuito cerrado de televisión-CCTV.
Seguridad en el Cableado	El cableado estructurado correctamente etiquetado.
Antivirus	La organización cuenta con contratos continuos de antivirus cada tres años.
Firewall	El bloqueo del acceso no autorizado de la red se lo realiza mediante Firewall de hardware.
UTM	Uno de los controles más importantes con los que la entidad cuenta es un UTM, mismo que tiene la función de salvaguardar toda la red.
Capacitación al personal.	Capacitación al personal sobre el manejo de correo electrónico e Internet. Inducción del manejo de los equipos tecnológicos y aplicaciones. Divulgación de medidas de seguridad
Uso de recursos de red	Restricciones de direcciones por hardware en conexión de red inalámbrica. Bloqueo de acceso a páginas no autorizadas en el Internet.
Usuario y contraseña	Roles de usuario controladas por contraseña. Protector de pantalla protegido con contraseña. Registro de intentos de autenticación fallida.
Seguros y Garantías	Los equipos (laptops, equipos de escritorio, servidores) están asegurados. Los equipos cuentan con garantía de fábrica.
Licencias	Los sistemas operativos Windows cuentan con sus respectivas licencias.

	La suite de Microsoft office cuenta con licencias, estas unicamente se encuentran instaladas en equipos de la alta gerencia, para los demás usuarios que lo requieran se encuentra instalado open office.
Detección de intrusos	Software de detección de intrusos Políticas de acceso de control remoto Software de detección y eliminación de spyware
Cifrado.	Uso de algoritmos de encriptación de datos.
Segmentación en la red	Uso de VPNs Implementación de DMZ

Fuente: Elaborado por el autor.

2.3.5 Determinación de Probabilidades

La determinación de la probabilidad de que una amenaza llegue a materializarse se lo realizará mediante los criterios definidos en la *Tabla 2.1*. En el ejemplo que se presenta a continuación (*Tabla 2.8*), la probabilidad de que un Fenómeno volcánico ocurra en Ambato, ciudad donde se encuentra la entidad analizada, es alto por lo que su valoración es 1,0.

Tabla 2.8: Ejemplo Determinación de Probabilidad de la Amenaza.

Tipo de amenaza	Amenaza	Probabilidad de la amenaza	
Naturales	Fenómenos volcánicos	**ALTO**	1,0

Fuente: Elaborado por el autor.

La determinación de probabilidad para cada uno de las amenazas se encuentra en la sección 2.3.7 Determinación del Riesgo.

2.3.6 Análisis de Impacto

El impacto es el costo que una empresa tiene por un incidente, pudiendo ser o no en términos financieros es decir pérdida de reputación, implicaciones legales, etc. [14].

La valoración del impacto que una amenaza ejerce sobre un activo en específico se lo realizará mediante los criterios definidos en la *Tabla 2.2*, es decir el promedio del impacto (*Tabla 2.3*) que puede sufrir el activo en términos de confidencialidad (C), integridad (I) y disponibilidad (D). En el ejemplo que se presenta a continuación (*Tabla 2.9*), el impacto en la disponibilidad de los servicios, de llegar a materializarse un fenómeno volcánico y no poseer un plan de continuidad de negocio, es alto por lo que su valoración es 3, mientras que la integridad y la confidencialidad no se verían afectadas por lo que el impacto es bajo, es decir con una valoración de 1

para cada criterio, por lo tanto el impacto de la vulnerabilidad “No poseer un Plan de Continuidad del Negocio” ante la amenaza “Fenómenos volcánicos” es 1,67 ≈ 2, que se obtiene del promedio de los tres impactos (3+1+1)/3, 2 es Moderado por lo tanto toma el valor de 50.

Tabla 2.9: Ejemplo Análisis de Impacto de la Vulnerabilidad.

Tipo de amenaza	Amenaza	Vulnerabilidad	Impacto			Impacto de la vulnerabilidad		
			D	I	C			
Naturales	Fenómenos volcánicos	No poseer un Plan de Recuperación de desastres.	3	1	1	1,67 ≈ 2	**MODERADO**	50

Fuente: Elaborado por el autor.

El análisis de impacto para cada vulnerabilidad se encuentra en la sección 2.3.7 Determinación del Riesgo.

2.3.7 Determinación del Riesgo

Un riesgo es la posibilidad de que una amenaza en concreto explote una vulnerabilidad causando pérdida o daño en un activo de información. Es decir, es la combinación de la probabilidad de un evento y sus consecuencias [14].

La *Tabla 2.10* que se presenta a continuación muestra los resultados obtenidos de la determinación del riesgo para el tipo de amenaza “Naturales”. La matriz de riesgos completa se encuentra en el *ANEXO VII - Matriz de riesgos*.

Tabla 2.10: Ejemplo Matriz de Riesgos.

Tipo de amenaza	Amenaza	Vulnerabilidad	Probabilidad de ocurrencia de la amenaza		Impacto			Impacto de la vulnerabilidad			Nivel de Riesgo		Id Riesgo
					D	I	C						
Naturales	Inundaciones	No poseer un Plan de Recuperación de desastres.	0,5	MODERADO	3	1	1	2	50	MODERADO	25	MODERADO	R01
	Fenómenos sísmicos	No poseer un Plan de Continuidad del Negocio.	1,0	ALTO	3	1	1	2	50	MODERADO	50	MODERADO	R02
		No poseer un Plan de Recuperación de desastres.			3	1	1	2	50	MODERADO	50	MODERADO	R03
		No se realizan periódicamente la validación del plan de evacuación.			1	1	1	1	10	BAJO	10	BAJO	R04
		Falta de sociabilización del plan de evacuación.			1	1	1	1	10	BAJO	10	BAJO	R05
	Fenómenos volcánicos	No se realizan periódicamente la validación del plan de evacuación.	1,0	ALTO	1	1	1	1	10	BAJO	10	BAJO	R06
		No poseer un Plan de Recuperación de desastres.			3	1	1	2	50	MODERADO	50	MODERADO	R07

		No poseer un Plan de Continuidad del Negocio.			3	1	1	2	50	MODERADO	50	MODERADO	R08
		Falta de sociabilización del plan de evacuación.			1	1	1	1	10	BAJO	10	BAJO	R09
	Tormentas eléctricas	Falla de la planta de energía.	0,1	BAJO	3	1	1	2	50	MODERADO	5	BAJO	R10
		Falla en los reguladores de voltaje.			3	1	1	2	50	MODERADO	5	BAJO	R11
		Falta de seguro en los equipos tecnológicos (que sobrepasan los 5 años de vida)			2	1	1	1	10	BAJO	1	BAJO	R12
		Falla en los UPS			2	1	1	1	10	BAJO	1	BAJO	R13

Fuente: Elaborado por el autor.

Una vez que se tiene la matriz de riesgo se procede a realizar la *Figura 2.2* (tomando en cuenta únicamente la columna “Nivel de Riesgo”) en la cual se diferencia los porcentajes por nivel de riesgo que posee la entidad. El color rojo representa el nivel de riesgo alto, el color amarillo el nivel de riesgo moderado y el verde el nivel de riesgo bajo.

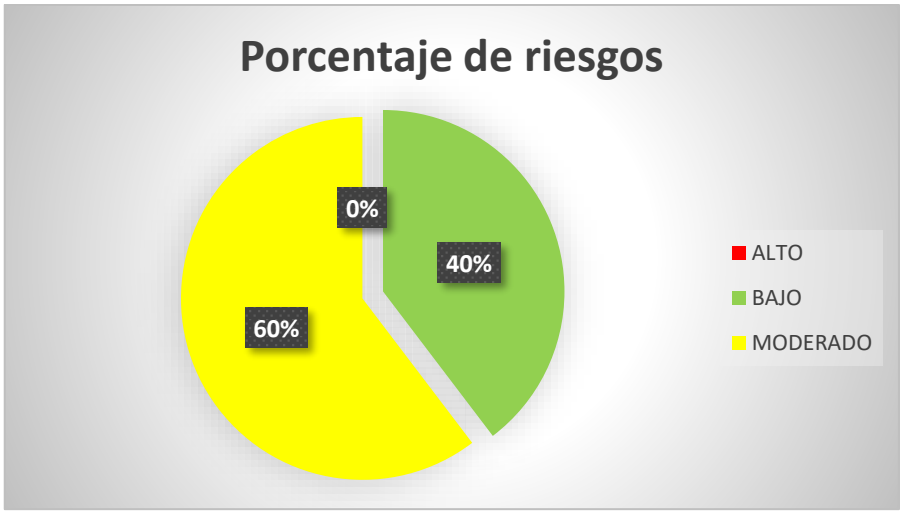

Figura 2.2: Porcentaje de riesgos encontrados

Fuente: Elaborado por el autor.

Cabe mencionar, que como se puede observar no existe ningún riesgo con un nivel de criticidad alto.

De manera similar se realiza la *Figura 2.3* en la que se muestra los riesgos por tipo de amenaza.

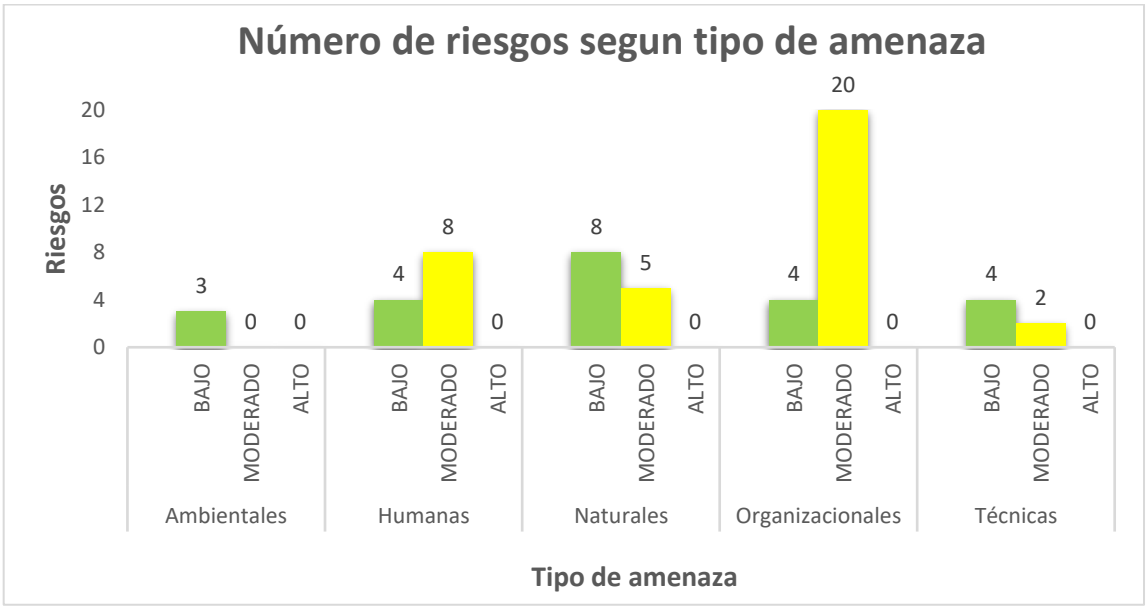

Figura 2.3: Número de riesgos según tipo de amenaza.

Fuente: Elaborado por el autor.

Queda claro que el mayor número de riesgos se concentra en aquellas amenazas organizacionales, seguida de las humanas y naturales.

2.3.8 Recomendación de Controles

La recomendación de controles es uno de los pasos del plan de tratamiento de riesgos, mismo que consiste en:

Paso 1: Definir la forma en que se realizará el tratamiento de riesgos, es decir determinar la acción que se llevará a cabo frente a los riesgos obtenidos de acuerdo a la estrategia de la entidad, dichas acciones serán:

- **Aceptar:** aquellos riesgos que den como resultado nivel BAJO serán aceptados, es decir no es necesario la implementación de controles inmediatos para estos riesgos. La implementación de controles para estos riesgos podrá ser tomados en cuenta después de haber reducido los riesgos de nivel moderado y alto.
- **Reducir:** aquellos riesgos que den como resultado nivel MODERADO y ALTO serán mitigados por medio de la implementación de controles, misma que tomará un tiempo no mayor a seis meses.

Paso 2: Clasificar los riesgos de nivel MODERADO y ALTO para cada criterio de seguridad de la NIST 800-30 según el área. La *Tabla 2.11* muestra dicha clasificación.

Tabla 2.11: Criterios de seguridad

Área de seguridad	Criterios de seguridad	Riesgos
Seguridad Administrativa	Asignación de responsabilidades y separación de obligaciones para Seguridad de la Información	R36, R37, R38, R39, R40, R48, R49, R50, R52, R53, R54, R55, R56, R58
	Continuidad del negocio	R01, R02, R03, R07, R08
	Revisión Periódica de los controles de Seguridad	R42, R43, R44, R45, R46, R48, R49, R50, R52, R53, R54, R55, R56, R58
	Evaluación de Riesgos	R01, R02, R03, R07, R08
	Plan de seguridad del sistema	R17, R18, R19, R20, R22, R23, R42, R43, R44, R45, R46, R48,

		R49, R50, R52, R53, R54, R55, R56, R58
	Compromiso con la seguridad de la información.	R48, R49, R50, R52, R53, R54, R55, R56, R58
	Capacitación Técnica y de seguridad.	R28, R36, R37, R38, R39, R40
	Controles de seguridad personal, mínimos privilegios y acorde al cargo o funciones de la persona	R35
Seguridad Operacional	Distribución de datos externos y etiquetado	R17, R18, R19, R20, R22, R23
	Control de las condiciones ambientales (humedad y temperatura)	R01, R02, R03, R07, R08
	Protección de Estaciones de trabajo, laptops y computadoras personales independientes.	R18, R30, R32
	Control de Virus o Vulnerabilidades técnicas	R17, R18, R19, R20, R22, R23
Seguridad Técnica	Comunicaciones (por ejemplo, acceso telefónico, interconexión de sistemas, enrutadores)	R30, R32
	Identificación y Autenticación	R24, R48, R49, R50, R52, R53, R54, R55, R56, R58
	Configuración de la seguridad en los sistemas tecnológicos de la información	R42, R43, R44, R45, R46
	Auditoria del Sistema	R48, R49, R50, R52, R53, R54, R55, R56, R58

Fuente: Elaborado por el autor en base a la NIST SP 800-30

Paso 3: Seleccionar los controles que permitirán mitigar los riesgos cuya acción es reducir, dichos controles se los tomará de la NTE INEN-ISO/IEC 27002. Esta selección será realizada en base a los resultados obtenidos de la determinación del riesgo y conjuntamente con el personal del departamento de Tecnología con el objetivo de que se adapten de mejor manera a las necesidades de la entidad.

Tabla 2.12: Selección de controles

Amenaza	Vulnerabilidad	Nivel de Riesgo		Id Riesgo	Control Seleccionado
Inundaciones	No poseer un Plan de Recuperación de desastres.	25	MODERADO	R01	A.9.1.4 Protección contra las amenazas externas y de origen ambiental. A.14.1.2. Continuidad del negocio y evaluación de riesgos. A.14.1.3. Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información.
Fenómenos sísmicos	No poseer un Plan de Continuidad del Negocio.	50	MODERADO	R02	A.9.1.4 Protección contra las amenazas externas y de origen ambiental. A.14.1.2. Continuidad del negocio y evaluación de riesgos. A.14.1.3. Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información.
	No poseer un Plan de Recuperación de desastres.	50	MODERADO	R03	
Fenómenos volcánicos	No poseer un Plan de Recuperación de desastres.	50	MODERADO	R07	A.9.1.4 Protección contra las amenazas externas y de origen ambiental. A.14.1.2. Continuidad del negocio y evaluación de riesgos. A.14.1.3. Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información.
	No poseer un Plan de Continuidad del Negocio.	50	MODERADO	R08	
Incumplimiento de las Políticas de Seguridad	No existe política que exija documentar toda actividad realizada	50	MODERADO	R17	A.5.1.1 Documento de la política de seguridad de la información. A.7.2.2 Etiquetado y manejado de la información. A.9.2.6 Reutilización o retirada segura de equipos. A.9.2.7 Retirada de materiales propiedad de la organización. A.10.7.3 Procedimientos de manipulación de la información A.12.4.1 Control del software en explotación.
	No posee política de entrada, salida y transferencia de información	50	MODERADO	R18	
	No tienen una metodología para el ciclo de vida de desarrollo de sistemas	50	MODERADO	R19	
	No poseer un proceso de revisión de cuentas administrativas inactivas, de uso interno, de proveedores, usuario o acceso remoto.	50	MODERADO	R20	
	El personal puede enviar cualquier documentación vía correo electrónico	50	MODERADO	R22	
	No poseer política de etiquetado de información	50	MODERADO	R23	

Crimen Computacional	Falla de control en accesos remotos	50	MODERADO	R24	A.11.4.2 Autenticación de usuario para conexiones externas.
Divulgación de la información	Falta de conciencia en la seguridad de la información por parte del personal de la entidad	25	MODERADO	R28	A.8.2.2 Concienciación, formación y capacitación en seguridad de la información.
Manipulación del hardware y software	Las configuraciones de algunos servicios no se realizan tomando en cuenta la seguridad de la información	25	MODERADO	R30	A.7.1.3 Uso aceptable de los activos. A.10.6.1 Controles de red.
	Debilidad en el diseño de los protocolos utilizados en la red	25	MODERADO	R32	
Falta o pérdida de personal	Falta de deshabilitación de cuentas de usuarios	50	MODERADO	R35	A.8.3.3 Retiro de los derechos de acceso.
Falta de capacitación al personal	El personal no ha recibido un adecuado entrenamiento para cumplir con sus responsabilidades de seguridad	25	MODERADO	R36	A.8.2.1 Responsabilidades de la dirección. A.8.2.2 Concienciación, formación y capacitación en seguridad de la información. A.13.1.2 Notificación de los puntos débiles de seguridad.
	Desconocimiento y falta de sensibilización de los usuarios y de los responsables de la informática	25	MODERADO	R37	
	Falta de conciencia en la seguridad de la información por parte del personal de la entidad	25	MODERADO	R38	
	No existe capacitación para los desarrolladores sobre seguridad	25	MODERADO	R39	
	Los controles son efectuados por la experiencia más que por una política o un procedimiento	25	MODERADO	R40	
Falta e inadecuada documentación	No poseer documentación para la regulación de asignación de direcciones TCP/IP	50	MODERADO	R42	A.5.1.1 Documento de la política de seguridad de la información. A.5.1.2 Revisión de la política de la seguridad de la información. A.10.1.1 Documentación de los procedimientos de operación.
	Falta de registro de actividades	50	MODERADO	R43	
	Las políticas de seguridad no se encuentran documentadas	50	MODERADO	R44	
	No tiene un plan de seguridad para la gestión de la información	50	MODERADO	R45	

	Inexistencia de un manual de políticas de seguridad de la información	50	MODERADO	R46	
Falta o Insuficiente gestión de la seguridad de la información	Falta de asignación adecuada de responsabilidades en la seguridad de la información	50	MODERADO	R48	A.5.1.1 Documento de la política de seguridad de la información. A.5.1.2 Revisión de la política de la seguridad de la información. A.6.1.1 Compromiso de la Dirección con la seguridad de la información. A.6.1.2 Coordinación de la seguridad de la información. A.6.1.3 Asignación de responsabilidades relativas a la seguridad de la información. A.6.1.8 Revisión independiente de la seguridad de la información. A.11.2.3 Gestión de contraseñas de usuario. A.11.3.1 Uso de contraseñas. A.15.2.1 Cumplimiento de las políticas y normas de seguridad A.15.3.1 Controles de auditoría de los sistemas de información.
	No se tiene designado formalmente a un "Responsable de Seguridad Informática"	50	MODERADO	R49	
	No tiene auditorias	50	MODERADO	R50	
	Servidores muestran versión del sistema operativo y direcciones IP	50	MODERADO	R52	
	Falta de monitorización que verifique que los controles se están realizando y que están cumpliendo el propósito para el cual fueron implementados	50	MODERADO	R53	
	Existe compartición de claves entre los usuarios	50	MODERADO	R54	
	Desconocimiento del estado actual de la seguridad de la información	50	MODERADO	R55	
	Habilitación de puertos USB	50	MODERADO	R56	
	No se revisan los controles de seguridad	50	MODERADO	R58	

Fuente: Elaborado por el autor.

Paso 4: Mapear cada control seleccionado en el Paso 3 con los criterios de seguridad de la NIST 800-30.

Tabla 2.13: Mapeo de los controles seleccionados de la NTE INEN-ISO/IEC 27001 con los Criterios de Seguridad de la NIST 800-30

Control ISO 27002		Área de Seguridad			Criterio de Seguridad
		Seguridad Administrativa	Seguridad Operacional	Seguridad Técnica	
A.5.1.1	Documento de la política de seguridad de la información.	X			Plan de seguridad del sistema
A.5.1.2	Revisión de la política de la seguridad de la información.	X			Revisión periódica de los controles de seguridad
A.6.1.1	Compromiso de la Dirección con la seguridad de la información.	X			Compromiso de la seguridad de la información.
A.6.1.2	Coordinación de la seguridad de la información.	X			Compromiso de la seguridad de la información.
A.6.1.3	Asignación de responsabilidades relativas a la seguridad de la información.	X			Asignación de responsabilidades y separación de obligaciones para seguridad de la información
A.6.1.8	Revisión independiente de la seguridad de la información.	X			Revisión periódica de los controles de seguridad
A.7.1.3	Uso aceptable de los activos.		X		Protección de estaciones de trabajo, Laptops y computadores personales independientes
A.7.2.2	Etiquetado y manejado de la información.		X		Distribución de datos externos y etiquetado
A.8.2.1	Responsabilidades de la dirección.	X			Asignación de responsabilidades y separación de obligaciones para seguridad de la información
A.8.2.2	Concienciación, formación y capacitación en seguridad de la información.	X			Capacitación técnica y de seguridad
A.8.3.3	Retiro de los derechos de acceso.	X			Control de seguridad personal, mínimos privilegios y acorde al cargo o funciones de la persona
A.9.1.4	Protección contra las amenazas externas y de origen ambiental.		X		Control de las condiciones ambientales (Humedad y Temperatura)
A.9.2.6	Reutilización o retirada segura de equipos.		X		Protección de Estaciones de trabajo, laptops y computadoras personales independientes.

A.9.2.7.	Retirada de materiales propiedad de la organización.		X		Protección de Estaciones de trabajo, laptops y computadoras personales independientes.
A.10.1.1	Documentación de los procedimientos de operación.			X	Configuración de la seguridad en los sistemas Tecnológicos de la información
A.10.6.1	Controles de red.			X	Comunicaciones (por ejemplo, acceso telefónico, interconexión del sistema, enrutadores)
A.10.7.3	Procedimientos de manipulación de la información		X		Distribución de datos externos y etiquetado
A.11.2.3	Gestión de contraseñas de usuario.			X	Identificación y Autenticación
A.11.3.1	Uso de contraseñas.			X	Identificación y Autenticación
A.11.4.2	Autenticación de usuario para conexiones externas.			X	Identificación y Autenticación
A.12.4.1	Control del software en explotación.		X		Control de virus o vulnerabilidades técnicas
A.13.1.2	Notificación de los puntos débiles de seguridad.	X			Capacitación Técnica y de seguridad.
A.14.1.2	Continuidad del negocio y evaluación de riesgos.	X			Evaluación de riesgos Continuidad del negocio
A.14.1.3	Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información.	X			Continuidad del Negocio
A.15.2.1	Cumplimiento de las políticas y las normas de la seguridad.	X			Revisión periódica de los controles de seguridad
A.15.3.1	Controles de auditoría de los sistemas de información.			X	Auditoria del sistema

Fuente: Elaborado por el autor.

Paso 5: Realizar la propuesta de implementación de controles aplicables en la entidad.

El establecer el plan de acción a seguir, permitirá gestionar los riesgos identificados mediante la aplicación de los controles seleccionados, las acciones del personal y la disponibilidad de la infraestructura tecnológica, conjuntamente con la estrategia administrativa que evalúe la puesta en marcha del tratamiento para los riesgos identificados.

Los riesgos con acción de tratamiento REDUCIR requieren atención inmediata y seguimiento de los altos directivos quienes deben priorizar y establecer dicho tratamiento de acuerdo al costo/beneficio de implementar el control en beneficio de la entidad, por esta razón la propuesta de implementación queda a criterio netamente del departamento de Tecnología y los altos directivos.

2.3.9 Documentación de Resultados

Ver ANEXO IX – Informe de Valoración de Riesgo.

3 RESULTADOS Y DISCUSIÓN

3.1 Plan de Gestión de Seguridad de la Información

El Plan de Gestión de Seguridad de la Información se conformará de acuerdo a las necesidades de la entidad, tomando en cuenta la información recopilada en los capítulos anteriores y basándose en la norma NTE INEN ISO/IEC 27001:2011.

Un Sistema de Gestión de Seguridad de la Información (SGSI) es el diseño, implementación y mantenimiento del conjunto de procesos para la gestión eficiente de la información, asegurando la confidencialidad, integridad y disponibilidad de los activos de información y minimizando los riesgos asociados a la seguridad de la información.

La familia ISO/IEC 27000 propone un modelo para el desarrollo y mantenimiento del SGSI, basado en el PDCA (Plan–Do–Check–Act) de mejora continua. La *Figura 3.1* muestra el modelo PDCA aplicado a los procesos del SGSI.

- **Planificar (creación del SGSI):** se deben definir políticas, objetivos, procesos y procedimiento del SGSI para la gestión del riesgo y mejora de la seguridad de la información.
- **Hacer (implementación y operación del SGSI):** implementación y operación de las políticas, controles, procesos y procedimientos planteados en la planificación.
- **Verificar (supervisión y revisión del SGSI):** evaluación y medición del rendimiento del proceso en relación a las políticas, objetivos y experiencia del SGSI. Además, se debe informar los resultados a la dirección para la respectiva revisión.
- **Actuar (mantenimiento y mejora del SGSI):** en base a los resultados de la auditoria interna del SGSI y los comentarios de la revisión de la dirección, se deben adoptar medidas correctivas y preventivas para lograr la mejora continua del SGSI.

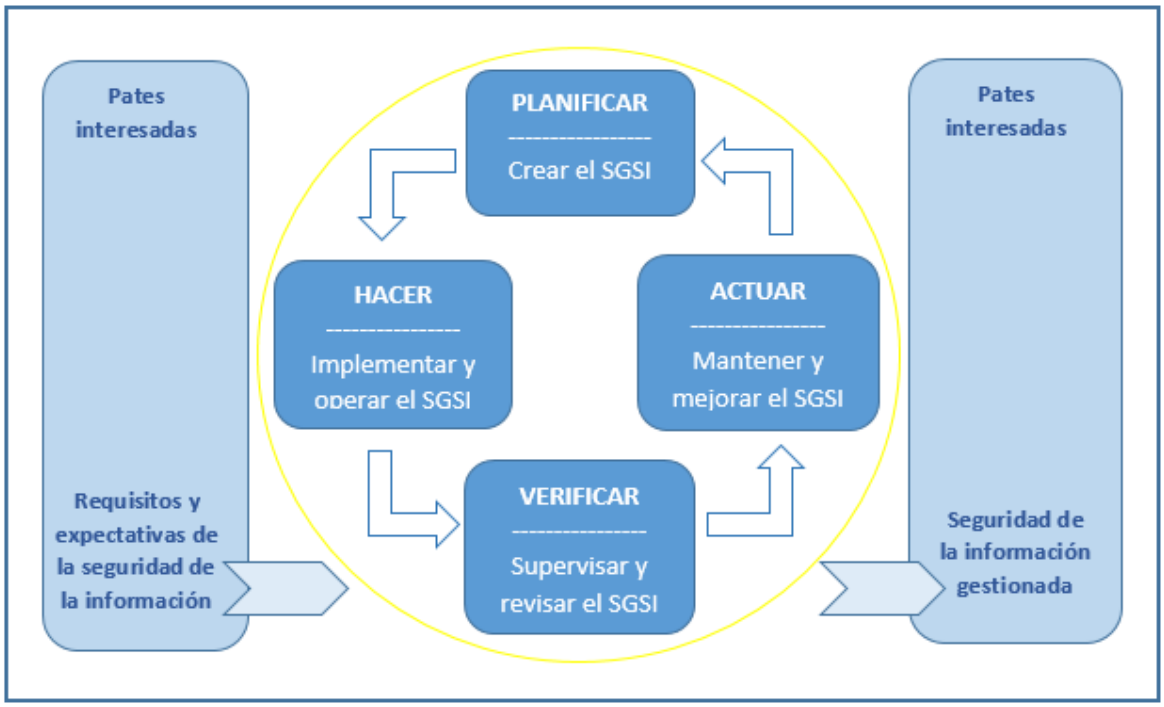

Figura 3.1: Modelo PDCA aplicado a los procesos del SGSI.

Fuente: Elaborado por el autor en bases a NTE-ISO-IEC 27001-2011.

3.2 Alcance y Limites de SGSI

El alcance del plan de gestión de seguridad de la información para la cooperativa de ahorro y crédito Kullki Wasi." fue definido junto con la entidad y abarca el análisis de los activos considerados como crítico (servidores: MicroScore, Base de Datos, Ventanillas Móviles, Cajeros Automáticos, Aplicaciones y Contingencias) dentro de la cooperativa y en lo que se refiere a la infraestructura tecnológica se evaluó el Departamento de Tecnología ubicado en la matriz en la ciudad de Ambato.

Se excluye una evaluación en sitio a la infraestructura de Hosting y Housing que posee la entidad, así como también a la infraestructura tecnológica de proveedores externos.

Los aspectos considerados en el proyecto de titulación abarcan los criterios de seguridad propuestos por la NIST 800-30 (Administrativa, Operacional y Técnica).

3.3 Elaboración del Plan de Gestión de Seguridad de la Información.

En el presente proyecto de titulación únicamente se llevará acabo la etapa PLANIFICAR puesto que en el alcance no se especifica llevar a cabo las demás etapas (hacer, verificar y actuar).

La etapa de planificación consiste en definir políticas, objetivos, procesos y procedimientos del SGSI para la gestión del riesgo y la mejora de la seguridad de la información [14]. Esta etapa tiene cinco fases en las cuales se deben ir generando documentación para llevar acabo el SGSI. La *Tabla 3.1* contiene cada fase, los principales documentos de salida y la documentación generada a lo largo de la realización de este proyecto de titulación.

Tabla 3.1: Fases y Entregables del Plan de Seguridad de la Información.

Fase	Objetivo	Documentación establecida por la ISO 27001	Documentación generada en el proyecto de titulación
Obtención de aprobación de la Dirección para la iniciación de un proyecto de SGSI	Obtener la aprobación y el compromiso de la Dirección para iniciar el proyecto de SGSI.	Aprobación de la dirección para la iniciación del Proyecto de SGSI.	Documento - Aprobación por parte de la entidad.
Definición del Alcance del SGSI y de la Política del SGSI.	Definir el alcance, los límites detallados y políticas del SGSI	El alcance y límites del SGSI. Política del SGSI	Documento - Plan de trabajo de titulación – Proyecto integrador. Sección 3.2 Alcance y Limites del SGSI Anexo XXX – Políticas del SGSI.
Realización del Análisis de la Organización.	Definir los requerimientos pertinentes para el SGSI. Identificar los activos de Información. Obtener el estado actual de la seguridad de la información	Requerimientos de seguridad de la información. Activos de Información. Resultado de la evaluación de la seguridad de la información	Sección 1.4.4.4 Infraestructura. Sección 1.6. Situación actual de la seguridad de la Información. Anexo II – Resultados de Medida de Defensa MSAT Anexo III – Manejo de la Seguridad de la Información NTE INEN-ISO-IEC 27001-2011 Auditoria Check List Anexo IV - Análisis del Estado de Cumplimiento Actual según la Norma NTE INEN-ISO-IEC 27001-2011 Sección 2.3.2 Identificación de Amenazas Sección 2.3.3 Identificación de vulnerabilidades Anexo V – Escaneo de Vulnerabilidades con Nessus y Nmap Anexo VI – Análisis de Vulnerabilidades. Sección 2.3.7 Determinación del riesgo. Anexo VII – Matriz de Riesgos. Anexo VIII- Documento Declaración de Aplicabilidad.
Realización de la Evaluación del Riesgo y planificación del Tratamiento del Riesgo.	Definir la metodología de evaluación de riesgo; identificar, analizar y evaluar los riesgos de seguridad de la información y seleccionar las opciones de tratamiento del riesgo y los controles.	Aprobación escrita de la dirección para la implementación del SGSI. Plan de tratamiento de riesgo. Declaración de aplicabilidad, incluyendo los objetivos y los controles seleccionados.	El presente proyecto de titulación solo contempla la fase de planificación del SGSI. Sección 2.3.8 Recomendación de controles. Anexo VIII- Documento Declaración de Aplicabilidad.
Diseño del SGSI.	Completar el plan de SGSI mediante el diseño de la seguridad organizacional basándose en las opciones de tratamiento de riesgos, los requerimientos de registros y documentación y el diseño de controles	Plan final de implementación del proyecto SGSI.	Sección 3.4 Guía de Implementación. Sección 3.5 Aplicabilidad de la propuesta

Fuente: Elaborado por el autor en base a la ISO/IEC 27003.

Además, en esta etapa la norma ISO/IEC 27001 establece la elaboración de los siguientes documentos:

- Procedimiento para control de documentos y registros. (ver *ANEXO P01 - Documento de procedimiento para control de documentos y registros*)
- Política del SGSI (ver *ANEXO P02 - Política de SGSI*)
- Declaración de Aplicabilidad (ver *Anexo VIII – Declaración de Aplicabilidad*)

Por otro lado, una vez seleccionado los controles a implementarse para ayudar a reducir los riesgos, es necesario la elaboración de algunos documentos que formarán parte del plan de gestión de seguridad de la información, los cuales serán también entregables para este proyecto y son:

- *ANEXO P03- Política Uso aceptable de los activos*
- *ANEXO P04 - Política de Contraseñas*
- *ANEXO P05- Política de Clasificación y Manejo de la Información*
- *ANEXO P06 - Política de Capacitación, Sensibilización y Comunicación de seguridad de la información*
- *ANEXO P07 - Política de Eliminación y Reutilización de Equipos*
- *ANEXO P08 - Política de Instalación y Uso de Software*
- *ANEXO P09 - Política de Retiro de los Derechos de Acceso*
- *ANEXO P10- Política de Autenticación de usuarios para conexiones externas*
- *ANEXO P11 - Política de Documentación de los Procedimientos de Operación*
- *ANEXO P12- Política Aspectos Organizativos de la Seguridad de la Información*
- *ANEXO P13 - Política de los Controles de Red*
- *ANEXO P14 - Procedimiento para la recuperación de desastres*
- *ANEXO P15 - Política de los Controles de auditora de los sistemas de información*

3.4 Guía de Implementación

Una vez elaborados todos los documentos entregables se procede a elaborar una guía de implementación del plan SGSI, dicha guía contendrá una secuencia de actividades basadas en la ISO/IEC 27003 que se deben realizar en el caso de que se quiera implementar el SGSI. Cabe mencionar que se puede añadir otras actividades dependiendo de las necesidades de la entidad.

Tabla 3.2: Guía de Implementación del SGSI

Actividad	Descripción	Entregable
Aprobación de la dirección para iniciar un proyecto SGSI	Obtener aprobación de la Dirección para iniciar el proyecto de SGSI.	Documento - Aprobación por parte de la entidad.
Marco Legal	Investigación sobre todas las normas, leyes y reglamentos vigentes en el Ecuador, donde se defina los controles y regulaciones para las instituciones financieras (específicamente cooperativas de ahorro y crédito)	Documento – Marco Legal
Definición del Alcance y los Límites del SGSI.	Definir el alcance y los límites para SGSI	Sección 3.2 Alcance y Limites de SGSI
Análisis de la situación actual de la seguridad de la información.	Conocer el estado actual de la entidad con respecto a la seguridad de la información	Sección 1.6 Situación actual de la seguridad de la información
Identificación de los activos críticos	Evaluación y selección de los activos críticos	Documento – Activos Críticos
Análisis y evaluación de riesgos	Selección y aplicación de la metodología de análisis y evaluación de riesgos	Sección 2.3 Evaluación de riesgos según la metodología NIST SP 800-30
Elaboración de documentos	Elaboración del Procedimiento para control de documentos y registros. Elaboración de la política de SGSI. Elaboración de la Declaración de Aplicabilidad. Elaboración de las políticas necesarias en relación a los resultados del análisis y evaluación de riesgos.	ANEXO P01 - Documento de procedimiento para control de documentos y registros ANEXO P02 - Política de SGSI Anexo VIII-Declaración de Aplicabilidad. ANEXO P03- Política Uso aceptable de los activos ANEXO P04 - Política de Contraseñas ANEXO P05- Política de Clasificación y Manejo de la Información

		ANEXO P06 - Política de Capacitación, Sensibilización y Comunicación de seguridad de la información ANEXO P07 - Política de Eliminación y Reutilización de Equipos ANEXO P08 - Política de Instalación y Uso de Software ANEXO P10- Política de Autenticación de usuarios para conexiones externas ANEXO P11 - Política de Documentación de los Procedimientos de Operación ANEXO P12- Política Aspectos Organizativos de la Seguridad de la Información ANEXO P14 - Procedimiento para la recuperación de desastres ANEXO P09 - Política de Retiro de los Derechos de Acceso ANEXO P13 - Política de los Controles de Red ANEXO P15 - Política de los Controles de auditora de los sistemas de información
Implementación de las políticas	Implementación de los controles sugeridos.	No aplica
Capacitación al personal	Capacitación al personal para lograr la correcta ejecución de los controles a ser implementados.	No aplica

Fuente: Elaborado por el autor en base a la ISO/IEC 27003.

3.5 Aplicabilidad de la propuesta

Para evidenciar la mejora que se daría en la seguridad de la información en relación a la ISO 27001 dentro de la entidad, una vez que sean implementadas las políticas y/o controles aplicables de acuerdo a la evaluación de riesgos efectuada (2.3 Evaluación de riesgos según la metodología NIST SP 800-30), se calcula el porcentaje del nivel de cumplimiento esperado. Obteniendo como resultado la *Tabla*

3.3 (el *Anexo X- Análisis del Estado de Cumplimiento Esperado* contiene los resultados por cada dominio) que se muestra a continuación:

Tabla 3.3: Estado de Cumplimiento Esperado

Dominio	% Si Cumple	% Cumple Parcialmente	% No Cumple
A.5 Políticas de Seguridad	100%	0%	0%
A.6 Aspectos Organizativos de la Seguridad de la Información	73%	18%	9%
A.7 Gestión de Activos	80%	20%	0%
A.8 Seguridad ligada a los recursos humanos	56%	22%	22%
A. 9 Seguridad Física y Ambiental	85%	15%	0%
A.10 Gestión de Comunicaciones y Operaciones	44%	15%	41%
A.11 Control de Acceso	64%	24%	12%
A.12 Adquisición, Desarrollo y Mantenimiento de los Sistemas de información	62%	25%	13%
A.13 Gestión de Incidentes de Seguridad de la Información	40%	20%	40%
A.14 Gestión de la Continuidad del Negocio	40%	0%	60%
A.15 Cumplimiento	80%	0%	20%

Fuente: Elaborado por el autor en base al ANEXO X – Análisis del Cumplimiento Esperado.

La *Tabla 3.4* muestra el porcentaje del nivel de cumplimiento actual como el del nivel de cumplimiento esperado.

Tabla 3.4: Comparación del cumplimiento actual y el cumplimiento esperado

Dominio	Nivel de Cumplimiento Actual	Nivel de Cumplimiento Esperado
A.5 Políticas de Seguridad	0%	100%
A.6 Aspectos Organizativos de la Seguridad de la Información	36%	73%
A.7 Gestión de Activos	40%	80%
A.8 Seguridad ligada a los recursos humanos	22%	56%
A. 9 Seguridad Física y Ambiental	62%	85%
A.10 Gestión de Comunicaciones y Operaciones	34%	44%
A.11 Control de Acceso	52%	64%
A.12 Adquisición, Desarrollo y Mantenimiento de los Sistemas de información	56%	62%
A.13 Gestión de Incidentes de Seguridad de la Información	20%	40%

A.14 Gestión de la Continuidad del Negocio	0%	40%
A.15 Cumplimiento	60%	80%

Fuente: Elaborado por el autor al ANEXO X – Análisis del Cumplimiento Esperado

Como se puede observar todos los dominios incrementan su nivel de cumplimiento, unos en mayor cantidad que otros. En aquellos dominios en donde el incremento es considerable, se debe a que sus objetivos de control y controles están relacionados directamente con los resultados obtenidos en el análisis de riesgos de los activos críticos, mientras que los dominios que presentan poco incremento no están relacionados de forma directa con dicho análisis.

Cabe mencionar que, si el análisis fuera llevado a cabo en toda la entidad, el nivel de cumplimiento esperado tendría un incremento con mayor notoriedad.

A.5 Políticas de Seguridad

Para este dominio el incremento sería del 100% debido a que la entidad no aplicaba ninguno de los dos controles que establece la norma ISO 27001 (A.5.1.1 Documento de política de seguridad de la información y A.5.1.2 Revisión de política de seguridad de la información.)

A.6 Aspectos Organizativos de la Seguridad de la Información

El incremento para este dominio sería de 37%, esto debido a que los controles seleccionados (A.6.1.1 Compromiso de la Dirección con la seguridad de la información, A.6.1.2 Coordinación de la seguridad de la información, A.6.1.3 Asignación de responsabilidades relativas a la seguridad de la información y A.6.1.8 Revisión independiente de la seguridad de la información) permitirían a la entidad la gestión adecuada de la seguridad de la información mediante asignación de roles de seguridad, coordinación y revisión de la implantación de la seguridad.

A.7 Gestión de Activos

El incremento para este dominio sería de 40%, esto debido a que los controles seleccionados (A.7.1.3 Uso aceptable de los activos y A.7.2.2 Etiquetado y manejado de la información) permitirían a la entidad tener dar un tratamiento correcto a la información, por medio de su clasificación y niveles de protección.

A.8 Seguridad ligada a los recursos humanos

El incremento para este dominio sería de 34%, esto debido a que los controles seleccionados (A.8.2.1 Responsabilidades de la dirección, A.8.2.2 Concienciación, formación y capacitación en seguridad de la información y A.8.3.3 Retiro de los derechos de acceso) permitirá a la entidad mejorar y documentar estos controles que actualmente se están practicando únicamente por experiencia.

A. 9 Seguridad Física y Ambiental

El incremento para este dominio sería de 23%, esto debido a que los controles seleccionados (A.9.1.4 Protección contra las amenazas externas y de origen ambiental, A.9.2.6 Reutilización o retirada segura de equipos y A.9.2.7 Retirada de materiales propiedad de la organización) permitirá a la entidad mejorar y aplicar las prácticas de estos controles de manera formal.

A.10 Gestión de Comunicaciones y Operaciones

El incremento para este dominio sería de 10%, esto debido a que los controles seleccionados (A.10.1.1 Documentación de los procedimientos de operación, A.10.7.3 Procedimientos de manipulación de la información y A.10.6.1 Controles de red) permitirán a la entidad por un lado mejorar aquellos controles que actualmente práctica y por otro el control que permite manipular la información de forma correcta.

A.11 Control de Acceso

El incremento para este dominio sería de 12%, esto debido a que los controles seleccionados (A.11.2.3 Gestión de contraseñas de usuario, A.11.3.1 Uso de contraseñas y A.11.4.2 Autenticación de usuario para conexiones externas) permitirían a la entidad el control eficiente para la autenticación con uso de contraseñas.

A.12 Adquisición, Desarrollo y Mantenimiento de los Sistemas de información

El incremento para este dominio sería de 6%, esto debido a que el control seleccionado (A.12.4.1 Control del software en explotación) permitirá a la entidad controlar de forma clara la instalación de software en sus sistemas.

A.13 Gestión de Incidentes de Seguridad de la Información

El incremento para este dominio sería de 20%, esto debido a que los controles seleccionados (A.13.1.2 Notificación de los puntos débiles de seguridad) permitirán que los usuarios de la entidad sean quienes comuniquen de las posibles debilidades de seguridad a las que se esté expuesto.

A.14 Gestión de la Continuidad del Negocio

El incremento para este dominio sería de 40%, esto debido a que los controles seleccionados (A.14.1.2 Continuidad del negocio y evaluación de riesgos y A.14.1.3 Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información) permitirá que la entidad sepa cómo y pueda reaccionar ante la interrupción de las actividades de negocio de forma correcta de manera que el core de negocio no se vea afectado.

A.15 Cumplimiento

El incremento para este dominio sería de 20%, esto debido a que los controles seleccionados (A.15.2.1 Cumplimiento de las políticas y las normas de la seguridad y A.15.3.1 Controles de auditoría de los sistemas de información) permitirá a la entidad realizar revisiones regulares de la seguridad de la información.

4 CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Comparar las metodologías de análisis de riesgos permitió identificar las fortalezas de cada una en correspondencia a los elementos relacionados con el departamento de TI, seleccionando la que obtuvo mayor valoración.
- La Cooperativa de Ahorro y Crédito “KULLKI WASI” tiene implementados controles de seguridad que no cuentan con una evidencia formal debido a que estos no se encuentran documentados y se los lleva a cabo por experiencia y/o necesidad, sin embargo, estos controles fueron parte del análisis de estado de cumplimiento actual respecto a la norma ISO/IEC 27001 tomándolos como “cumplimiento parcial”.
- La Declaración de Aplicabilidad permitió identificar controles que no están directamente relacionados con los activos críticos analizados, controles que

apoyan la toma de decisiones y el compromiso de la dirección con la seguridad de la información.

- Las políticas elaboradas, que forman parte de los entregables, contienen todos los controles seleccionados en la declaración de aplicabilidad, no como un documento formal por cada control, pero si cumpliendo toda la selección que permitirá asegurar los activos críticos analizados de acuerdo al alcance del plan, por ello la entidad podrá crear o modificar políticas si el alcance del análisis se ampliase.
- El aumento del porcentaje en el estado de cumplimiento esperado se daría siempre y cuando se ponga en marcha los controles propuestos, además de que dicho porcentaje sería mayor si el análisis se lo realizaría todos los activos de la entidad y no únicamente a los activos considerados como críticos.
- Los activos considerados como críticos dentro de la Cooperativa de Ahorro y Crédito “KULLKI WASI” no poseen riesgos de nivel alto lo que significa que los controles que actualmente se ejecutan están de una u otra forma reduciendo las vulnerabilidades frente a las amenazas existentes. Por otra parte, de los 58 riesgos encontrados, 35 están en un nivel moderado y de acuerdo al plan de tratamiento de riesgos establecido, estos riesgos son los que fueron tomados en cuenta para la selección de controles con el objeto de mitigarlos. Los 23 riesgos restantes, con nivel de riesgo bajo, únicamente fueron presentados y deberán ser controlados después de haber implementado los controles propuestos para la mitigación de los que se encuentran en nivel moderado.
- El Manual de Políticas de Tecnologías de la Información que actualmente posee la Cooperativa de Ahorro y Crédito “KULLKI WASI” no cumple la función de la Política de Seguridad, no contiene todos los dominios de seguridad que la cooperativa requiere y se encuentra redactado sin lineamientos y conforme a las necesidades inmediatas por lo cual genera confusión y falta de orden.
- El Departamento de Tecnología de la Cooperativa de Ahorro y Crédito “KULLKI WASI” tiene como debilidad la falta de personal, cuenta con muy

poco talento humano para el área y las responsabilidades que se deben llevar a cabo.

4.2 Recomendaciones

- La Cooperativa de Ahorro y Crédito “KULLKI WASI” tiene como misión llegar al segmento 1, al encontrarse en este segmento deberá cumplir con el Art.15 literal b. de la Resolución No. SB-2018-771 de la Superintendencia de Bancos, en el cual se plantea la creación de un área independiente y especializada para la gestión de seguridad de la información, por ello la entidad debería asignar en su plan estratégico responsables para la creación del área en mención.
- Planificar análisis de vulnerabilidades, pruebas de penetración y/o hackeo ético periódicos (al menos una vez al año) como parte de las tareas que el Departamento de Tecnología debe cumplir con el objeto de mantener al día los posibles riesgos a los que se encuentra expuesta la cooperativa.
- El análisis de riesgo realizado no reflejó riegos en el nivel alto sin embargo día a día van apareciendo nuevas amenazas, por ellos es necesario que la cooperativa lleve a cabo análisis de riesgo de manera continua (en lo posible una vez al año) lo que le permitirá tener claro los peligros que podrían afectar al CORE del negocio.
- Los controles que fueron seleccionados y que se recomiendan sean implementados únicamente se relacionan con los riesgos de nivel moderado, por ello es importante que el Departamento de Tecnología de la cooperativa una vez que se haya implementado los mismos, tome medidas de control para aquellos riesgos que obtuvieron un nivel bajo o se continúe aplicando las medidas que hasta el momento se han llevado a cabo, documentando de manera formal dichos procedimientos.
- La implementación del presente Plan de Gestión de Seguridad de la Información únicamente podrá ser llevado a cabo si existe el compromiso por parte de la Alta Gerencia, el Departamento de Tecnología y los usuarios de la entidad.

- A medida que la tecnología avanza es necesario integrar las mismas a la entidad lo que generaría nuevas fuentes de amenazas y con esto nuevos riesgos, por ello es importante que se realicen revisiones periódicas del presente plan debido a que el mismo podría quedar obsoleto con el paso del tiempo.
- Realizar campañas y/o capacitaciones para concientizar las buenas prácticas de seguridad de la información y de esta manera salvaguardar la información sensible que maneja la entidad.
- Llevar a cabo las políticas y/o controles no solo como solución o necesidad tecnológica sino como procedimientos formalmente documentados y controlados.
- La implementación de un Active Directory facilitaría la administración de los usuarios dentro de la red de la entidad, lo que permitía crear niveles de permisos, políticas y asignar adecuadamente los recursos en función a los roles establecidos.

5 REFERENCIAS BIBLIOGRÁFICAS

[1] Burgos J. y Campos P., «CEUR-WS.org - Modelo Para Seguridad de la Información en TIC,» [En línea]. Available: http://ceur-ws.org/Vol-488/paper13.pdf. [Último acceso: 2017].

[2] Kullki Wasi - Cooperativa de ahorro y crédito, «Kullki Wasi - Cooperativa de ahorro y crédito- Nosotros,» 2013. [En línea]. Available: http://kullkiwasi.com.ec/index.php/nosotros. [Último acceso: 2017].

[3] Superintendencia de Economía Popular y Solidaria, «¿Qué es la SEPS?,» 2018. [En línea]. Available: http://www.seps.gob.ec/interna?-que-es-la-seps-.

[4] Superintendencia de Economía Popular y Solidaria, «RESOLUCIÓNNo.SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103,» Quito, 2017.

[5] Junta de Política y Regulación Monetaria y Financiera, «Resolución N° 128-2015-F,» Quito, 2015.

[6] Gerente entidad Financiera., Interviewee, Primera entrevista- Conociendo la empresa y solicitud de auspicio.. [Entrevista]. 2017.

[7] Cooperativa de Ahorro y Crédito Kullki Wasi, «Kullki Wasi Historia,» Ambato, 2018.

[8] Cooperativa de Ahorro y Credito Kullki Wasi, Plan estratégico, Ambato, 2017-2020.

[9] ISACA, «The Risk IT Framework,» ISACA, 2018. [En línea]. Available: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx.

[10] Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, «MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información,» Octubre 2012. [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.W9sxhdVKi1s.

[11] NIST-National Institute of Standards and Technology, «Risk Management Guide for Information Technology Systems,» 2002.

[12] Instituto Ecuatoriano de Normalización- INEN, «NTE INEN-ISO/IEC 27001:2011 TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD - SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) - REQUISITOS,» Quito.

[13] Microsoft, «Microsoft Security Assessment Tool 4.0,» Microsoft, [En línea]. Available: https://www.microsoft.com/en-us/download/details.aspx?id=12273. [Último acceso: 21 Septiembre 2018].

[14] INEN, «NTE INEN-ISO/IEC 27001:2011 Tecnología de la información. Técnicas de seguridad. Sistema de gestión de la seguridad de la información (SGSI). Requisitos,» 2012.

[15] I. Maldonado y J. Guanoluisa, Análisis de riesgo y diseño de un plan de seguridad de la información para el consejo nacional de igualdad de discapacidades "CONADIS", Quito, 2015.

ANEXOS

Documento - Aprobación por parte de la entidad

Documento - PlanificacionDeActividades

Documento - Activos Críticos

ANEXO - Análisis de la situacion actual

ANEXO - Escaneo de Vulnerabilidades con Nessus y Nmap

ANEXO I - Selección de Metodolog¡a para el Análisis de Riesgos

ANEXO II - Resultado de Medidas de Defensa MSAT

ANEXO III - Manejo de Seguridad de la Informaci¢n NTE INEN-ISO-IEC 27001-2011 Auditoría Check List

ANEXO IV - Análisis del Estado de Cumplimiento Actual según la Norma NTE INEN-ISO-IEC 27001-2011

ANEXO lX - Informe de Valoración de Riesgo

ANEXO V - Escaneo de Vulnerabilidades con Nessus y Nmap

ANEXO VI - Análisis de Vulnerabilidades

ANEXO VII - Matriz de riesgos

ANEXO Vlll - Declaración de Aplicabilidad

ANEXO X - Análisis del Estado de Cumplimiento Esperado

Documento - Marco Legal

ANEXO P01 - Documento de procedimiento para control de documentos y registros

ANEXO P02 - Política de SGSI

ANEXO P03- Política Uso aceptable de los activos

ANEXO P04 - Política de Contraseñas

ANEXO P05- Política de Clasificación y Manejo de la Información

ANEXO P06 - Política de Capacitación, Sensibilización y Comunicación de seguridad de la información

ANEXO P07 - Política de Eliminación y Reutilización de Equipos

ANEXO P08 - Política de Instalación y Uso de Software

ANEXO P09 - Política de Retiro de los Derechos de Acceso

ANEXO P10- Política de Autenticación de usuarios para conexiones externas

ANEXO P11 - Política de Documentación de los Procedimientos de Operación

ANEXO P12- Política Aspectos Organizativos de la Seguridad de la Información

ANEXO P13 - Política de los Controles de Red

ANEXO P14 - Procedimiento para la recuperación de desastres

ANEXO P15 - Política de los Controles de auditora de los sistemas de informa*ción*