UNIVERSIDAD NACIONAL
"PEDRO RUIZ GALLO"

FACULTAD DE CIENCIAS FISICAS
Y MATEMATICAS

Escuela Profesional de Computación e Informática

Tesis para optar por el Título Profesional de Ingeniero en Computación e Informática

Plan de Gestión de Riesgos de Tecnologías de la Información en los procesos críticos de créditos y captaciones para la Caja de Ahorro y Créditos SIPAN SA de Chiclayo - 2016

PRESENTADO POR:

Bach. Calderón Pérez Artemio

Bach. Vásquez Hoyos Alvaro

ASESOR

MSc. Ing. Jessie Leila Bravo Jaico

LAMBAYEQUE – PERÚ 2018

FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS

Escuela Profesional de Computación e Informática

TESIS

Plan de Gestión de Riesgos de Tecnologías de la Información en los procesos críticos de créditos y captaciones para la Caja de Ahorro y Créditos SIPAN SA de Chiclayo - 2016

Para optar el título profesional de

INGENIERO EN COMPUTACIÓN E INFORMÁTICA

DR. ARMANDO JOSÉ MORENO HEREDIA

PRESIDENTE

M.SC PEDRO FIESTAS RODRIGUEZ

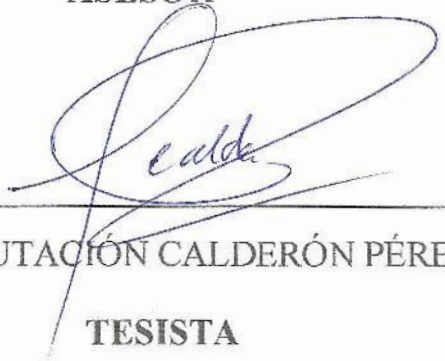
SECRETARIO

M. SC. JANET DEL ROSARIO AQUINO LALUPÚ

VOCAL

MSC. ING. JESSIE LEILA BRAVO JAICO

ASESOR



BACH. ING. EN COMPUTACIÓN CALDERÓN PÉREZ ARTEMIO

TESISTA

BACH. ING. EN COMPUTACIÓN VÁSQUEZ HOYOS ÁLVARO

TESISTA

DEDICATORIA

A Dios por permitirme llegar a este momento tan especial en mi vida, por los triunfos y los momentos difíciles que me han enseñado a valorarlo cada día más, A mi padre quien con sus consejos a sabido guiarme, para culminar mi carrera profesional, y también por ser la persona que me ha acompañado durante todo mi trayecto estudiantil, a mi madre por demostrarme su amor incondicional, A mi esposa, que ha sabido impulsarme para poder lograr terminar ésta etapa de mi vida, a mis hijos Leandro Benjamín y Fátima de los Ángeles, que han sido el motor y motivo de superación personal, a mi mejor amigo Álvaro, que ha estado allí presente en los buenos momentos y en los malos momentos y que gracias a su perseverancia y constante lucha por superarnos estamos culminando esta tesis.

Artemio Calderón Pérez

DEDICATORIA

Dedico esta tesis principalmente a Dios, por haberme dado la vida, la salud y haber permitido concluir muchos sueños que he emprendido en la vida, pero sin lugar a dudas este es uno de mis mayores logros al que estoy por concluir dar gracias por todo ello. A mis padres Adela y José; por ser el pilar más importante y por demostrarme su amor, confianza y su apoyo incondicional en todo lo que he emprendido en la vida, aunque en algunas veces me he equivocado, pero siempre estuvieron presentes para apoyarme y mejorar en el caminar de la vida. A mi hija Akemi Luana, que me permitió experimentar ese mágico y extraordinario sentimiento de ser padre, y tal es así que me permite seguir el día a día con mucha fuerza, me motiva a seguir creciendo en lo personal como profesionalmente para así darle una camino y guía con el ejemplo que quiero construir.

Alvaro Vásquez Hoyos

AGRADECIMIENTO

Agradezco a Dios por protegerme durante todo mi camino y darme fuerzas para superar cada obstáculo y dificultades a lo largo de toda mi vida.

A mi padre, que con su demostración de un padre ejemplar me ha enseñado a no desfallecer ni rendirme ante nada y siempre perseverar a través de sus sabios consejos.

A mis hermanas Mavila y Aldonía, que confiaron siempre en mi

A nuestra asesora Jessie Bravo Jaico que con sus conocimientos y apoyo constante se pudo lograr la culminación esta tesis.

A mi amigo Álvaro por haber logrado nuestro gran objetivo con mucha perseverancia.

Artemio Calderón Pérez

AGRADECIMIENTO

Agradezco a Dios por haberme dado la salud, las fuerzas, porque bajo su bendición me permite presentar ante ustedes esta tesis de grado.

A nuestra Alma mater UNPRG, por acogernos a sus aulas y vivir una maravillosa experiencia de forjarnos unos profesionales de calidad y a nuestros Docentes en general que nos impartieron y trasmitieron sus conocimientos para nuestra formación integral como Ing. en Computación e Informática.

A mi madre por su dedicación incondicional y su apoyo en el crecimiento integral como persona de bien en el aspecto personal.

A mi amigo Artemio por haber logrado nuestro gran objetivo con mucha perseverancia y por su apoyo a lo largo de nuestra permanencia en aulas.

Alvaro Vásquez Hoyos

RESUMEN

De acuerdo a los recientes estudios de investigación de IBM Company (2012) han demostrado que las empresas que adoptan un criterio equilibrado ante la madurez de la gestión de riesgos de TI, no sólo tienen menos incidentes en este ámbito, sino que obtienen mayor rentabilidad del negocio y de TI respecto de la competencia. La falta de acción con respecto a los riesgos se debe al temor de tomar decisiones negativas y señalen a un responsable ante la perdida por un derivado. Esta es una de las medidas más importantes que una empresa puede implementar para reducir de forma potencial los Riesgos de TI.

El presente trabajo de investigación tiene por objeto definir y construir un Plan de Gestión de Riesgos de TI en la institución financiera Caja de Ahorro y Crédito Sipán SAC, a partir de un marco referencial normativo asociado como la familia de ISO 27000, y la exigencia de la Superintendencia de Banca y Seguros.

Esta propuesta se debe a que la institución actualmente tiene problemas para disminuir la brecha de incidencias y ocurrencia de riesgos que puedan paralizar parcial o totalmente sus procesos críticos de créditos y colocaciones; así como también para que le sirva como una herramienta de apoyo en la toma de decisiones relacionadas con las inversiones en seguridad de la información. Los datos de prueba se tomarán directamente de sus registros de incidente y problemas relacionados con la seguridad de la información, mediante técnicas como análisis documental, observación directa y entrevistas.

La evaluación del plan propuesto se realizará a través de la medición de los resultados de amenazas, vulnerabilidades, impactos y niveles de riesgo a través de una serie de pruebas relacionados con las políticas de seguridad, la organización de la estructura de seguridad, los activos tecnológicos, la seguridad física y lógica de los sistemas, la continuidad del negocio y el cumplimiento normativo.

Palabras claves:
Critical process, IT asset , vulnerability, threat, impact , risk level , risk appetite control objective , control, risk matrix , residual risk.

ABSTRACT

According to recent research studies IBM Company (2012) have shown that companies that adopt a balanced approach to the maturity of risk management IT not only have fewer incidents in this area but achieve greater profitability and IT over the competition. The lack of action regarding the risks due to the fear of taking negative decisions and responsible to point to a loss on a derivative. This is one of the most important steps that a company can implement to reduce the risks of potential IT.

This research aims to define and build a Plan Risk Management IT in the financial institution Caja Savings and Credit Sipan SAC, from a normative frame of reference associated as the family of ISO 27000, and the requirement the Superintendency of Banking and Insurance.

This proposal is that the institution currently has problems to decrease the gap occurrence of incidents and risks that may partially or totally paralyze critical processes credit and loans; as well as to serve him as a support tool in decision-making related to investments in information security. The test data will be taken directly from their records incident and problems related to information security, through techniques such as document analysis, direct observation and interviews.

The evaluation of the proposed plan will be made by measuring the results of threats, vulnerabilities, impacts and risk levels through a series of tests related to security policies, the organization of the security structure, technological assets, physical and logical security systems, business continuity and regulatory compliance.

Keywords:
Critical process, IT asset, vulnerability, threat, impact, risk level, risk appetite control objective, control, risk matrix, residual risk.

INDICE GENERAL

INDICE DE FIGURAS

INTRODUCCIÓN

Según en el Nuevo Acuerdo de Capitales de **BASILEA** con la inclusión del Riesgo Operacional refleja uno de los cambios más significativos en la gestión financiera, donde su importancia está desplazando el tradicional interés por los riesgos de crédito y mercado, centrando los esfuerzos actuales del sector financiero. Ahí se definió que los riesgos asociados a las operaciones de las entidades financieras son de diferentes tipos, entre las cuales destacan: personas, procesos, tecnología de información y aspectos externos.

Existen numerosas metodologías para la gestión de riesgos de TI, tales como MagerIT, Nist 800-30, Cramm, RiskIT, Octave, Neozelandesa, Australiana, etc. Así mismo, existen estándares como la familia ISO 27000 (específicamente las ISOs 27001, 27002, 27005 y 31000) e ISO 20000, que pueden utilizarse para gestión de riesgos de Tecnologías de la Información. Sin embargo, sus procedimientos o no son adecuadas para el tamaño de infraestructura de Tecnologías de la Información o no son adecuados para el grado de madurez de Tecnologías de la Información de las instituciones o su implementación requiere fuertes inversiones o simplemente no cuentan con herramientas flexibles y que se adecuen al tipo de organizaciones de nuestro medio, y específicamente a las del rubro del sistema financiero lo que son del tipo Cajas de Ahorro.

La Caja de Ahorro y Créditos SIPAN SA de Chiclayo, dedicada al rubro de créditos y servicios financieros, cuenta con cerca de 19 años de experiencia en el mercado.

El presente proyecto, plantea en resolver el problema de riesgos operativos relacionados con Tecnologías de la Información en la Caja de Ahorro y Crédito Sipán SA que existen en sus dos principales procesos críticos y que son los procesos de Créditos y Captaciones de clientes en la cual se tiene que cumplir con las exigencias de la Superintendencia de Banca y Seguros, en relación a la gestión de Tecnologías de la Información, de la seguridad y de riesgos de Tecnologías de la Información.

Se plantea el objetivo de aplicar un Plan de Gestión de Riesgos de Tecnologías de la Información en los Procesos críticos de Créditos y Captaciones para Caja de Ahorro y Crédito Sipán SA Chiclayo.

La presente investigación se justifica en mejorar la eficacia y eficiencia en la evaluación y tratamiento de los riesgos en Tecnologías de la Información, ahorrar tiempo en la detección oportuna de las amenazas, permitir una mejor administración de la información para establecer un orden en la organización de acuerdo a controles establecidos y así tomar las decisiones a tiempo, y que sea parametrizable y flexible, ajustado a las características de la organización y sobre todo sea manejable, todo esto con el fin de asegurar continuidad en el negocio y la disminución de daños en la Caja de Ahorro y Crédito Sipán SA.

CAPÍTULO I: DATOS GENERALES DE LA ORGANIZACIÓN

1.1. Descripción de la organización

La Caja de Ahorros y Créditos Sipán S.A.; es una sociedad anónima de derecho privado, con 1200 accionistas de la región aproximadamente, orientada a promover servicios de intermediación financiera, en forma especial del sector de la pequeña y microempresa. Está sujeta a la Ley General del Sistema Financiero, Ley General de Sociedades y directivas que dicten la Superintendencia de Banca y Seguros y Banco Central de Reserva del Perú.

1.2. Misión, visión y objetivos de la organización

1.1.1. Misión

Impulsar el crecimiento sostenible de nuestros clientes, colaboradores, accionistas y de la ciudad de Chiclayo

1.1.2. Visión

Ser la empresa de créditos líder en ofrecer soluciones financieras a nuestro mercado objetivo, brindando calidad de servicio, eficiencia y oportunidad

1.3. Valores corporativos

- Orientación al cliente:
  - Conocer y satisfacer sus necesidades de los clientes
  - Simplicidad y transparencia
  - Disponibilidad y cercanía
  - Amabilidad
- Orientación a las Personas
  - Confianza
  - Equidad
  - Reconocimiento y desarrollo
  - Trabajo en equipo
- Orientación al logro

- Visión global
- Integridad
- Proactividad
- Responsabilidad y compromiso

CAPÍTULO II: PROBLEMÁTICA DE LA INVESTIGACIÓN

2.1. Realidad problemática

En nuestra región de Lambayeque, todas las instituciones financieras que cuentan con la autorización de la Superintendencia de Banca y Seguros (SBS) y que gozan de una autonomía económica, financiera y administrativa, brindan servicios de ahorros, que es la captación de los fondos de las personas a través de las diferentes formas de créditos y estos créditos son la colocación de los fondos captados.

A través de la resolución SBS N° 37-2008 del 10 de enero de 2008, se aprobó el Reglamento de la Gestión Integral de Riesgos, y que establece que todas las empresas que son supervisadas deben contar con una gestión integral de riesgos adecuada a su tamaño y a lo complejo de sus operaciones y servicios que brinde mediante la resolución SBS N° 2116-2009 del 02 de abril del 2009, se aprobó el Reglamento para la Gestión del Riesgo Operacional, y dicho reglamento debe de aplicarse para todo el sistema financiero peruano.

Existen innumerables metodologías para tratar la gestión de riesgos de Tecnologías de la Información(TI), tales como MagerIT, Nist 800-30, Cramm, RiskIT, Octave, Neozelandesa, Australiana, etc. Así mismo, existen estándares como la familia ISO 27000 (específicamente las ISOs 27001, 27002, 27005 y 31000) e ISO 20000, que pueden ser utilizadas para la gestión de riesgos de Tecnologías de la Información(TI). Sin embargo, los procedimientos que utilizan las metodologías o no son adecuadas para el tamaño de la infraestructura de Tecnologías de la Información o no son adecuados para el grado de madurez de Tecnologías de la Información de las instituciones o en varios casos su implementación requiere una fuerte inversión o simplemente no cuentan con herramientas que sean flexibles y que se adecuen al tipo de instituciones de nuestro medio, y específicamente a las del sistema financiero tipo cajas de Ahorro.

En cuanto a las entidades privadas, en nuestro medio, las empresas del sistema financiero son el tipo de instituciones que tratan de tener una gran ventaja competitiva utilizando Tecnologías de la Información como eje de sus procesos

críticos, relacionados principalmente con los créditos y captaciones de créditos, así como también el recupero de éstos; por lo tanto, se hacen muy dependientes de las Tecnologías de la Información. La Superintendencia de Banca y Seguros es el organismo encargado de regular y supervisar a éste tipo de instituciones, y controla también las exigencias en relación a la seguridad que se le debe de dar a la información, la gestión de riesgos de Tecnologías de la Información está normado en Resolución N° 006-2002, que es el reglamento para la administración de riesgos de operación y en su documento que es la Circular N° G-105-2002, es en estos dos documentos que son muy importantes y es en donde podremos encontrar los criterios mínimos para la identificación y administración de los riesgos asociados a las Tecnologías de Información.

Para la presente investigación, se ha tomado como caso de estudio el de la Caja de Ahorro y Créditos SIPAN SA de la ciudad de Chiclayo que es una sociedad anónima de carácter privado, actualmente cuenta con 1200 accionistas de la región aproximadamente, dicha sociedad está orientada a promover servicios de intermediación financiera, en forma especial del sector de la pequeña, mediana y microempresa.

La Caja de Ahorro y Créditos SIPAN SA está sujeta a las siguientes leyes reguladoras:

- Ley General del Sistema Financiero
- Ley General de Sociedades y directivas que dicten la Superintendencia de Banca y Seguros y Banco Central de Reserva del Perú.

Existen dos principales procesos críticos que son Créditos y Captaciones de clientes en la cual se tiene que cumplir con las exigencias que da la Superintendencia de Banca y Seguros, en relación a la gestión de Tecnologías de la Información, de la seguridad y de riesgos de Tecnologías de la Información.

El proceso de crédito, consta en reunir y revisar toda la información de los potenciales clientes de créditos mediante visitas domiciliarias o al centro de negocio del cliente para poderle otorgar el crédito que éste va a solicitar. Luego de

haber pasado estos datos anteriores es entonces que se evalúan y verifican dichos datos proporcionados para luego realizar el desembolso de los créditos aprobados.

El proceso de captaciones, consiste en que se debe de apertura la cuenta de ahorro, cuentas a plazo u órdenes de pago, y las operaciones que puede realizar con dichas cuentas solicitados por los clientes.

De acuerdo a su estructura orgánica la Caja de Ahorro cuenta con un Área de Tecnologías de la Información, con una Jefatura, la Unidad Desarrollo, la Unidad de Producción y Soporte y la Unidad de Organización y Métodos. En la Unidad de Desarrollo trabajan seis (06) analistas programadores. En la Unidad de Producción trabajan dos (02) especialistas en infraestructura, redes y comunicaciones. En la Unidad de O&M trabaja una (01) persona.

La Caja de Ahorro también tiene una Unidad de Riesgos que es el área encargada de dar evaluación y tratamiento a los riesgos entre los cuales están los relacionados con Tecnologías de la Información y de la planificación de la continuidad del negocio. Además, la Caja de Ahorro en ésta unidad tiene una jefatura, un (01) oficial de seguridad de la información y dos (02) analistas de riesgos operativos como trabajadores directos en dicha unidad.

Cuenta con una infraestructura tecnológica, caracterizada por tener:

- Un DATA CENTER con servidores centrales (Datos, Aplicaciones, ISA server, respaldo), equipos de comunicaciones (Switch central, Router alquilado)
- Un DATA CENTER alterno (que se encuentra ubicado en la ciudad de Trujillo), con equipamiento mínimo, ya que es solo para respaldo
- Comunicaciones a través de un VPN alquilado a una operadora local (Empresa Telefónica) que viene con un ancho de banda de 512 Kb, que ayuda interconectar las agencias de Jaén, Trujillo, Chepén y Moshoqueque.

PROBLEMAS QUE SE PRESENTA EN LA INSTITUCIÓN:

- Existen muchos retrasos en la entrega cuando se quieren desarrollar nuevos

proyectos de Tecnologías de la Información y también cuando se requiere la atención de requerimientos para realizar actualizaciones y modificaciones a los sistemas que existen y esto ocasiona los siguientes problemas:

  - Altos costos de producción y desarrollo.
  - Impactos negativos por falta de atención oportuna de necesidades.
  - Pérdida de muchas oportunidades de negocio.

- El Plan Estratégico de Tecnologías de Información que se tiene en la Caja de Ahorro no considera el procedimiento más adecuado para definir modelo de empresa soportado sobre Tecnologías de la Información, de tal forma que permita un más adecuado seguimiento y control de la ejecución de los proyectos y las actualizaciones, así como también de las adecuaciones en las estructuras de datos y de las aplicaciones. Esto ocasiona que las aplicaciones que se desarrollan o que son desarrolladas no atiendan las verdaderas necesidades y requerimientos.
- Se puede observar la ausencia de presupuesto e inversión en la seguridad de la información, y esto ocasiona el aumento del impacto negativo con la ocurrencia de incidencias relacionadas con la seguridad de la información.
- Las políticas, procedimientos y normativas relacionada con la seguridad de la información y la gestión de riesgos no existen concordancia con las exigencias de la Superintendencia de Banca y Seguros, ocasionando que se incumpla la normatividad que exige dicha Superintendencia de Banca y Seguros, lo cual podría demandar en una futura multa o sanción ya que es requisito indispensable que se tiene que cumplir para que se permanezca en funcionamiento.
- No se tiene muy bien definido ni se tiene priorizado los activos tecnológicos y su relación con los procesos de una manera correcta y esto ocasiona que no exista información confiable y que sea priorizada para cuando se tenga que tomar decisiones en relación a las inversiones en seguridad de la información y gestión de riesgos de Tecnologías de la Información

- Falta llevar un control de la clasificación de la información para que se pueda determinar los niveles de acceso con los respectivos controles de comunicación, transmisión y divulgación y esto ocasiona que no exista información confiable y que sea priorizada para cuando se tenga que tomar decisiones en relación a las inversiones en seguridad de la información y gestión de riesgos de Tecnologías de la Información

  – Se puede observar y evidenciar que falta de un procedimiento adecuado para que se puedan registrar los incidentes y la atención de los problemas; así como también la trazabilidad de las transacciones registradas, ocasionando falta de atención oportuna de las incidencias y atención de problemas que se puedan suscitar y que esto conlleva a que vayan aumentando potencialmente sus impactos negativos sobre la seguridad de la información.

  – La Unidad de Riesgos que posee la Caja de Ahorros emite un informe trimestral sobre la gestión de riesgos de Tecnologías de la Información, y es en uno de estos informes que se puede evidenciar que, en el año 2014, se ha registrado la siguiente estadística en incidentes:

    - Caídas en comunicaciones: 27 eventos.
    - Caídas en red interna (todas las agencias): 103 eventos
    - Accesos lógicos no autorizados externos: 84 eventos.
    - Accesos lógicos no autorizados internos: 55 eventos
    - Problemas con el suministro de energía eléctrica: 08 eventos
    - Errores por negligencia: 137 eventos

    Todos estos incidentes ocasionan la inadecuada gestión de riesgos de Tecnologías de la Información.

  – Además, la Caja de Ahorro no cuenta con un proceso que le permita evaluar y dar tratamiento a los riesgos, que analice adecuadamente las amenazas, vulnerabilidades e impactos asociados con cada activo, y al no tener este proceso ocasiona el aumento potencial de los impactos negativos sobre la seguridad de la información.

Luego de esto, se hace indispensable la implementación de un plan adecuado para la gestión de los riesgos relacionados con Tecnologías de la Información en la Caja de Ahorro y Crédito Sipán SA, y que éste plan diseñado se ajuste a las exigencias de la Superintendencia de Banca y Seguros, pero basados en estándares relacionados con la seguridad de la información, la continuidad del negocio y la gestión de riesgos relacionados con Tecnologías de la Información.

2.2. Formulación del problema

¿De qué manera se puede mejorar la gestión de riesgos de Tecnologías de la Información en los procesos críticos de créditos y captaciones para la Caja de Ahorro y Créditos SIPAN SA?

2.3. Justificación e importancia de la investigación

La presente investigación se justifica porque un Plan de Gestión de Riesgos es importante y necesaria en áreas indispensables que en donde su funcionamiento sea importante para la Caja de Ahorro en el ámbito tecnológico basado en estándares internacionales como la ISO/IEC 27001, ISO 17799, CobIT y MagerIT, donde se va mejorar la eficacia en la evaluación y tratamiento de los riesgos, y en donde éste mejoramiento le va a permitir ahorrar tiempo en la detección oportuna de amenaza así como también le permitirá mejorar la administración de información para establecer un orden de acuerdo a controles establecidos y así tomar las decisiones a tiempo dichos controles deben de ser parametrizables y flexibles y que se ajusten a las características de la organización. En lo Social a través de un conjunto de normas y procedimientos, permitirá administrar los incidentes de seguridad reduciendo los impactos negativos en los procesos, que puedan ocasionar pérdidas de vidas humanas o caídas de los activos tecnológicos.

En lo económico donde se proveerá de la suficiente información para que la dirección de la Caja de Ahorro pueda tomar decisiones acerca de la inversión correcta en la implantación de los controles como un mecanismo de salvaguarda de todos los activos tecnológicos que posee, reduciendo así los gastos innecesarios en las salvaguardas que no tienen efecto positivo o en controles que no se puedan

monitorear y así maximizar los beneficios de la inversión en tecnología que se tendría que realizar.

Con la implementación de un Plan de Gestión de Riesgos de Tecnologías de la Información, permitirá en el aspecto científico aportar a la ciencia demostrando nos ayudará a mejorar la eficacia y eficiencia de la evaluación y tratamiento de los riesgos relacionados con Tecnologías de la Información de una organización basados en estándares internacionales.

2.4. Objetivos de la investigación

2.4.1. Objetivo general

Elaborar un plan de gestión de riesgos de Tecnologías de la Información en los procesos críticos de créditos y captaciones para la Caja de Ahorro y Créditos SIPAN SA.

2.4.2. Objetivos específicos

1. Identificar los factores que se deben considerarse en el plan de gestión de riesgo de Tecnologías de la Información a partir de la revisión de las normativas del Superintendencia de Banca y Seguros.
2. Definir los activos críticos relacionados con Tecnologías de la Información en los procesos críticos de créditos y captaciones.
3. Definir los procedimientos de evaluación y tratamiento de riesgos de Tecnologías de la Información al plan de gestión de riesgo basados en COBIT.
4. Identificar y procedimentar las formas de identificación y valorización de las amenazas (impacto y probabilidad de ocurrencia), las vulnerabilidades y el cálculo de los niveles de activos de riesgos
5. Determinar la efectividad de los controles a través de la definición de brechas de seguridad.
6. Ofrecer un método sistemático para analizar los riesgos derivados del uso de Tecnologías de la Información y Comunicaciones (TIC)

7. Determinar y planificar el tratamiento oportuno para mantener los riesgos bajo control.

2.5. Limitaciones de la investigación

Se encontró limitaciones para acceder a la infraestructura tecnológica y a la información de la institución donde se aplica el experimento, es decir no es posible manejar la variable independiente; se opta por observar los efectos del plan propuesto a través de las evaluaciones que realicen los actores directos de los procesos relacionados con la investigación al diseño y aplicabilidad del plan propuesto.

CAPÍTULO III: MARCO METODOLÓGICO

3.1. Tipo de investigación

Tecnológica aplicada

3.2. Hipótesis

Con la implementación de un plan de gestión de riesgos de Tecnologías de la Información se mejorará la gestión de riesgos en los procesos críticos de créditos y captaciones para la Caja de Ahorro y Créditos SIPAN SA.

3.3. Variables

3.3.1. Variable independiente

Plan de gestión de riesgos Tecnologías de la Información

3.3.2. Variable dependiente

Gestión de riesgos relacionados con Tecnologías de la Información en los procesos críticos de créditos y captaciones

Tabla N° 01: Operacionalización de variables

Variable	Indicadores	Dimensiones	Técnicas	Instrumentos
Variable Dependiente: Gestión de Riesgos en Tecnologías de la Información	- Gobierno de los riesgos de Tecnologías de la Información	- Visión común de riesgo. - Conciencia de los riesgos del negocio. - Cumplimiento con la norma en las variables exigidas por la Superintendencia de Banca y Seguros - Efectividad de los componentes del plan de gestión de Tecnologías de la Información: controlando amenazas, vulnerabilidades, impactos, frecuencias. - Efectividad de las actividades de gestión de riesgos de Tecnologías de la Información. - Tiempo de recuperación ante los incidentes (RTO)	- Encuesta. - Observación.	- Modelo de Madurez del Gobierno de Riesgo. - Guía de Observación.
	- Evaluación de Riesgos.	- Recolección de datos. - Análisis de riesgos de Tecnologías de la Información. - Mantenimiento del perfil de riesgo. - Nivel de integración del plan en la gestión de riesgos corporativo.	- Encuesta. - Observación.	- Modelo de Madurez del Gobierno de Riesgo.

				- Guía de Observación.
	- Respuesta a los Riesgos.	- Efectividad en la implantación de los controles y seguimiento de las brechas de seguridad. - Efectividad de los niveles de riesgos referentes a Tecnologías de la Información. - Articulación del riesgo. - Gestión del riesgo. - Reacción a los eventos. - Grado de satisfacción por la información resultante del plan - Grado de satisfacción del plan para la toma de decisiones en relación a las inversiones de los controles de seguridad.	- Encuesta. - Observación.	- Modelo de Madurez del Gobierno de Riesgo. - Guía de Observación.

Fuente: Elaboración Propia

CAPÍTULO IV: MARCO TEÓRICO

4.1. ANTECEDENTES DE INVESTIGACIÓN

4.1.1. Antecedentes en el contexto internacional

TITULO : Diseño del Plan de la Gestión de Riesgos en los proyectos de consultoría de estudios técnicos y diagnóstico del estado mecánico y de corrosión de tuberías, tanques, y vasijas desarrollados por CIMA.

AUTOR : Claudia Patricia Carreño Herrera

AÑO : 2012

UNIVERSIDAD: Universidad para la Cooperación Internacional, Costa Rica

RESUMEN

En esta tesis se planteó como objetivo general de este proyecto fue: Diseñar el plan de gestión de riesgos para los proyectos de consultoría de estudios técnicos y diagnóstico del estado mecánico y de corrosión de tuberías, tanques y vasijas para empresas del sector de hidrocarburos. Este diseño permitió hacer un seguimiento y análisis de los riesgos involucrados en estos proyectos y un plan de respuesta.

La relación con la investigación está en la implantación de una adecuada gestión de seguridad de información en una institución, el primer paso es obtener el apoyo y soporte de la alta gerencia dando a conocer la importancia de la seguridad de información en los procesos que manejan.

TITULO : Gestión de Riesgo de crédito de la Cooperativa de ahorro y crédito maquita Cushunchic: análisis y preparación estadística de variables para el diseño de un modelo credit score de cartera de consumo

AUTOR : Milton Efraín Guamán Guanopatín

AÑO : 2011

UNIVERSIDAD: Universidad Andina Simón Bolívar, Sede Ecuador

RESUMEN

El presente estudio busca analizar y preparar estadísticamente un conjunto de variables para el diseño de un modelo de aprobación CREDIT SCORE de cartera de consumo, tipo probabilístico, que apoye al oficial de crédito en la toma de la decisión antes de conceder o no un crédito de consumo; para que la decisión no sea subjetiva sino objetiva, medible (probabilística) apoyada en una ecuación que contenga sustento teórico y empírico dado por la base de datos histórica de la Cooperativa de ahorro y crédito Maquita Cushunchic.

La relación con la investigación está en la implantación de una adecuada gestión de seguridad de información en una institución financiera, el primer paso es obtener el apoyo y soporte de la alta gerencia dando a conocer la importancia de la seguridad de información en los procesos que manejan.

4.1.2. Antecedentes en el contexto nacional

TITULO : PLAN DE SEGURIDAD PARA UNA ENTIDAD FINANCIERA

AUTOR : Córdova Rodríguez Norma Edith

AÑO : 2003

UNIVERSIDAD: UNMSM – Lima-Perú

RESUMEN

Se usó la metodología Enterprice Security Arquitecture (ESA) para el diseño del modelo de seguridad, tomando como referencia el estándar para la seguridad de información ISO 17799 así como los requerimientos de la Circular N° G-105-2002 publicada por la SBS sobre Riesgos de Tecnología de Información y las normas internas del Banco referidas a la seguridad de información

La relación con la investigación está dada por la aplicación del ISO/IEC 17799 adecuado a las exigencias de la Circular N° G-105-2002 publicada por la SBS sobre Riesgos de Tecnología de Información.

TITULO: **PLANTEAMIENTO DE UN ESQUEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN QUE PUEDE SER EMPLEADO POR UNA INSTITUCIÓN FINANCIERA EN EL PERÚ**

AUTOR: **Moisés Antonio Villena Aguilar**

AÑO: **2006**

UNIVERSIDAD: PUCP – Lima-Perú

RESUMEN

En esta tesis se planteó como objetivo el establecer los principales lineamientos para poder implementar de manera exitosa, un adecuado modelo de sistema de gestión de seguridad de información (SGSI) en una institución financiera en el Perú, el cual apunte a asegurar que la tecnología de información usada esté alineada con la estrategia de negocio y que los activos de información tengan el nivel de protección acorde con el valor y riesgo que represente para la organización, en base al estándar ISO/IEC 17799. Para lo cual se tomó como referencia el modelo de seguridad de información de Mc Cumber, por ser uno de los más influyentes, dado que abarca los principales estados de la información, características y medidas de seguridad.

La relación con la investigación está en la implantación de una adecuada gestión de seguridad de información en una institución financiera, el primer paso es obtener el apoyo y soporte de la alta gerencia dando a conocer la importancia de la seguridad de información en los procesos que manejan.

4.1.3. Antecedentes en el contexto regional

TITULO : **MIGRO TI/SI- Metodología Integral para la gestión de riesgos operativos relacionados con tecnologías y sistemas de información**

AUTOR : **Ampuero Chang, Carlos Enrique**

AÑO : **2006, Chiclayo – Lambayeque**

UNIVERSIDAD: UNPRG Lambayeque -Perú

RESUMEN

La MIGRO TI/SI se ha realizado con el objeto de integrar metodologías dispersas e independientes, tratando de normalizar los objetivos de control, ya que en ciertas metodologías referidas a la gestión de riesgos operativos relacionados con TI/SI, existían redundancias y otras no consideraban aspectos importantes que debían de revisarse. De tal forma concluimos que la MIGRO TI/SI expone un proceso metodológico a seguir, y reúne los aspectos fundamentales a revisar, en el proceso constante de gestión de riesgos operativos relacionados con TI/SI.

Migro TI/SI es consistente porque está basada en normas exigidas por la SBS, los estándares aplicables y aceptados para mejorar las prácticas de control y seguridad de las tecnologías de información propuestos por COBIT.

TITULO : Políticas de seguridad organizacional y control de activos según la norma técnica peruana NTP-ISO/IEC 17799 en la Oficina Central de Informática (OCI) – Universidad Nacional Pedro Ruiz Gallo

AUTOR : Campos Pérez, Jahaira Zuleika y Herrera Piscoya, Francisco Richard

AÑO : 2006, Chiclayo – Lambayeque

UNIVERSIDAD: UNPRG Lambayeque -Perú

RESUMEN

De acuerdo a la Metodología de Gestión de Riesgos en Activos de TI/SI, se consigue clasificar a los Activos de la organización evaluada, ello con la finalidad de poder incidir en la identificación de los riesgos a los que se encuentran expuestos los Activos de tecnología de información y poner énfasis en la mitigación de los mismos.

Este trabajo de investigación permite realizar un inventario de activos de TI/SI en base a estándares y normas, necesario para la implementación de la propuesta.

4.2. BASE TEÓRICA

4.2.1. RIESGO

De acuerdo (Serra, 2011), en su presentación de "ISO 31000:2009. Herramienta para evaluar la gestión de riesgos" realizada en Uruguay por ISACA define a riesgo como "el efecto de la incertidumbre en la consecución de los objetivos", y también dice:

- Incertidumbre porque puede que nunca ocurra.
- El riesgo importa y debe gestionarse porque tiene un efecto (positivo y negativo).
- Ese efecto es sobre los objetivos fijados.

También define al riesgo como el potencial de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y, por consiguiente, ocasione pérdida o daño a la organización.

Según Alejandro Medina (2007) "Riesgo se define como la probabilidad de que las amenazas exploten los puntos débiles, causando pérdidas o daños a los activos e impactos al negocio, es decir, afectando: La confidencialidad, la integridad y la disponibilidad de la información […]. Riesgo es:

- La condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos de la empresa.
- La posibilidad de un impacto negativo sobre los objetivos de la empresa.

El riesgo es una característica de la vida del negocio y debido a que resulta impráctico y poco económico eliminar los riesgos, cada organización tiene un nivel de riesgo aceptable. (Medina, 2007).

El Riesgo de Tecnologías de Información es la pérdida potencial por daños, interrupción, alteración o fallas derivadas del uso o dependencia en el hardware, software, sistemas, aplicaciones, redes y cualquier otro canal de distribución de información que la empresa dispone para prestar sus servicios.

Se asocia con la capacidad de la empresa en que la tecnología disponible satisfaga las necesidades actuales y futuras de la empresa y soporten el cumplimiento de la misión.

El concepto de riesgo de TI puede definirse también como el efecto de una causa multiplicado por la frecuencia probable de ocurrencia dentro del entorno de TI. Es el control el que actúa sobre la causa del riesgo para minimizar sus efectos. Cuando se dice que los controles minimizan los riesgos, lo que en verdad hacen es actuar sobre las causas de los riesgos, para minimizar sus efectos.

ISACA (2009) afirma:

"Un riesgo de TI es también un riesgo del negocio, riesgos del negocio asociados con el uso, propiedad, operación, participación, la influencia y la adopción de las TI en una organización. Se compone de los eventos relacionados con TI que potencialmente podrían afectar el negocio. Este hecho puede ocurrir con una frecuencia y magnitud inciertas, y supone dificultades para alcanzar las metas y objetivos estratégicos." (p. 11)

En muchas organizaciones, los riesgos relacionados con TI se consideran un componente de riesgo operativo, por ejemplo, el sector financiero en el marco de Basilea II. Sin embargo, incluso el riesgo estratégico de TI puede tener un componente financiero, especialmente en aquellas organizaciones en las que es el elemento clave de nuevas iniciativas empresariales. Lo mismo se aplica para el riesgo de crédito, donde una política pobre en cuanto a seguridad de la información se refiere, puede conducir a menores calificaciones de crédito. Por esta razón, es mejor no describir los riesgos de TI con una dependencia jerárquica en una de las categorías de riesgo, tal como se muestra en el ejemplo orientado a la industria financiera de la Figura 1.

Figura 1 : Los riesgos de TI como un componente del universo de riesgos

Fuente: (ISACA, 2009)

PROCESO DE GESTIÓN DE RIESGO

Costas Santos (2011) indica que la Gestión de los Riesgos permite tener control sobre el desarrollo, la implementación y funcionamiento de los procesos, lo cual llevará a lograr de manera eficiente el cumplimiento de sus objetivos estratégicos y estar preparados para enfrentar cualquier incidente que pueda presentarse en sus actividades. (Costas, 2011)

Sobre éstos procesos en donde existe incertidumbre se tienen que realizar acciones y/o construir elementos de control con la finalidad de poder mitigar la frecuencia de las amenazas o para poder reducir las consecuencias que existirán si las acciones de amenaza ocurrieran, hasta llevarlas a la eliminación definitiva de la amenaza o a un nivel de riesgo aceptable para la organización

Una organización puede afrontar un riesgo de cuatro formas diferentes:

- **Aceptar el riesgo**. – Se acepta un riesgo siempre en cuando éste riesgo no es sumamente crítico para le organización, es decir se toma conciencia que el riesgo existe y se tiene que monitorear sobre el daño que pueda causar.

- **Transferir el riesgo**. – Se realizan ésta acción siempre en cuando el riesgo representa una amenaza muy importante para la seguridad de la información, y se opta por transferir al área adecuada para su tratamiento respectivo.
- **Mitigar el riesgo**. – Se mitiga el riesgo o se reduce el riesgo cuando se observa que el riesgo representa una amenaza muy importante para la seguridad de la información y que dicho riesgo es difícil de eliminar, entonces se debe de tomar la decisión de reducir el daño causado reduciendo dicho riesgo.
- **Evitar el riesgo**. - Si el nivel de riesgo es demasiado alto para que la organización lo asuma, puede optar por Evitar el riesgo, eliminando los activos de información o el proceso asociado.

Luego que los controles para poder aceptar, transferir, mitigar, evitar los riesgos han sido aplicados, el nivel de riesgo que queda es el riesgo residual o riesgo sobrante tal como se establece en los Requerimientos de los Sistemas de Gestión de Seguridad de la Información en la norma ISO 27001; la Dirección es el ente encargado que debe establecer el nivel de riesgo aceptable para la organización; Luego de ello los riesgos que excedan de ese nivel deben ser reducidos o minimizados para que no afecten a ninguna actividad de dicha organización.

ORIGEN DEL RIESGO DE TI

Considerando que los riesgos que se encuentran asociados a la tecnología, desde su concepción, desarrollo y utilización, los cuales no solo impactan a las organizaciones que las conciben durante su periodo de desarrollo; los orígenes pueden ser diversos, de los cuales, los más frecuentes según Antonio Hidalgo Nuchera, son:

- Derivado del proceso de adquisición o transferencia de tecnología: regularmente estos son ocasionados por razones internas originadas de planificaciones deficientes o son ocasionados por la falta de adaptación de los recursos humanos que se encuentran implicados en el proceso.

- Originados por dificultades en la organización receptora: son causas que tienen su origen en la organización que dará uso a la TI y que afectan el desarrollo o implantación.
- Derivadas de la tecnología utilizada para su desarrollo: regularmente son originados por el uso de una tecnología inestable o que se vuelve obsoleta.
- Derivadas de factores externos a la organización: corresponden a factores fuera del alcance de la organización que imposibilitan el acceso a la tecnología, su mantenimiento o soporte para continuar con su uso, cuyos factores pueden estar relacionados a causas socioeconómicas o políticas, entre otras.
- Derivadas del mercado y su evolución durante el desarrollo de la tecnología: se encuentran relacionadas a acontecimientos no previstos que pueden impactar directamente en los resultados esperados durante el desarrollo de la tecnología; se encuentran relacionados a aspectos económicos y de penetración tecnológica que, a pesar de no estar ligados a las TI, les impacta desfavorablemente, como, por ejemplo, una crisis económica global, recesión económica y caídas del valor del dinero.

Figura 2 : Fuentes de Riesgo

Fuente: (Amutio Gómez, Candau, & Mañas, 2012)

Los orígenes del riesgo tecnológico no son únicos y estos muchas veces se encuentran relacionados entre sí, por lo cual es importante que al momento de realizar un análisis de riesgos se realice de forma diferente para cada escenario, evaluando el entorno aplicable para el caso estudiado. La Figura 3, muestra la relación entre los diferentes orígenes del riesgo tecnológico que como se podrá observar, se encuentran relacionados, sin embargo, no en todos los casos se presenta esta situación.

Dado que se tienen múltiples orígenes de riesgo y estos pueden presentarse en diferentes circunstancias, generando escenarios diferentes acordes a eventos que se presenten en el momento en que se genera el riesgo o se llega a concebir, los posibles eventos relacionados a un riesgo pueden estar sujetos a fraudes internos, fraudes externos, clientes, productos y servicios, daños físicos, interrupción de negocios e incluso la administración de procesos.

RIESGO ACEPTABLE

De acuerdo a Costas Santos (2011), "Riesgo aceptable es el que conlleva un potencial de perdida menor y que de producirse fallas operacionales no afectan significativamente las condiciones de la operación. […] los activos con riesgo extremo e intolerable deben ser llevados al menos al nivel tolerable. Y en el caso de activos críticos deben ser llevados al nivel aceptable". (Costas, 2011)

Para la aceptación de los riesgos se debe tener en cuenta:

- La Política organizacional.
- Nivel de sensibilidad y de criticidad de los activos.
- Niveles aceptables de los impactos que pudieran suceder.
- Rentabilidad de la implementación.

4.2.2. NORMA ISO 27001

Existen instrumentos que estando alineados con estos estándares ISO 27001 y que facilitan a una empresa enfocarse en implementar herramientas y metodologías que satisfagan los requerimientos básicos de la administración de

riesgos en sus sistemas de información tales como la metodología MAGERIT para realizar el análisis y gestión del riesgo enfatizando en las políticas y controles de seguridad por cada capa de la norma ISO 27001

Según Pablo Casto (2014) "*La norma ISO/IEC 27001 estipula que debe utilizarse un método de análisis de riesgo, pero esto no es una parte del estándar, y no se propone ningún método específico, aparte de la integración del proceso recursivo PDCA (Plan, Do, Check, Act) del modelo definido para la creación del SGSI*".

Por una parte, tenemos a ISO y por otra parte tenemos a NIST cada una de estas instituciones ha propuesto un marco de trabajo para el tema se la seguridad informática, antes de todo debemos de aclarar cuál es el inicio de ambas organizaciones.

La ISO (Organización Internacional de Normalización), es una organización para la creación de estándares internacionales compuesto por diversas organizaciones nacionales de estandarización, dicha organización se encarga de fijar normas aceptadas en Europa y en muchos países del mundo.

El NIST (Instituto Nacional de Estándares y Tecnología) participa en los EEUU, es una organización conocida como Instituto Nacional de Normas y Tecnología, es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos.

Según ISACA (2009), "Esta norma muestra cómo aplicar los controles propuestos en la ISO 17799, estableciendo los requisitos para construir un SGSI, "auditable" y "certificable", respecto a los controles, aparecen como anexos. Estos más los que la organización desee incorporar, deberán conformar un sólido sistema que permita el fin último: la seguridad de la información."

El SGSI de la ISO 27001 le permite prevenir o reducir eficazmente el nivel de riesgo mediante la implantación de los controles adecuados, preparando la organización ante posibles emergencias, garantizando la continuidad del negocio.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo lo referente a seguridad de la información:

- **Confidencialidad**: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad**: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad**: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Todas estas características pueden ser requeridas o no dependiendo de cada caso. Cuando se requieren, no es evidente que se disfruten sin más. Lo habitual que haya que poner medios y esfuerzo para conseguirlas. A racionalizar este esfuerzo se dedican las metodologías de análisis y gestión de riesgos que comienzan con una definición:

RIESGO:

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema.

ANÁLISIS DE RIESGOS:

Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización. Sabiendo lo que podría pasar, hay que tomar decisiones.

GESTIÓN DE RIESGOS:

Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

Obsérvese que una opción legítima es aceptar el riesgo. Es frecuente escuchar que la seguridad absoluta no existe; en efecto, siempre hay que aceptar un riesgo que, eso sí, debe ser conocido y sometido al umbral de calidad que se requiere del servicio.

Como todo esto es muy delicado, no es meramente técnico, e incluye la decisión de aceptar un cierto nivel de riesgo, deviene imprescindible saber en qué condiciones se trabaja y así poder ajustar la confianza que merece el sistema. Para ello qué mejor que una aproximación metódica que permita tomar decisiones con fundamento y explicar racionalmente las decisiones tomadas.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial.

Entre los principales beneficios de la implementación de ésta norma se tiene:

- Establecimiento de una metodología de gestión de la seguridad de la información clara y bien estructurada.
- Reducción de riesgos de pérdida, robo de la información.
- Los clientes tienen acceso a la información de manera segura, lo que se traduce en confianza.
- Los riesgos y sus respectivos controles son revisados constantemente.
- Las auditorías externas permiten identificar posibles debilidades del sistema con respecto a la gestión de la información.
- Permite la continuidad en las operaciones del negocio tras incidentes de gravedad que pudieran ocurrir.
- Garantizar el cumplimiento de las leyes y regulaciones establecidas en materia de gestión de información.

- Incrementa el nivel de concientización del personal con respecto a la seguridad informática.
- Proporciona confianza y reglas claras al personal de la empresa.
- Provee la seguridad como una ventaja competitiva para las empresas que realizan operaciones de crédito y captaciones.

4.2.3. COBIT (CONTROL OBJETIVES FOR INFORMATION AND RELATED TECHNOLOGY) (Objetivos de Control para la Información y Tecnologías Relacionadas).

DEFINICIÓN:

De acuerdo a CobIT (2000), "Es una metodología que integra todas las entidades dentro de una organización; gerencia, responsables de información y usuarios finales. Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que COBIT hace referencia como requerimientos de negocio para la información. (COBIT, 2000)

La manera en que COBIT provee este marco para el control y la gobernabilidad de TI. Es una herramienta de gestión de TI que vincula tecnología informática y prácticas de control, COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, mini computadoras y ambientes distribuidos. Está basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

MISIÓN DE COBIT:

En COBIT (2000), se plantea que la misión de COBIT es investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de

control para tecnología de información que sea de uso cotidiano para gerentes y auditores

PRINCIPIOS:

En COBIT (2000), se establece que el enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con las TI que deben ser administrados por procesos de TI.

REQUERIMIENTOS DE LA INFORMACIÓN DEL NEGOCIO:

Según COBIT (2000), para alcanzar los requerimientos de negocio, la información necesita satisfacer ciertos criterios:

- Requerimientos de Calidad: Calidad, Costo y Entrega.
- Requerimientos Fiduciarios: Efectividad y Eficiencia operacional, Confiabilidad de los reportes financieros y Cumplimiento le leyes y regulaciones.
    - Efectividad: La información debe ser relevante y pertinente para los procesos del negocio y debe ser proporcionada en forma oportuna, correcta, consistente y utilizable.
    - Eficiencia: Se debe proveer información mediante el empleo óptimo de los recursos (la forma más productiva y económica).
    - Confiabilidad: Proveer la información apropiada para que la administración tome las decisiones adecuadas para manejar la empresa y cumplir con sus responsabilidades.
    - Cumplimiento: de las leyes, regulaciones y compromisos contractuales con los cuales está comprometida la empresa.
- Requerimientos de Seguridad: Confidencialidad, Integridad y Disponibilidad
    - Confidencialidad: Protección de la información sensible contra divulgación no autorizada.

- Integridad: Refiere a lo exacto y completo de la información, así como a su validez de acuerdo con las expectativas de la empresa.
- Disponibilidad: accesibilidad a la información cuando sea requerida por los procesos del negocio y la salvaguarda de los recursos y capacidades asociadas a la misma.

RECURSOS DE TECNOLOGÍAS DE LA INFORMACIÓN

En COBIT (2000) se establecen los siguientes recursos en Tecnologías de la Información necesarios para alcanzar los objetivos de negocio:

- Datos: Todos los objetos de información. Considera información interna y externa, estructurada o no, gráficas, sonidos, etc.
- Aplicaciones: entendido como los sistemas de información, que integran procedimientos manuales y sistematizados.
- Tecnología: incluye hardware y software básico, sistemas operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones, multimedia, etc.
- Instalaciones: Incluye los recursos necesarios para alojar y dar soporte a los sistemas de información.
- Recurso Humano: Por la habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorear los sistemas de Información.

ESTRUCTURA DE COBIT

COBIT (2000) estructura en su propuesta Dominios, los cuales contienen declaraciones de los resultados deseados o propósitos a ser alcanzados mediante la implementación de 302 objetivos de control detallados y específicos a través de los 34 procesos los cuales aseguran un adecuado sistema de control para el entorno TI de la empresa.

El concepto de dominios permite agrupar los objetivos de control de COBIT en distintas áreas de actividad de la organización, COBIT esta agrupado en 4

dominios: planificación y organización, adquisición e implantación, entrega y soporte, y monitoreo.

- **PLANEACIÓN Y ORGANIZACIÓN.**

  Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

- **ADQUISICIÓN E IMPLANTACIÓN**

  Para llevar a cabo la estrategia de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

- **ENTREGA Y SOPORTE**

  En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad.

  Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

- **MONITOREO.**

  En este dominio se hace referencia a las actividades de verificación de cumplimiento y eficacia de los servicios implementados: auditoría, revisiones a posteriori, etc.

4.2.4. METODOLOGÍA DE GESTIÓN DE RIESGO DE TECNOLOGÍAS DE LA INFORMACIÓN (ISACA)

Una metodología de gestión de riesgos consiste en cómo debe llevarse a cabo para cumplir con lo establecido por la Norma ISO 27001. En un contexto general debe estimar el grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización y posteriormente implementar el o los controles adecuados para su tratamiento.

Según ISACA (2009), "Las etapas mínimas que debe contemplar una metodología de gestión de riesgos de Tecnologías de la Información son":

ESTIMACIÓN DE RIESGOS

Según (Flores, 2010) en su publicación "Análisis y Gestión de Riesgo" indica que "la estimación de riesgos describe cómo estudiar los riesgos dentro de la planeación general del entorno informático y se divide en los siguientes pasos":

- La identificación de riesgos, genera una lista de riesgos capaces de afectar el funcionamiento normal del entorno informático.
- El análisis de riesgos, mide su probabilidad de ocurrencia y su impacto en la organización.
- La asignación de prioridades a los riesgos.

IDENTIFICACIÓN DE RIESGOS

Según (Flores, 2010) indica que en este paso se identifican los factores que introducen una amenaza en la planificación del entorno informático. Los principales factores que se ven afectados son:

- Creación de la planificación; Incluye la planificación excesivamente optimista, planificación con tareas innecesarias, y organización de un entorno informático sin tener en cuenta áreas desconocidas y la envergadura del mismo.
- La organización y gestión; Presupuestos bajos, El ciclo de revisión/decisión de las directivas es más lento de lo esperado.

- El entorno de trabajo; mal funcionamiento de las:
  - Herramientas de desarrollo, espacios de trabajo inadecuados y la curva de aprendizaje de las nuevas tecnologías es más larga de lo esperado.
  - Las decisiones de los usuarios finales; Falta de participación de los usuarios finales y la falta de comunicación entre los usuarios y el departamento de informática
  - El personal contratado; Falta de motivación, falta de trabajo en equipo y trabajos de poca calidad.
- Los procesos, que incluye: La burocracia, falta de control de calidad y la falta de entusiasmo.
- Se puede considerar como los orígenes de la Administración de los Riesgos de Tecnologías de la Información a los siguientes aspectos:
  - Requerimientos legales, regulatorios, contractuales
  - Acelerados avances tecnológicos
  - Incidentes de seguridad (comunicaciones divulgadas)
  - Preocupación de los usuarios
  - Pérdidas económicas
  - Crecimiento generalizado de procesos de negocio soportados en tecnología de información.

ANÁLISIS DE RIESGOS

Según (Belen Haro, 2014) define al Análisis de Riesgos como que una vez que se hayan identificado los riesgos en la planificación, el paso siguiente es analizarlos para determinar su impacto, tomando así las posibles alternativas de solución.

EXPOSICIÓN A RIESGOS

Una actividad útil y necesaria en el análisis de riesgos es determinar su nivel de exposición en cada uno de los procesos en que se hayan identificado.

1. ESTIMACIÓN DE LA PROBABILIDAD DE PÉRDIDA

Las principales formas de estimar la probabilidad de pérdida son las siguientes:

- Disponer de la persona que está más familiarizada con el entorno informático para que estime la probabilidad de ocurrencia de eventos perjudiciales.
- Usar técnicas Delphi o de consenso en grupo.
- El método Delphi consiste en reunir a un grupo de expertos para solucionar determinados problemas. Dicho grupo realiza la categorización individual de las amenazas y de los objetos del riesgo.
- Utilizar la calibración mediante adjetivos, en la cual las personas involucradas eligen un nivel de riesgo entre (probable, muy probable) y después se convierten a estimaciones cuantitativas.

2. PRIORIZACIÓN DE RIESGOS

En este paso de la estimación de riesgos, se estiman su prioridad de forma que se tenga forma de centrar el esfuerzo para desarrollar la gestión de riesgos. Cuando se realiza la priorización (elementos de alto riesgo y pequeños riesgos), estos últimos no deben ser de gran preocupación, pues lo verdaderamente crítico se puede dejar en un segundo plano.

3. CONTROL O TRATAMIENTO DE RIESGOS

Una vez que se hayan identificado los riesgos del entorno informático y analizado su probabilidad de ocurrencia, existen bases para controlarlos que son:

- Planificación
- Resolución de riesgos
- Monitorización de riesgos

A) PLANIFICACIÓN DE RIESGOS

Su objetivo, es desarrollar un plan que controle cada uno de los eventos perjudiciales a que se encuentran expuestas las actividades informáticas.

B) RESOLUCIÓN DE RIESGOS (INCLUYE MITIGACIÓN Y TRANSFERENCIA DE RIESGOS)

La resolución de los riesgos está conformada por los métodos que controlan el problema de un diseño de controles inadecuado, los principales son:

- Evitar el Riesgo: No realizar actividades arriesgadas.
- Conseguir información acerca del riesgo.
- Planificar el entorno informático de forma que, si ocurre un riesgo, las actividades informáticas sean cumplidas.
- Eliminar el origen del riesgo, si es posible desde su inicio.
- Asumir y comunicar el riesgo.

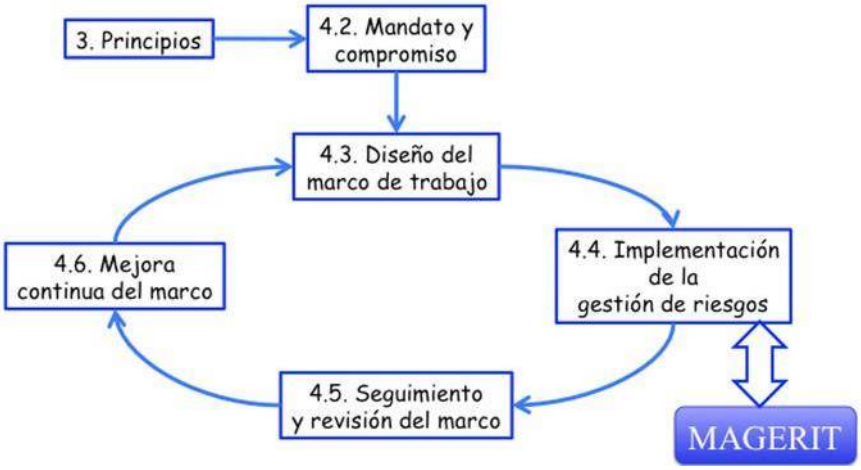
C) MONITORIZACIÓN DE RIESGOS

La vida en el mundo informático sería más fácil si los riesgos apareciesen después de que hayamos desarrollado planes para tratarlos. Pero los riesgos aparecen y desaparecen dentro del entorno informático, por lo que se necesita una monitorización para comprobar cómo protegerse el control de un riesgo e identificar como aparecen nuevos eventos perjudiciales en las actividades informáticas.

4.2.5. MAGERIT VERSION 3.0

Siguiendo la terminología de la normativa ISO 31000, MAGERIT responde a lo que se denomina "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos". En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Figura 3 : ISO 31000 - Marco de trabajo para la gestión de riesgos



Fuente: MAGERIT – versión 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I – Método del Ministerio de Hacienda y Administraciones Públicas de Secretaría General Técnica del Gobierno de España 2012, Página 07

Según (MAGERIT, 2012) Hay varias aproximaciones al problema de analizar los riesgos soportados por los sistemas TIC: guías informales, aproximaciones metódicas y herramientas de soporte. Todas buscan objetivar el análisis de riesgos para saber cuán seguros (o inseguros) son los sistemas y no llamarse a engaño. El gran reto de todas estas aproximaciones es la complejidad del problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poco fiar. Es por ello que en MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

MAGERIT persigue los siguientes objetivos:

DIRECTOS:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

INDIRECTOS:

1. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso También se ha buscado la uniformidad de los informes que recogen los hallazgos y las conclusiones de las actividades de análisis y gestión de riesgos:

MODELO DE VALOR

Caracterización del valor que representan los activos para la Organización, así como de las dependencias entre los diferentes activos.

DE MAPA RIESGOS

Relación de las amenazas a que están expuestos los activos.

DECLARACIÓN DE APLICABILIDAD

Para un conjunto de salvaguardas, se indica sin son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.

EVALUACIÓN DE SALVAGUARDAS

Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

ESTADO DE RIESGO

Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar to-mando en consideración las salvaguardas desplegadas.

INFORME DE INSUFICIENCIAS

Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema. Es decir, recoge las vulnerabilidades del sistema, entendidas como puntos débilmente protegidos por los que las amenazas podrían materializarse.

CUMPLIMIENTO DE NORMATIVA

Satisfacción de unos requisitos. Declaración de que se ajusta y es conforme a la normativa correspondiente.

PLAN DE SEGURIDAD

Conjunto de proyectos de seguridad que permiten materializar las decisiones de tratamiento de riesgos

4.2.6. PILAR. (Procedimiento Informático Lógico para el Análisis de Riesgos)

PILAR es una herramienta desarrollada para soportar el análisis y la gestión de riesgos de sistemas de información siguiendo la metodología MAGERIT. Las siglas de PILAR provienen de "Procedimiento Informático Lógico para el Análisis de Riesgos" creado por el Centro Nacional de Inteligencia, actualmente se encuentra disponible la versión 5.4.

Analiza los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Para tratar el riesgo se proponen: salvaguarda o contramedidas, normas y procedimientos de seguridad.

Esta herramienta soporta las fases del método MAGERIT:

- Caracterización de los activos: identificación, clasificación, dependencias y valoración
- Caracterización de las amenazas
- Evaluación de las salvaguardas

Evalúa el impacto y el riesgo, acumulado y repercutido, potencial y residual, presentándolo de forma que permita el análisis de por qué se da cierto impacto o cierto riesgo.

Las salvaguardas se califican por fases, permitiendo la incorporación a un mismo modelo de diferentes situaciones temporales. Se puede incorporar el resultado de los diferentes proyectos de seguridad a lo largo de la ejecución del plan de seguridad, monitorizando la mejora del sistema.

PILAR presenta los resultados en varias formas, ya sea en informes RTF, gráficas o tablas que se pueden agregar a una hoja de cálculo, logrando elaborar diferentes tipos de informes y presentaciones de los resultados.

Finalmente, la herramienta calcula calificaciones de seguridad respecto a normas ampliamente conocidas, como son UNE-ISO/IEC 27002:2009: sistemas de gestión de seguridad, RD 1720/2007: datos de carácter personal y RD 3/2010: Esquema Nacional de Seguridad.

Cabe destacar que esta herramienta incorpora tanto los modelos cualitativos como cuantitativos, logrando alternarse entre estos para extraer el máximo beneficio de las posibilidades teóricas de cada uno de ellos.

4.3. CONCEPTOS Y DEFINICIONES

ACTIVO ISACA (2009)

Según ISACA (2009), un activo es cualquier elemento en el entorno de la organización, al cual se le asigna valor y por ende requiere algún grado de protección. Esto podría incluir aplicaciones de software o hardware y otros elementos menos tangibles como datos o personas.

AMENAZAS Peña Gloria y Peña Lillo (2005),

Según Peña Gloria y Peña Lillo (2005), amenazas son los eventos que pueden desencadenar un Incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus Activos. Las amenazas se pueden materializar y transformarse en agresiones.

GESTIÓN DE RIESGOS Alejandro Medina (2007)

Alejandro Medina (2007) define gestión de riesgos como el proceso efectuado por la dirección y el personal, para identificar, analizar, evaluar y controlar el riesgo.

IMPACTO Peña Gloria y Peña Lillo (2005)

Según Peña Gloria y Peña Lillo (2005), impacto es el daño producido a la organización por un posible incidente y es el resultado de la agresión sobre el activo, o visto de manera más dinámica, la diferencia en las estimaciones de los estados (de seguridad) obtenidas antes y después del evento.

POLÍTICA DE SEGURIDAD Costas Santos (2011)

De acuerdo a Costas Santos (2011), políticas de seguridad es el conjunto de directivas y normas emitidas por la gerencia que escriben los objetivos de la organización respecto a la protección de sus activos de información

VULNERABILIDAD Peña Gloria y Peña Lillo (2005)

Según Peña Gloria y Peña Lillo (2005), vulnerabilidad es la ocurrencia real de materialización de una amenaza sobre un activo, la vulnerabilidad es una propiedad de la relación entre un activo y una amenaza. Ejerce entre ambos una función de mediación en el cambio del estado de seguridad del activo; siendo también el mecanismo de paso desde la amenaza a la agresión

CAPÍTULO V: DESARROLLO DE LA PROPUESTA

POBLACIÓN, MUESTRA DE ESTUDIO y MUESTREO

Se tomará como población muestral a los siguientes trabajadores de la Caja:

- Jefe de Tecnologías de la Información.
- Jefe del Área de desarrollo.
- Especialista en comunicaciones.
- Especialista en base de datos.
- Analistas programadores (5).
- Jefes de las áreas usuarias (9).

MÉTODOS, TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

En la presente investigación se usarán diversas técnicas e instrumentos que permitirán la recolección de información: documentación, entrevistas, encuestas y observaciones directas.

TÉCNICAS

- **ENCUESTA**: Según Arias (2006) Es una técnica que pretende obtener información que suministra un grupo o muestra de sujetos acerca de si mismos, o en relación con un tema en particular." (Pág. 72). Esta técnica permitió la recolección de información directamente del personal que participa en los procesos de Gestión de Riesgos de Tecnología de Información de la Caja.

  Se realizarán encuestas escritas, donde los actores participantes evaluarán la madurez de la gestión de riesgos de Tecnologías de la Información. Están orientados básicamente a los usuarios de los sistemas informáticos de las diferentes áreas de la Caja, caso de estudio. (Ver Anexo N° 01). Se aplicará en el pre test.

- **OBSERVACIÓN**: Es una técnica que permitió tener contacto directo con la realidad y con quienes se hicieron las entrevistas, lo cual ayudó a obtener un mayor

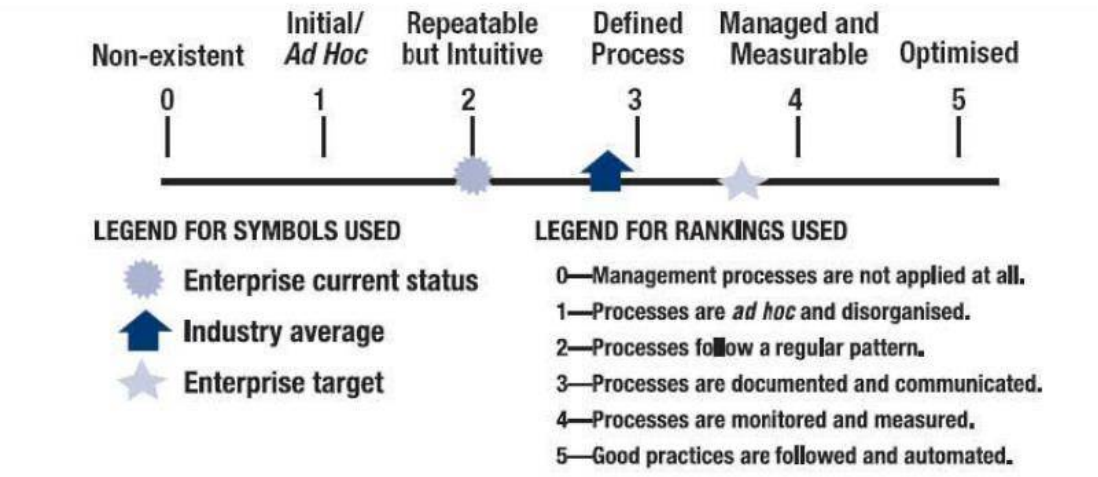
conocimiento de la realidad de la Gestión de Riesgos de Tecnología de Información.

Para complementar el análisis de riesgos operativos relacionados con Tecnologías de la Información resultante de las entrevistas. (proceso evaluación de la implementación y cumplimiento de los controles). Se elaboraron formatos del tipo CHEKCLIST de acuerdo al tipo activo tecnológico que se evalúa. Se aplicará en el pre test y post test.

INSTRUMENTOS

- **MODELO DE MADUREZ**: Este instrumento ha sido utilizado para determinar el nivel de madurez de la Gestión de Riesgos de Tecnología de Información, dicho modelo consta de 209 preguntas, de los cuales 100 corresponden al indicador de "Gobierno del Riesgo", 55 corresponden al indicador de "Evaluación del Riesgo" y 54 corresponden al indicador de "Respuesta al Riesgo".

Figura 4 : Modelo de Madurez



Fuente: (ISACA, 2009)

A continuación, se describen todos los niveles establecidos en el Modelo de Madurez:

- **Nivel O - No Existe**: En este nivel la empresa no ha implementado ningún proceso para gestionar el riesgo o no ha logrado alcanzar su propósito. No se

cuenta con evidencias de logros obtenidos y posiblemente la organización no ha reconocido los riesgos por lo cual no existe comunicación alguna de los mismos y no se tiene consciencia de la necesidad de implementar controles ni se cuenta con la capacidad para reaccionar ante el riesgo buscando limitar la frecuencia y el impacto de incidentes relacionados con las TI.

- **Nivel 1 - Proceso Iniciado o Ad Hoc**: en este nivel la mayoría de procesos son Ad Hoc y caóticos, la empresa realiza acciones para mitigar el riesgo reconociendo las necesidades de reaccionar ante estos, sin embargo, se limitan solamente a evitarlos cumpliendo con requisitos o transfiriendo el riesgo ya sea a través de la adquisición de seguros o compartiendo el riesgo con algún proveedor.

  En éste nivel, se cuenta con controles implementados, enfocados al cumplimiento de requisitos del negocio que han sido aplicados de forma aislada lo cual puede ocasionar que áreas diferentes controlen sus riesgos de forma independiente.

- **Nivel 2 - Proceso Manejable**: en este nivel se pone en orden el caos, se tiene consciencia individual de las amenazas con definición de puntos de contacto para reaccionar ante el riesgo si estos se materializan; existe una comunicación de los riesgos y las respuestas ante estos se ve afectada por un lenguaje de negocio de una unidad específica y por competencia entre áreas.

  Regularmente los riesgos que se presentan en éste nivel presentan un patrón, los cuales normalmente ocurren cuando se trabaja sobre la implementación de controles para mitigarlos; se cuenta con requisitos mínimos para formar áreas críticas que gestionan el riesgo y es posible que se detecten deficiencias en los controles que no son atendidos de forma oportuna ya que este nivel solamente intuye los riesgos.

- **Nivel 3 - Proceso Definido**: al igual que el anterior, se tiene una consciencia de las amenazas con la diferencia que en este nivel se comprende el impacto que representa para el negocio y las acciones concretas que deben realizarse si

el riesgo llegara a materializarse. Un beneficio fundamental que se tiene en el nivel 3, es que los procesos se encuentran debidamente documentados y son comunicados a los diferentes niveles de la organización, asimismo, los procesos se encuentran estandarizados de tal forma que aplican para todo proyecto, a diferencia del nivel 2 en donde pueden existir procesos por proyecto los cuales difieren entre ellos.

Bajo este modelo de respuesta al riesgo, se observa capacitación constante del personal para gestionar las amenazas y riesgos relacionados a TI, escenarios de riesgo y controles relacionados a sus funciones y responsabilidades. Se cuenta con herramientas para automatizar la reducción de riesgos y se cuenta con un plan para realizarlo.

- **Nivel 4 - Proceso Gestionado o Manejado Cuantitativamente**: la empresa cuenta con un proceso de gestión de riesgos planificado, supervisado y ajustado, donde sus resultados se encuentran definidos, controlados y son mantenidos; se tiene una comprensión individual y organizativa de requisitos para gestionar los riesgos. Hay involucramiento de la alta gerencia que con apoyo de la gestión de TI determinan si una condición de riesgos se encuentra o no en los umbrales de tolerancia.

  En este nivel existe un crecimiento, mejora y redefinición que permite actualizar continuamente la gestión del riesgo que incluye la forma de articular el riesgo, mitigación, reacción ante la materialización del mismo y aprovechamiento de las oportunidades que conlleva la mitigación; para esto se utilizan los controles para establecer causas comunes de variación en los procesos y así modificar los procesos para alcanzar mejores resultados. Se utilizan herramientas para gestionar el riesgo de cartera del negocio, supervisar los controles, recursos y capacidades de la empresa.

- **Nivel 5 - Proceso Optimizado**: el proceso definido para la gestión del riesgo es mejorado continuamente a través de mejoras continuas, incrementales y tecnológicas, de tal forma que cumple con las metas y requisitos del negocio

presentes y futuros. Se implementan mejores prácticas para la gestión del riesgo y se automatizan controles.

Se cuenta con una estrategia para dar respuesta al riesgo, aplicando de forma integral las estrategias y se aplican controles que consideran el costo-beneficio para mitigar el riesgo continuamente, analizando que la inversión sea justificable para la empresa. A diferencia del nivel 4 que se orienta a encontrar causas de variación y proveer una predicción estadística de los resultados, el nivel 5 se enfoca en causas comunes de variación de procesos para mejorarlos.

- La encuesta del modelo de madurez se basa en los tres dominios que cubre el Marco de Trabajo la cual contiene una serie de preguntas puntuales que permiten establecer la frecuencia con la cual se realizan ciertas actividades relacionadas a la Gestión de Riesgos de Tecnología de Información.

Esta investigación se centró solamente en describir el nivel de madurez de la Caja de Ahorro y Créditos SIPAN S.A. para gestionar el riesgo no incluyendo la identificación de riesgos puntuales ni el nivel de exposición a cada uno de estos.

La recopilación de datos se dio mediante entrevistas a los principales roles de la organización relacionados a la Gestión de Tecnologías de la Información y la Gestión de Riesgos de Tecnologías de la Información, asimismo a través de la observación y la experiencia del investigador.

Para describir la frecuencia con que se realizan las actividades relacionadas a la Gestión de Riesgos de Tecnologías de la Información, se trabajó con una escala de 6 niveles los cuales se citan en el siguiente cuadro.

Tabla Nº 02: Escalas de Evaluación

Valor	Descripción	Nivel de Madurez	Frecuencia
0	Los procesos de manejo de riesgos no son aplicados.	No Existe	Nunca

1	Los procesos son Ad Hoc y desorganizados.	Inicial	Rara Vez
2	Los procesos siguen un patrón regular.	Repetible	A Veces
3	Los procesos son documentados y comunicados.	Definido	Frecuentemente
4	Los procesos son supervisados y medidos.	Gestionado	Casi Siempre
5	Las mejores prácticas son seguidas y automatizadas.	Optimizado	Siempre

Fuente: Elaboración Propia

- **GUÍA DE OBSERVACIÓN**: Este instrumento se utilizó para establecer el contexto de observación durante la presente investigación.
- **DOCUMENTACIÓN**, Es en donde se incluye los documentos estratégicos, administrativos y legales pertenecientes a la Caja, y se elaborarán fichas de revisión de datos de cada documento que se revise, conteniendo información esencial de cada uno de ellos. Los documentos a revisar serán los siguientes:

DOCUMENTACIÓN INSTITUCIONAL

a. Plan estratégico de La Caja
b. Acuerdos de confidencialidad

DE LA JEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN

a. Plan estratégico de Tecnologías de la Información
b. Plan anual de Tecnologías de la Información
c. Sistema de Gestión de Seguridad de la Información

ÁREA DE DESARROLLO

a. Metodología de desarrollo
b. Arquitectura de base de datos
c. Procedimiento de atención a requerimientos de áreas usuarias

d. Procedimiento de certificación de módulos

e. Biblioteca de cambios (casos)

ÁREA DE PRODUCCIÓN

a. Inventario de hardware y software y su correspondiente procedimiento de actualización

b. Listado de licencias de software

c. Procedimientos de respaldo de la información

d. Procedimientos de altas, bajas y modificación de usuarios de los sistemas

e. Procedimiento para la administración de perfiles de usuarios

f. Procedimiento para respaldo de la información

g. Políticas y normativa de uso de correo electrónico

h. Plan de mantenimiento de equipos y Cartera de proveedores

i. Listado de usuarios del sistema con sus correspondientes niveles de acceso según el perfil de usuario asignado

j. Manuales de usuario de los diferentes módulos de los Sistemas de La Caja

k. Arquitectura física y lógica de la red de datos

GESTIÓN DE RIESGOS

a. Manual de gestión de riesgos operativos de Tecnologías de la Información, con sus correspondientes informes y plan de pruebas.

b. Plan de continuidad del negocio, con sus correspondientes informes y plan de pruebas

c. Plan y procedimientos de recuperación de desastres relacionados con Tecnologías de la Información, con sus correspondientes informes y plan de pruebas

d. Estructura de pistas de auditoria

e. Políticas de clasificación de la información

f. Matrices de riesgos de las áreas de Tecnologías de la Información

- **ENTREVISTAS**, las entrevistas nos ayudaran a obtener información de la implementación y cumplimiento de los controles que se implementen para cada uno de los activos tecnológicos evaluados. Serán llevados mediante un formato tipo CHECKLIST preparados para el cumplimiento de los controles (Ver Anexo N° 02).

  Se entrevistará a:

  - Jefe del Área de Tecnologías de la Información.
  - Jefe de la unidad/sección de desarrollo.
  - Jefe de la unidad/sección de producción.
  - Jefe del área de riesgos.
  - Oficial de seguridad de la información.

PLAN DE PROCESAMIENTO PARA ANÁLISIS DE DATOS

Para el análisis estadístico de los datos, se procederá en función al análisis univariado de la siguiente manera:

- Se utilizarán el promedio y porcentaje como estadísticos de medición de cada uno de los indicadores de las variables dependientes tanto para los valores obtenidos en el PRETEST como en el POSTEST, de modo que finalmente se efectuarán comparaciones de estos resultados por cada variable y se efectuará el contraste de hipótesis correspondiente.
- Además, se aplicará el estadístico Desviación estándar para determinar si los datos recopilados se encuentran ampliamente distribuidos o no.
- Haciendo uso de algunos de los estadísticos antes mencionados se efectuará el cálculo del estadístico Distribución Muestral Estándar (Z), de modo que esta prueba confiera mayor rigor a la contrastación de la hipótesis.
- Como herramienta informática para el análisis estadístico de datos se empleará el software SPSS 2.0.

METODOLOGIA

Se llevó a cabo la propuesta de un Plan de Gestión de Riesgo lo cual permitió analizar, clasificar y determinar el riesgo para luego establecer herramientas que permita controlar.

Identificando y evaluando los componentes, estándares y metodologías que se establecen en la Gestión de Riesgo de Tecnologías de la Información como las vulnerabilidades, las amenazas, los activos, los impactos y las probabilidades de identificar el riesgo de nivel de riesgo existente como el riesgo aceptable en la empresa.

En el proceso de construcción de la propuesta, se ha tomado como referencia las exigencias de la Superintendencia de Banca y Seguros, a través de sus normativas: Resolución SBS 2116-2009 que norma el sistema de Riesgo Operacional que deben implementar las organizaciones financieras en el Perú y la Circular G-105-2002 que establece los lineamientos para la Gestión de Riesgos de TI de éste tipo de empresas.

Por lo tanto, el Plan propuesto se basa en las políticas de seguridad, normas y reglas exigidas a las entidades financieras en el Perú por parte de su ente supervisores como es la SBS

El Plan propuesto contiene cuatro fases, que abarcan las etapas de evaluación de riesgos y tratamiento de los mismos:

A. ANÁLISIS DE RIESGOS

Consiste en determinar aquellos riesgos que pueden afectar al a los procesos críticos de créditos y captaciones de la Caja Sipán, informarse acerca de sus características. El peor riesgo es aquel que no se identifica, dado que si se sabe de su existencia se pueden tomar las medidas necesarias para que no influya en el proyecto o incluso poder sacar partido de él. Por ello, se los debe conocer, así no ignorarlos, sino controlarlos.

Tras la identificación, es importante proceder a clasificar los riesgos que se han detectado. Para ello se pueden definir distintos sistemas de clasificación de los

riesgos en categorías tanto por el tipo de riesgo (técnico, externo, de organización, de gestión, etc.), por la influencia sobre el proyecto (riesgos de leve, moderado o severo impacto sobre el proyecto) o la probabilidad de que se presenten (riesgos de baja, intermedia o elevada probabilidad).

B. CLASIFICACIÓN Y EVALUACIÓN DE LOS RIESGOS

Habiendo identificado los principales activos, el siguiente paso consiste en identificar las amenazas a las que estos están expuestos. Tal y como imaginamos, el conjunto de amenazas es amplio y diverso por lo que debemos hacer un esfuerzo en mantener un enfoque práctico y aplicado. Por ejemplo, si nuestra intención es evaluar el riesgo que corremos frente a la destrucción de nuestro servidor de documentos, es conveniente, considerar las averías del servidor, la posibilidad de daños por agua (rotura de una tubería o inundación) o los daños por fuego, en lugar de plantearnos el riesgo de que el activo sea destruido por un meteorito.

C. IMPLEMENTACIÓN DE CONTROLES

Una vez clasificado y evaluado los riesgos, debemos tratar aquellos riesgos que superen un límite que nosotros mismos hayamos establecido. Por ejemplo, trataremos aquellos riesgos cuyo valor sea superior a “4” o superior a “Medio” en caso de que hayamos hecho el cálculo en términos cualitativos. A la hora de tratar el riesgo, existen cuatro estrategias principales:

Por último, cabe señalar que como realizamos este análisis de riesgos en el contexto de un Plan de Gestión de Riesgos, las acciones e iniciativas para tratar los riesgos pasarán a formar parte del mismo. Por lo tanto, deberemos clasificarlas, priorizarlas e implementar controles o salvaguardas que ayuden a minimizar o desaparecer el riesgo que se tenga, llevar a cabo un análisis de riesgos nos proporciona información de gran valor y contribuye en gran medida a mejorar la seguridad de la organización.

D. CONTROL DE EFICIENCIA Y MADUREZ

Para poder prever la aparición de un riesgo que afecte a los activos de Tecnologías de la Información es necesario conocer signos de alarma que permitan anticiparse

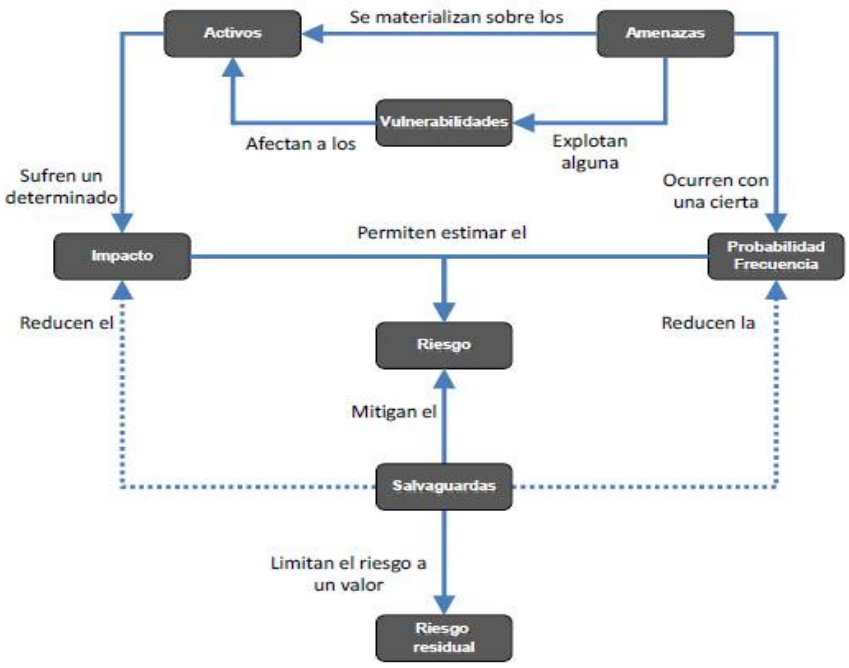
a él. Si esto no es posible, al menos, se deben poseer mecanismos de monitorización de los activos con los que se pueda conseguir detectar un riesgo en el mismo momento en el que se presenta.

La finalidad de éste control es poner en práctica las actitudes previstas para enfrentarse a un riesgo o los planes de contingencia establecidos en el momento adecuado: antes de que el riesgo haya influido de manera significativa en el activo de Tecnología de la Información.

Además, la propia monitorización de la reacción ante los riesgos y de la ocurrencia de los mismos puede permitir, a posteriori, mejorar las medidas de prevención, reducir los tiempos y aumentar la efectividad de la reacción.

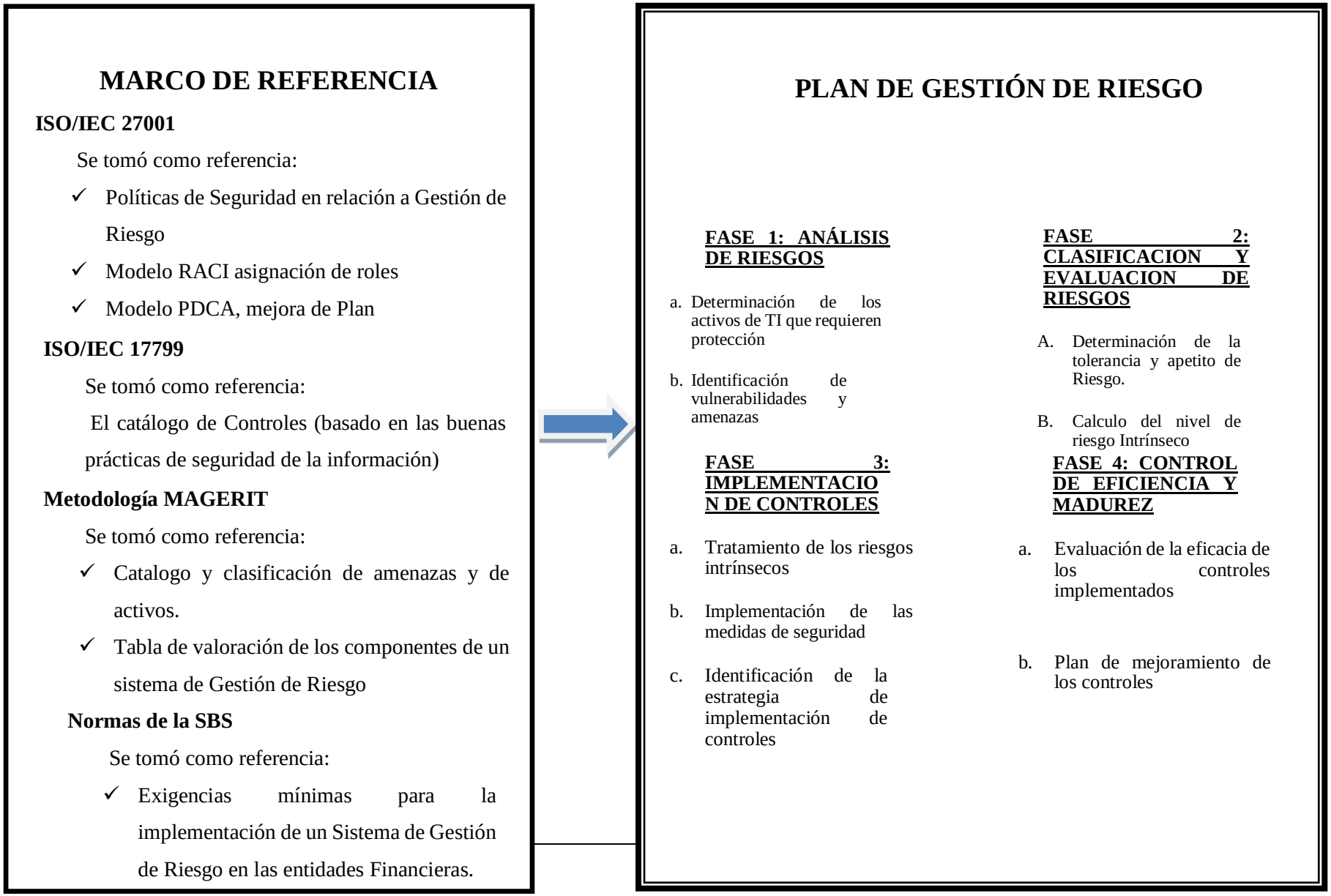
También se analizará el funcionamiento, la efectividad y el cumplimiento de las medidas de protección para determinar y ajustar las medidas deficientes y sancionar el incumplimiento de las mismas.

Figura 5 : Diagrama de conceptos genéricos implicados en el Análisis de Riesgos



Fuente: Elaboración propia

Figura 6 Metodología para la aplicación del Plan de análisis de riesgos propuesto



FASE 1: ANÁLISIS DE RIESGOS

El análisis de riesgos es conocido como el proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización. Permite determinar cómo es, cuánto vale y cómo de protegido se encuentra un sistema, siguiendo los objetivos, estrategia y política de la organización para elaborar un plan de seguridad. Al implantar y operar este plan debe satisfacer los objetivos propuestos con el nivel de riesgo aceptado por la Dirección de la organización.

Al conjunto de estas actividades se le denomina Proceso de Gestión de Riesgos.

El análisis de riesgo se realiza ya sea cuantitativa o cualitativamente. El análisis cualitativo es recomendable hacerlo en primer lugar, utiliza una escala de calificación de atributos para describir la magnitud de las consecuencias potenciales ya sea bajo, medio o alto; y la probabilidad de que se produzcan estas consecuencias. Un análisis cualitativo permite:

- Identificar los activos más significativos.
- Identificar el valor relativo de los activos.
- Identificar las amenazas más relevantes.
- Identificar las salvaguardas presentes en el sistema.
- Establecer claramente los activos críticos, aquellos sujetos a un riesgo máximo.

El análisis cuantitativo es más detallado y utiliza una escala con valores numéricos para las consecuencias y probabilidad, permitiendo:

- Detallar las consecuencias económicas de la materialización de una amenaza en un activo.
- Estimar la tasa anual de ocurrencia de amenazas.
- Detallar el coste de despliegue y mantenimiento de las salvaguardas.
- Permitir ser más precisos en la planificación de gastos de cara a un plan de mejora de seguridad.

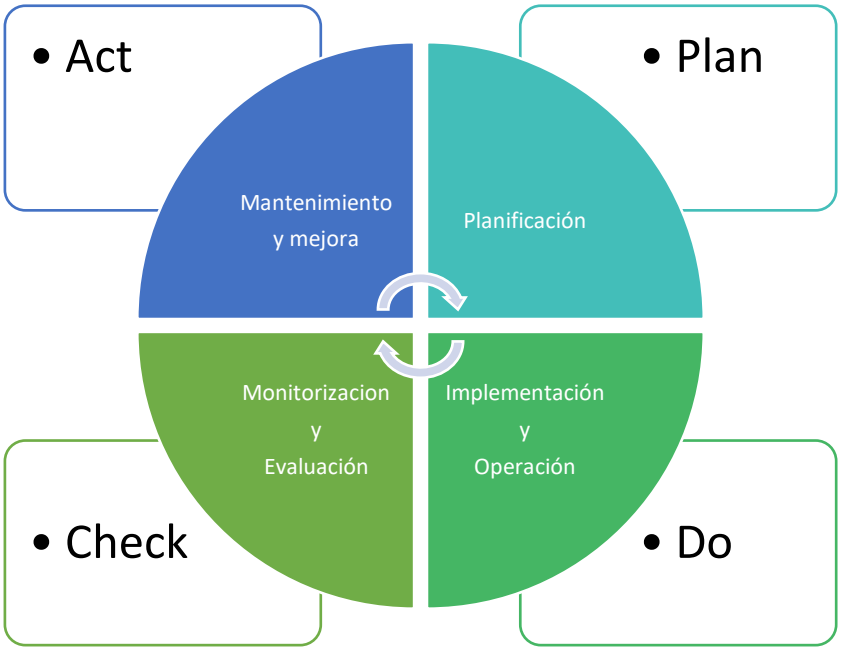
Los sistemas de gestión de la seguridad de la información formalizan cuatro etapas cíclicas donde el análisis de riesgos es parte de las actividades de planificación, se

toman decisiones de tratamiento, estas decisiones se materializan en la etapa de implantación, en el cual se despliegan elementos que permiten la monitorización de las medidas tomadas para poder evaluar la efectividad de las mismas y actuar dependiendo a éstas, dentro de un círculo de excelencia o mejora continua. Ver Figura Nº 07

El riesgo es una función de la probabilidad y el impacto.

Riesgo = Probabilidad * Impacto

Figura 7 : Ciclo PDCA



Fuente: Elaboración Propia

Esta fase contempla las siguientes actividades y tareas:

A. Identificación de activos de TI y definición de su criticidad

Aquí identificamos los activos importantes dentro de los procesos críticos identificados de la entidad, lo cual lo caracterizamos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia.

Tabla N° 03: Ficha técnica de la actividad identificación de activos de TI y definición de su criticidad

Tarea 1 Identificar activos

Objetivo: identificamos los activos que componen el sistema relacionando sus características, atributos y clasificación de acuerdo a los tipos determinados.

Entradas de insumos	Salidas	Técnicas
✓ Descripción de los procesos críticos del negocio ✓ Inventario de servicios prestados por el sistema ✓ Inventario de equipamiento lógico ✓ Inventario de equipamiento físico ✓ Locales y sedes de la organización ✓ Caracterización funcional de los puestos de trabajo	✓ Inventario de activos de TI a evaluar ✓ Clasificación de los activos de TI	✓ Diagramación de flujo de datos ✓ Entrevistas con los propietarios de los activos de TI ✓ Reuniones con los responsables del uso y mantenimiento de los activos de TI ✓ Utilizar Tabla de referencia para el inventario y clasificación de activos de TI (Ver anexo N° 03)

Tarea 2 definición de la criticidad de los activos de TI

Objetivo: Identificar las dimensiones de la información relacionadas con cada activo de TI Valorar el coste que para la organización de la no disponibilidad de cada activo de TI

Entradas de insumos	Salidas	Técnicas
✓ Inventario de activos de TI ✓ Descripción de los procesos críticos del negocio: ✓ Diagramas de flujo de Datos	✓ Modelo de valor: ✓ Informe del valor de los activos de TI	✓ Entrevistas con los propietarios de los activos de TI ✓ Reuniones con los responsables del uso y mantenimiento de los activos de TI ✓ Valoración Delphi ✓ Usar Tablas de referencia para la valoración de la equivalencia de los activos de TI (ver Anexo n°04)

1. Identificación de activos de TI

Se denomina activos a los recursos del Sistema de Información o relacionados con éste, y que son indispensables para que la organización funcione de manera correcta y que su correcto funcionamiento permita el alcance de los objetivos propuestos por la parte directiva de ja Caja Sipán.

El activo esencial es la información; es decir los datos. Y alrededor de estos datos se pueden identificar otros activos relevantes que integran los Sistemas de Información como son:[1]

- Datos que permiten materializar la información con la cual trabajan los Sistemas de Información.
- Los servicios que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
- Las aplicaciones informáticas(Software) que permiten manejar los datos.
- Los equipos informáticos(Hardware) que permiten hospedar datos, aplicaciones y servicios.
- Las Redes de Comunicaciones que permiten intercambiar datos.
- Los Soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan los elementos mencionados anteriormente.

No todos los activos son de la misma especie. Dependiendo del tipo de activo, las amenazas y las salvaguardas son diferentes.

[1] Miguel Angel Amutio Gómez, Javier Candau 2012, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. – Método de Administraciones Públicas, España p.17

En esta parte se identificarán a todos los activos que dan soporte a los procesos principales de Créditos y Captaciones. Se podrá clasificar los activos de TI, según sus características, en los siguientes tipos:

Equipamiento - Hardware

- Servidores. - Se consideran todos los equipos físicos de tipo torre y rack que alojan algún programa o aplicación, se encuentran dentro del centro de datos y son administrados por el personal de infraestructura y sistemas.
- Equipos de comunicaciones. - Se consideran todos los equipos que conforman la red de voz y datos ubicados en el centro de datos que son administrados por personal de infraestructura.
- Robot de cintas. - Equipo físico que realiza los respaldos en cinta de la información de los servidores ubicado en el centro de datos y es administrado por el personal de infraestructura.
- Computador de personal. - Equipo de computación que utiliza el personal de GTSI para trabajar.

Equipamiento - Software

- Sistemas financieros y administrativos. - Se consideran a los sistemas prioritarios para la administración de la organización que son gestionados por los desarrolladores.
- Almacenamiento – bases de datos. - Se considera a la información almacenada y respaldada originada de los datos de los servicios prestados, esto es administrado por administrador de bases de datos. También se consideran a las cintas magnéticas que almacenan la información respaldada.
- Correo electrónico. - se considera al sistema de correo electrónico.
- Virtualización. - se considera al servicio que permite el funcionamiento de los servidores virtuales.

Comunicaciones

- Internet. - Se considera al servicio y demás elementos necesarios para lograr el acceso hacia el Internet.
- Red alámbrica. - se considera a las conexiones alámbricas ya sean de fibra óptica o cable UTP.
- Red inalámbrica. - se considera a la señal de red emitida por los puntos de acceso.
- Enlace con proveedor. - se considera al servicio y equipos que conlleva la comunicación exitosa con el proveedor de Internet.

Equipamiento Auxiliar

- UPS. - se consideran a las baterías que protegen a los servidores y equipos de comunicación de fallos eléctricos.
- Generador eléctrico. - se considera al dispositivo que genera energía eléctrica cuando no hay servicio eléctrico.
- Equipos de climatización. - se consideran a los elementos que mantienen la temperatura adecuada en el centro de datos y cuartos de rack.
- Cableado eléctrico. - se considera a la red eléctrica existente entre el centro de datos, cuarto de rack y cuarto del generador eléctrico.

Instalaciones

- Centro de datos. - es el lugar donde se concentran todos los servidores y equipos de comunicación.
- Cuarto de rack. - o cuarto de telecomunicaciones, están ubicados en los diferentes edificios de la organización y es donde se encuentran los equipos de comunicación que tienen un enlace directo con el centro de datos.

Personal

- Equipo de desarrollo. - se considera al personal encargado de desarrollar las aplicaciones o sistemas.

- Equipo técnico. - se considera al personal encargado de dar asesoría técnica.
- Administradores. - se consideran a los jefes de cada área.

Para la clasificación de los activos de TI se utilizará el siguiente formato y se tomará como referencia la catalogación de activos del Anexo N° 03:

Tabla N° 04: Plantilla para el registro de los activos de TI por tipo de activo

N°	Tipo de activo de TI	Activo de TI
1		
2		
3		

B. Definición de la criticidad de los activos de TI identificados

Para realizar la valoración de los activos de Información de los Procesos que se analicen y sus correspondientes Subprocesos, se tendrán en cuenta las siguientes características de la Información:

1) **Disponibilidad**: La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera.

Nivel	Valor	Criterio
5	**Crítico**	La falta o no disponibilidad de la información que posea el activo de información o el mismo impacta negativamente la prestación de servicios de tecnología y de información en la Caja de Ahorro Crédito Sipán S.A.
4	**Alto:**	La falta o no disponibilidad parcial de la información que posea el activo de información o el mismo impacta negativamente la prestación de servicios de tecnología y de información en la Caja de Ahorro Crédito Sipán S.A.
3	**Medio**	La falta o no disponibilidad de algún dato que posea el activo de información o el mismo impacta negativamente al proceso que gestiona la información y/o a otros procesos de la Caja de Ahorro Crédito Sipán S.A.

2	**Bajo**	La falta o no disponibilidad del activo de información en su componente puede tener algún impacto negativo en los procesos de la Caja de Ahorro Crédito Sipán S.A.
1	**Mínimo**	La falta o no disponibilidad del activo de información no tiene ningún impacto negativo en los procesos de la Caja de Ahorro Crédito Sipán S.A.

2) **Integridad**: La integridad se refiere a la exactitud y completitud de la información (ISO 27000), esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción.

Nivel	Valor	Criterio
5	**Crítico**	La pérdida de exactitud y estado completo del activo impacta negativamente la prestación de servicios de tecnología y de información en la Caja de Ahorro y Crédito Sipán S.A.
4	**Alto:**	La pérdida en la exactitud de algún dato o estado del activo impacta negativamente la prestación de servicios de tecnología y de información en la Caja de Ahorro y Crédito Sipán S.A.
3	**Medio**	La pérdida posible de en la exactitud de algún dato o estado completo del activo puede impactar negativamente al proceso que gestiona la información y/o a otros procesos de la Caja de Ahorro y Crédito Sipán S.A.
2	**Bajo**	La pérdida posible de en la exactitud de algún dato o estado completo del activo puede tener algún impacto negativo en los procesos de la Caja de Ahorro y Crédito Sipán S.A.
1	**Mínimo**	La pérdida de exactitud y estado completo activo no tiene ningún impacto negativo en los procesos de la Caja de Ahorro y Crédito Sipán S.A.

3) **Confidencialidad**: La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados

Nivel	Valor	Criterio
5	**Crítico**	Es la existencia de información más crítica (Calificada, Vital o Esencial) a nivel de pérdida de su confidencialidad que cualquier otra y que por ende debe tener una mayor protección. A la información (Calificada, Vital o Esencial) sólo pueden tener acceso las personas que expresamente han sido declaradas usuarios legítimos de esta información, y con los privilegios asignados.

4	**Alto:**	Es la información que es utilizada por los funcionarios de la Caja de Ahorro y Crédito para realizar sus labores en los procesos y que no puede ser conocida por terceros sin autorización del propietario del activo.
3	**Medio**	Es la información que es utilizada por los funcionarios de la Caja de Ahorro para realizar sus labores en los procesos y que puede ser conocida por terceros con la autorización del propietario del activo.
2	**Bajo**	Es la información que ha sido calificada como de conocimiento público. Esta información puede ser entregada o publicada con ciertas restricciones dadas por el propietario del activo a los funcionarios o a cualquier persona sin que implique daños a terceros ni a las actividades y procesos de la Caja de Ahorro.
1	**Mínimo**	Es la información que ha sido calificada como de conocimiento público. Esta información puede ser entregada o publicada sin restricciones a los funcionarios o a cualquier persona sin que implique daños a terceros ni a las actividades y procesos de la Caja de Ahorro.

4) **Requerimientos Legales**: esta define la importancia si no cumplen con los requisitos legales.

Teniendo en cuenta las características de la información antes mencionada se determina la probabilidad de ocurrencia para cada riesgo teniendo en cuenta los siguientes criterios de valoración.

Tabla N° 05: Tabla de probabilidades de ocurrencia de los riesgos de Tecnologías de la Información

NIVEL	CONCEPTO	DESCRIPCIÓN	FRECUENCIA
1	**Rara Vez**	Puede que no se haya presentado u ocurrir solo en circunstancias excepcionales.	Nunca o no se ha presentado en los últimos 5 años
2	**Improbable**	Pudo ocurrir en algún momento, es poco común o frecuente	Al menos una vez en los últimos 5 años
3	**Posible**	Puede ocurrir en algún momento	Al menos una vez en los últimos 2 años
4	**Probable**	Ocurrirá en la mayoría de las circunstancias.	Al menos una vez en el último año

NIVEL	CONCEPTO	DESCRIPCIÓN	FRECUENCIA
5	**Casi Seguro**	Se espera que ocurra en la mayoría de las circunstancias	Más de una vez al año

Se analizarán todos los activos de información del proceso/ subproceso, tanto los informáticos como aquellos que se emiten en papel incluyendo los manuales de Procedimiento del área y aquellos que directa o indirectamente, se relacionan con las operaciones.

La valoración del impacto que puede ocasionar a la Caja de Ahorro y Crédito Sipán S.A, la materialización del Riesgo de Seguridad o Privacidad de la Información, se representa con la descripción de los siguientes niveles:

Tabla N° 06: Tabla de valoración del impacto de los riesgos de Tecnologías de la Información

NIVEL	CONCEPTO	DESCRIPCIÓN	SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
1	**Insignificante**	Si el hecho llegara a presentarse tendría consecuencias o efectos mínimos sobre la organización	Afecta a una actividad del proceso.
2	**Menor**	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la organización.	Afecta a un grupo de trabajo, a una persona, grupo de personas o algunas actividades del proceso.
3	**Moderado**	Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la organización.	Afecta un conjunto de datos personales o el proceso.
4	**Mayor**	Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la organización.	Afecta varios conjuntos de datos personales o procesos de la organización.
5	**Catastrófico**	Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos sobre la organización.	Afecta toda la organización. Multas por incumplimiento de la Legislación. Suspensión de las

NIVEL	CONCEPTO	DESCRIPCIÓN	SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
			actividades de la Caja de Ahorro y Crédito Sipán S.A.

Para la valoración de la criticidad de los activos de TI se utilizará el siguiente formato:

Tabla N° 07: Plantilla para la calificación de la criticidad de los activos de Tecnologías de la Información

N°	Activo	Criterios de seguridad			Total	Nivel de criticidad
		Confidencialidad	Integridad	Disponibilidad		
1						
2						
3						

Los niveles de criticidad de los activos de TI se obtendrán del producto de las calificaciones realizadas para cada criterio de seguridad y se clasificarán de la siguiente manera:

Tabla N° 08: Niveles de valoración de la criticidad de los activos de Tecnologías de la Información

Nivel de criticidad	Dimensión del Riesgo de Seguridad y Privacidad de la Información	Valor Asignado	Acción Requerida
1	**Riesgo Extremo**	**Mayor o igual a 21 y menor o igual a 25**	Evitar el riesgo empleando controles que busquen reducir el nivel de probabilidad. Reducir el riesgo empleando controles orientados a minimizar el impacto si el riesgo se materializa. Compartir o transferir el riesgo mediante la ejecución de pólizas.
2	**Riesgo Alto**	**Mayor o igual a 16 y menor o igual a 20**	Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permitan llevarlo a la zona de riesgo moderado. Compartir o transferir el riesgo.
3	**Riesgo Moderado**	**Mayor o igual a 11 y menor o igual a 15**	Evitar o mitigar el riesgo mediante medidas prontas y adecuadas que permitan llevarlo

			a la zona de riesgo menor. Compartir el riesgo.
4	**Riesgo Menor**	**Mayor o igual a 6 y menor o igual a 10**	Mitigar el riesgo mediante de medidas momentáneas y efectivas del proceso que permitan prevenirlo o llevarlo a la zona de riesgo bajo. Asumir el riesgo.
5	**Riesgo Bajo**	**Mayor a 0 menor o igual a 5**	Asumir el riesgo. Mitigar el riesgo con actividades propias del proceso y por medio de acciones detectivas y preventivas.

C. Identificación de amenazas por activo

En esta parte se listará un conjunto de amenazas consideradas vitales que se vincularan a los grupos de activos de información formados según su función y tipo, para poder evaluar el riesgo que generan a la organización y definir controles.

Los controles de seguridad protegerán a los activos de información contra los siguientes tipos de amenazas:

- Amenazas Lógicas
- Amenazas a las Comunicaciones
- Amenazas físicas o Fallos Técnicos
- Errores Humanos

En la siguiente tabla se identificará las amenazas para cada grupo de activo de información.

Tabla N° 09 Identificación de las amenazas a los activos de Tecnologías de la Información

Nº	GRUPO DE ACTIVOS DE TECNOLOGÍAS DE LA INFORMACIÓN	AMENAZAS
01	PROGRAMAS FUENTE	Control de cambios
		Daño malintencionado por internos.
		Error de herramientas de programación
		Software malicioso o virus
02	DOCUMENTOS FÍSICOS	Alteración y/o plagio
		Entrega incorrecta
		Falsificación
		Incendio, Desastres naturales

03	SERVIDORES	Error en el mantenimiento de hardware
		Daño intencionado por externos
		Falla de servicio de red y otros servicios
		Falla de software aplicación o Software malicioso
		Incendio y/o desastres naturales
		Suplantación identidad
		Abuso de los recursos del sistema y repudio
04	EQUIPOS	Error de operador
		Error en el mantenimiento de hardware
		Suplantación identidad
		Abuso de los recursos del sistema y repudio
		Falla de equipo
05	DATA ALMACENADA	Falla de operador
		Falla en dispositivo de almacenamiento
		Backup no autorizado
06	SOFTWARE	Robo de licencias
		Software malicioso y virus
		Error de usuario
		Uso no autorizado.
		Error de Actualización

Fuente: Elaboración propia

Luego de haber descrito las amenazas en la tabla anterior, también podremos identificar a lo que se enfrenta el sistema, qué puede pasar, qué consecuencias se derivarían y cuán probable es que pase. Se tomará en cuenta lo siguiente para poder identificar las amenazas significativas de cada activo de Tecnologías de la Información identificado:

- El tipo de activo
- Las dimensiones de seguridad con las que cada activo está relacionado
- La experiencia de la organización
- Los reportes de incidentes de seguridad

Tabla N° 10: Ficha técnica de la actividad Identificación de amenazas por activo

Tarea: Identificación de amenazas
Objetivo Identificar las amenazas relevantes sobre cada activo de TI

Entradas o insumos necesarios	Salidas	Técnicas
– Modelo de valor: Informe del valor de los activos – Informes relativos las vulnerabilidades de la Organización – Reportes de incidentes de seguridad de TI	– Relaciones de amenazas significativas por activo	– Entrevistas con los propietarios de los activos – Reuniones con los responsables del uso y mantenimiento de los activos tomarán en cuenta en la valoración de los activos de TI – Utilizar Tabla de Inventario de las amenazas por activo y dimensión de seguridad de la información (ver Anexo N° 05)

Tomando como referencia la tabla de inventario de las amenazas por activo y dimensión de seguridad de la información del Anexo N° 05 y el informe de valor de los activos de la actividad anterior, se debe obtener la relación de amenazas por cada activo de TI. Se utilizará el siguiente formato:

Tabla N° 11: Plantilla para la identificación de amenazas por activo

N°	Activo	Amenaza
1		
2		
3		

D. Identificación de vulnerabilidades

En esta actividad se realiza el análisis de las deficiencias, debilidades y carencias que tiene la organización en los diferentes procesos de TI relacionados a la protección de los activos que han sido identificados. El resultado de esta actividad permitirá determinar cuáles son las debilidades internas que pueden ser aprovechadas por las amenazas para materializarse y hacer fallar o atacar a los activos de TI.

Tabla N° 12: Ficha técnica de la actividad Identificación de vulnerabilidades por activo

Tarea: Identificación de vulnerabilidades por activo		
Objetivo Identificar las vulnerabilidades relevantes sobre cada activo de TI		
Entradas o insumos necesarios	**Salidas**	**Técnicas**
– Modelo de valor: Informe del valor de los activos – Informes y registro de incidentes de seguridad de la información	– Relaciones de vulnerabilidades posibles por activo	– Entrevistas con los propietarios de los activos – Reuniones con los responsables del uso y mantenimiento de los activos tomarán en cuenta en la valoración de los activos de TI – Utilizar el Listado de vulnerabilidades potenciales (ver Anexo N° 06)

Tomando como referencia el Listado de las vulnerabilidades del Anexo N° 06 y adecuándolo a cada relación activo - amenaza, se identificarán las vulnerabilidades por activo, utilizando el siguiente formato:

Tabla N° 13: Plantilla para la identificación de las vulnerabilidades por cada Activo-Amenaza

N°	Activo	Amenaza	Activo
1	Activo 1	Amenaza 1.1	Vulnerabilidad 1.1.1
			Vulnerabilidad 1.1.2
		Amenaza 1.2	Vulnerabilidad 1.2.1
			Vulnerabilidad 1.2.2
2	Activo 2	Amenaza 2.1	Vulnerabilidad 2.1.1

			Vulnerabilidad 2.1.2
		Amenaza 2.2	Vulnerabilidad 2.2.1
			Vulnerabilidad 2.2.2

E. Valorización del impacto y la probabilidad de ocurrencia de las amenazas

Se permitirá valorizar la materialización de cada una de las amenazas identificadas para cada activo de TI, tomando como referencia las vulnerabilidades encontradas para cada una de ellas. La valorización de las amenazas se realizará en base a la calificación de sus dos insumos principales, como son: el impacto que pueden ocasionar y la probabilidad de su ocurrencia.

Para la realización de dicha valorización, el estándar ISO 27005 propone varios ejemplos de métodos con los cuales se puede llevar a cabo la valorización de riesgos de manera adecuada. En la propuesta, se optó por la realización de una matriz de calor, la cual tiene como criterios la probabilidad que cierta amenaza explote cierta vulnerabilidad y el impacto al negocio estimado que la ocurrencia del riesgo pueda ocasionar al negocio.

Tabla N° 14: Ficha técnica de la actividad Estimación del impacto y la probabilidad de ocurrencia de las amenazas

Tarea: Estimación del impacto y la probabilidad de ocurrencia de las amenazas		
Objetivos – Estimar la frecuencia de ocurrencia de cada amenaza sobre cada activo – Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse		
Entradas o insumos necesarios	**Salidas**	**Técnicas**
– Listado de amenazas identificadas por activo de TI	– Mapa de riesgos: informe de amenazas posibles, caracterizadas por su	– Entrevistas con los propietarios de los activos

– Informes de vulnerabilidades – Historia o antecedentes de incidentes de seguridad de TI	frecuencia de ocurrencia y la degradación que causarían en los activos	– Reuniones con los responsables del uso y mantenimiento de los activos tomarán en cuenta en la valoración de los activos de TI – Valoración Delphi

F. Estimación del impacto de una amenaza

Para la estimación del impacto de cada una de las amenazas identificadas se utilizará la siguiente tabla que define los niveles de impacto de las amenazas:

Tabla N° 15: Valoración de los niveles de impacto de una amenaza

Nivel	Impacto	Descripción
1	Insignificante	– Tiene un efecto nulo o muy pequeño en las operaciones de créditos y captaciones
2	Menor	– Afecta parcialmente las operaciones de créditos y captaciones. – Paraliza servicios que no afectan directamente al cliente.
3	Moderado	– Operativamente es sostenible, pero dificulta o retrasa las Operaciones de créditos y captaciones. – Paraliza parcialmente los servicios críticos a clientes
4	Mayor	– Paraliza la atención de servicios críticos a clientes, debido a la caída significativa de las operaciones de créditos y captaciones – Pérdida potencial de clientes
5	Catastrófico	– Paraliza todas las operaciones de créditos y captaciones de la entidad

G. Estimación de la probabilidad de ocurrencia de una amenaza

Al determinar la amenaza que perjudica a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos: Degradación, es decir conocer cuán perjudicado resultaría el activo y por la probabilidad, es decir cuán probable o

improbable es que se materialice la amenaza.

La probabilidad de ocurrencia se modela de forma cualitativa y cuantitativa. Ver tabla 3.

Tabla N° 16: Modelación de la probabilidad de ocurrencia

Cualitativamente				Cuantitativamente		
MA	Muy Alta	Casi Seguro	Fácil	100	Muy Frecuente	A Diario
A	Alta	Muy Alto	Medio	10	Frecuente	Mensualmente
M	Media	Posible	Difícil	1	Normal	Una vez al año
B	Baja	Poco probable	Muy difícil	1/10	Poco Frecuente	Cada varios años
MB	Muy Baja	Muy Raro	Extremadamente difícil	1/100	Muy poco frecuente	siglos

Para la estimación de la probabilidad de ocurrencia de cada una de las amenazas consideradas se utilizará la siguiente tabla que define los niveles de probabilidad de ocurrencia o frecuencia de las amenazas:

Tabla N° 17: Valoración de los niveles de probabilidad de ocurrencia de una amenaza

Nivel	Probabilidad	Descripción
1	Raro	No se registra en los últimos 5 años
2	Improbable	Se podría presentar una vez cada 5 años
3	Posible	Se podría presentar una vez al año
4	Probable	Se podría presentar una vez cada mes
5	Casi seguro	Se podría presentar varias veces en el mes

FASE 2: CLASIFICACION Y EVALUACION DE RIESGOS

A. Determinación del apetito y la tolerancia al riesgo

En el plan propuesto determinamos el apetito y la tolerancia al riesgo, siempre y cuando se entienda que éste está enmarcado dentro del Riesgo Operacional, entendiéndose éste, como un incidente que ocasiona que el resultado de un proceso de negocio difiera del resultado esperado, debido a fallas en los procesos internos, las personas, los sistemas o por eventos externos. El riesgo operacional incluye el riesgo tecnológico y excluye el riesgo estratégico y reputacional. Por tanto, para determinar el apetito y la tolerancia al riesgo de TI solo se contemplará las que provienen del Riesgo Operacional Tecnológico, es decir de las fallas de los sistemas tecnológicos (hardware y software).

Dado que los riesgos operacionales se originan por debilidades del control, es decir por las deficiencias en los controles que muestran que los riesgos operacionales no se encuentran identificados y/o no se encuentran adecuadamente mitigados, lo que conllevaría a no lograr un objetivo del negocio y/o producir una pérdida financiera.

Los posibles escenarios de riesgo de TI que se tomarán en cuenta para la clasificación se muestran en la tabla 13

Tabla N° 18. Catálogo de posibles escenarios de riesgo de TI

Ámbito del escenario de riesgo de TI	Escenario de riesgo de TI
Infraestructura física de TI	Obsolescencia
	Daño o destrucción
	Robo
	Inadecuada arquitectura
	Instalación y cambios
	Ausencia del personal
	Falta de habilidades y experiencia del personal

Relacionados con el personal de TI	Insuficiencia de personal especializado
Gestión de proyectos	Proyectos no finalizados
	Riesgos económicos del proyecto
	Retraso en entrega de proyectos
	Baja calidad en los proyectos
	Falta de visión de programa de proyectos
Gestión de la seguridad	Ataque lógico a la seguridad
	Traspasar la seguridad
	Alteración de la integridad de la información
	Exposición de la información
Aplicaciones	Incorrectas decisiones de inversión en aplicaciones
	Envejecimiento de las aplicaciones de negocio
	Implementación inadecuada de las aplicaciones
	Inestabilidad de las aplicaciones
	Falta de capacidad de las aplicaciones
	Envejecimiento de las aplicaciones de infraestructura
	Aplicaciones intrusas
Entrega y soporte de servicios de TI	Incorrectas decisiones de inversión en aplicaciones
	Entrega y soporte de servicios
	Rendimiento de los servicios
Cumplimiento corporativo	Cumplimiento de acuerdos y compromisos
	Cumplimiento de licenciamiento
	Cumplimiento de regulaciones
Cumplimiento legal	Cumplimiento legal
Otros escenarios	Rendición de cuentas de TI
	Integración de TI y los procesos de Negocio
	Errores operativos de TI
	Procesos operativos de TI

Para clasificar los niveles de riesgo de TI se utilizará la siguiente escala de 5 puntos:

a. Muy Bajo: cuando la deficiencia del control no impide el logro de un objetivo y no representa exposición a una pérdida significativa para la Caja. Es irrelevante. Se califica con este nivel para los escenarios siguientes:

Obligaciones legales	Pudiera causar el incumplimiento leve o técnico de una ley o regulación
Seguridad	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
Intereses comerciales y económicos	supondría pérdidas económicas mínimas
Interrupción del servicio	Pudiera causar la interrupción de actividades propias de la Caja
Operaciones	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
Administración y gestión	pudiera impedir la operación efectiva de una parte de la Caja
Pérdida de confianza (reputación)	no supondría daño a la reputación o buena imagen de las personas u organizaciones
Persecución de delitos	Dificulte la investigación o facilite la comisión de delitos
Tiempo de recuperación del servicio	5 días < RTO

b. Bajo: cuando la deficiencia del control genera daños menores a la Caja, es decir genera pérdidas, pero no significativas. Se califica con este nivel para los escenarios siguientes:

Obligaciones legales	Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
Seguridad	Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
Intereses comerciales y económicos	De bajo interés para la competencia De bajo valor comercial
Interrupción del servicio	Probablemente cause la interrupción de actividades propias de la Caja
Operaciones	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
Administración y gestión	Probablemente impediría la operación efectiva de una parte de la Caja
Pérdida de confianza (reputación)	Probablemente afecte negativamente a las relaciones internas de la Organización

Persecución de delitos	Dificulte la investigación o facilite la comisión de delitos
Tiempo de recuperación del servicio	1 día < RTO < 5 días

c. **Medio**: cuando la deficiencia del control podría resultar en una pérdida significativa o importante, pero dentro de rangos aceptables para la Caja. Se califica con este nivel para los escenarios siguientes:

Obligaciones legales	Probablemente sea causa de incumplimiento de una ley o regulación
Seguridad	Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
Intereses comerciales y económicos	De cierto interés para la competencia causa de pérdidas financieras o merma de ingresos
Interrupción del servicio	Probablemente cause la interrupción de actividades propias de la Caja con impacto en otras organizaciones o en los clientes
Operaciones	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
Administración y gestión	Probablemente impediría la operación efectiva de más de una parte de la Organización
Pérdida de confianza (reputación)	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
Persecución de delitos	Dificulte la investigación o facilite la comisión de delitos
Tiempo de recuperación del servicio	4 horas < RTO < 1 día

d. **Alto**: cuando la deficiencia del control podría resultar en una pérdida significativa, del tipo económico u operativo.

Obligaciones legales	Probablemente cause un incumplimiento grave de una ley o regulación
Seguridad	Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes

	serios
Intereses comerciales y económicos	De alto interés para la competencia De elevado valor comercial Causa de graves pérdidas económicas
Interrupción del servicio	Probablemente cause una interrupción seria de las actividades propias de la Caja con un impacto significativo en otras organizaciones
Operaciones	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
Administración y gestión	Probablemente impediría la operación efectiva de la Caja
Pérdida de confianza (reputación)	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
Persecución de delitos	Impida la investigación de delitos graves o facilite su comisión
Tiempo de recuperación del servicio	1 hora < RTO < 4 horas

e. Muy Alto: cuando la deficiencia del control expone a la Caja a una pérdida sustancial material, económica y/o sanción regulatoria, no aceptable para la Caja.

Obligaciones legales	Probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
Seguridad	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
Intereses comerciales y económicos	De enorme interés para la competencia De muy elevado valor comercial Causa de pérdidas económicas excepcionalmente elevadas
Interrupción del servicio	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
Operaciones	Probablemente cause un daño excepcionalmente serio

	a la eficacia o seguridad de la misión operativa o logística
Administración y gestión	Probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
Pérdida de confianza (reputación)	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
Persecución de delitos	Impida la investigación de delitos graves o facilite su comisión
Tiempo de recuperación del servicio	RTO < 1 hora

Para determinar el apetito y la tolerancia en cada uno de los escenarios de riesgos de TI definidos que podrían afectar el no cumplimiento de los objetivos estratégicos u operacionales, se utilizará la siguiente estructura:

Tabla N° 19. Plantilla para determinar el apetito y la tolerancia al riesgo de TI por cada objetivo estratégico u operacional

Objetivo Estratégico u Operacional de la Caja		
Apetito de riesgo		
Tolerancia de riesgo		
Escenario de Riesgo de TI	**Impacto**	**Probabilidad de ocurrencia**
Infraestructura física de TI		
Relacionados con el personal de TI		
Gestión de proyectos		
Gestión de la seguridad		
Entrega y soporte de servicios de TI		

Cumplimiento corporativo		
Cumplimiento legal		
Otros escenarios		

B. Cálculo de los niveles de riesgos intrínseco (NRI)

El cálculo del nivel de riesgos intrínseco de cada una de las amenazas identificadas para cada activo, estará en función de la valoración y clasificación del impacto y la probabilidad de su ocurrencia. Se utilizará la siguiente relación:

NRI = Probabilidad de ocurrencia x Impacto

El producto de esta relación se ubicará en el siguiente mapa de calor (ver tabla 15), tomando como referencia los niveles de riesgo definidos anteriormente.

Tabla N° 20: Matriz de calor para la valoración del impacto y probabilidad de las amenazas

Impacto en los procesos	Probabilidad de ocurrencia				
	Raro	Improbable	Posible	Probable	Casi seguro
Catastrófico	Bajo	Medio	Alto	Muy alto	Muy alto
Mayor	Bajo	Bajo	Medio	Alto	Muy alto
Moderado	Muy bajo	Bajo	Medio	Medio	Alto
Mínimo	Muy bajo	Bajo	Bajo	Bajo	Medio
Insignificante	Muy bajo	Muy bajo	Muy bajo	Bajo	Bajo

FASE 3: IMPLEMENTACION DE CONTROLES

En esta fase se definirá e implementará los controles o salvaguardas necesarias para tratar cada una de las amenazas en cuya evaluación se haya obtenido niveles de Riesgos no tolerantes, es decir, con el calificativo de "Alto" o "Muy Alto"

Esta fase contempla las siguientes actividades y tareas:

a. Plan de tratamiento de los riesgos intrínsecos
b. Implementación de las medidas de seguridad
c. Identificación de la estrategia de implementación de controles
d. Evaluación de la brecha de seguridad: nivel de riesgo residual (NRR)

A. Plan de tratamiento de los riesgos intrínsecos

Luego de definir los niveles de riesgos intrínsecos para cada una de las vulnerabilidades de cada amenaza de cada activo que puedan afectar su integridad, confidencialidad o disponibilidad; se debe definir el criterio de aceptación del riesgo, el cual determina si el riesgo es aceptable o si requiere de algún tratamiento. Esto se determina con el Apetito del Riesgo de TI definido anteriormente.

Se presenta los criterios de aceptación o no aceptación para cada uno de los niveles de los riesgos intrínsecos:

Tabla N° 21: Apetito al riesgo de TI según el nivel de exposición al riesgo

Nivel de Riesgo	Política para la toma de Acciones
Muy alto	Riesgo no aceptable
Alto	Riesgo no aceptable
Medio	Riesgo aceptable
Bajo	Riesgo aceptable
Muy bajo	Riesgo aceptable

B. Implementación de las medidas de seguridad

Los controles que se seleccionarán para el tratamiento de los riesgos no aceptables se obtendrán en el anexo N°07, que pertenecen al estándar ISO 17799 (ISO/IEC 27002 el cual contiene una lista completa de objetivos de control comúnmente importantes para la entidad.

Mediante la Declaración de la Aplicabilidad se mostrarán los controles que se implementarán, adaptados a la realidad organizacional y capacidad instalada de La Caja.

Para empezar, se deberá definir las políticas de seguridad que La Caja deberá declarar o mejorar para alcanzar el nivel de seguridad de la información deseado. Éstos deberán ser desarrollados y promovidos por la Dirección de La Caja.

C. Identificación de la estrategia de implementación de controles

Seleccionado el control, con su correspondiente objetivo de control, para cada NRI no aceptable, se debe definir la estrategia de implementación del control, que puede ser:

- Aceptar el riesgo
- Elección de controles para mitigar los riesgos
- Transferencia del riesgo a terceros
- Evitar aumento del riesgo

D. Cálculo Nivel de Riesgo Residual (NRR) para determinar la brecha de seguridad

El cálculo del Nivel de Riesgo Residual (NRR) se realizará luego de implementado el control y de la evaluación de su efectividad y cumplimiento, obteniendo luego la brecha de seguridad con respecto al Nivel de Riesgo Intrínseco.

FASE 4: CONTROL DE EFICIENCIA Y MADUREZ

A. Identificación y clasificación de los Activos de TI de los procesos principales de la Caja Sipán

Aplicando el enfoque bottom-up (de abajo arriba), se ha identificado los siguientes activos de TI que le dan soporte a los procesos de créditos y captaciones de la financiera:

Tabla N° 22: Inventario de activos de TI de los procesos de Créditos y Captaciones

N°	ACTIVO
1	Servidor principal de dominio (DNS) Incluye: Gestión del Directorio Activo (Activity Directory)
2	Servidor principal de base de datos en SQL Server y aplicaciones
3	Red de comunicaciones Incluye: Firewall, gabinetes de comunicación, switch central, switchs de borde
4	Sala de servidores del Centro de Procesamiento Central y del Centro de Procesamiento Alterno
5	Base de Datos en SQL Server
6	Backups de Base de Datos
7	Personal de área de TI Incluye especialista en comunicaciones, especialista de base de datos, jefatura de TI
8	Aplicaciones informáticas de créditos y captaciones Incluye: Sistema de Información Financiera(SIIF)
9	Correo electrónico institucional
10	Equipos de cómputo terminales de ventanilla y analistas de créditos

11	Código fuente de las aplicaciones Incluye: biblioteca de versiones, librerías
12	Archivos de acta de conformidad
13	Archivos de requerimientos informáticos
14	Analistas de sistemas
15	Equipos de cómputo del área de desarrollo Incluye: terminales, servidor de desarrollo, laptops
16	Backups o respaldos de desarrollo y mantenimiento Incluye: código fuente, librerías
17	Herramientas de Desarrollo Incluye: base de datos de desarrollo licenciamiento de software de desarrollo
18	Registros de control de cambios de las aplicaciones Incluye: scripts, cambios en estructuras de datos, carga de datos, manuales de usuario, pruebas realizadas
19	Backups de documentos normativos y de gestión Incluye: reglamentaciones y procedimientos operacionales de gestión, desarrollo, calidad y seguridad), planes de TI, inventarios, contratos, etc.

Utilizando la clasificación propuesta por la ISO 27005:2008, se tiene el siguiente resultado:

Tabla N° 23: Clasificación de los activos de TI identificados

N°	Tipo de activo	Activo
1	Aplicaciones	Aplicaciones informáticas de créditos y captaciones
2	Aplicaciones	Herramientas de desarrollo
3	Comunicaciones	Red de comunicaciones
4	Datos o documentos	Código fuente de las aplicaciones

5	Datos o documentos	Archivos de Actas de conformidad
6	Datos o documentos	Archivo de requerimientos informáticos (físico)
7	Datos o documentos	Registros de control de cambios de las aplicaciones
8	Equipos informáticos	Equipos de cómputo terminales de ventanilla y analistas de créditos
9	Equipos informáticos	Equipos de cómputo del Área de Desarrollo
10	Información	Bases de Datos
11	Información	Backups de documentos normativos y de gestión
12	Instalaciones	Sala de servidores o Centro de Procesamiento Central
13	Personal	Personal de área de TI
14	Personal	Analistas de sistemas (Responsables de la implementación de requerimientos)
15	Servicios	Servidor principal de dominio
16	Servicios	Servidor principal de base de datos y aplicaciones
17	Servicios	Correo electrónico institucional
18	Soporte de información	Backups de base de datos
19	Soporte de información	Backups o respaldos de desarrollo y mantenimiento

B. Definición de la criticidad de los activos de TI identificados

Una vez inventariados los activos de TI se ha valorado y clasificado su nivel de importancia o criticidad, tomando como base la calificación dada a cada característica o dimensión de seguridad de la información, de acuerdo a las escalas de valoración propuestas, obteniéndose los siguientes resultados (usando el formato de la tabla N° 04):

Tabla N° 24: Valoración del nivel de criticidad de los activos de TI identificados

N°	Activo	Criterios de seguridad			Total	Nivel de criticidad
		C	I	D		
1	Servidor principal de dominio	4	5	5	4	Alto
2	Servidor principal de base de datos y aplicaciones	5	5	5	5	Muy Alto
3	Red de comunicaciones	4	1	5	3	Medio
4	Sala de servidores	4	1	5	3	Medio
5	Bases de Datos	5	5	5	5	Muy Alto
6	Backups de base de datos	5	5	5	5	Muy Alto
7	Personal de área de TI	4	1	5	3	Medio
8	Aplicaciones informáticas de créditos y captaciones	4	4	5	4	Alto
9	Correo electrónico institucional	4	4	5	4	Alto
10	Equipos de cómputo terminales de ventanilla y analistas de créditos:	5	5	5	5	Muy Alto
11	Código fuente de las aplicaciones	4	5	5	4	Alto
12	Archivos de Actas de conformidad	2	3	5	3	Medio
13	Archivo de requerimientos informáticos (físico)	2	3	5	3	Medio
14	Analistas de sistemas	4	1	5	3	Medio
15	Equipos de cómputo del Área de Desarrollo	4	5	5	4	Alto
16	Backups o respaldos de desarrollo y mantenimiento	4	5	5	4	Alto
17	Herramientas de desarrollo	3	4	4	3	Medio
18	Registros de control de cambios de las aplicaciones	4	4	5	4	Alto
19	Backups de documentos normativos y de gestión:	3	3	5	3	Medio

C. Identificación de las amenazas de los Activos de TI

Para cada activo de TI se han identificado las siguientes amenazas (usando el formato de la tabla N° 07):

Tabla N° 25: Listado de amenazas por Activo de TI

N°	Activo	Amenaza
1	Servidor principal de dominio	Paralización de procesos y actividades del negocio, no se accede a los servicios de red
2	Servidor principal de base de datos y aplicaciones	Pérdida de recursos, multas y sanciones debido a modificación de información sensible (datos de clientes)
3	Red de comunicaciones	Paralización de servicios de comunicación
4	Sala de servidores	Sabotaje a las instalaciones
		Pérdida de Activos de TI en la sala de servidores (Costo de hardware paralización de Operaciones)
5	Bases de Datos	Multas y sanciones, Perdida de información sensible de la empresa debido a accesos inadecuados a las bases de datos
		Falta de espacio de almacenamiento
6	Backups de base de datos	Paralización de procesos, debido a pérdida de información sensible por falta de protección en los dispositivos de almacenamiento.
7	Personal de área de TI	Retraso en las actividades, paralización de procesos, pérdida de información debido a fuga de talentos
		Modificación, divulgación y destrucción de la información
8	Aplicaciones informáticas de créditos y captaciones	Paralización de procesos debido a problemas en el procesamiento de transacciones a nivel de usuario/cliente.
		Información brindada al personal del negocio para el desarrollo de los procesos del negocio es inexacta debido errores en la integridad de los datos
9	Correo electrónico institucional	Retraso de actividades debido a Caídas del servicio de correo electrónico
		Pérdida de datos por gestión inadecuada del servidor de correo electrónico por parte del proveedor

10	Equipos de cómputo, terminales de ventanilla y analistas de créditos	Pérdida de información sensible debido a fallas de equipos de cómputo que soportan las operaciones del negocio
11	Código fuente de las aplicaciones	Pérdida de la correlación del código fuente de la versión existente en producción.
		Perdida de información, multas y sanciones por Manipulación de códigos fuente para beneficio del trabajador
12	Archivos de Actas de conformidad	Observaciones de entes supervisores sobre procesos que están en Producción no sustentados.
13	Archivo de requerimientos informáticos (físico)	Pérdida de información no permite el cumplimiento de Desarrollo de Requerimientos.
14	Analistas de sistemas (Responsables de la implementación de requerimientos)	Tiempo de desarrollo de requerimientos que exceden cronograma de actividades.
		Pérdida de información sensible debido a fuga a través de correos electrónicos y/o páginas web
		Pérdida de recursos debido a Implementaciones no acordes a metodología y Estándares de desarrollo de Software
15	Equipos de cómputo del Área de Desarrollo	Retraso en las actividades, pérdida de recursos debido a Infección de Virus Informáticos
16	Backups o respaldos de desarrollo y mantenimiento	Reversión de adecuaciones a los sistemas, no es posible.
17	Herramientas de desarrollo	Paralización de continuidad de Desarrollo de Requerimientos
18	Registros de control de cambios de las aplicaciones	No poder determinar el origen de los cambios en código Fuente
19	Backups de documentos normativos y de gestión	Pérdida de información, Multas y/o sanciones por no cumplir con el requerimiento de información histórica por parte de ente supervisor

D. Identificación de las vulnerabilidades de los Activos de TI

Para cada relación de activo de TI - amenaza se han identificado las siguientes vulnerabilidades (usando el formato de la tabla N° 09), el cual es el resultado

del análisis de incidentes de seguridad de la información que tiene registrado La Caja:

Tabla N° 26: Listado de vulnerabilidades por Activo de TI –Amenaza

N°	Activo	Amenaza	Vulnerabilidad
1	Servidor principal de dominio	Paralización de procesos y actividades del negocio, no se accede a los servicios de red	Falta de personal especializado, para dar el mantenimiento necesario al servidor de dominio
			Falla en los componentes físicos
			Fallas en el sistema operativo, falta de actualización de parches
			No se cuenta con un plan de mantenimiento de los servidores
			Ataque de virus
2	Servidor principal de base de datos y aplicaciones	Pérdida de recursos, multas y sanciones debido a modificación de información sensible (datos de clientes)	Administrador tiene acceso total a la base de datos y puede realizar modificaciones
			Deficiencia en el diseño de base datos (normalización de BD).
			Usuarios acceden a servidor de base de datos por canales no autorizados
3	Red de comunicaciones	Paralización de servicios de comunicación	Falla de la línea principal de comunicaciones
			Falla de la red de comunicaciones con otras agencias
			Fallas eléctricas que generen la interrupción de los procesos y servicios
			No se cuenta con servidor de firewall a nivel de hardware
4	Sala de servidores o Centro de Procesamiento Central	Sabotaje a las instalaciones	Acceso de Personal no autorizado (interno/externo) a la sala de servidores.
			Falta de un sistema de vigilancia y de seguridad del equipamiento en la sala de servidores.
		Pérdida de Activos de TI en la sala de servidores (costo de hardware /	No se mantiene un control o registro de acceso a las áreas restringidas
			Falta de un registro de acceso a la sala de servidores

		paralización de Operaciones)	No se tiene una política y procedimiento para el personal que realiza mantenimiento en la institución
			Personal de vigilancia no lleva un control de los equipos de entrada / salida (personal de mantenimiento). Y revisión de maletines.
5	Bases de Datos	Multas y sanciones, Perdida de información sensible de la empresa debido a accesos inadecuados a las bases de datos	Falta de un adecuado procedimiento para la asignación de perfiles para accesos a la BD
			Existencia de passwords no adecuados para usuarios locales y de red
			Privilegios para los usuarios de acceso a las aplicaciones no son revisados periódicamente
			Acceso a la BD desde otras aplicaciones
			Virus informáticos
			Realización de copias no autorizadas de la Base de Datos.
			Modificación no autorizada de BD
		Falta de espacio de almacenamiento	Incremento de transacciones
			No existe un procedimiento de mantenimiento de a BD.
			Incremento de espacio por virus.
6	Backups de base de datos	Paralización de procesos, debido a pérdida de información sensible por falta de protección en los dispositivos de almacenamiento.	Fallas en los dispositivos de almacenamiento (disco duro del servidor)
			Falta de un lugar adecuado para su resguardo y protección de las copias de respaldo
			Errores en el proceso de generación de backups.
			No se lleva un registro de la generación de backups.
7	Personal de área de TI	Retraso en las actividades, paralización de	Inadecuada segregación de funciones
			No existe un plan de capacitación adecuado

		procesos, pérdida de información debido a fuga de talentos	Indisponibilidad del personal (enfermedad, accidente y/o otros actos que impiden al personal realizar sus actividades)
		Modificación, divulgación y destrucción de la información	Abuso de privilegios de accesos
			Falta de control y seguimiento de accesos.
			Falta de acuerdos de confidencialidad.
			Impulsos mezquinos que hace que el personal actúe de manera anormal en el desarrollo de sus labores
			Falta de procedimiento de mantenimiento de usuarios
8	Aplicaciones informáticas de créditos y captaciones	Paralización de procesos debido a problemas en el procesamiento de transacciones a nivel de usuario/cliente.	Errores operativos por parte del usuario (registro de información errada)
			Fallas en las conexiones de red o en equipo de computo
			Fallas eléctricas (a partir de 2 horas).
		Información brindada al personal del negocio para el desarrollo de los procesos del negocio es inexacta debido errores en la integridad de los datos	Falta de soporte realizado al sistema Integrado de Información Financiera
			No llevar un control de la historia del código fuente
9	Correo electrónico institucional.	Retraso de actividades debido a caídas del servicio de correo electrónico.	Problemas de conexión o servidor del servicio que brinda el proveedor.
		Pérdida de datos por gestión inadecuada del servidor de correo electrónico por parte del proveedor.	No generación de copias de respaldo (cuentas creadas, permisos y configuración)
			Capacidad de almacenamiento limitada.
			Borrado de cuentas por accesos no autorizados por personal que administra el correo.

			Bajo nivel de complejidad del contraseñas de correo vía acceso-página web.
10	Equipos de cómputo terminales de ventanilla y analistas de créditos.	Pérdida de información sensible debido a fallas de equipos de cómputo que soportan las operaciones del negocio.	Personal no capacitado para el mantenimiento de equipos de computo
			No se ha determinado la vida útil de los equipo
			Incumplimiento del plan de mantenimiento de equipos.
			Fallas en sistema de alimentación eléctrica
			Errores de configuración de los equipos
			Mal uso del equipo por parte del usuario
			Condiciones de ambientes inadecuadas
			No se tienen identificados los equipos críticos en caso de evacuación.
			El personal guarda información sensible en sus equipos y no las guarda en el servidor.
11	Código fuente de las aplicaciones.	Pérdida de la correlación del código fuente de la versión existente en producción.	No se realizan copias de seguridad
			Accesos no autorizados a la PC de Integración de Software
		Perdida de información, multas y sanciones por Manipulación de códigos fuente para beneficio del trabajador.	Accesibilidad a todo el código fuente sin restricción por parte del personal de Desarrollo (no se tiene restricción de acceso al personal de desarrollo).
			No se realiza una revisión minuciosa de los controles de cambios entregado por el analista de sistema.
			No complejidad de contraseñas en el respaldo de código fuente
			Manipulación del código fuente que puede alterar el desarrollo normal de un proceso.
12	Archivo de Actas de conformidad	Observaciones de entes supervisores sobre procesos que están en Producción no sustentados.	Registro – Inventario no adecuado de documentación.

13	Archivo de requerimientos informáticos (físico)	Pérdida de información no permite el cumplimiento de Desarrollo de Requerimientos.	Registro - Inventario no adecuado de documentación de requerimiento
14	Analistas de sistemas (Responsables de la implementación de requerimientos)	Tiempo de desarrollo de requerimientos que exceden cronograma de actividades.	Personal de desarrollo (nuevo) con poco conocimiento en todos los Procesos de Negocio
			Falta de personal para cumplir con la sobrecarga de requerimientos a desarrollar.
		Pérdida de información sensible debido a fuga a través de correos electrónicos y/o páginas web.	Falta de monitoreo de envío y recepción de correos.
			Acceso total a la Web
		Pérdida de recursos debido a Implementaciones no acordes a metodología y Estándares de desarrollo de Software	Plan de Inducción no adecuado
15	Equipos de cómputo del Área de Desarrollo (concentra toda la información de desarrollo y de configuración de las aplicaciones)	Retraso en las actividades, pérdida de recursos debido a Infección de Virus Informáticos	Acceso total a la Web

16	Backups o respaldos de desarrollo y mantenimiento	Reversión de adecuaciones a los sistemas, no es posible.	No se trasladan copias de respaldo en sitios alternos
17	Herramientas de desarrollo	Paralización de continuidad de desarrollo de Requerimientos	Copia de seguridad en lugares seguros
18	Registros de control de cambios de las aplicaciones	No poder determinar el origen de los cambios en código Fuente.	No identificar a los responsables de modificaciones asignadas a los analistas de sistemas.
19	Backups de documentos normativos y de gestión	Pérdida de información, Multas y/o sanciones por no cumplir con el requerimiento de información histórica por parte de ente supervisor	No se ha establecido la periodicidad para la generación de backups de la normatividad histórica.
			No se ha identificado un lugar adecuado para el resguardo de los backups

E. Determinación del apetito y la tolerancia al riego de TI

En su Plan estratégico 2015 –2019, la Caja ha planteado los siguientes objetivos estratégicos u operacionales, clasificados en las siguientes cuatro perspectivas:

A. Mejora de la gestión de la cartera de créditos

- Optimizar los procesos de gestión de cartera.
- Diseñar nuevos productos que respondan a las necesidades del mercado.
- Profundizar la expansión geográfica.

B. Gestión financiera para el crecimiento

- Asegurar recursos para el crecimiento de la cartera

- Asegurar la rentabilidad de las agencias en las plazas con mayor riesgo.
- Aplicar mecanismos y herramientas para monitorear y reducir costos operativos

C. Mejorar el posicionamiento

- Posicionar a la Caja en la Región Nor-Oriente.
- Fidelizar clientes a través del servicio.

D. Gestión del talento humano

- Fidelizar de personal con la seguridad de la información.
- Esquematizar incentivos focalizado en la rentabilidad y calidad de cartera.

La infraestructura tecnológica informática está directamente relacionada con dar soporte a los siguientes objetivos:

Tabla N° 27. Identificación de los objetivos estratégicos u operacionales soportados por TI

Objetivo Estratégico u Operacional de la Caja	Estrategia relacionada con TI
Optimizar los procesos de gestión de cartera de créditos.	– Gestionar proyectos de TI para dar soporte a nuevos productos y servicios de créditos. – Perfeccionar las aplicaciones informáticas para la supervisión y control con fines de minimizar los riesgos operacionales. – Implementar sistemas de comunicación robustos para las nuevas oficinas
Aplicar mecanismos y herramientas para monitorear y reducir costos operativos.	– Gestionar proyectos de TI para implementación de controles de TI como mecanismo de seguimiento, trazabilidad y reacción oportuna frente a amenazas

Fidelizar clientes a través del servicio	– Asegurar la continuidad de los servicios de TI a través de la disponibilidad operativa de a infraestructura física de TI – Aseguramiento de la integridad y oportunidad de la información relacionadas a las cuentas de cliente – Implementar servicios de soporte basados en buenas prácticas como ITIL y COBIT: gestión de incidentes, gestión de problemas, gestión de configuraciones, gestión de cambios, gestión de niveles de Servicios
Fidelizar de personal con la seguridad de la información.	– Capacitación y entrenamiento del personal de TI y los usuarios de TI – Concientización del personal en material de seguridad de la información – Plan de incentivos y sanciones en materia de cumplimiento de políticas de seguridad de TI, gestión de riesgos y continuidad de procesos de TI

A continuación, se determina el apetito y tolerancia al riesgo para cada uno de los objetivos estratégicos u operacionales relacionados con TI.

Tabla N° 28. Determinación del apetito y la tolerancia al riesgo de TI por cada objetivo estratégico u operacional

Objetivo Estratégico u Operacional de la Caja	Optimizar los procesos de gestión de cartera de créditos
Apetito de riesgo	– Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación. – Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente. – Efectos de bajo interés para la competencia. – Efectos de bajo valor comercial – Probablemente cause la interrupción de actividades propias de la Caja.

	– Dificulte la investigación o facilite la comisión de delitos. – 1 hora < RTO < 4 horas.
Tolerancia de riesgo	– Probablemente sea causa de incumplimiento de una ley o regulación. – Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves. – De cierto interés para la competencia. – Causa de pérdidas financieras o merma de ingresos. – Probablemente cause la interrupción de actividades propias de la Caja con impacto en otras organizaciones o en los clientes. – Dificulte la investigación o facilite la comisión de delitos. – 4 horas < RTO < 1 día

Escenario de Riesgo de TI	**Impacto**	**Probabilidad de ocurrencia**
Infraestructura física de TI	Mayor	Probable
Relacionados con el personal de TI	Moderado	Posible
Gestión de proyectos	Mínimo	Raro
Gestión de la seguridad	Mínimo	Posible
Entrega y soporte de servicios de TI	Catastrófico	Casi seguro
Aplicaciones	Catastrófico	Casi seguro

Cumplimiento corporativo	Mínimo	Improbable
Cumplimiento legal	Mínimo	Raro
Otros escenarios	Mayor	Probable

Objetivo Estratégico u Operacional de la Caja	Aplicar mecanismos y herramientas para monitorear y reducir costos operativos
Apetito de riesgo	– Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación. – Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente. – Probablemente cause la interrupción de actividades propias de la Caja – Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local). – Probablemente impediría la operación efectiva de una parte de la Caja. – Dificulte la investigación o facilite la comisión de delitos
Tolerancia de riesgo	– Probablemente sea causa de incumplimiento de una ley o regulación. – Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves – Probablemente cause la interrupción de actividades propias de la Caja con impacto en otras organizaciones o en los clientes. – Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local. – Probablemente impediría la operación efectiva de más de una parte de la Caja – Dificulte la investigación o facilite la comisión de Delitos

Escenario de Riesgo de TI	Impacto	Probabilidad de ocurrencia
Infraestructura física de TI	Catastrófico	Casi seguro
Relacionados con el personal de TI	Mínimo	Raro
Gestión de proyectos	Moderado	Posible
Gestión de la seguridad	Mayor	Probable
Entrega y soporte de servicios de TI	Mínimo	Posible
Cumplimiento corporativo	Moderado	Probable
Cumplimiento legal	Insignificante	Raro
Otros escenarios	Mayor	Probable

Objetivo Estratégico u Operacional de la Caja	Fidelizar clientes a través del servicio
Apetito de riesgo	– De bajo interés para la competencia. de bajo valor comercial. – Probablemente cause la interrupción de actividades propias de la Caja. – Probablemente impediría la operación efectiva de una parte de la Caja. – Probablemente afecte negativamente a las relaciones internas de la Caja. – Dificulte la investigación o facilite la comisión de delitos. – 1 hora < RTO < 4 horas.
Tolerancia de riesgo	– De cierto interés para la competencia. – Causa de pérdidas financieras o merma de ingresos. – Probablemente cause la interrupción de actividades propias de la Caja con impacto en otras organizaciones o en los clientes. – Probablemente impediría la operación efectiva de más de una parte de la Caja. – Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones y los clientes. – 4 horas < RTO < 1 día

Escenario de Riesgo de TI	Impacto	Probabilidad de ocurrencia
Infraestructura física de TI	Mayor	Posible
Relacionados con el personal de TI	Mayor	Probable
Gestión de proyectos	Mínimo	Raro
Gestión de la seguridad	Moderado	Posible
Entrega y soporte de servicios de TI	Catastrófico	Casi seguro
Cumplimiento corporativo	Mayor	Posible
Cumplimiento legal	Moderado	Posible
Otros escenarios	Moderado	Posible

Objetivo Estratégico u Operacional de la Caja	Fidelizar de personal con la seguridad de la información
Apetito de riesgo	– Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación. – Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente. – Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local). – Probablemente impediría la operación efectiva de una parte de la Caja. – Dificulte la investigación o facilite la comisión de delitos
Tolerancia de riesgo	– Probablemente sea causa de incumplimiento de una ley o regulación. – Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves. – Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local – Probablemente impediría la operación efectiva de más de una parte de la Caja. – Dificulte la investigación o facilite la comisión de delitos.

Escenario de Riesgo de TI	Impacto	Probabilidad de ocurrencia
Infraestructura física de TI	Mínimo	Improbable
Relacionados con el personal de TI	Catastrófico	Probable
Gestión de proyectos	Insignificante	Improbable
Gestión de la seguridad	Mayor	Posible
Entrega y soporte de servicios de TI	Mínimo	Raro
Cumplimiento corporativo	Mayor	Probable
Cumplimiento legal	Mayor	Probable
Otros escenarios	Moderado	Probable

F. Valoración del impacto y probabilidad de ocurrencia de las amenazas

Para la valoración del impacto y probabilidad de ocurrencia, y en consecuencia, para obtener el nivel de riesgo al que está expuesto cada activo de TI en la financiera, se realizó un levantamiento de información para evaluar los controles existentes actualmente y la efectividad de su implementación. Esta información se registra en el Anexo N° 02 y fue obtenida a través de entrevistas, observación directa y testeos de penetración (en la medida que fue permitido).

Los resultados de las valoraciones para los impactos y probabilidad de ocurrencia de cada amenaza para cada activo de TI; así como la obtención del nivel de riesgo intrínseco (usando los formatos y niveles de valoración de las tablas N° 10, 11, 13 y 14), se muestran en la siguiente tabla:

Tabla N° 29 Valoración del Nivel de Riesgo Intrínseco (NRI)

N°	Activo	Amenaza	Vulnerabilidad	Impacto estimado en los procesos		Probabilidad de que la amenaza explote la vulnerabilidad		Nivel de Riesgo Intrínseco(NRI)		
				Nivel	Categoría	Nivel	Categoría	ID Riesgo	Nivel	Categoría
1	Servidor principal de dominio	Paralización de procesos y actividades del negocio, no se accede a los servicios de red	Falta de personal especializado, para dar el mantenimiento necesario al servidor de dominio	3	Moderado	2	Improbable	R1	2	Bajo
			Falla en los componentes físicos	4	Mayor	3	Posible	R2	3	Medio
			Fallas en el sistema operativo, falta de actualización de parches.	5	Catastrófico	4	Probable	R3	5	Muy Alto
			No se cuenta con un plan de mantenimiento de los servidores	3	Moderado	2	Improbable	R4	2	Bajo
			Ataque de virus	2	Menor	2	Improbable	R5	2	Bajo

2	Servidor principal de base de datos y aplicaciones	Pérdida de recursos, multas y sanciones debido a modificación de información sensible (datos de clientes)	Administrador tiene acceso total a la base de datos y puede realizar modificaciones.	4	Mayor	4	Probable	R6	4	Alto
			Deficiencia en el diseño de base datos (normalización de BD).	2	Menor	3	Posible	R7	2	Bajo
			Usuarios acceden a servidor de base de datos por canales no autorizados	5	Catastrófico	4	Probable	R8	5	Muy Alto
3	Red de comunicaciones	Paralización de servicios de comunicación	Falla de la línea principal de comunicaciones	5	Catastrófico	3	Posible	R9	4	Alto
			Falla de la red de comunicaciones con otras agencias.	4	Mayor	4	Probable	R10	4	Alto
			Fallas eléctricas que generen la interrupción de los procesos y servicios.	4	Mayor	3	Posible	R11	3	Alto

			No se cuenta con servidor de firewall a nivel de hardware	3	Moderado	2	Improbable	R12	2	Bajo
4	Sala de servidores o Centro de Procesamiento Central	Sabotaje a las instalaciones	Acceso de Personal no autorizado (interno/externo) a la sala de servidores	5	Catastrófico	2	Improbable	R13	3	Medio
			Falta de un sistema de vigilancia y de seguridad del equipamiento en la sala de servidores.	2	Menor	3	Posible	R14	2	Bajo
		Pérdida de Activos de TI en la sala de servidores (costo de hardware / paralización de operaciones)	No se mantiene un control o registro de acceso a las áreas restringidas.	2	Menor	2	Improbable	R15	2	Bajo
			Falta de un registro de acceso a la sala de servidores.	3	Moderado	2	Improbable	R16	2	Bajo
			No se tiene una política y procedimiento para el personal que	2	Menor	3	Posible	R17	2	Bajo

			realiza mantenimiento en la institución							
			Personal de vigilancia no lleva un control de los equipos de entrada / salida (personal de mantenimiento). y revisión de maletines.	4	Mayor	3	Posible	R18	3	Medio
5	Bases de Datos	Multas y sanciones, Perdida de información sensible de la empresa debido a accesos inadecuados a las bases de datos	Falta de un adecuado procedimiento para la asignación de perfiles para accesos a la BD.	4	Mayor	3	Posible	R19	3	Alto
			Existencia de passwords no adecuados para usuarios locales y de red	3	Moderado	2	Improbable	R20	2	Bajo
			Privilegios para los usuarios de acceso a las aplicaciones no son revisados periódicamente.	3	Moderado	2	Improbable	R21	2	Bajo

			Acceso a la BD desde otras aplicaciones.	4	Mayor	3	Posible	R22	3	Medio
			Virus informáticos	3	Moderado	3	Posible	R23	3	Medio
			Realización de copias no autorizadas de la Base de Datos.	4	Mayor	3	Posible	R24	3	Medio
			Modificación no autorizada de BD	5	Catastrófico	4	Probable	R25	5	Muy Alto
		Falta de espacio de almacenamiento	Incremento de transacciones	3	Moderado	3	Posible	R26	3	Medio
			No existe un procedimiento de mantenimiento de a BD.	3	Moderado	2	Improbable	R27	2	Bajo
			Incremento de espacio por virus.	3	Moderado	1	Raro	R28	1	Muy Bajo
6	Backups de base de datos	Paralización de procesos, debido a pérdida de información sensible por falta de protección en los dispositivos de almacenamiento.	Fallas en los dispositivos de almacenamiento (disco duro del servidor).	4	Mayor	3	Posible	R29	3	Alto
			Falta de un lugar adecuado para su resguardo y	2	Menor	2	Improbable	R30	2	Bajo

			protección de las copias de respaldo.							
			Errores en el proceso de generación de backups.	5	Catastrófico	4	Probable	R31	5	Muy Alto
			No se lleva un registro de la generación de backups	3	Moderado	3	Posible	R32	3	Medio
7	Personal de área de TI	Retraso en las actividades, paralización de procesos, pérdida de información debido a fuga de talentos	Inadecuada segregación de funciones	3	Moderado	2	Improbable	R33	2	Bajo
			No existe un plan de capacitación adecuado	2	Menor	3	Posible	R34	2	Bajo
			Indisponibilidad del personal (enfermedad, accidente y/o otros actos que impiden al personal realizar sus actividades)	2	Menor	3	Posible	R35	2	Bajo
		Modificación, divulgación y	Abuso de privilegios de accesos	4	Mayor	3	Posible	R36	3	Alto

		destrucción de la información.	Falta de control y seguimiento de accesos	5	Catastrófico	3	Posible	R37	4	Alto
			Falta de acuerdos de confidencialidad	4	Mayor	3	Posible	R38	3	Alto
			Impulsos mezquinos que hace que el personal actúe de manera anormal en el desarrollo de sus labores	3	Moderado	3	Posible	R39	3	Medio
			Falta de procedimiento de mantenimiento de usuarios	3	Moderado	2	Improbable	R40	2	Bajo
8	Aplicaciones informáticas de créditos y captaciones.	Paralización de procesos debido a Problemas en el procesamiento de transacciones a nivel de usuario/cliente.	Errores operativos por parte del usuario (registro de información errada)	3	Moderado	3	Posible	R41	3	Medio
			Fallas en las conexiones de red o en equipo de cómputo.	3	Moderado	3	Posible	R42	3	Medio

			Fallas eléctricas (a partir de 2 horas)	4	Mayor	3	Posible	R43	3	Medio
		Información brindada al personal del negocio para el desarrollo de los procesos del negocio es inexacta debido errores en la integridad de los datos.	Falta de soporte realizado al sistema Integrado de Información Financiera.	3	Moderado	2	Improbable	R44	2	Bajo
			No llevar un control de la historia del código fuente.	4	Mayor	3	Posible	R45	3	Medio
9	Correo electrónico institucional	Retraso de actividades debido a Caídas del servicio de correo electrónico.	Problemas de conexión o servidor del servicio que brinda el proveedor.	3	Moderado	3	Posible	R46	3	Medio
		Pérdida de datos por gestión inadecuada del servidor de correo electrónico	No generación de copias de respaldo (cuentas creadas, permisos y configuración).	3	Moderado	3	Posible	R47	3	Medio

		por parte del proveedor.	Capacidad de almacenamiento limitada.	2	Menor	2	Improbable	R48	2	Bajo
			Borrado de cuentas por accesos no autorizados por personal que administra el correo.	3	Moderado	2	Improbable	R49	2	Bajo
			Bajo nivel de complejidad de contraseñas de correo vía acceso-página web.	3	Moderado	3	Posible	R50	3	Medio
10	Equipos de cómputo terminales de ventanilla y analistas de créditos	Pérdida de información sensible debido a fallas de equipos de cómputo que soportan las operaciones del negocio.	Personal no capacitado para el mantenimiento de equipos de cómputo.	4	Mayor	2	Improbable	R51	2	Bajo
			No se ha determinado la vida útil de los equipo.	2	Menor	2	Improbable	R52	2	Bajo
			Incumplimiento del plan de mantenimiento de equipos.	2	Menor	3	Posible	R53	2	Bajo

			Fallas en sistema de alimentación eléctrica	3	Moderado	3	Posible	R54	3	Medio
			Errores de configuración de los equipos	2	Menor	3	Posible	R55	2	Bajo
			Mal uso del equipo por parte del usuario	3	Moderado	4	Probable	R56	3	Medio
			Condiciones de ambientes inadecuadas	2	Menor	3	Posible	R57	2	Bajo
			No se tienen identificados los equipos críticos en caso de evacuación.	3	Moderado	2	Improbable	R58	2	Bajo
			El personal guarda información sensible en sus equipos y no las guarda en el servidor.	4	Mayor	4	Probable	R59	4	Alto
11	Código fuente de las aplicaciones.	Pérdida de la correlación del código fuente de la versión existente en producción.	No se realizan copias de seguridad	4	Mayor	2	Improbable	R60	2	Bajo
			Accesos no autorizados a la PC	4	Mayor	2	Improbable	R61	2	Bajo

			de Integración de Software.							
		Perdida de información, multas y sanciones por Manipulación de códigos fuente para beneficio del trabajador	Accesibilidad a todo el código fuente sin restricción por parte del personal de Desarrollo (no se tiene restricción de acceso al personal de desarrollo).	4	Mayor	3	Posible	R62	3	Medio
			No se realiza una revisión minuciosa de los controles de cambios entregado por el analista de sistema.	4	Mayor	3	Posible	R63	3	Medio
			No complejidad de contraseñas en el respaldo de código fuente.	3	Moderado	3	Posible	R64	3	Medio
			Manipulación del código fuente que puede alterar el desarrollo normal de un proceso.	5	Catastrófico	4	Probable	R65	5	Muy Alto

12	Archivos de Actas de conformidad.	Observaciones de entes supervisores sobre procesos que están en Producción no sustentados.	Registro - Inventario no adecuado de documentación.	3	Moderado	3	Posible	R66	3	Medio
13	Archivo de requerimientos informáticos (físico).	Pérdida de información no permite el cumplimiento de Desarrollo de Requerimientos.	Registro - Inventario no adecuado de documentación de requerimiento.	3	Moderado	3	Posible	R67	3	Medio
14	Analistas de sistemas (Responsables de la implementación de requerimientos).	Tiempo de desarrollo de requerimientos que exceden cronograma de actividades.	Personal de desarrollo (nuevo) con poco conocimiento en todos los Procesos de Negocio.	2	Menor	4	Probable	R68	2	Bajo
			Falta de personal para cumplir con la sobrecarga de requerimientos a desarrollar.	3	Moderado	3	Posible	R69	3	Medio
		Pérdida de información sensible debido a fuga a	Falta de monitoreo de envío y recepción de correos.	3	Moderado	2	Improbable	R70	2	Bajo

		través de correos electrónicos y/o páginas web.	Acceso total a la Web	4	Mayor	3	Posible	R71	3	Medio
		Pérdida de recursos debido a Implementaciones no acordes a metodología y estándares de desarrollo de software.	Plan de Inducción no adecuado	2	Menor	2	Improbable	R72	2	Bajo
15	Equipos de cómputo del Área de Desarrollo.	Retraso en las actividades, pérdida de recursos debido a Infección de Virus Informáticos.	Acceso total a la Web	3	Moderado	3	Posible	R73	3	Medio
16	Backups o respaldos de desarrollo y mantenimiento.	Reversión de adecuaciones a los sistemas, no es posible.	No se trasladan copias de respaldo en sitios alternos.	5	Catastrófico	3	Posible	R74	4	Alto
17	Herramientas de desarrollo.	Paralización de continuidad de	Copia de seguridad en lugares seguros.	3	Moderado	3	Posible	R75	3	Medio

		Desarrollo de Requerimientos.								
18	Registros de control de cambios de las aplicaciones.	No poder determinar el origen de los cambios en código Fuente.	No identificar a los responsables de modificaciones asignadas a los analistas de sistemas.	3	Moderado	3	Posible	R76	3	Medio
19	Backups de documentos normativos y de gestión.	Pérdida de información, Multas y/o sanciones por no cumplir con el requerimiento de información histórica por parte de ente supervisor.	No se ha establecido la periodicidad para la generación de backups de la normatividad histórica.	3	Moderado	2	Improbable	R77	2	Bajo
			No se ha identificado un lugar adecuado para el resguardo de los backups.	2	Menor	2	Improbable	R78	2	Bajo

G. Definición de métricas para gestión de riesgos de TI

Para determinar qué tan posible es que la probabilidad de un evento, combinada con sus consecuencias, supere el apetito de riesgo de la financiera (es decir, el nivel de riesgo que la financiera está preparada para aceptar), y que a su vez tenga un impacto negativo, se realizará a través de métricas basadas en indicadores de riesgos clave (KRI).

El objetivo de estos indicadores, es que sirvan como variables que funcionen como alertas tempranas que avisen de los cambios en los perfiles de riesgo de TI que pudiesen ocurrir en la financiera.

De acuerdo a RMA[2] las categorías de riesgos para una entidad financiera son:

- Riesgos de conciliación de cuentas
- Riesgos de Cambios
- Riesgo de Cumplimiento
- Riesgos de Desembolso
- Riesgo de Fraude
- Riesgo de Seguridad de la Información

Para cada una de estas categorías RMA define una serie de KRIs. Específicamente, las KRI que se plantean como métricas del plan propuesto de gestión de riesgos de TI son los propuestos por RMA para los Riesgos de Seguridad de la Información, que son las que están directamente relacionadas con el objetivo de esta investigación. Adicionalmente se plantean

[2] Risk Management Association

Tabla N° 30: Indicadores de riesgo clave propuestos para el plan de gestión de riesgos

Indicador	Fuente	Frecuencia de Medición
Número de personas que manejan información sensible de clientes	Retail Banking KRI Working Group	Trimestral
Número de ataques reportados por Seguridad Informática.	Retail Banking KRI Working Group	Trimestral
Porcentaje de terceros donde haya excepciones o preocupaciones por la seguridad de la información.	Retail Banking KRI Working Group	Trimestral
Número de derechos de acceso a los aplicativos por el personal (sobre el umbral).	Retail Banking KRI Working Group	Trimestral
Número de fallos relacionados con el sistema de TI y otros equipos.	Propio	Mensual
Número de llamadas para ayudar escritorio en sistema informático y otro equipo	Propio	Mensual
Promedio de tiempo de inactividad del sistema de TI y otros equipos	Propio	Mensual
Aumento de la carga de transacciones en los sistemas	Propio	Mensual

H. Propuesta de políticas de seguridad de la información de acuerdo a la ISO/IEC 27001

Antes de la implementación de los controles y salvaguardas para tratar los niveles de riesgo no aceptados, primero se definieron e implementaron las políticas de seguridad de la información, las cuales se tomaron del marco de referencia ISO/IEC 27001 necesarias para lograr la implantación, cumplimiento y efectividad de cada uno de los controles propuestos.

Estas políticas de seguridad a implantar se detallan en el cuadro siguiente:

Tabla N° 31: Políticas de seguridad necesarias para la implementación de los controles

Clausula	Categoría de Seguridad	Nombre del Control	Descripción de la política
Política de Seguridad	Política de Seguridad de Información	Documentar política de seguridad de información	La Gerencia debe aprobar un documento de política, estese debe publicar y comunicar a todos los empleados y entidades importantes a la organización
		Revisión de la Política de Seguridad de Información	La Política de seguridad de la información debe ser revisada a intervalos planeados o si ocurren cambios importantes que aseguren la continuidad y eficiencia
Organización de la seguridad de la información	Organización Interna	Compromiso de la gerencia con la seguridad de la información	La alta gerencia debe apoyar activamente la seguridad dentro de la organización a través de un alinea clara, compromiso detallado y reconocimiento de responsabilidades en cuanto a seguridad de la información.
		Coordinación de la seguridad de la información	Las actividades de la seguridad de información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles relevante.
		Asignación de responsabilidades de la seguridad de la información	Se debe definir de manera clara la responsabilidad de la seguridad de la información.
		Proceso de autorización para los medios de procesamiento de información	Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información.
		Acuerdos de confidencialidad	Se debe identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no divulgación reflejando las necesidades de la organización para la protección de la información.
	Entidades externas	Tratamiento de la seguridad cuando se interactúa con clientes	Se debe tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización.

Gestión de activos	Responsabilidad por la gestión de activos	Inventario de activos	Todos los activos deben estar claramente identificados y se debe elabora y mantener un inventario de todos los activos importantes.
		Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados.
	Clasificación de la información	Lineamientos de clasificación	La información debe ser clasificada de acuerdo a su valor, requerimientos legales, confidencialidad y grado crítico para la organización.
		Etiquetado y manejo de la información	Se debe desarrollar e implementar un conjunto apropiado de procedimientos para etiquetar y manejar la información de acuerdo con el esquema de clasificación hecho por la organización
Gestión de incidentes en la seguridad de la información	Reporte de eventos y debilidades de la seguridad de la información	Reporte de eventos en la seguridad de la información	Los eventos en seguridad de la información deben reportarse a través de los canales gerenciales lo más rápido posible
		Reporte de debilidades en la seguridad	Se debe solicitar que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de la información tomen nota y reporten cualquier debilidad observada y/o sospecha en cuanto a seguridad de la información se refiere.
	Gestión de incidentes y mejoras en la seguridad de la información	Responsabilidad y procedimientos	Se debe establecer las responsabilidades y procedimientos gerenciales, para asegurar la respuesta rápida, efectiva y ordenada a los incidentes a seguridad de la información
		Aprendizaje en los incidentes de la seguridad de la información.	Debe existir mecanismos para cuantificar y monitorear los tipos , volúmenes y costos en los incidentes en la seguridad de la información.
		Recolección de evidencia	Cuando la acción de seguimiento contra una persona u organización después de un incidente, involucra una acción legal, se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia establecidas en las jurisdicciones relevantes.

Cumplimiento	Cumplimiento con requerimientos legales	Protección de los registros organizacionales	Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.
		Protección de la data y privacidad de información personal	Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.
Gestión de las comunicaciones y operaciones	Procedimientos y responsabilidades operacionales	Procedimientos de operación documentados	Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.
Control de acceso	Gestión del acceso al usuario.	Revisión de los derechos de acceso del usuario	La alta gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.
Adquisición, desarrollo y mantenimiento de los sistemas de información	Seguridad en los procesos de desarrollo y soporte	Desarrollo de outsourcing software	El desarrollo de software que ha sido outsourcing debe ser supervisado y monitoreado por la organización.

I. Implementación de las medidas de seguridad y de las estrategias de su implantación.

Luego de definir las políticas de seguridad que La financiera debería adoptar, se procedió a definir los controles para el tratamiento de los diversos riesgos identificados; especificando el control, su descripción según la norma ISO 27002, los riesgos que mitigará y la adaptación de dicho control con la realidad organizacional de La financiera.

Los resultados de esta actividad se muestran en el cuadro siguiente:

Tabla N° 32: Implementación de controles según el NRI calculado

Nivel de Riesgo Intrínseco (NRI)			Control		Estrategia de implementación
ID riesgo	Nivel	Categoría	ID Control	Descripción	
R1	2	Bajo	C1	Servicio de Mantenimiento por parte del fabricante correctivo.	Evitar aumento del Riesgo.
R2	3	Medio	C2	Se cuenta con un servicio de mantenimiento por parte del fabricante.	Evitar aumento del Riesgo.
			C3	Sala de servidores con controles ambientales.	Evitar aumento del Riesgo.
R3	5	Muy Alto	C4	Personal capacitado en administración de Windows server y actualizaciones de parches.	Transferencia del riesgo a terceros
R4	2	Bajo	C5	Incluir en el Plan de mantenimiento a los servidores.	Evitar aumento del Riesgo.
R5	2	Bajo	C6	Se cuenta con software antivirus instalado en toda la red y con actualizaciones automáticas.	Evitar aumento del Riesgo.
			C7	Se cuenta con copias de seguridad de la BD	Evitar aumento del Riesgo.
			C8	Se cuenta con un servidor de backups	Evitar aumento del Riesgo.
			C9	Se tiene implementado un centro de cómputo alterno (CCA), el cual permite generar copias de respaldo en línea.	Evitar aumento del Riesgo.
R6	4	Alto	C10	El Oficial de Seguridad de la Información monitorea de manera bimensual las pistas	Elección de controles

				de auditoría al administrador de la BD, así como también las operaciones que realiza en la arquitectura de la BD.	
R7	2	Bajo	C11	En el proceso de desarrollo se cuenta con una fase de pruebas y revisión, donde se analizan el diseño de las tablas y de las modificaciones.	Evitar aumento del Riesgo.
			C12	La Jefe de Producción, realiza un análisis de los ejecutables y códigos fuentes que pasa la División de desarrollo.	Evitar aumento del Riesgo.
R8	5	Muy Alto	C13	Se tiene establecido restricciones de acceso mediante la asignación de perfiles de usuario (no pueden instalar aplicaciones), se desactivan herramientas adicionales que permiten acceder a la base de datos.	Elección de controles
			C14	La contraseña de acceso a la base de datos tiene un nivel de complejidad, distinta a las contraseñas que manejan los usuarios locales	Elección de controles
			C15	Los perfiles de usuarios que acceden a la base de datos tiene accesos restringidos.	Elección de controles
R9	4	Alto	C16	Se cuenta con línea de contingencia para comunicaciones	Transferencia del riesgo a terceros
			C17	Reporte de averías al proveedor	Transferencia del riesgo a terceros
R10	4	Alto	C18	Reporte de averías al proveedor	Transferencia del riesgo a terceros
R11	4	Alto	C19	Se cuenta con UPS y grupo electrógeno, el cual permite mantener la operatividad de los equipos ante una posible interrupción del corte de energía eléctrica.	Elección de controles
			C20	Se realizan pruebas de operatividad de los equipos eléctricos, con el fin de evaluar su funcionamiento.	Elección de controles
			C21	Se cuenta con un plan de mantenimiento al sistema eléctrico	Elección de controles
R12	2	Bajo	C22	Se cuenta con firewall a nivel de software	Evitar aumento del Riesgo.

R13	3	Medio	C23	Se cuentan con políticas de seguridad	Evitar aumento del Riesgo.
			C24	Se registran los accesos a sala de servidores y el área de TI, mediante una bitácora de acceso.	Evitar aumento del Riesgo.
			C25	Los accesos por parte de personal a realizar mantenimiento, se realiza acompañado de personal del área.	Evitar aumento del Riesgo.
			C26	El acceso al ambiente de la sala de servidores, tiene acceso restringido mediante una puerta con llave. La llave la maneja únicamente el Jefe de Producción y Soporte y el Operador de Sistemas.	Evitar aumento del Riesgo.
			C27	Sala de servidores se encuentra en un ambiente aislado al ambiente de producción y de Desarrollo.	Evitar aumento del Riesgo.
			C28	Se tiene implementado una cámara de vigilancia que monitorea el ingreso de personas internas como externas al área de TI.	Evitar aumento del Riesgo.
R14	2	Bajo	C29	Se cuenta con un equipo de aire acondicionado el cual no permite el recalentamiento de los equipos.	Evitar aumento del Riesgo.
			C30	Se tiene instalado extintores y sensores de humo	Evitar aumento del Riesgo.
			C31	La sala de servidores se encuentra en un ambiente aislado al ambiente de Producción y de Desarrollo. Este ambiente cuenta con una puerta de acceso bajo llave.	Evitar aumento del Riesgo.
			C32	Se cuenta con luces de emergencia	Evitar aumento del Riesgo.
			C33	Se registran los accesos a sala de servidores, mediante una bitácora.	Evitar aumento del Riesgo.
			C34	Se cuenta con una cámara de vigilancia en la entrada al área de TI.	Evitar aumento del Riesgo.
			C35	Se tiene designado personal para el manejo de llaves	Evitar aumento del Riesgo.
			C36	Se cuenta con sala de servidor alterno	Evitar aumento

					del Riesgo.
			C37	Mantenimiento de los equipos de seguridad	Evitar aumento del Riesgo.
			C38	Se cuenta con un plan de pruebas de los sensores por parte del personal de ASBANC.	Evitar aumento del Riesgo.
R15	2	Bajo	C39	Se cuenta con vigilancia al ingreso a la institución, quién mediante su cuaderno de cargos registra al personal que ingresa a las zonas de acceso restringido (TI).	Evitar aumento del Riesgo.
R16	2	Bajo	C40	Se cuenta con una bitácora, donde el personal interno y externo que desea ingresar a la sala de servidores deberá registrar la hora de ingreso, salida y nombre.	Evitar aumento del Riesgo.
R17	2	Bajo	C41	No se tienen controles	Evitar aumento del Riesgo.
R18	3	Medio	C42	Se cuenta con formatos de entrada salidas de para los equipos que el personal de la Caja saca fuera de las instalaciones.	Evitar aumento del Riesgo.
R19	4	Alto	C43	Reglamento de administración de usuarios al SIIF, en el que incluye las opciones para la asignación de perfiles por usuarios.	Elección de controles
R20	2	Bajo	C44	Se permite la creación de contraseñas con un nivel de seguridad y complejidad, teniendo en cuenta caracteres numéricos y alfanuméricos.	Evitar aumento del Riesgo.
R21	2	Bajo	C45	Incluir en el Plan de trabajo de la oficialía de seguridad	Evitar aumento del Riesgo.
R22	4	Alto	C46	Se han deshabilitado acceso al Excel en todas las máquinas.	Elección de controles
			C47	Acceso a la BD protegida por un password que es de conocimiento del jefe de área de producción y soporte.	Elección de controles
R23	3	Medio	C48	Se realiza la actualización del antivirus en línea	Evitar aumento del Riesgo.
R24	3	Medio	C49	BD protegidas con clave y esta clave únicamente la conoce solo personal	Evitar aumento del Riesgo.

				autorizado.	
			C50	No se tiene carpetas compartidas de la BD	Elección de controles
R25	5	Muy Alto	C51	Se efectúa una revisión general de los script que envía la sección desarrollo para el pase a producción.	Elección de controles
R26	3	Medio	C52	La Jefe de Producción y Soporte supervisa de manera manual la disponibilidad de la capacidad del disco del servidor, a fin de que exista espacio suficiente para la BD.	Evitar aumento del Riesgo.
R27	2	Bajo	C53	Se realiza un mantenimiento de la BD, pero no está documentado.	Evitar aumento del Riesgo.
R28	1	Muy Bajo	C54	Se cuenta con un antivirus que se actualiza en línea	Elección de controles
			C55	Puertos de control de acceso al servidor se encuentran bloqueados.	Elección de controles
R29	4	Alto	C56	Se cuenta con políticas y procedimientos de generación de backups.	Elección de controles
			C57	Se generan dos copias de respaldo, la cual una de ellas se mantiene en el sitio alterno (Ag. Moshoqueque) y la otra en bóveda(Oficina Principal).	Elección de controles
			C58	Se lleva un control trimestral del estado de almacenamiento de los medios de respaldo.	Elección de controles
			C59	Se realiza un monitoreo del procedimiento de respaldo de los backups.	Elección de controles
			C60	Se cuenta con un centro de cómputo alterno que replica información de la BD de manera automática; asimismo se cuenta con un servidor de base de datos de respaldo en el centro de cómputo principal (CCP) en caso de caída del servidor primario.	Elección de controles
R30	2	Bajo	C61	Se realiza una verificación de estado de almacenamiento y resguardo de los medios de respaldo.	Evitar aumento del Riesgo.
R31	5	Muy Alto	C62	La herramienta que comprime la BD, realiza una verificación automática de los	Elección de controles

				archivos comprimidos.	
			C63	El programa que graba los archivos comprimidos en los medios, realiza una verificación después de la grabación.	Elección de controles
			C64	Se realiza la verificación periódica de las copias generadas	Elección de controles
R32	3	Medio	C65	Se cuenta con un cuaderno de cargos en el cual se consigna el envío de las copias de respaldo por fechas de generación, responsable de envío y recepción, tanto en el CCP como en la agencia Moshoqueque.	Evitar aumento del Riesgo.
R33	2	Bajo	C66	Se cuenta con manual de organización y funciones en el que se tiene establecido las responsabilidades que debe cumplir el personal en la operativa diaria.	Evitar aumento del Riesgo.
R34	2	Bajo	C67	Existe un plan de capacitación presentado por el jefe de TI	Evitar aumento del Riesgo.
R35	2	Bajo	C68	Se tiene personal de reemplazo, pero no está totalmente capacitado en las actividades diarias.	Evitar aumento del Riesgo.
R36	4	Alto	C69	La asignación de privilegios va de acuerdo al manual de funciones.	Elección de controles
			C70	Se generan pistas de auditoria que son revisadas periódicamente.	Elección de controles
R37	4	Alto	C71	Se cuenta con un procedimiento para la revisión de usuarios del sistema de manera semestral, lo cual deberá ser verificado por personal de Recursos Humanos	Elección de controles
R38	4	Alto	C72	Existen acuerdos de confidencialidad, los cuales han sido entregados al personal al momento de su ingreso a la institución y estos acuerdos están previamente firmados	Elección de controles
R39	3	Medio	C73	Al inicio de la relación laboral, se realizan evaluaciones psicológicos al personal y evaluación de historial.	Evitar aumento del Riesgo.
			C74	Se cuenta con políticas de seguridad y se cuenta con reglamentos internos que establecen sanciones.	Evitar aumento del Riesgo.

R40	2	Bajo	C75	Se cuenta con reglamento de altas, bajas y modificación de usuarios.	Evitar aumento del Riesgo.
R41	3	Medio	C76	Existen validaciones en el sistema para el registro de información. Esta validación se ha determinado a nivel de base de datos.	Evitar aumento del Riesgo.
			C77	En los perfiles del puesto, se ha designado como requisito que el personal cuente con conocimientos básicos de computación.	Evitar aumento del Riesgo.
R42	3	Medio	C78	Se cuenta con equipos de respaldo de cómputo y soporte técnico (interno), además de asignar una categoría de urgencia de equipos.	Evitar aumento del Riesgo.
			C79	Se cuenta con personal técnico externo	Evitar aumento del Riesgo.
			C80	Personal interno puede resolver problemas hasta cierto nivel de complejidad.	Evitar aumento del Riesgo.
R43	3	Medio	C81	Se cuenta con grupo electrógeno y un sistema de alimentación ininterrumpida (UPS).	Evitar aumento del Riesgo.
R44	2	Bajo	C82	Se da soporte de mantenimiento basado en requerimientos de los usuarios y mejoras de los procesos existentes de manera continua.	Evitar aumento del Riesgo.
R45	3	Medio	C83	Toda versión del sistema de información histórica se encuentra documentado en files.	Evitar aumento del Riesgo.
R46	3	Medio	C84	Se comunica vía telefonía la incidencia presentada	Evitar aumento del Riesgo.
R47	3	Medio	C85	El proveedor genera copias de respaldo de las configuraciones de los correos.	Evitar aumento del Riesgo.
R48	2	Bajo	C86	Se revisa el estado de almacenamiento en el hosting de correo y se asigna cuota por cuenta de acuerdo al tipo de usuario.	Evitar aumento del Riesgo.
R49	2	Bajo	C87	Se actualiza las contraseñas, cuando el personal que administró el correo ya no forma parte de la institución.	Evitar aumento del Riesgo.
			C88	Se firma un acuerdo de confidencialidad	Evitar aumento del Riesgo.
R50	3	Medio	C89	Se tiene un reglamento de uso de correo, donde se establecen indicaciones para la	Evitar aumento del Riesgo.

				creación de contraseñas.	
R51	2	Bajo	C90	Se cuenta con un proceso de evaluación del personal nuevo por parte de Recursos Humanos.	Evitar aumento del Riesgo.
			C91	Se cuenta con una lista de técnicos que permiten realizar el mantenimiento de los equipos.	Evitar aumento del Riesgo.
			C92	La empresa proveedora, brinda servicios de mantenimiento a los equipos arrendados	Evitar aumento del Riesgo.
R52	2	Bajo	C93	Los equipos de cómputo se han arrendado a un proveedor por un periodo de tres años; asimismo se ha firmado un acuerdo un acuerdo de niveles de servicio con el arrendador.	Evitar aumento del Riesgo.
R53	2	Bajo	C94	Se realiza un seguimiento al cumplimiento del plan por parte de la persona responsable de Continuidad del negocio y el seguimiento es reportado en el informe de continuidad de Negocio de manera bimensual.	Evitar aumento del Riesgo.
R54	3	Medio	C95	Existe un plan de mantenimiento del sistema eléctrico, este mantenimiento se realiza de manera semestral.	Evitar aumento del Riesgo.
			C96	Se cuenta con una red eléctrica estabilizada	Evitar aumento del Riesgo.
			C97	Las PCs de misión crítica están conectadas a UPS.	Evitar aumento del Riesgo.
			C98	Se realizan pruebas periódicas del sistema de respaldo eléctrico (UPS, Grupo electrógeno y motor).	Evitar aumento del Riesgo.
			C99	Se realiza mantenimiento programado a los equipos eléctricos.	Evitar aumento del Riesgo.
R55	2	Bajo	C100	Se cuenta con personal capacitado para realizar las configuraciones de los equipos.	Evitar aumento del Riesgo.
R56	3	Medio	C101	En el MOF indica: Es responsabilidad de los usuarios, que el buen uso y conservación de los bienes o activos que la Caja asigna al trabajador para el cumplimiento de sus	Evitar aumento del Riesgo.

				funciones.	
R57	2	Bajo	C102	Existe un ambiente para la ubicación de los equipos, así mismo estos ambientes cuentan con ambientes de ventilación.	Evitar aumento del Riesgo.
R58	2	Bajo	C103	Se tienen identificados los equipos críticos del área de TI y centro de cómputo principal.	Evitar aumento del Riesgo.
			C104	Se cuenta con políticas para la clasificación de la información.	Evitar aumento del Riesgo.
R59	4	Alto	C105	Política de escritorios y pantallas limpias	Elección de controles
R60	2	Bajo	C106	Se realizan copias de seguridad de manera semanal, así mismo se lleva un control de los backups del código fuente generado por el personal de desarrollo.	Evitar aumento del Riesgo.
			C107	Se mantiene tres copias de respaldo (Of. Principal. Moshoqueque y Sección de desarrollo).	Evitar aumento del Riesgo.
R61	2	Bajo	C108	Seguridad de acceso local de usuario	Evitar aumento del Riesgo.
			C109	La PC de integración de desarrollo está separada de la red de producción.	Evitar aumento del Riesgo.
			C110	Se generará copias de seguridad del código fuentes/ existe registro de versiones.	Evitar aumento del Riesgo.
R62	4	Alto	C111	El código fuente es clasificada como información restringida y controlada por el Jefe de TI.	Elección de controles
R63	4	Alto	C112	Se mantiene un documento de control de cambios, donde se detalla todo lo que se modifica a nivel de código fuente , a nivel de base de datos y a nivel de dato.	Elección de controles
			C113	Se realiza un control de calidad de todos los puntos integrados de los analistas de sistemas.	Elección de controles
			C114	Control de calidad por parte de la División de producción antes de su implantación.	Elección de controles
R64	3	Medio	C115	Se ha asignado una complejidad en las contraseñas teniendo en caracteres y	Evitar aumento del Riesgo.

				números, la contraseña cambia en cada respaldo.	
R65	5	Muy Alto	C116	Las modificaciones solo tienen impacto en las aplicaciones, ya que en la integración solo se actualizan los objetos de acuerdo al requerimiento del usuario	Elección de controles
			C117	El especialista en sistemas de Información puede detectar cambios no programados.	Elección de controles
			C118	Existe una fase de prueba en desarrollo y certificación antes del pase a producción.	Elección de controles
R66	3	Medio	C119	Se cuenta con file de versiones en donde se adjuntan los requerimientos de los usuarios, control de cambios, manuales de usuarios, conformidades y otra documentación según corresponda el tipo de requerimiento.	Evitar aumento del Riesgo.
R67	3	Medio	C120	Se mantiene un listado de inventario denominado matriz de requerimientos.	Evitar aumento del Riesgo.
R68	2	Bajo	C121	Al ingresar cada analista de sistemas recibe inducción sobre los procesos del negocio y de los procesos automatizados de negocio. Asignación de tareas de manera gradual. Asignación de requerimientos teniendo en cuenta el nivel de experiencia en el desarrollo del proceso del negocio.	Evitar aumento del Riesgo.
R69	3	Medio	C122	Se priorizan los requerimientos de implementación de procesos más importantes.	Evitar aumento del Riesgo.
R70	2	Bajo	C123	Existe reglamento específico de acceso a Internet	Evitar aumento del Riesgo.
R71	4	Alto	C124	Existe restricción de acceso a Internet según niveles de acceso de usuarios.	Elección de controles
R72	2	Bajo	C125	Se realiza un proceso de inducción de los procesos del negocio y de los procesos automatizados en el sistema.	Evitar aumento del Riesgo.
R73	3	Medio	C126	Instalación de Antivirus	Evitar aumento del Riesgo.
R74	4	Alto	C127	Se mantiene un inventario de los backups generados, así mismo se generan tres	Elección de controles

				copias de respaldo que son enviados al sitio alterno	
R75	3	Medio	C128	Se cuenta con licencias de uso de software de desarrollo (lenguaje de programación y manejador de BD. Se puede solicitar al proveedor copias de los instaladores.	Evitar aumento del riesgo.
R76	3	Medio	C129	En la integración de código fuente, el especialista de sistemas verifica los comentarios de identificación en el código fuente (identificador del analista de sistemas, la fecha de cambio y motivo o descripción del cambio).	Evitar aumento del riesgo.
R77	2	Bajo	C130	Se genera una copia mensual de la normativa vigente, se lleva un control de cambios en cada documento normativo.	Evitar aumento del riesgo.
R78	2	Bajo	C131	No se cuenta con controles	Evitar aumento del riesgo.

Tabla 33: Total de Riesgos según categoría

Nivel	Cantidad
Muy Bajo	01
Bajo	33
Medio	24
Alto	15
Muy Alto	05

- Los riesgos críticos (rojo) deben ser revisados y controlados por lo menos Semanalmente.
- Los riesgos importantes (marrón) deben ser revisados y controlados por lo menos mensualmente.
- Los riesgos sugeridos (amarillo) deben ser revisados y controlados por lo menos trimestralmente.

J. Valorización del riesgo residual y determinación de la brecha de seguridad

Definidos los controles que se han implementado, corresponde la evaluación de su efectividad, para determinar el Nivel de Riesgo Residual (NRR) y por consiguiente determinar la brecha de seguridad para lograr los niveles de riesgo aceptables por la Caja. De acuerdo al

apetito de riesgo definido, sólo se evaluarán los niveles de riesgo que hayan obtenido valores de “Alto” y “Muy alto”.

Esta evaluación se realizó después de seis (06) meses luego de diseñados e implementados formalmente los controles. Los resultados de la segunda evaluación se muestran en el cuadro siguiente:

Tabla N° 34: Valorización del NRR y determinación de la brecha de seguridad

Nivel de Riesgo Intrínseco (NRI)		Control Implantado		Valorización del Nivel de Riesgo Residual (NRR)						Apetito de riesgo
Id riesgo	Categoría	ID Control	Descripción	Nivel	Categoría	Nivel	Categoría	Nivel	Riesgo	
R3	Muy Alto	C4	Personal capacitado en administración de Windows server y actualizaciones de parches.	4	Mayor	3	Posible	3	Medio	Riesgo Aceptable
R6	Alto	C10	El Oficial de Seguridad de la Información monitorea de manera bimensual las pistas de auditoría al administrador de la BD, así como también las operaciones que realiza en la arquitectura de la BD	4	Mayor	3	Posible	3	Medio	Riesgo Aceptable
R8	Muy Alto	C13	Se tiene establecido restricciones de acceso mediante la asignación de perfiles de usuario (no pueden instalar aplicaciones), se desactivan herramientas adicionales que permiten acceder a la base de datos.	5	Catastrófico	2	Improbable	3	Medio	Riesgo Aceptable
		C14	La contraseña de acceso a la base de datos tiene un nivel de complejidad, distinta a las contraseñas que manejan los usuarios locales.							Riesgo Aceptable

		C15	Los perfiles de usuarios que acceden a la base de datos tiene accesos restringidos							Riesgo Aceptable
R9	Alto	C16	Se cuenta con línea de contingencia para comunicaciones.	4	Mayor	3	Posible	3	Medio	Riesgo Aceptable
		C17	Reporte de averías al proveedor							Riesgo Aceptable
R10	Alto	C18	Reporte de averías al proveedor	4	Mayor	3	Posible	3	Medio	Riesgo Aceptable
R11	Alto	C19	Se cuenta con UPS y grupo electrógeno, el cual permite mantener la operatividad de los equipos ante una posible interrupción del corte de energía eléctrica.	4	Mayor	4	Probable	4	Alto	Riesgo no Aceptable
		C20	Se realizan pruebas de operatividad de los equipos eléctricos, con el fin de evaluar su funcionamiento.							Riesgo Aceptable
		C21	Se cuenta con un plan de mantenimiento al sistema eléctrico							Riesgo Aceptable
R19	Alto	C43	Reglamento de administración de usuarios al SIIF, en el que incluye las opciones para la asignación de perfiles por usuarios.	4	Mayor	2	Improbable	2	Bajo	Riesgo Aceptable
R22	Alto	C46	Se han deshabilitado acceso al Excel en todas las máquinas	3	Moderado	3	Posible	3	Medio	Riesgo Aceptable

		C47	Acceso a la BD protegida por un password que es de conocimiento del jefe de área de producción y soporte.							Riesgo Aceptable
		C50	No se tiene carpetas compartidas de la BD							Riesgo Aceptable
R25	Muy Alto	C51	Se efectúa una revisión general de los script que envía la sección desarrollo para el pase a producción.	4	Mayor	3	Posible	3	Medio	Riesgo Aceptable
R29	Alto	C56	Se cuenta con políticas y procedimientos de generación de backups	4	Mayor	2	Improbable	2	ajo	Riesgo Aceptable
		C57	Se generan dos copias de respaldo, la cual una de ellas se mantiene en el sitio alterno (Ag. Moshoqueque) y la otra en bóveda(Oficina Principal).							Riesgo Aceptable
		C58	Se lleva un control trimestral del estado de almacenamiento de los medios de respaldo							Riesgo Aceptable
		C59	Se realiza un monitoreo del procedimiento de respaldo de los backups							Riesgo Aceptable
		C60	Se cuenta con un centro de cómputo alterno que replica información de la BD de manera automática; asimismo se cuenta con un servidor de base de datos							Riesgo Aceptable

			de respaldo en el centro de cómputo principal (CCP) en caso de caída del servidor primario.							
R31	Muy Alto	C62	La herramienta que comprime la BD, realiza una verificación automática de los archivos comprimidos.	3	Moderado	3	Posible	3	Medio	Riesgo Aceptable
		C63	El programa que graba los archivos comprimidos en los medios, realiza una verificación después de la grabación.							Riesgo Aceptable
		C64	Se realiza la verificación periódica de las copias generadas							Riesgo Aceptable
R36	Alto	C69	La asignación de privilegios va de acuerdo al manual de funciones	3	Moderado	3	Posible	3	Medio	Riesgo Aceptable
		C70	Se generan pistas de auditoria que son revisadas periódicamente							Riesgo Aceptable
R37	Alto	C71	Se cuenta con un procedimiento para la revisión de usuarios del sistema de manera semestral, lo cual deberá ser verificado por personal de Recursos Humanos.	3	Moderado	3	Posible	3	Medio	Riesgo Aceptable
R38	Alto	C72	Existen acuerdos de confidencialidad, los cuales han sido entregados al personal al momento de su ingreso a la institución y estos acuerdos están previamente firmados.	3	Moderado	3	Posible	3	Medio	Riesgo Aceptable

R59	Alto	C105	Política de escritorios y pantallas limpias	4	Mayor	2	Improbable	2	Bajo	Riesgo Aceptable
R62	Alto	C111	El código fuente es clasificada como información restringida y controlada por el Jefe de TI	4	Mayor	2	Posible	3	Medio	Riesgo Aceptable
R63	Alto	C112	Se mantiene un documento de control de cambios, donde se detalla todo lo que se modifica a nivel de código fuente, a nivel de base de datos y a nivel de dato.	4	Mayor	3	Posible	3	Medio	Riesgo Aceptable
		C113	Se realiza un control de calidad de todos los puntos integrados de los analistas de sistemas.							Riesgo Aceptable
		C114	Control de calidad por parte de la División de producción antes de su implantación							Riesgo Aceptable
R65	Muy Alto	C116	Las modificaciones solo tienen impacto en las aplicaciones, ya que en la integración solo se actualizan los objetos de acuerdo al requerimiento del usuario	4	Mayor	4	Probable	4	Alto	Riesgo No Aceptable
		C117	El especialista en sistemas de Información puede detectar cambios no programados							Riesgo Aceptable
		C118	Existe una fase de prueba en desarrollo							Riesgo

			y certificación antes del pase a producción							Aceptable
R71	Alto	C124	Existe restricción de acceso a Internet según niveles de acceso de usuarios	3	Moderado	2	Improbable	2	Bajo	Riesgo Aceptable
R74	Alto	C127	Se mantiene un inventario de los backups generados, así mismo se generan tres copias de respaldo que son enviados al sitio alterno.	3	Moderado	2	Improbable	2	Bajo	Riesgo Aceptable

Tabla 35: Total de Riesgos según categoría

Nivel	Cantidad
Alto	15
Muy Alto	05

- Los riesgos críticos (rojo) deben ser revisados y controlados por lo menos Semanalmente.
- Los riesgos importantes (marrón) deben ser revisados y controlados por lo menos mensualmente.

K. Simulación del plan de Gestión de Riesgos de Tecnologías de la Información propuesto en el software PILAR (5.4.9 - 18.7.2016)

Objetivo de la simulación

El objetivo es probar y demostrar que el Plan de Gestión de Riesgos de Tecnologías de la Información (PGR-TI) desarrollado en el trabajo de tesis, permite lograr resultados similares a un software comercial que cumple con los estándares internacionales sobre la materia, en este caso, se optó por la aplicación PILAR, que se ajusta a la metodología del plan propuesto en la tesis (Ver anexo N° 11).

Acerca de la aplicación PILAR utilizada

PILAR es un software comercial para gestionar riesgos de TI. Es un producto español.

Utiliza estándares y marcos de referencia de aceptación internacional, como:

- Metodología Magerit v3:2012
- ISO/IEC 31000:2009 - Risk management - Principles and guidelines
- ISO/IEC 27005:2011 - Information security risk management –entre otras

La versión utilizada, es una versión con licencia de evaluación, descargada de http://www.pilar-tools.com/.

Especificaciones previas

El PGR-TI desarrollado en el trabajo de tesis:

- Se tomó en cuenta los requerimientos de seguridad de la información y de gestión de riesgos de TI exigidos por la SBS en sus normativas, por tanto, **es un plan ajustado a las exigencias de la SBS**.
- Nos basamos en los siguientes marcos de referencia: ISO/IEC 27001, ISO/IEC 17799, Magerit. Por tanto, **es un resultado híbrido de estos frameworks, no necesariamente exactos, pero sí básicos y personalizados a la Caja Sipán** para cumplir con las exigencias de la SBS.

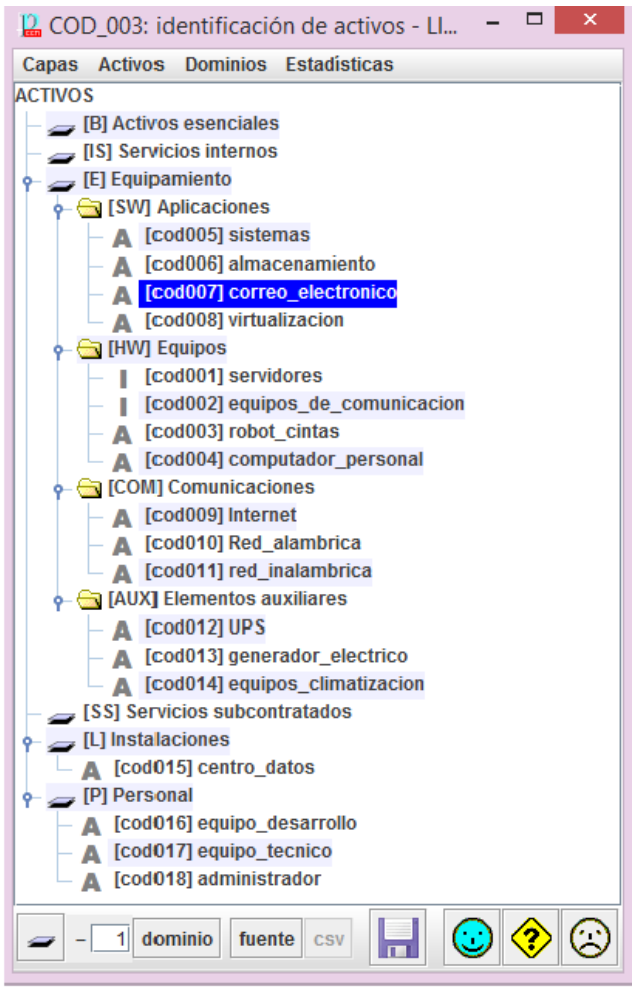
Desarrollo del plan propuesto utilizando PILAR.

A. Identificación de Activos en PILAR

El primer paso a realizar en la herramienta PILAR es la creación de un nuevo proyecto siguiendo el manual de usuario, luego identificar los activos mediante un código y un nombre (ver figura 08) y clasificarlos entre las siguientes categorías:

- Activos esenciales
- Servicios internos
- Equipamiento
- Servicios Subcontratados
- Instalaciones
- Personal

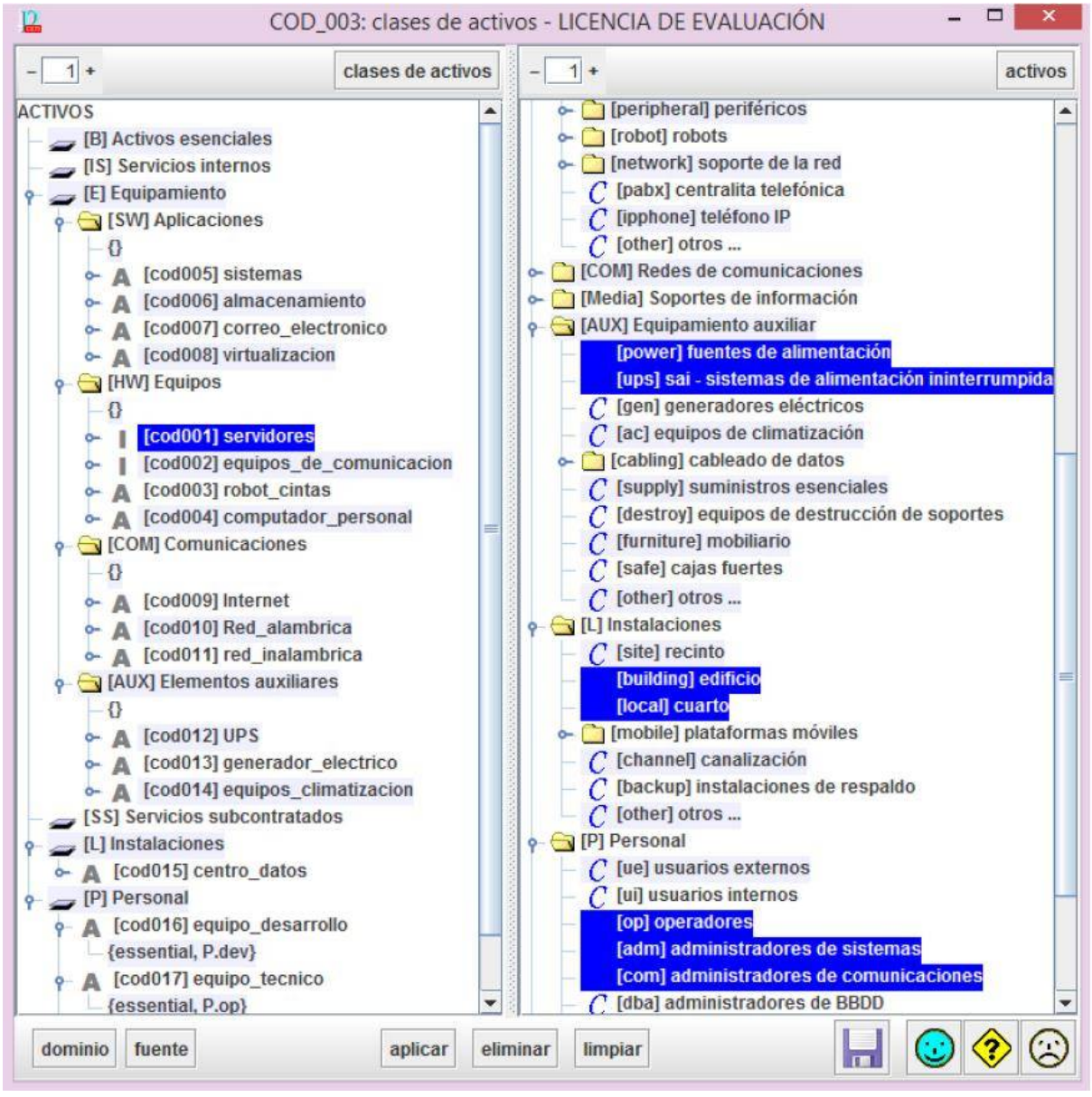
Figura 8 : Identificación de activos



B. Dependencia de Activos en PILAR

Para definir las dependencias de los activos se ha seguido el diagrama de dependencias detallado en el apartado anterior. En la figura 09 se ha determinado la dependencia existente entre los servidores con el equipamiento auxiliar, personal e instalaciones. El proceso se repite para cada uno de los activos.

Figura 9 : Definiendo la Dependencia entre activos

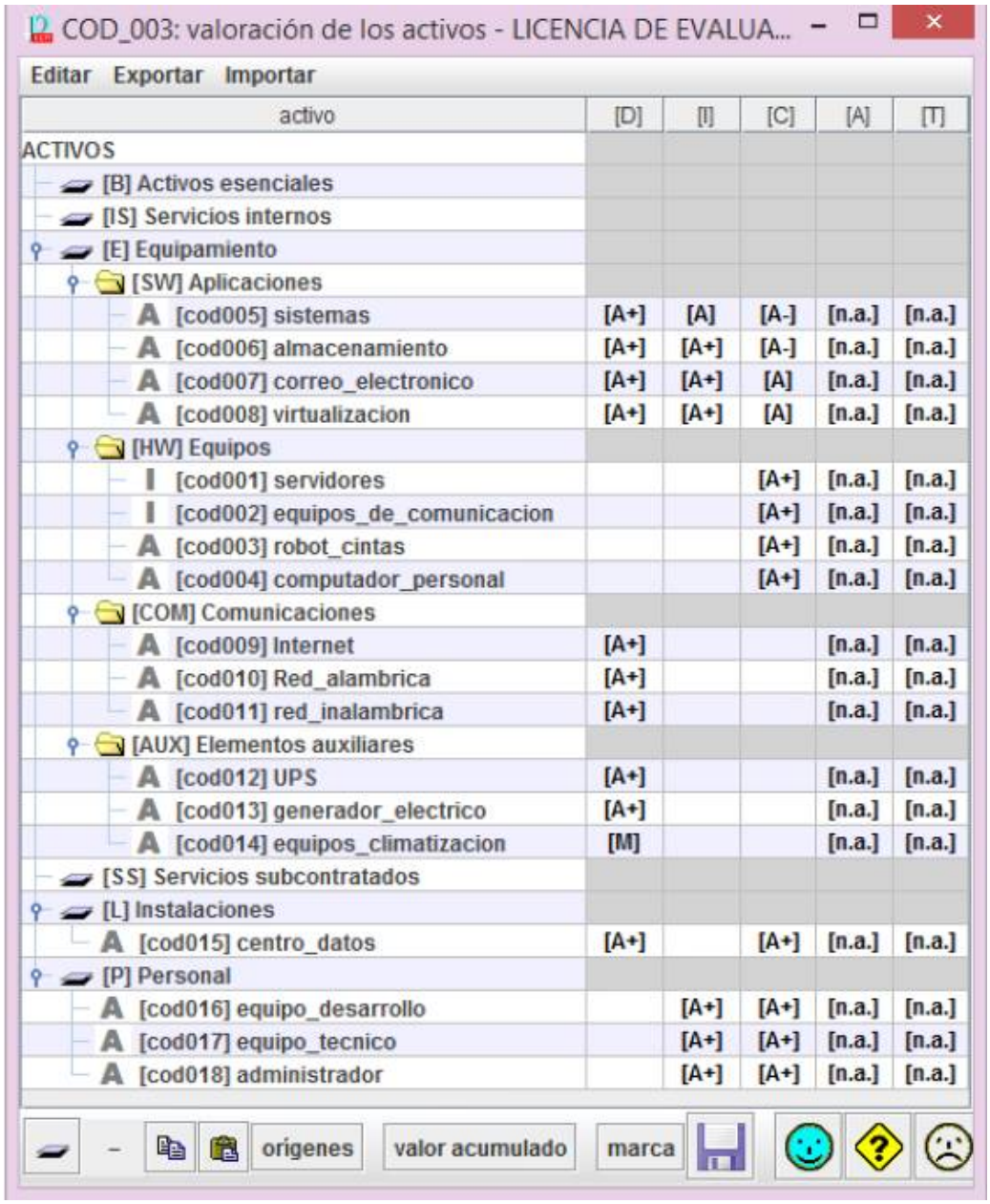


C. Valoración de Activos

A continuación, se realizará la evaluación de los activos en cada uno de los parámetros de seguridad en que se verían afectados al exponerse ante los diversos tipos de amenazas que causarían la pérdida de información o daños sobre el equipo que la almacena

PILAR permite valorar los activos en base a tres niveles: alto, medio y bajo; en la figura 10 se presenta la evaluación de activos en cada uno de los parámetros de seguridad.

Figura 10 : Valoración de los activos

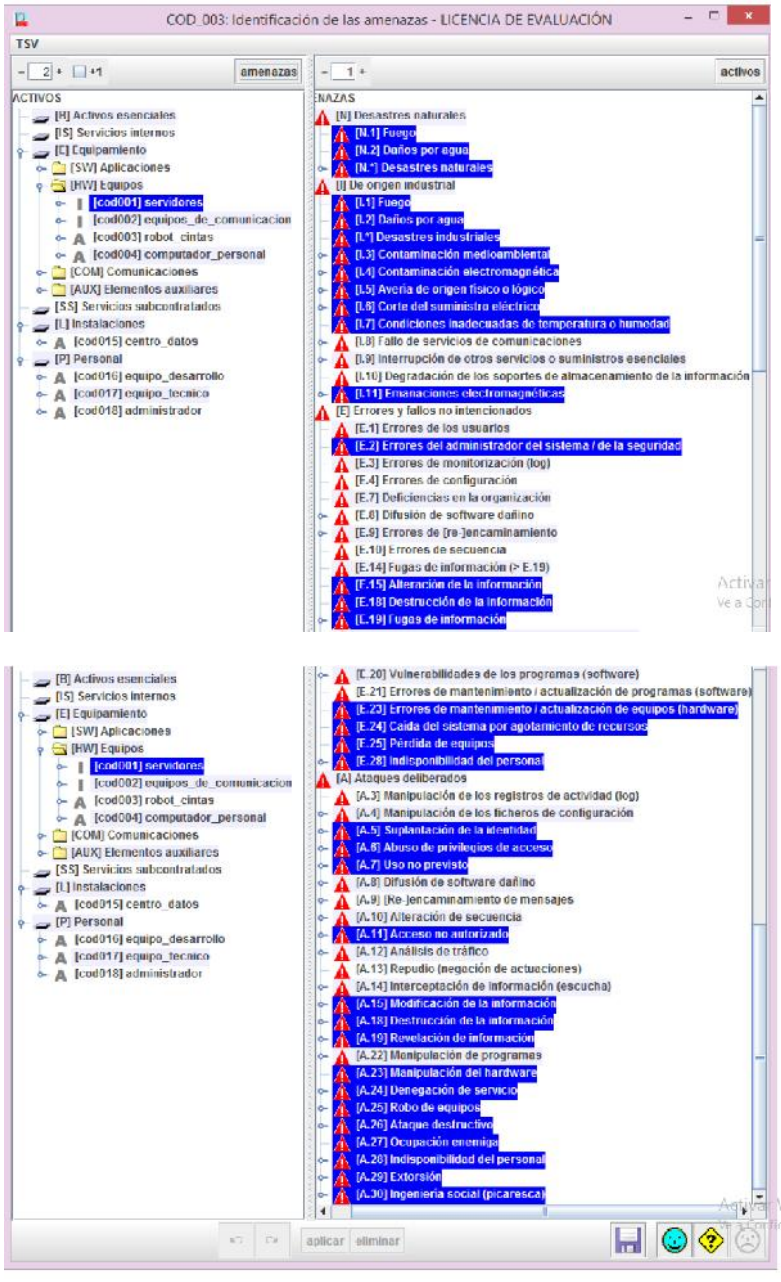


activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
[cod005] sistemas	[A+]	[A]	[A-]	[n.a.]	[n.a.]
[cod006] almacenamiento	[A+]	[A+]	[A-]	[n.a.]	[n.a.]
[cod007] correo_electronico	[A+]	[A+]	[A]	[n.a.]	[n.a.]
[cod008] virtualizacion	[A+]	[A+]	[A]	[n.a.]	[n.a.]
[HW] Equipos					
[cod001] servidores			[A+]	[n.a.]	[n.a.]
[cod002] equipos_de_comunicacion			[A+]	[n.a.]	[n.a.]
[cod003] robot_cintas			[A+]	[n.a.]	[n.a.]
[cod004] computador_personal			[A+]	[n.a.]	[n.a.]
[COM] Comunicaciones					
[cod009] Internet	[A+]			[n.a.]	[n.a.]
[cod010] Red_alambrica	[A+]			[n.a.]	[n.a.]
[cod011] red_inalambrica	[A+]			[n.a.]	[n.a.]
[AUX] Elementos auxiliares					
[cod012] UPS	[A+]			[n.a.]	[n.a.]
[cod013] generador_electrico	[A+]			[n.a.]	[n.a.]
[cod014] equipos_climatizacion	[M]			[n.a.]	[n.a.]
[SS] Servicios subcontratados					
[L] Instalaciones					
[cod015] centro_datos	[A+]		[A+]	[n.a.]	[n.a.]
[P] Personal					
[cod016] equipo_desarrollo		[A+]	[A+]	[n.a.]	[n.a.]
[cod017] equipo_tecnico		[A+]	[A+]	[n.a.]	[n.a.]
[cod018] administrador		[A+]	[A+]	[n.a.]	[n.a.]

De la valoración de los activos realizada se han considerado las amenazas que producen más daños, para evaluar el nivel de degradación, frecuencia y el riesgo implicado, tal como fue detallado en la *Tabla N° 28 Valoración del Nivel de Riesgo Intrínseco (NRI)* donde se dado una valoración a los activos de acuerdo a las amenazas que puede tener.

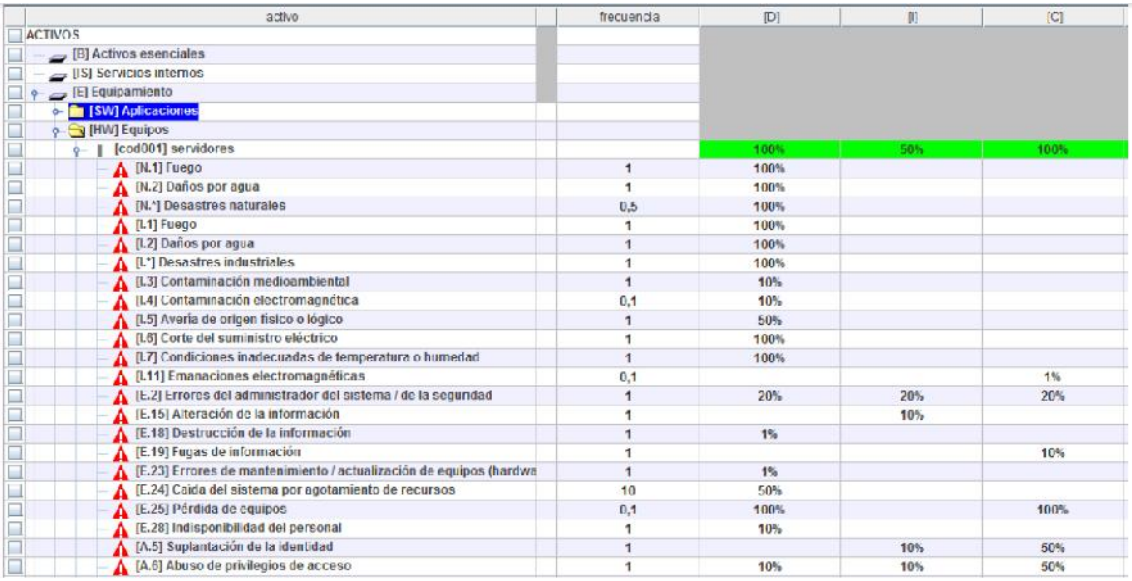
En PILAR es posible identificar las amenazas que pueden influir sobre un activo, en la figura 11 se presenta las amenazas que afectan a los servidores.

Figura 11 : Identificación de amenazas – Servidores



PILAR también permite obtener la valoración de las amenazas de forma automática considerando la frecuencia de materialización y el impacto que tendrían en la organización según las dimensiones. En la figura 12 se aprecian los resultados obtenidos en la valoración de las amenazas que afectan a los servidores.

Figura 12 : Valoración de amenazas - Servidores



activo	frecuencia	[D]	[I]	[C]
ACTIVOS				
[B] Activos esenciales				
[S] Servicios internos				
[E] Equipamiento				
[SW] Aplicaciones				
[HW] Equipos				
[cod001] servidores		100%	50%	100%
[N.1] Fuego	1	100%		
[N.2] Daños por agua	1	100%		
[N.*] Desastres naturales	0,5	100%		
[I.1] Fuego	1	100%		
[I.2] Daños por agua	1	100%		
[I.*] Desastres industriales	1	100%		
[I.3] Contaminación medioambiental	1	10%		
[I.4] Contaminación electromagnética	0,1	10%		
[I.5] Avería de origen físico o lógico	1	50%		
[I.6] Corte del suministro eléctrico	1	100%		
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%		
[I.11] Emanaciones electromagnéticas	0,1			1%
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%
[E.15] Alteración de la información	1		10%	
[E.18] Destrucción de la información	1	1%		
[E.19] Fugas de información	1			10%
[E.23] Errores de mantenimiento / actualización de equipos (hardwa	1	1%		
[E.24] Caída del sistema por agotamiento de recursos	10	50%		
[E.25] Pérdida de equipos	0,1	100%		100%
[E.28] Indisponibilidad del personal	1	10%		
[A.5] Suplantación de la identidad	1		10%	50%
[A.6] Abuso de privilegios de acceso	1	10%	10%	50%

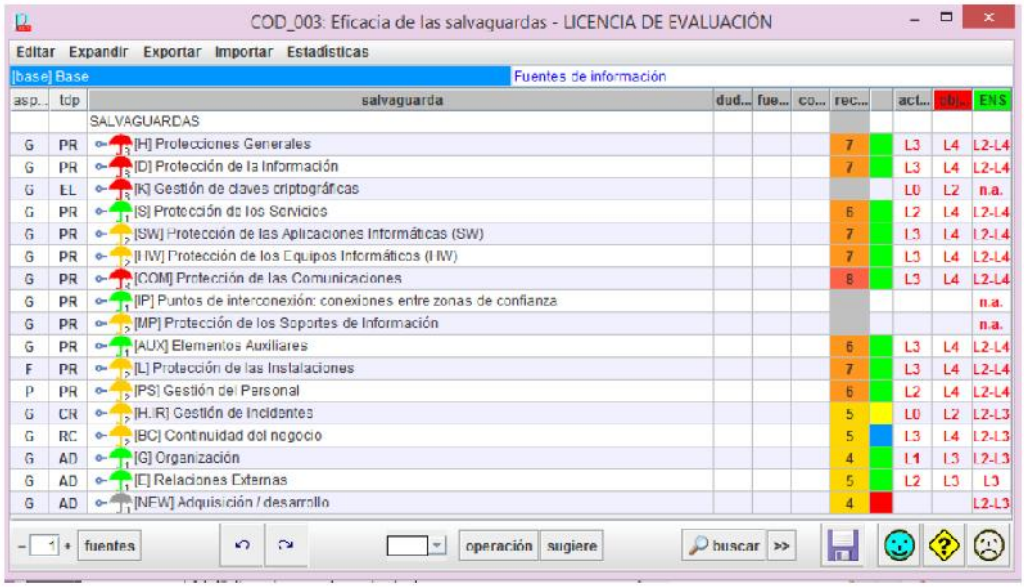
D. Evaluación de Salvaguardas PILAR

Las salvaguardas en PILAR se tratan bajo 4 aspectos:

- Gestión
- Técnico
- Seguridad física
- Gestión de personal

La columna “recomendación” indica la valoración estimada de la salvaguarda teniendo en cuenta el tipo de activos, el rango va desde el 0 al 10. En las siguientes columnas se ingresan los niveles de las salvaguardas actuales, objetivo y por último el nivel que PILAR recomienda.

Figura 13 : Identificación de salvaguardas



Como se puede visualizar en la figura 13, el nivel de salvaguardas actuales está entre 2 y 3 lo cual indica que aún faltan definir procesos para mejorar la protección de la información; el objetivo es mejorar estos procesos hasta que sean gestionables y medibles.

E. Impacto Acumulado

Figura 14 : Impacto Acumulado Potencial

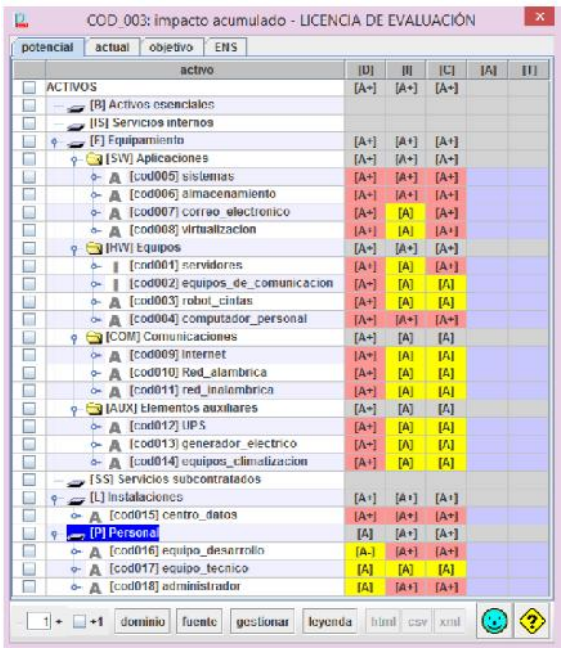


Figura 15 : Impacto Acumulado Actual

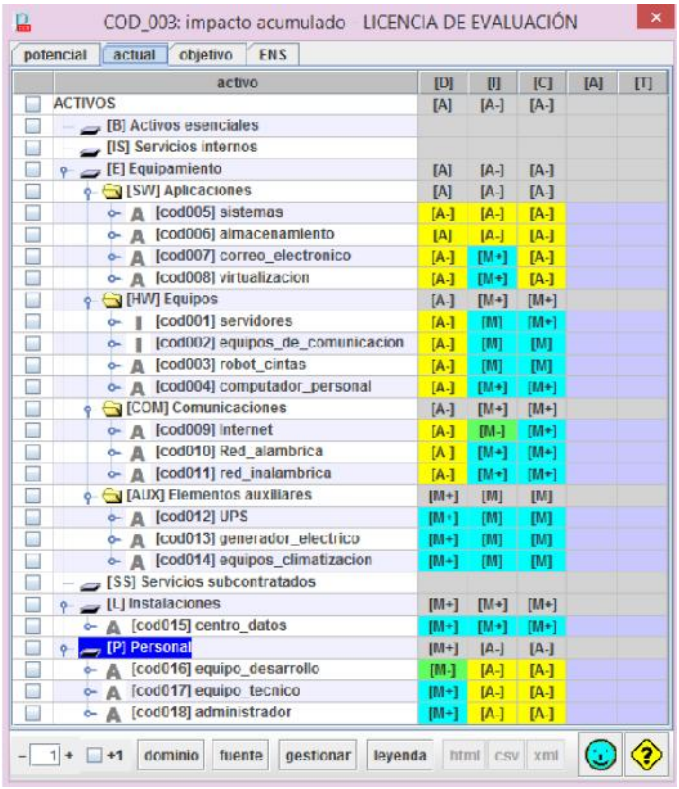
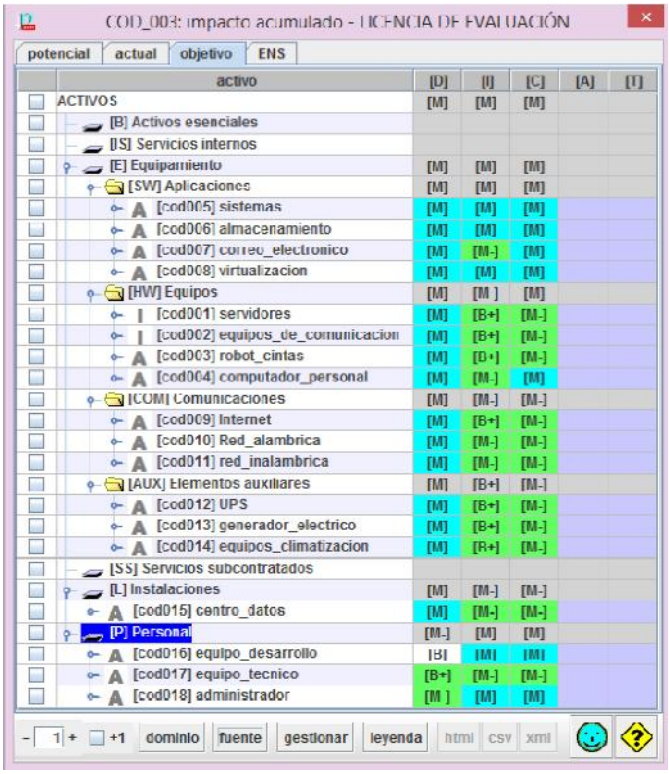


Figura 16 : Impacto Acumulado Objetivo



En las figuras 14 y 15 se puede contrastar la importancia de aplicar salvaguardas para disminuir los niveles del impacto, actualmente están en nivel medio, y el nivel objetivo es llegar a obtener un bajo impacto, ver la figura 16.

F. Riesgo Acumulado

PILAR permite medir los niveles de criticidad de los riesgos a los cuales se encuentran expuestos lo activos. Como se visualiza en la figura 17, el parámetro que se encuentra más expuesto es la disponibilidad en el caso que no existiesen salvaguardas. En la figura 18 refleja el nivel del riesgo actual, el cual es medio al igual que los resultados realizados manualmente y en la figura 19 se obtiene el riesgo acumulado objetivo que debe seguir en evaluación para tratar de disminuirlo o si es posible eliminarlo.

Figura 17 : Riesgo Acumulado Potencial

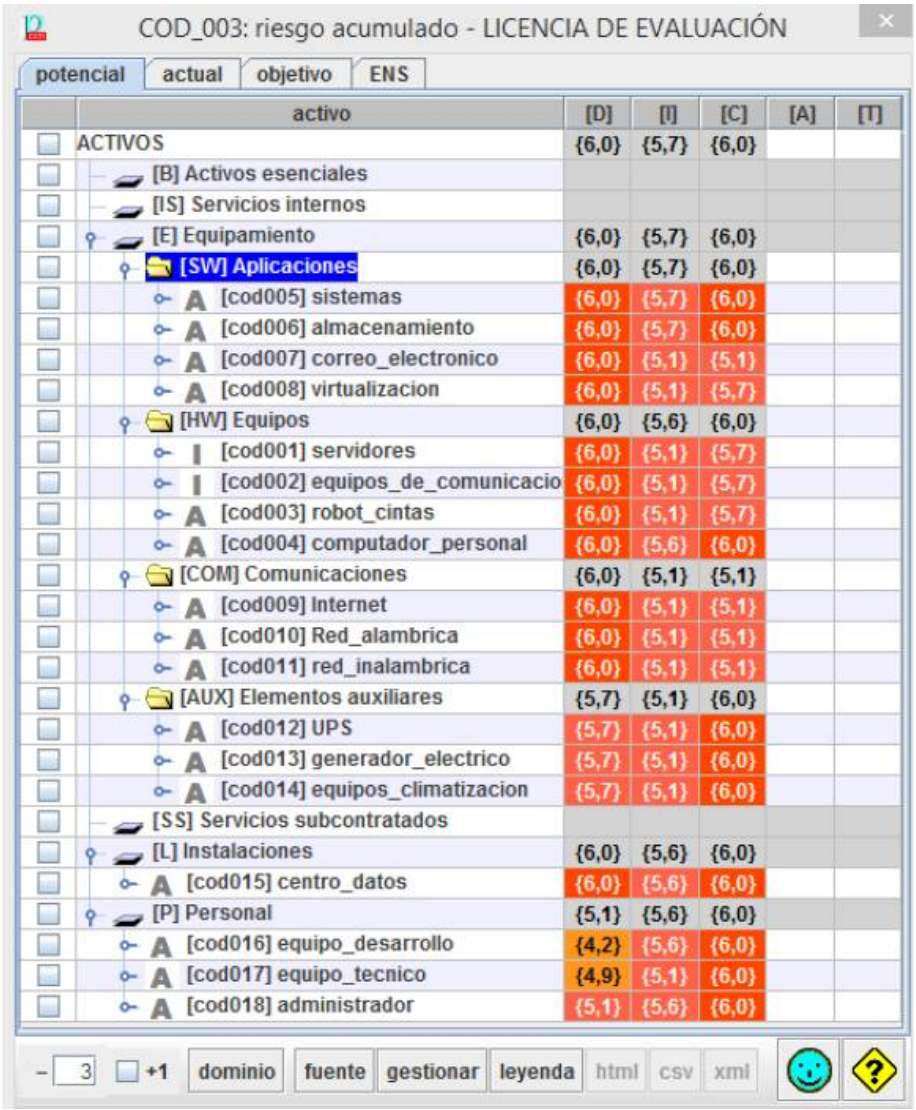


Figura 18 : Riesgo Acumulado Actual

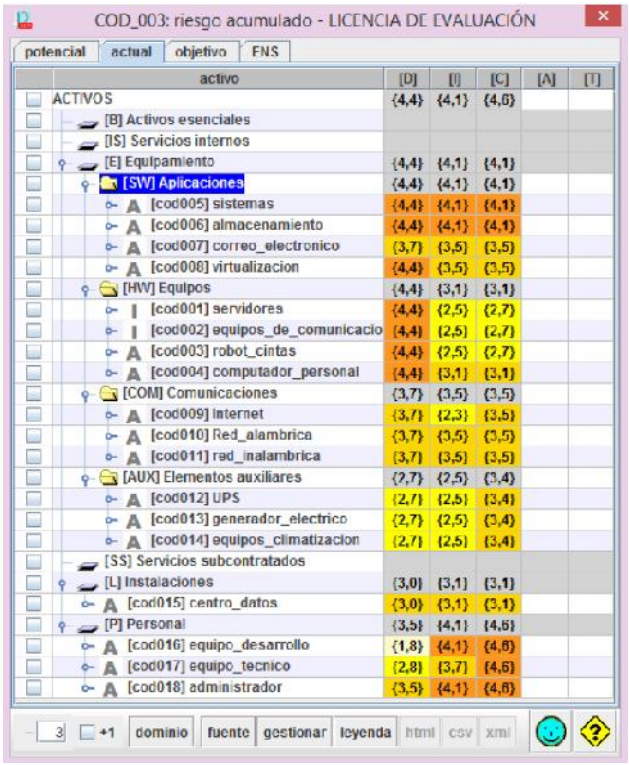
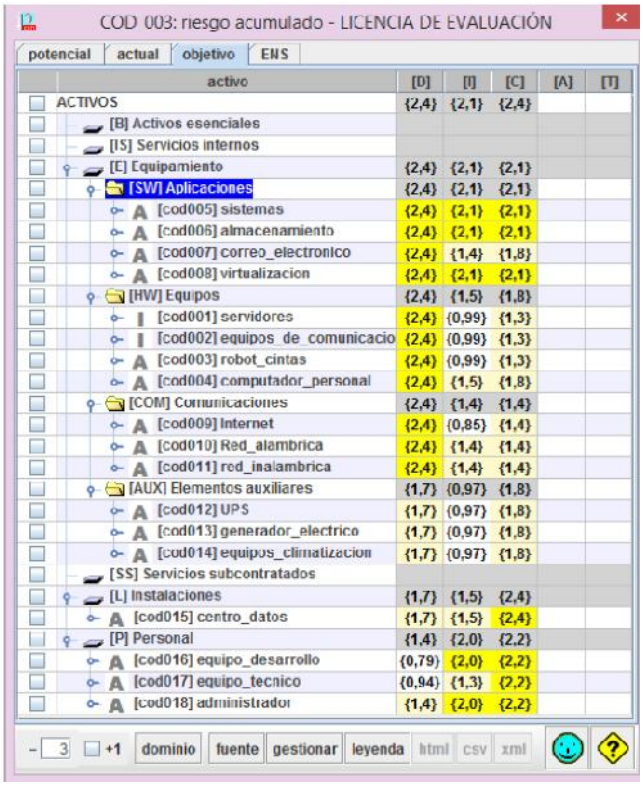


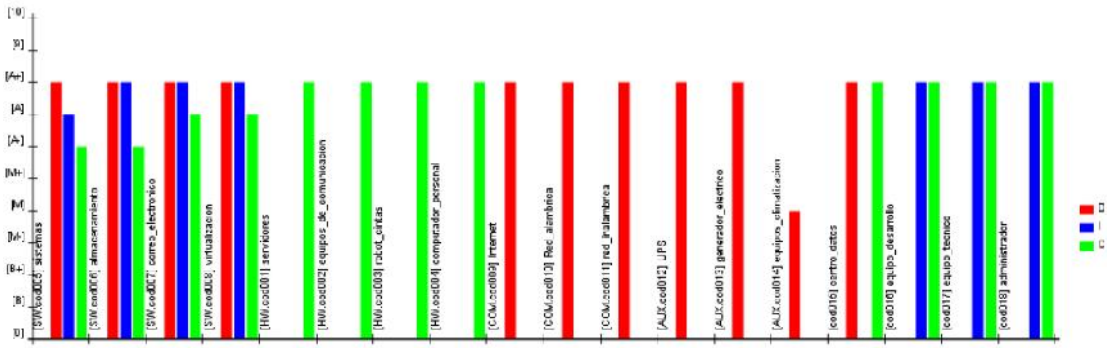
Figura 19 : Riesgo Acumulado Objetivo



G. Informes

Se han obtenido los gráficos resultantes de las evaluaciones realizadas. La figura 20 presenta los parámetros de seguridad que se afectan en cada activo, prevaleciendo la confiabilidad en la mayoría de activos.

Figura 20 : Valor de Activo



En las figuras 21 y 22 se reflejan los valores del impacto y riesgos acumulados sobre cada uno de los activos definidos en las gráficas radiales, en el cual se consideran la implementación de las salvaguardas antes planteadas que permiten que estos valores disminuyan los parámetros de vulnerabilidad de los activos hasta el nivel objetivo.

Figura 21 : Impacto Acumulado

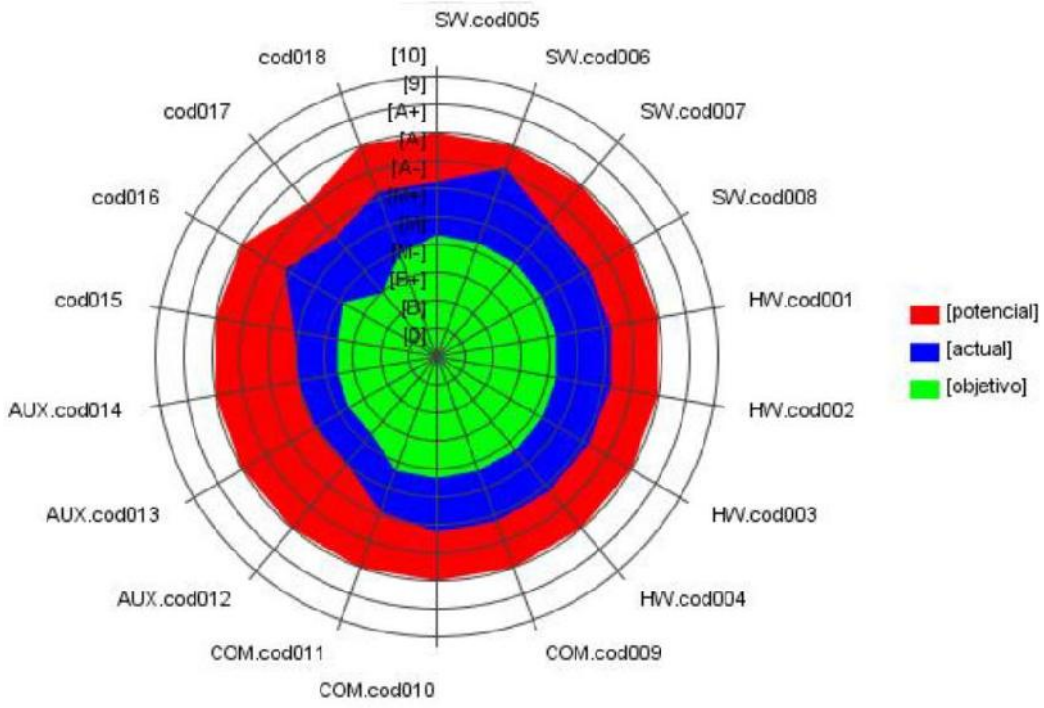
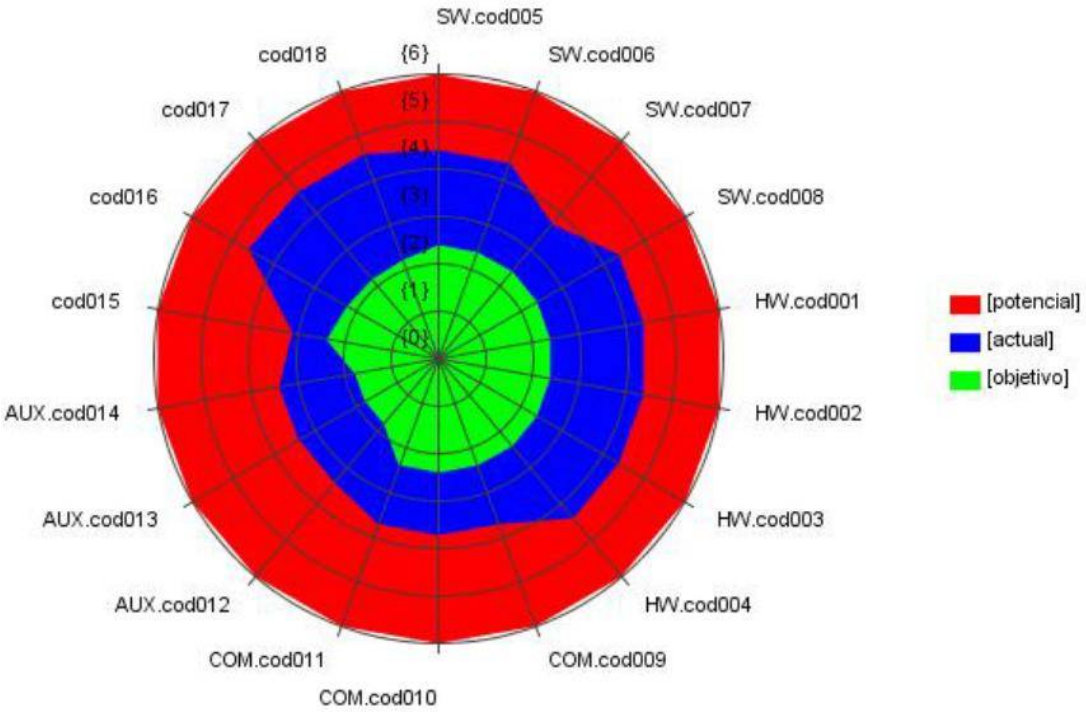


Figura 22 : Riesgo Acumulado



H. Plan de Seguridad

En esta etapa final es necesario informar al personal de las áreas implicadas de la Caja de Ahorro y Crédito Sipán SA. sobre los activos evaluados con sus respectivas amenazas y salvaguardas factibles.

En el presente análisis de riesgos se han considerado los activos que forman parte de los principales servicios que brinda la caja a la población, entre los cuales están: acceso a los sistemas financieros y administrativos, proveer el acceso a la intranet e internet de forma alámbrica e inalámbrica y almacenar de forma segura la información que se genera diariamente.

Las amenazas presentes que requieren eliminarse o reducirse de forma urgente son las referentes al acceso no autorizado, las desconexiones físicas y lógicas, y el agotamiento de recursos; luego se encuentran las amenazas que están siendo controladas por el momento, pero requieren de algunos cambios o mejoras para incrementar la seguridad.

Respecto a las salvaguardas citadas, es primordial tener el apoyo y colaboración de todo el personal implicado como son los jefes y administradores de cada área para que la

adaptación de nuevas normas y procedimientos se realice de forma progresiva y consciente. Entre las principales salvaguardas se encuentran las relacionadas a aumentar la seguridad de la información, y esto se logra incrementando las medidas de seguridad a las cuentas de acceso a los sistemas, monitoreando las reglas de acceso y adquiriendo los procedimientos necesarios para restaurar la información si sucediera algún desastre natural.

Para que la gestión de riesgos sea un proceso exitoso, este debe permanecer siempre en revisión por el grupo de seguridad a contratar para que ellos se aseguren que los niveles de riesgo no aumenten y las salvaguardas se apliquen de forma correcta y continua; para ello es necesario analizar datos estadísticos alimentados por la respectiva revisión de documentación como los registros de incidentes y resultados de encuestas realizadas al personal.

CAPÍTULO VI: COSTOS Y PLANIFICACION DE LA PROPUESTA

6.1. Análisis de costos

Análisis de la implantación del Plan de gestión de riesgos en TI para los procesos críticos de créditos y captaciones de la caja SIPAN SA..

Valor Actual Neto –(proceso para obtener el valor presente de cantidades monetarias futuras

- El VAN equivale al valor actualizado de una serie de flujos de fondos en el futuro. Esta actualización se realiza mediante el descuento al momento actual (es decir, actualizar mediante una tasa) todos los flujos de caja futuros del proyecto. A este valor se le resta la inversión inicial, de tal modo que el valor obtenido es el valor actual neto del proyecto.

Tasa Interna de Retorno

- La TIR representa la rentabilidad promedio por período generada por un proyecto de inversión. También es la tasa de descuento requerida para que el Valor Actual Neto sea igual a cero.

Análisis de Costo Beneficio: Costos (Flujo de Caja)
(Ver tabla de costo en anexo 12)

Id Riesgo	Costos Posibles: Riesgo	Costos Posibles: Control aplicado para mitigar los riesgos	Mes 0	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6
R3	Fallas en el sistema operativo, falta de actualización de parches			S/ 500.00	S/ 500.00	S/ 500.00	S/ 500.00	S/ 500.00	S/ 500.00
	C4	Personal capacitado en administración de Windows server y actualizaciones de parches.	-S/2,400.00						
R6	Administrador tiene acceso total a la base de datos y puede realizar modificaciones.			S/ 500.00	S/ 500.00	S/ 500.00	S/ 500.00	S/ 500.00	S/ 500.00
	C10	El Oficial de Seguridad de la Información monitorea de manera bimensual las pistas de auditoría al administrador de la BD, así como también las operaciones que realiza en la arquitectura de la BD	-S/9,000.00						
R8	Usuarios acceden a servidor de base de datos por canales no autorizados			S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00
	C13	Se tiene establecido restricciones de acceso mediante la asignación de perfiles de usuario (no pueden instalar aplicaciones), se desactivan herramientas adicionales que permiten acceder a la base de datos.							
	C14	La contraseña de acceso a la base de datos tiene un nivel de complejidad, distinta a las contraseñas que manejan los usuarios locales							
	C15	Los perfiles de usuarios que acceden a la base de datos tiene accesos restringidos.							
R9	Falla de la línea principal de comunicaciones			S/ 500.00	S/ 500.00	S/ 500.00	S/ 500.00	S/ 500.00	S/ 500.00
	C16	Se cuenta con línea de contingencia para comunicaciones	-S/600.00						
	C17	Reporte de averías al proveedor							

R10	Falla de la red de comunicaciones con otras agencias.			S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00
	C18	Reporte de averías al proveedor							
R11	Fallas eléctricas que generen la interrupción de los procesos y servicios.			S/ 2,500.00	S/ 2,500.00	S/ 2,500.00	S/ 2,500.00	S/ 2,500.00	S/ 2,500.00
	C19	Se cuenta con UPS y grupo electrógeno, el cual permite mantener la operatividad de los equipos ante una posible interrupción del corte de energía eléctrica.	-S/3,720.00						
	C20	Se realizan pruebas de operatividad de los equipos eléctricos, con el fin de evaluar su funcionamiento.	-S/3,450.00						
	C21	Se cuenta con un plan de mantenimiento al sistema eléctrico							
R19	Falta de un adecuado procedimiento para la asignación de perfiles para accesos a la BD.			S/ 1,000.00	S/ 1,000.00	S/ 1,000.00	S/ 1,000.00	S/ 1,000.00	S/ 1,000.00
	C43	Reglamento de administración de usuarios al SIIF, en el que incluye las opciones para la asignación de perfiles por usuarios.							
R22	Acceso a la BD desde otras aplicaciones.			S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00
	C46	Se han deshabilitado acceso al Excel en todas las máquinas.							
	C47	Acceso a la BD protegida por un password que es de conocimiento del jefe de área de producción y soporte.							
R25	Modificación no autorizada de BD			S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00
	C51	Se efectúa una revisión general de los script que envía la sección desarrollo para el pase a producción.							
R29	Fallas en los dispositivos de almacenamiento (disco duro del servidor).			S/ 10,000.00	S/ 10,000.00	S/ 10,000.00	S/ 10,000.00	S/ 10,000.00	S/ 10,000.00
	C56	Se cuenta con políticas y procedimientos de generación de backups.	-S/1,260.00						

	C57	Se generan dos copias de respaldo, la cual una de ellas se mantiene en el sitio alterno (Ag. Moshoqueque) y la otra en bóveda(Oficina Principal).	-S/46,617.00						
	C58	Se lleva un control trimestral del estado de almacenamiento de los medios de respaldo.							
	C59	Se realiza un monitoreo del procedimiento de respaldo de los backups.							
	C60	Se cuenta con un centro de cómputo alterno que replica información de la BD de manera automática; asimismo se cuenta con un servidor de base de datos de respaldo en el centro de cómputo principal (CCP) en caso de caída del servidor primario.	-S/12,540.00						
R31	Errores en el proceso de generación de backups.			S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00
	C62	La herramienta que comprime la BD, realiza una verificación automática de los archivos comprimidos.							
	C63	El programa que graba los archivos comprimidos en los medios, realiza una verificación después de la grabación.							
	C64	Se realiza la verificación periódica de las copias generadas							
R36	Abuso de privilegios de accesos			S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00
	C69	La asignación de privilegios va de acuerdo al manual de funciones.							
	C70	Se generan pistas de auditoria que son revisadas periódicamente.							
R37	Errores en el proceso de generación de backups.			S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00
	C71	Se cuenta con un procedimiento para la revisión de usuarios del sistema de manera semestral, lo cual deberá ser verificado por personal de Recursos Humanos							
R38	Falta de acuerdos de confidencialidad			S/ 200.00	S/ 200.00	S/ 200.00	S/ 200.00	S/ 200.00	S/ 200.00

	C72	Existen acuerdos de confidencialidad, los cuales han sido entregados al personal al momento de su ingreso a la institución y estos acuerdos están previamente firmados							
R59	El personal guarda información sensible en sus equipos y no las guarda en el servidor.			S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00
	C105	Política de escritorios y pantallas limpias							
R62	Accesibilidad a todo el código fuente sin restricción por parte del personal de Desarrollo (no se tiene restricción de acceso al personal de desarrollo).			S/ 1,600.00	S/ 1,600.00	S/ 1,600.00	S/ 1,600.00	S/ 1,600.00	S/ 1,600.00
	C111	El código fuente es clasificada como información restringida y controlada por el Jefe de TI.							
R63	No se realiza una revisión minuciosa de los controles de cambios entregado por el analista de sistema.			S/ 1,600.00	S/ 1,600.00	S/ 1,600.00	S/ 1,600.00	S/ 1,600.00	S/ 1,600.00
	C112	Se mantiene un documento de control de cambios, donde se detalla todo lo que se modifica a nivel de código fuente , a nivel de base de datos y a nivel de dato.							
	C113	Se realiza un control de calidad de todos los puntos integrados de los analistas de sistemas.							
	C114	Control de calidad por parte de la División de producción antes de su implantación.							
R65	Manipulación del código fuente que puede alterar el desarrollo normal de un proceso.			S/ 1,600.00	S/ 1,600.00	S/ 1,600.00	S/ 1,600.00	S/ 1,600.00	S/ 1,600.00
	C116	Las modificaciones solo tienen impacto en las aplicaciones, ya que en la integración solo se actualizan los objetos de acuerdo al requerimiento del usuario							
	C117	El especialista en sistemas de Información puede detectar cambios no programados.							
	C118	Existe una fase de prueba en desarrollo y certificación antes del pase a producción.							
R71	Existe restricción de acceso a Internet según niveles de acceso de usuarios.			S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00

	C124	Existe restricción de acceso a Internet según niveles de acceso de usuarios.							
R74	No se trasladan copias de respaldo en sitios alternos.			S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00	S/ 600.00
	C127	Se mantiene un inventario de los backups generados, así mismo se generan tres copias de respaldo que son enviados al sitio alterno							
Flujo de Caja			-S/81,487.00	S/ 26,000.00	S/ 26,000.00	S/ 26,000.00	S/ 26,000.00	S/ 26,000.00	S/ 26,000.00

TIR 22.43%

VAN S/64,150.20

El Plan de Gestión de tecnologías de la información en los procesos críticos de créditos y captaciones para la caja de Ahorro y crédito SIPAN SA. Es rentable ya que la TIR sobrepasa el 2% que es la tasa de interés promedio para préstamos de inversión, además el VAN es S/64,150.20 y que sobrepasa el monto de inversión.

6.2. Planificación

Id	Nombre de tarea	Duración
1	**Plan de Gestión de Riesgos de TI**	**110 días**
2	**Establecer marco General**	**7 días**
3	Establecer el Contexto Estratégico	2 días
4	Establecer el Contexto Organizacional	2 días
5	Identificar Objetos Críticos	2 días
6	**Identificar los Riesgos de TI**	**27 días**
7	Establecer un marco específico de administración de riesgos	5 días
8	Desarrollar criterios de evaluación de riesgos	5 días
9	Identificar la estructura	10 días
10	Identificar riesgos	10 días
11	Identificar causas	5 días
12	**Análisis de los Riesgos de TI**	**33 días**
13	Valorar el riesgo inherente	15 días
14	Determinar Controles Existentes	8 días
15	Identificar Nivel de Exposición	10 días
16	**Evaluar y priorizar los Riesgos de TI**	**5 días**
17	Comparar contra Criterios y Definir prioridades de riesgo	5 días
18	**Tratamiento de los Riesgos de TI**	**31 días**
19	Identificar opciones de tratamiento	10 días
20	Evaluar opciones de tratamiento	8 días
21	Preparar planes de tratamiento	10 días
22	Implementar Plan de tratamiento	5 días
23	Monitorizar y Revisar	10 días

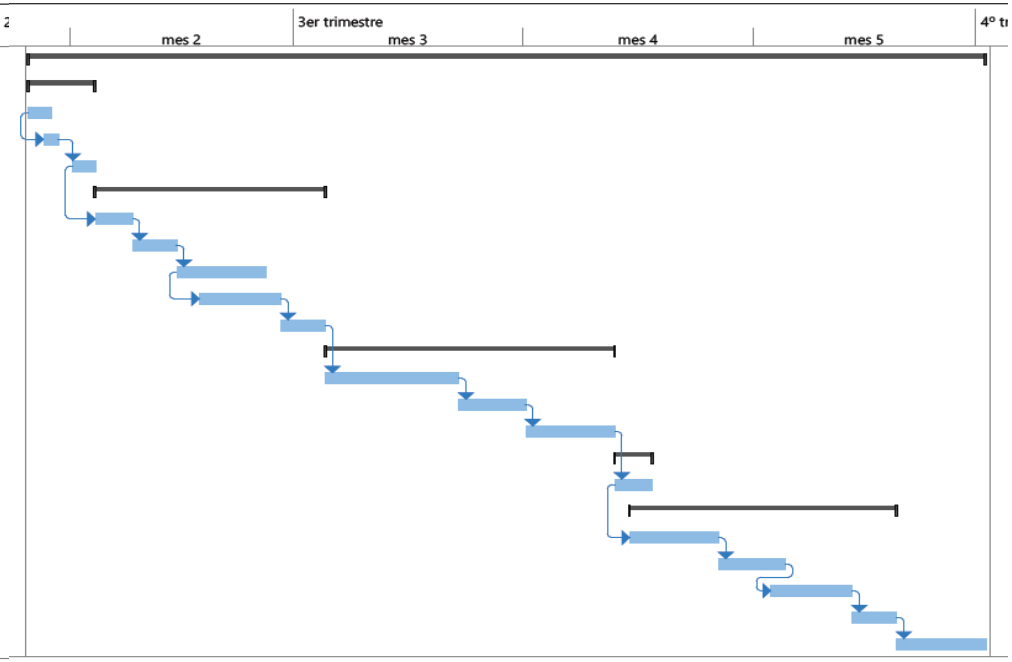


Figura 23 Planificación de la implementación del Plan de Gestión de Riesgos

Detalle de cada una de las fases con las que se ha realizado la planificación:

1. Establecer el marco general

1.1. Establecer el Contexto Estratégico

Aspectos financieros, operacionales, competitivos, políticos, imagen, sociales, clientes, culturales y legales, Stakeholders Organización, propietarios, personal, clientes, proveedores, comunidad local y sociedad.

1.2. Establecer el Contexto Organizacional

Objetivos del negocio:

Apoyados en COSO (de operaciones, de Información Financiera y de cumplimiento legal).

Otros: la rentabilidad, el crecimiento institucional, posicionamiento competitivo, imagen, servicio al cliente, productividad, calidad, recursos humanos, impacto en la comunidad.

1.3. Identificar Objetos Críticos

Definiendo los criterios Pérdida Financiera, Pérdida de Imagen, Incumplimiento de la misión, etc., que nos permitan elaborar una clasificación de las áreas, proyectos, procesos, sistemas o actividades sobre los cuales se llevará a cabo la administración de riesgos.

2. Establecer el marco general

2.1. Establecer un marco específico de administración de riesgos

Entender la actividad o parte de la organización para la cual se aplicará el proceso de administración de riesgos

2.2. Desarrollar criterios de evaluación de riesgos

Definir e identificar los criterios de análisis y el nivel de aceptación de los riesgos

2.3. Identificar la estructura

Separar la actividad o proyecto en un conjunto de elementos que facilite su comprensión y análisis

2.4. Identificar riesgos

Responder ¿qué puede ocurrir? Identificar los eventos que puedan afectar los elementos de la estructura identificada en el numeral 2.3.

2.5. Identificar causas

¿Cómo y por qué pueden ocurrir los eventos identificados como riesgos? Identificar lo que motiva, dispara o genera los eventos y los escenarios más significativos.

3. Análisis de Riesgos

3.1. Valorar el riesgo inherente Asignar valor al evento de materialización del riesgo propio del objeto de análisis.

3.2. Determinar Controles Existentes Identificar las actividades o mecanismos de control implementados para mitigar los riesgos inherentes.

3.3. Identificar Nivel de Exposición Resultante de aplicar la fórmula: Nivel de Exposición = Riesgo inherente Controles.

4. Evaluar y Priorizar Riesgos

4.1. Comparar contra Criterios y Definir prioridades de riesgo Comparar el resultado del análisis de riesgo realizado contra los criterios establecidos en el numeral 1. Marco general de referencia. Las comparaciones de análisis de riesgo realizadas sobre diferentes áreas de la organización o sobre los diferentes procesos le permitirán priorizar los riesgos sobre los cuales ha de centrar la atención para definir una opción de tratamiento.

5. Tratamiento del Riesgo

5.1. Identificar opciones de tratamiento Para la actividad o componente al cual aplicó el proceso de administración de riesgos, determine las posibles formas de reducir o mitigar el riesgo.

5.2. Evaluar opciones de tratamiento Bajo las consideraciones del marco de referencia definido, establecer cuáles de las opciones de tratamiento identificadas se ajustan a la organización y reducen el riesgo a un nivel de exposición aceptable.

5.3. Preparar planes de tratamiento Elaborar los planes que le permitan poner en práctica las opciones de tratamiento del riesgo seleccionadas.

5.4. Implementar Plan de tratamiento Poner en marcha el plan definido.

CAPÍTULO VII: CONCLUSIONES

En el presente proyecto de Tesis fueron descritos los conceptos e importancia de los términos relacionados con la gestión del riesgo presentes en la seguridad de la información que es administrada mediante los diversos equipos, servicios y personal del área de Tecnologías de la Información; además de conocer los estándares, metodologías y herramientas que posibilitan el desarrollo del análisis de riesgo en una organización.

Entre los lineamientos de futuros trabajos a desarrollarse se debería considerar desarrollar un análisis de riesgos de tipo cuantitativo considerando varios aspectos, como son: las consecuencias económicas de la materialización de una amenaza en cada activo, el costo del despliegue y mantenimiento de las salvaguardas; y estimar la probabilidad de ocurrencia de amenazas basándose en registros reales. También considerar los períodos de tiempo de recuperación de los procesos antes que las pérdidas se conviertan en irreparables y un análisis de aplicaciones críticas para definir prioridades de procesos, los puntos que se deben de tomar en cuenta para la elección del plan de Gestión de Riesgos para la Caja de Ahorro y Crédito Sipán S.A se detallan a continuación.

1. Con el logro de implementar un plan de gestión de riesgos de Tecnologías de la Información, que identifica, evalúa y trata nítidamente los activos de Tecnologías de la Información, sus amenazas, debilidades y niveles de riesgo relacionadas con las categorías: disponibilidad, integridad y confidencialidad de la información, que exige la SBS para este tipo de organizaciones en sus planes de seguridad (Circular G-139-2009 –SBS (Gestión de la continuidad del negocio), Circular G-140-2009 –SBS (Gestión de la seguridad de la información) y Resolución S.B.S.N° 2116 -2009). Esto ha permitido lograr establecer pautas para evaluar la magnitud de los riesgos de modo coherente y contar con indicadores clave para monitorizar periódicamente la eficacia de las actividades de gestión evaluación de brechas de efectividad de los controles de seguridad de la información.

2. Con la correcta identificación de los procesos críticos de la Caja de ahorro y crédito Sipán S.A, que ha partido principalmente de los dueños de los procesos, con su correspondiente priorización, se ha logrado identificar la infraestructura de Tecnologías de la Información más crítica y aplicar las estrategias para su recuperación y continuidad, lo que ha conllevado a disminuir el número de caídas o problemas.

3. El producto tangible de la metodología de gestión de riesgos es la matriz de riesgos y a través de ella se ha logrado disponer de un registro permanentemente y actualizado de los principales activos de Tecnologías de la Información a proteger, de modo que se garantice la continuidad operativa vía los planes mitigación, de los riesgos inmersos en cada activo. Esto ha permitido una adecuada sinergia con los procedimientos de continuidad del negocio.
4. Se comprueba que los resultados obtenidos de la valoración cualitativa de los niveles de riesgo de Tecnologías de la Información, en el software comercial PILAR y en el desarrollo del caso de estudio con el PGR-TI propuesto son similares. Este es un indicador de que el PGR-TI propuesto funciona.

   Las diferencias que podemos encontrar entre el sistema comercial y el PGR-TI son:

   - las escalas de valoración. Esto no es una deficiencia del plan propuesto, puesto que cada organización crea sus propias escalas de valoración de acuerdo a su contexto tecnológico, procesos y políticas de seguridad.

   - El software comercial no considera vulnerabilidades. En el PGR-TI si se considera la identificación de vulnerabilidades. Esto se debe a que este elemento de la Gestión de Riesgos es una característica propia de la organización y no se puede generalizar, por tanto, es difícil que sea evaluado en un software comercial.

5. Hoy en día las organizaciones son conscientes de la necesidad de identificar los riesgos asociados a Tecnologías de la Información, pero también es un hecho que al tener esta preocupación y no aplicar una metodología adecuada para cada negocio, es decir; entendiendo su cultura organizacional, sus procesos, sus operaciones críticas, es imposible lograr que estas metodologías alcancen el propósito de minimizar los riesgos.

   Es por esta razón que además de conocer estándares, normas y regulaciones, es recomendable llevar a cabo una metodología de análisis y evaluación de riesgos que identifique claramente las directrices estratégicas para mitigar, aceptar, reducir o transferir dichos riesgos.

6. Se ha logrado establecer un nivel de conocimiento, concientización y cultura en el personal de la Caja de Ahorro y Crédito Sipán S.A orientado hacia el control y la

seguridad de la información, que se expresa en la disminución de incidencias relacionados con las caídas de las TI que dan soporte a los principales procesos: créditos y captaciones, con la definición de políticas de seguridad de la información, en procedimientos, reglamentos y controles.

CAPÍTULO VIII: RECOMENDACIONES

1. Es conveniente que la oficialía de la seguridad de la información designe responsabilidades que permitan, mediante la automatización de la propuesta metodológica, alimentar permanentemente de la información necesaria por los verdaderos dueños de los procesos: lista de procesos/servicios críticos, activos, riesgos, amenazas, vulnerabilidades, controles, etc., de tal forma que permita obtener rápidamente la información del nivel de criticidad de sus procesos, porcentaje de desviación de riesgo de los activos o procesos, capital necesario a invertir en la protección de un activo o proceso, entre otra información relevante.

2. Dado que la evaluación de los riesgos es permanente se recomienda que el plan de matriz de riesgos que se propone sea implementado en una aplicación informática, que permita actualizaciones más dinámicas, con posibilidades de generar indicadores/resultados gráficos y generación de escenarios.

3. Para lograr mejores resultados en la gestión de riesgos de Tecnologías de la Información y en la continuidad de procesos, la financiera deberá de tener en cuenta factores estratégicos como: el apoyo y compromiso de la Dirección, difusión y sensibilización permanente sobre control y seguridad de la información, orientación hacia la formalización de procesos y actividades, una permanente verificación y pruebas de control que garanticen la disponibilidad, integridad y confidencialidad de información y finalmente un adecuado plan de despliegue de la cultura de riesgos que garantice la participación general de los empleados.

CAPÍTULO IX: REFERENCIAS BIBLIOGRÁFICAS

Borghello, C. F. (2001). *Seguridad informática sus Implicancias e Implementación.* (Tesis) Universidad Tecnológica Nacional, Buenos Aires - Argentina

Carreño, H. C. P. (2012) Diseño del Plan de Gestión de Riesgos en los Proyectos de Consultoría de estudios técnicos y diagnóstico del estado mecánico y de corrosión de tuberías, tanques, y vasijas (Tesis) - Universidad para la Cooperación Internacional, Costa Rica

Aldegani, G. M. (1997). Seguridad Informática. Buenos Aires, Argentina: MP Ediciones.

Medina M. A (2007). Seguridad Informática. (Tesis). Universidad Nacional de San Marcos, Facultad de Economía.

Asociación de Auditoría y Control de Sistemas de Información (ISACA). 2005. Manual de Preparación al examen CISA, 2005. Madrid - España: ISACA, 15° Edición.

Asociación Española de Empresas de Tecnologías de la Información (SEDISI). 2005. Seguridad Informática. Madrid - España: s/E, Guía de Seguridad Informática.

Chiavenato, A. (1981). Introducción a la Teoría General de la Administración. Brasil: Editorial McGraw Hill.

CobIT. 2000. Governance, Control and Audit. for information and Related Technology. s/l: CobIT 3era edición, MetodologíaCobIT.

Consejo de Auditoría Interna General de Gobierno. (1999). Auditoría Interna de Gobierno, La experiencia chilena 1994/1999. Santiago de Chile: Editorial Antártica Quebecor. Primera Edición.

COSO. (1996). Informe COSO. Washington: s/E, Internal Control Integrated Framework.

Costas Santos, J. (2011). Seguridad informática. Bogotá, Colombia: Ra-ma editorial.

Casto Pablo (Setiembre 2014), Metodología Magerit. En línea: http://gr2dest.org/metodologia-de-analisis-de-riesgosmagerit/

Echenique, J. A. (1996). Auditoria en informática. México: Editorial Prentice. Hall Hispanoamericana.

Freemon, E. Kast y Rosenweig, James E. (1985). Administración en las Organizaciones. Enfoque de Sistemas y de Contingencias. México: Editorial McGraw Hill. Cuarta Edición.

ONGEI. 2004. Norma Técnica Peruana. ISO/IEC 17799. Lima - Perú: ONGEI,1° Edición, Norma Técnica.

Peña, Gloria y Peña, Lillo. (2005). Gestión de Riesgo Tecnológico. Módulo 6.México: s/E, Mejores Prácticas y Estándares Internacionales en Gestión de Riesgos y Control Interno

Superintendencia de banca y seguro. (2002). Criterios mínimos para la identificación y administración de los riesgos asociados a la tecnología de información. Lima, Perú: SBS, Circular N° G-105-2002.

Superintendencia de banca y seguro. (2002). Reglamento para la administración de riesgos de operación. Lima, Perú: SBS, Resolución N° 006-2002.

Varios Autores. (1992). Gran Diccionario del Saber Humano. México: Editorial Selecciones del Reader'sDigest

Flores, F. (2010). *Análisis y Gestión de Riesgo,* Recuperado de

https://fabricioflores.wordpress.com/2010/12/29/analisis-y-gestion-de-riesgo/.

Serra, C. (2011). Presentación de ISACA 2011, Recuperado de

http://www.isaca.org/chapters8/Montevideo/cigras/Documents/cigras2011-cserra-presentacion1%20modo%20de%20compatibilidad.pdf, Uruguay

MAGERIT. (2012). MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: Ministerio de Hacienda y Administraciones Públicas.

Villena Aguilar, M. A. (2006). Planeamiento de un esuema de gestión de seguridad de información que puede ser empleado por una institución financiera en el Perú. *Tesis*. Lima, Perú: Pontificia Universidad Católica del Perú - PUCP.

CAPÍTULO X: ANEXOS

ANEXO N° 01

TABLAS DE FACTORES Y VARIABLES DE EVALUACIÓN DEL PLAN

PROPUESTO

Tabla Factores y variables para probar la efectividad del diseño del plan propuesto

Variable	Factor Relevante (indicador)	SI/NO	Peso (Madurez)
Perspectiva: Seguridad de la Información			
Políticas de seguridad de la información	Se declara con claridad la política		
	Se han definido los objetivos deseados de la política		
	Se establece los procedimientos de implementación de la política		
	Están definidos los roles y responsabilidades de acuerdo al MOF de la Caja		
	Se establece las sanciones de su incumplimiento		
Gobierno de la seguridad de la información	Considera las exigencias de la normatividad de la SBS: Circular N° G-105-2002 y Resolución SBS N° 2116 -2009.		
	Se integra al Plan de Seguridad de la Información y de TI de la Caja.		
	Se puede identificar las excepciones potenciales a las políticas de seguridad de información.		
Perspectiva: Gestión de riesgos de TI			
Estructuración del plan de análisis y tratamiento de riesgos	Se ha definido nítidamente como disponibilidad, integridad y confidencialidad en las que se pueden agrupar los riesgos de TI. La gestión de riesgos de TI se integra en la gestión de riesgos general para todos los riesgos a nivel corporativo.		
	Su estructura está diseñada para que los empleados relacionados con la gestión de la seguridad de TI y de riesgos puedan entenderlo y alcanzar el grado de cultura y concientización deseado		
Gobierno de los riesgos de TI	Contempla todas las variables necesarias exigidas por la SBS para su evaluación		
	Se ha establecido pautas para evaluar la magnitud de los riesgos de modo coherente		

	Se cuenta con indicadores clave para monitorizar periódicamente la eficacia de la gestión de riesgos de TI		
Perspectiva: Continuidad de procesos			
Actividades básicas de continuidad de procesos.	Identifica los procesos críticos de La Caja a través de un BIA		
	Determina el RTO y RPO de cada proceso crítico		

Fuente: Elaboración propia

Tabla: Factores y variables para probar la efectividad de la operación del plan propuesto.

Variable	Factor Relevante (indicador)	SI/NO	Peso (Madurez)
Perspectiva: Seguridad de la Información			
Políticas de seguridad de la información.	A partir de las políticas de seguridad de la información definidas se puede normar y procedimentar los procesos de TI relacionados con la seguridad de TI, gestión de riesgos de TI y continuidad de procesos.		
	A partir de las políticas de seguridad de la información definidas se pueden definir objetivos de control y controles relacionados con la seguridad de TI, gestión de riesgos de TI y continuidad de procesos		
	A partir de las políticas de seguridad de la información definidas se pueden definir indicadores clave para monitorizar periódicamente las actividades de gestión de seguridad de TI, gestión de riesgos de TI y continuidad de procesos.		
Análisis y tratamiento de riesgos	A partir del plan propuesto se puede establecer un proceso formal y coherente para evaluar periódicamente los potenciales riesgos de TI		
	Se puede determinar con efectividad los niveles de riesgos inherentes de TI.		
	Se puede evaluar la efectividad de los controles y hacer seguimiento de las brechas de seguridad.		
Gobierno de los riesgos de TI	La información resultante del plan es significativa para cumplir con los informes exigidos por la SBS en relación a la gestión de riesgos de TI.		
	La información resultante del plan sirve para tomar decisiones con efectividad en relación a las inversiones e importancia de los controles de seguridad		
Perspectiva: Continuidad de procesos			
	La información resultante del plan es significativa para cumplir con los informes exigidos por la SBS en relación a la continuidad de procesos.		
	A partir del plan propuesto se puede establecer planes de contingencia y planes de mantenimiento de los activos de TI críticos.		

ANEXO N° 02

RESULTADOS DEL ANÁLISIS DE RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMATICA

En el siguiente formato contiene el resumen del análisis y evaluación de los posibles riesgos relacionados con Tecnología de la Información que afectan directamente los activos tecnológicos de La Caja.

I. SERVIDORES Y CONCENTRADORES CENTRALES

Activo	Factor de Riesgo	Se protege?	¿Cómo? / Por qué?
Servidores y concentradores centrales y de borde	Acceso no autorizado	Si	Central (equipos centrales) El acceso a los recursos críticos en los gabinetes de piso o de pared (servidores, switch, router, modem, ups, transformadores de aislamiento) del cuarto de comunicaciones en la agencia principal está protegido con un sistema de puertas con llave y tabiquería a los que sólo tiene acceso el personal autorizado.
		Parcialmente	En agencias (equipos de borde) Los gabinetes de comunicación están o disponibles a ser abiertos o ubicados en un ambiente no apropiado, como almacén de productos de limpieza o compartiendo ambientes con la ventanilla de atención a clientes
	Corte de luz, Sistema ininterrumpido de energía (UPS) descargado o variaciones de voltaje	Si	Se cuenta con un sistema de red múltiple de alimentación de energía que evita el fallo de suministro. Así mismo, se cuenta con un sistema de alimentación ininterrumpido de energía para caso extremos de suministro de energía. Este sistema mantiene en forma autónoma, de ser el caso, durante 20 minutos aprox. funcionando los equipos centrales y los terminales del área de tecnologías de información.
	Destrucción o fallo de un componente crítico del equipo	Se recomienda mejorar.	La seguridad para la entrada y salida de paquetes a Internet de todas las agencias está basada en un

	(microprocesador, memoria, fuente de poder, otros)		servidor ISA Server 2004 sin tolerancia a fallos por riesgos en fuente de poder, discos duros y procesador. No existen equipos de comunicación que toleren fallos este es el caso del switch core (aquí se conectan los servidores) ubicado en la oficina principal, y los switches ubicados en cada una de las agencias. Lo cual paralizaría las operaciones en todas las agencias en caso de avería.
	Errores de configuración	Se recomienda mejorar.	Se cuenta con servidor de respaldo donde se replica toda la configuración necesaria para reiniciar el sistema. El servidor activo tiene implementado políticas de acceso a ser mejoradas, y no se cuenta con redundancia para este equipo altamente importante
	Factores ambientales no adecuados. (ventilación, protección contra incendios, acondicionamiento de racks, otros)	Debilidad en agencias	Se cuenta con sistema de aire acondicionado con BTU/h adecuado en el cuarto de comunicaciones de la oficina principal y en cada una de las agencias con excepción de la agencia ubicada en la ciudad de Moshoqueque y Trujillo en este último esto es reemplazado por un ventilador. El área del servicio informático de La Caja está ubicada en una zona con perímetro de acceso restringido a personal no autorizado claramente definido, con controles de acceso a través de puertas, extintores contra incendios, alarmas de seguridad y vigilancia permanente.
	Límite de vida útil –Máquinas obsoletas (antigüedad del equipo, repotencionamiento de componentes)	Si	Se tiene pendiente un pedido para adquirir nuevos equipos centrales.
	Mal mantenimiento	Si	Hay un plan de mantenimiento de equipos.
	Robo	Si	Los equipos de cómputo están asegurados.
	Afectación por virus	Si	Protegidos con antivirus

II. BASE DE DATOS

Activo	Factor de Riesgo	Se protege?	¿Cómo? / Por qué?
Base de Datos	Copia no autorizada de uso a un medio de datos externos.	Si	Se generan backup diarios y son almacenados en DVD en bóveda, manejados y transportados por personal autorizado.
	Errores de software (motor y contenedor de base de datos).	Si	Se cuenta con servidor de respaldo donde se replica toda la configuración necesaria para reiniciar el sistema. El servidor activo tiene implementado políticas de acceso a ser mejoradas, y no se cuenta con redundancia para este equipo altamente importante.
	Falta de espacio de almacenamiento	Se recomienda mejorar.	Se estima que en un tiempo próximo la arquitectura de datos con la que actualmente se trabaja no va a ser funcional y bajará su performance de respuesta, debido a: (1) la capacidad instalada del servidor de base de datos será insuficiente, necesitándose más potencia y rendimiento y (2) al modelo de arquitectura de datos que se utiliza.
	Pérdida o falla de backups.	Si	Se genera backup diarios de la base datos completa.
	Pérdida de confidencialidad en datos privados y de sistema.	Si	El acceso a la base de datos está controlado a través de perfiles de usuario con niveles de acceso autorizados, según el área y responsabilidad.
	Directorios compartidos.	Si	Directorio de la base de datos solo esta compartido para usuarios autorizados.
	Sabotaje	Si	El área del servicio informático de La Caja está ubicada en una zona con perímetro de acceso restringido a personal no autorizado claramente definido.
	Afectación de virus	Si	Servidor de base de datos protegido con antivirus.

III. SOFTWARE BACKOFFICE Y SISTEMAS OPERATIVOS

Activo	Factor de Riesgo	Se protege?	¿Cómo? / Por qué?
Software de BackOffice y sistemas operativos instalados en servidores y terminales.	Aplicaciones sin licencias.	Si	Software licenciado
	Error de configuración	Si	Software licenciado, con evaluación y pruebas.
	Mala Administración de control de accesos.	Si	Se controla el acceso a las estaciones mediante política de acceso: niveles de acceso por perfiles de usuario.
	Pérdida de datos	Si	Mensualmente se generan backups.
	Afectación de virus	Si	Protegidos con antivirus

IV. BACKUP (SISTEMA DE RESPALDO)

Activo	Factor de Riesgo	Se protege?	¿Cómo? / Por qué?
	Copia no autorizada del backup.	Si	Solo personal autorizado tiene acceso a generar, copiar y trasladar backup de información.
	Errores de software para recuperación de información de backup (restore).	Si	Su procedimiento de restore es copiando la última base de datos backup. Se instala, de ser necesario, toda la configuración mínima en los servidores.
	Falla o deterioro del medio de almacenamiento externo del backup.	Si	Los backup son almacenados en dispositivos magnéticos (DVD), almacenados en bóveda.
	Falta de espacio de almacenamiento.	Si	Backup tamaño 8 Gb 1.5 Gb en zip.
	Mala integridad de los datos resguardados al recuperar la información de un backup.	Si	Los backups son revisados después de su grabación en los medios magnéticos.
	Medios de datos no están disponibles cuando son necesarios.	Si	Se generan dos copias de la base de datos una se guarda en bóveda de Agencia Moshoqueque y otro en nuestras oficinas.
	Pérdida o robo de backups.	Si	Solo personal autorizado tiene acceso a los backups.
	Sabotaje	Si	Solo personal autorizado tiene acceso a los backups.

V. CABLEADO Y CONCENTRADORES

Activo	Factor de Riesgo	Se protege?	¿Cómo? / Por qué?
Cableado y concentradores	Conexión de cables inadmisible (modificación de conexiones y mal etiquetado).	Mejorar	Las malas condiciones del cableado para las redes informáticas, la ausencia de documentación de las pruebas de cableado y de los planos de distribución de cableado en agencias como Moshoqueque, Jaen, Chepen, Trujillo y en la agencia principal tienen un impacto significativo en las conexiones ya sea a internet como a base de datos
	Daño o destrucción, de cables o equipamiento, inadvertido (mala ubicación, por limpieza, impedimento de libre tránsito, otros).	Si	El sistema de cableado de energía y cableado de la red de datos es empotrado en la pared y en el caso de extensiones, los cables están protegidos por canaletas. Se cumple con los requerimientos mínimos de las normas para cableado estructurado.
		Mejorar	En agencia de Moshoqueque el gabinete está abierto y sin un ambiente apropiado. En Chepen el ambiente es utilizado como almacén de productos de limpieza teniendo la llave puesta para el personal de limpieza y en Trujillo el gabinete comparte ambiente con la ventanilla de atención a clientes.
	Factores ambientales	Mejorar	Se cuenta con sistema de aire acondicionado con BTU/h adecuado en el cuarto de comunicaciones de la oficina principal y en cada una de las agencias con excepción de la agencia ubicada en la ciudad de Moshoqueque y Trujillo en este último esto es reemplazado por un ventilador
	Accesos no autorizados.	Mejorar	Es posible conectar equipos portátiles en puntos de acceso a la red de datos sin que se genere un registro. Esto hace posible que intrusos puedan escanear y vulnerar a la red de datos de las agencias.
	Longitud de los cables de red excedidos a las normas	Si	Longitud de cables cumple con las normas establecidas.

VI. RED

Activo	Factor de Riesgo	Se protege?	¿Cómo? / Por qué?
Red	Mantenimiento no adecuado de puertos. (restricciones de acceso a ciertos puertos, perfiles de acceso)	Mejorar	Es posibles conectar equipos portátiles en puntos de acceso a la red de datos sin que se genere un registro. Esto hace posible que intrusos puedan escanear y vulnerar a la red de datos de las agencias.
	Configuración inadecuada de componentes de red.	Si	Usuarios no pueden acceder a las configuraciones de red –acceso restringido.
	Errores de operación (mala estandarización de velocidades de transmisión y ancho de banda, otros).	Mejorar	El ancho de banda asimétrico contratado a Telefónica resulta ser insuficiente para las 40 conexiones concurrentes a la base de datos que realizan en determinado momento las maquinas estaciones de trabajo en las diferentes agencias. Las pruebas demostraron que con 3 conexiones concurrentes prácticamente se satura el ancho de banda.
	Mal uso de servicios de red (mal uso del netmeeting, transmisión de datos, otros)	Mejorar	Es posible enviar paquetes ICMP desde un equipo portátil conectado a un punto de acceso a la red de datos a los servidores existente en la oficina principal. Las políticas para el acceso a Internet en las agencias ya sea por dominios como gob.pe, edu.pe y listas de dominios de confianza se comprobó de que se podía ingresar a dominios que generar tráfico de paquetes innecesarios y al utilizar la misma conexión para el acceso a base de datos, esto afecta a la performance de la red IP/VPN. No está desinstalado el neetmeeting

VII. USUARIOS

Activo	Factor de Riesgo	Se protege?	¿Cómo? / Por qué?
Usuarios	Acceso no autorizado a datos.	Si	Cada usuario tiene un perfil y opciones asignadas para el acceso al sistema (Reporte de Perfiles – Opciones del Sistema Informático y Usuarios)
	Borrado, modificación o revelación de claves de acceso a la información y aplicaciones, desautorizada o inadvertida	Mejorar	Cada usuario cuenta con una clave personal, pero se comprobó que no existe una política adecuada para las contraseñas de los usuarios, pudiendo los mismos utilizar claves como la siguiente: 888888
	Condiciones de trabajo adversas (ergonomía, ubicación de equipos, otros)	Si	Local adecuado e instalaciones en todas las oficinas.
	Destrucción negligente de datos por parte de los usuarios.	Si	Acceso a la base de datos protegido por password.
	Documentación deficiente (manual de usuario).	Si	Se cuenta con manuales de usuario del sistema actualizados en casi 100%.
	Entrada sin autorización a ambientes.	Si	Solo personal autorizado tiene acceso a los ambientes de sistemas.
	Entrenamiento de usuarios inadecuado.	Si	Se capacita en el manejo operativo del sistema informático, además hay inducción en cada área/unidad.
	Falta de controles y log de las transacciones realizadas por los usuarios.	Si	Se ha generado bitácoras para registrar las operaciones y transacciones realizadas por los usuarios.
	No cumplimiento con las medidas de seguridad del sistema.	Si	Cada usuario tiene un perfil y opciones asignadas para el acceso al sistema y cada usuario cuenta con una clave personal intransferible.
	Desvinculación del personal con la institución.	Mejorar	Se verifico que en algunas agencias como la de la ciudad de Jaén no se actualizan los usuarios encontrándose casos en que personal ingresaba desde el terminal a su cargo con otro usuario. Por lo tanto en esos casos no es posible identificar las ocurrencias realizadas por usuarios físicos.

VIII. DOCUMENTACIÓN DEL SISTEMA

Activo	Factor de Riesgo	Se protege?	¿Cómo? / Por qué?
Documentación de programas, hardware, procedimientos administrativos locales, manuales, etc.	Acceso no autorizado a datos de documentación.	Si	La documentación está en el Área de Tecnologías de Información sólo es accedida por personal autorizado.
	Borrado, modificación o revelación desautorizada de información.	Si	La documentación es manipulada solo por el personal responsable.
	Copia no autorizada de un medio de documentación del sistema	Si	Sólo se proporciona copias de la documentación a personas autorizadas.
	Descripción de archivos y programas inadecuado	Mejorar	Se registran cambios con los formatos que se han definido en el PEI y PSI.
	Documentación insuficiente o faltante, funciones no documentadas	Mejorar	Documentación del Sistema, Políticas de Desarrollo de aplicaciones en físico. Los manuales de usuario no están implementados en línea. Falta implementar algunos formatos que se han definido en el PEI y PSI.
	Factores ambientales (almacén de documentación)	Si	La documentación está almacenada en medios magnéticos en instalaciones adecuadas.
	Mantenimiento y actualización inadecuado o ausente de la documentación.	Si	Se actualiza la documentación cada vez que se hacen cambios en el sistema.

IX.SISTEMA CONTABLE Y FINANCIERO ("SIPAN")

Activo	Factor de Riesgo	Se protege?	¿Cómo? / Por qué?
SIIF y SIG	Modificaciones inoportunas y no documentadas	Si	Se lleva el control detallado del desarrollo y mantenimiento por cada analista programador
	Funcionalidad del sistema (no atiende todos los requerimientos de los usuarios y áreas)	Si	Se reciben y analizan todos los requerimientos, los cuales son atendidos de acuerdo a su factibilidad y estimación de tiempos. (Prioridad Entidades Supervisoras –Negocios - Operaciones).
	Acceso a los programas fuentes no controlado	Si	Sólo el personal de la Sección de Desarrollo y Mantenimiento tiene acceso al código fuente del sistema informático.
	Validación en los procesos de captura y registro de transacciones	Mejorar	Existen observaciones de la SBS y de otras auditorias que indican falta de validación en algunos procesos.
	Sabotaje (eliminación de programas)	Si	Se maneja políticas de seguridad para los usuarios implementado en cada terminal.

ANEXO N° 03

TABLA DE REFERENCIA PARA LA CATALOGACIÓN DE ACTIVOS DE TI

Tipo de activo		Sub clasificación.		Descripción de aclaración
[info]	información	[adm]	datos de interés para la administración pública	
		[dv]	datos vitales (registros de la organización)	Información esencial para la supervivencia de la Organización. Su carencia o daño afectaría directamente a la existencia de la Organización. Se pueden identificar: Aquellos que son imprescindibles para que la Organización supere una situación de emergencia Aquellos que permiten desempeñar o reconstruir las misiones críticas Aquellas de naturaleza legal o los derechos financieros de la Organización o sus usuarios.
		[per]	datos de carácter personal	Información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar.
		[clasificado]	Datos clasificados	Información sometida a normativa específica de control de acceso y distribución; es decir aquellos cuya confidencialidad es especialmente

				relevante. La tipificación de qué datos deben ser clasificados y cuáles son las normas para su tratamiento, vienen determinadas por regulaciones gubernamentales, sectoriales, por acuerdos entre organizaciones o por normativa interna.
[dato]	Datos o documentos	[files]	ficheros	
		[backup]	copias de respaldo	
		[conf]	datos de configuración	Los datos de configuración son críticos para mantener la funcionalidad de las partes y del conjunto del sistema de información.
		[int]	datos de gestión interna.	Incluye la información referente a los niveles de acceso asignados a los distintos tipos de usuario según su función o puesto de trabajo
		[password]	credenciales	Claves de acceso a máquina asignada o a las aplicaciones
		[auth]	datos de validación de credenciales	Códigos de identificación de usuario
		[acl]	datos de control de acceso	
		[log]	registro de actividad	Los registros de actividad sustancian los requisitos de trazabilidad. Bitácoras o log.
		[source]	código fuente	
		[exe]	Código ejecutable	
		[test]	datos de prueba	Generados en las pruebas de las aplicaciones o módulos antes de puesta en producción
[keys]	Claves	[info]	protección de la	Claves públicas o privadas de

			información	cifrado o descifrado de la información
		[com]	protección de las comunicaciones	Claves de cifrado del canal de comunicación, claves de autenticación
		[disk]	cifrado de soportes de información.	Cifrado de soportes de información.
		[www]	acceso a Internet	
		[telnet]	acceso remoto a cuenta local.	
		[email]	Correo electrónico	Servidor de correo electrónico
		[file]	Almacenamiento de ficheros.	Servidor de datos
		[www]	transferencia de ficheros.	
		[edi]	Intercambio electrónico de datos	
		[dir]	servicio de directorio	Directorio activo. Localización de personas, permitiendo la identificación y facilitando los atributos que caracterizan al elemento determinado
		[idm]	gestión de identidades	Servicios que permiten altas y bajas de usuarios de los sistemas, incluyendo su caracterización y activando los servicios de aprovisionamiento asociados a sus cambios de estado respecto de la organización
		[ipm]	Gestión de Privilegios	Aplicación para definir niveles de acceso.
[sw]	Aplicaciones	[prp]	Desarrollo propio (in house)	
		[sub]	Desarrollo a	

			medida (subcontratado)	
		[browser]	navegador web	
		[app]	Servidor de aplicaciones.	
		[email_client]	Cliente de correo electrónico.	
		[email_server]	Servidor de correo electrónico	
		[file]	Servidor de ficheros	
		[dbms]	Sistema de gestión de bases de datos	
		[office]	Ofimática	
		[av]	Anti virus	
		[os]	Sistema operativo	
		[mv]	Gestor de máquinas virtuales.	
		[backup]	Sistema de backup.	
[hw]	Equipos informáticos	[host]	Grandes equipos	Se caracterizan por haber pocos, frecuentemente uno sólo, ser económicamente altos y requerir un entorno específico para su operación. Son difícilmente reemplazables en caso de destrucción
		[mid]	Equipos medios	Se caracterizan por haber varios, tener un coste económico medio tanto de adquisición como de mantenimiento e imponer requerimientos estándar como entorno de operación. No es difícil reemplazarlos en caso

				de destrucción
		[pc]	Informática personal	Se caracterizan por ser multitud, tener un coste económico relativamente pequeño e imponer solamente unos requerimientos mínimos como entorno de operación. Son fácilmente reemplazables en caso de destrucción
		[mobile]	Informática móvil	Se caracterizan por ser equipos afectos a la clasificación como informática personal que, además, son fácilmente transportables de un sitio a otro, pudiendo estar tanto dentro del recinto propio de la organización como en cualquier otro lugar
		[pda]	Agendas electrónicas	
		[vhost]	Equipo virtual	
		[backup]	Equipamiento de respaldo	Son aquellos equipos preparados para hacerse cargo inmediato de los equipos en producción.
		[perife]	Periféricos	Impresoras y servidores de impresión, escáneres
		[bp]	Dispositivo de frontera	Son los equipos que se instalan entre dos zonas de confianza.
		[network]	Soporte de la red	Dícese de equipamiento necesario para transmitir datos: routers, módems, etc. Modems, conmutadores, routers, bridges, firewalls, wap (punto de acceso inalámbrico)
		[pabx]	Centralita telefónica.	
		[ipphone]	Teléfono IP	
[com]	Comunicaciones	[PSTN]	Red telefónica	
		[ISDN]	RDSI (red	

			digital)	
		[X25]	X25 (red de datos)	
		[ADSL]	ADSL	
		[radio]	Comunicaciones radio.	
		[wifi]	Red inalámbrica	
		[mobile]	Telefonía móvil	
		[sat]	Por satélite	
		[LAN]	Red local	
		[MAN]	Red metropolitana	
		[Internet]	Internet	
[media]	Soporte de información	[electro]	Electrónicos	Dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo: discos, DVD, cintas, etc.
		[noelectro]	No electrónicos	Material impreso
[aux]	Equipamiento auxiliar.	[power]	Fuentes de alimentación	
		[ups]	Sistemas de alimentación ininterrumpida	
		[gen]	Generadores eléctricos	
		[ac]	Equipos de climatización	
		[cabling_wire]	Cable eléctrico	
		[cabling_utp]	Cable de datos	
		[fiber]	Fibra óptica	
		[supply]	Suministros esenciales	
		[furniture]	Mobiliario: Armario, etc.	
		[safe]	Cajas fuertes	
[Inmueb]	Instalaciones	[building]	Edificio	
		[data]	Cuarto de	

			procesamiento de datos	
		[backup]	Instalaciones de respaldo	
[pers]	Personal	[ue]	Usuarios externos	
		[ui]	Usuarios internos	
		[op]	Operadores	
		[adm]	Administradores de sistemas	
		[com]	Administradores de comunicaciones	
		[dba]	Administradores de BBDD	
		[sec]	Administradores de Seguridad	
		[des]	Desarrolladores/ Programadores	
		[sub]	Subcontratas	
		[prov]	Proveedores	

ANEXO N° 04

TABLAS DE REFERENCIA PARA LA VALORACIÓN DE LA CRITICIDAD DE LOS ACTIVOS DE TI

Para la valoración de los activos se tomarán en cuenta las siguientes dimensiones de seguridad:

Tabla de descripción de las dimensiones de seguridad de la información que se tomarán en cuenta en la valoración de la criticidad de los activos de TI

[pi] Información de carácter personal	
10	Probablemente afecte gravemente a un grupo de individuos y probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.
9	Probablemente afecte gravemente a un individuo y probablemente quebrante seriamente leyes o regulaciones
7-8	Probablemente afecte a un grupo de individuos y probablemente quebrante leyes o Regulaciones.
5-6	Probablemente afecte a un individuo y probablemente suponga el incumplimiento de una ley o regulación.
3-4	Pudiera causar molestias a un individuo y pudiera quebrantar de forma leve leyes o regulaciones.
1-2	Pudiera causar molestias a un individuo
[lpo] Obligaciones legales	
9-10	Probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7-8	Probablemente cause un incumplimiento grave de una ley o regulación
5-6	Probablemente sea causa de incumplimiento de una ley o regulación
3-4	Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1-2	Pudiera causar el incumplimiento leve o técnico de una ley o regulación
[si] Seguridad	
9-10	Probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios.
7-8	Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios.
5-6	Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
3-4	Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente.
1-2	Pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

[cei] Intereses comerciales económicos	
9-10	De enorme interés para la competencia de muy elevado valor comercial causa de pérdidas económicas excepcionalmente elevadas causa de muy significativas ganancias o ventajas para individuos u organizaciones constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros.
7-8	De alto interés para la competencia de elevado valor comercial causa de graves pérdidas económicas proporciona ganancias o ventajas desmedidas a individuos u organizaciones constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros.
5-6	De cierto interés para la competencia de cierto valor comercial causa de pérdidas financieras o merma de ingresos facilita ventajas desproporcionadas a individuos u organizaciones constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros.
3-4	De bajo interés para la competencia De bajo valor comercial
1-2	De pequeño interés para la competencia De pequeño valor comercial Supondría pérdidas económicas mínimas
[da] de interrupción del servicio	
9-10	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones probablemente tenga un serio impacto en otras organizaciones.
7-8	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones Probablemente tenga un gran impacto en otras organizaciones
5-6	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones Probablemente cause un cierto impacto en otras organizaciones.
3-4	Probablemente cause la interrupción de actividades propias de la Organización.
1-2	Pudiera causar la interrupción de actividades propias de la Organización.
[po] de orden público	
9-10	Alteración seria del orden público
7-8	Probablemente cause manifestaciones, o presiones significativas
3-6	Causa de protestas puntuales
1-2	Pudiera causar protestas puntuales
[op] operaciones	
10	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística.

7-8	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5-6	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local.
3-4	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local).
1-2	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local).
[adm] administración y gestión	
9-10	Probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7-8	Probablemente impediría la operación efectiva de la Organización
5-6	Probablemente impediría la operación efectiva de más de una parte de la Organización
3-4	Probablemente impediría la operación efectiva de una parte de la Organización
1-2	Pudiera impedir la operación efectiva de una parte de la Organización
[pc] pérdida de confianza (reputación)	
10	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
9	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
8	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
7	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
6	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
5	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
4	Probablemente afecte negativamente a las relaciones internas de la Organización
3	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1-2	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	No supondría daño a la reputación o buena imagen de las personas u organizaciones
[pd] persecución de delitos	
6-10	Impida la investigación de delitos graves o facilite su comisión
1-5	Dificulte la investigación o facilite la comisión de delitos
[trs] tiempo de recuperación del servicio	
9-10	RTO < 4 horas
7-8	4 horas < RTO < 1 día
4-6	1 día < RTO < 5 días
1-3	5 días < RTO

ANEXO N° 05

CATÁLOGO DE AMENAZAS POR ACTIVO Y DIMENSIÓN DE SEGURIDAD DE LA INFORMACIÓN SEGÚN MAGERIT

[N]	Desastres naturales			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[N.1]	Fuego	Incendios: posibilidad de que el fuego acabe con recursos del sistema.	[D] disponibilidad	– [HW] equipos informáticos (hardware) – [Media] soportes de información – [AUX] equipamiento auxiliar – [L] instalaciones
[N.2]	Daños por agua	Inundaciones: posibilidad de que el agua acabe con recursos del sistema	[D] disponibilidad	– [HW] equipos informáticos (hardware) – [Media] soportes de información – [AUX] equipamiento auxiliar – [L] instalaciones
[N.*]	Desastres naturales	Incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc. Se excluyen desastres específicos tales como incendios Se excluye al personal por cuanto se ha previsto una amenaza específica [E.31] para cubrir la Indisponibilidad	[D] disponibilidad	– [HW] equipos informáticos (hardware) – [Media] soportes de información – [AUX] equipamiento auxiliar – [L] instalaciones

		involuntaria del personal sin entrar en sus causas.		
[I]	**De origen industrial**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[I.1]	Fuego	Incendio: posibilidad de que el fuego acabe con los recursos del sistema.	[D] disponibilidad	– [HW] equipos informáticos (hardware) – [Media] soportes de información – [AUX] equipamiento auxiliar – [L] instalaciones
[I.2]	Daños por agua	Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	[D] disponibilidad	– [HW] equipos informáticos (hardware) – [Media] soportes de información – [AUX] equipamiento auxiliar – [L] instalaciones
[I.*]	Desastres industriales.	Desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico, etc. Se excluyen amenazas específicas como incendio por cuanto se ha previsto amenazas específicas. Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.31], para cubrir la indisponibilidad	[D] disponibilidad	– [HW] equipos informáticos (hardware) – [Media] soportes de información – [AUX] equipamiento auxiliar – [L] instalaciones

		involuntaria del personal sin entrar en sus causas.		
[I.3]	Contaminación mecánica.	Vibraciones, polvo, suciedad, etc.	[D] disponibilidad	– [HW] equipos informáticos (hardware) – [Media] soportes de información – [AUX] equipamiento auxiliar
[I.4]	Contaminación electromagnética.	Interferencias de radio, campos magnéticos, luz ultravioleta, etc.	[D] disponibilidad	– [HW] equipos informáticos (hardware) – [Media] soportes de información – [AUX] equipamiento auxiliar
[I.5]	Avería de origen físico o lógico.	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.	[D] disponibilidad	– [SW] aplicaciones (software) – [HW] equipos informáticos (hardware) – [Media] soportes de información – [AUX] equipamiento auxiliar
[I.6]	Corte del suministro eléctrico.	Cese de la alimentación de potencia	[D] disponibilidad	– [HW] equipos informáticos (hardware) – [Media] soportes de información – [AUX] equipamiento auxiliar

[I.7]	Condiciones inadecuadas de temperatura y/o humedad	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, etc.	[D] disponibilidad	– [HW] equipos informáticos (hardware) – [Media] soportes de información – [AUX] equipamiento auxiliar
[I.8]	Fallo de servicios de comunicaciones.	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.	[D] disponibilidad	– [COM] redes de comunicaciones
[I.9]	Interrupción de otros servicios y suministros esenciales.	Interrupción de otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante, etc.	[D] disponibilidad	– [AUX] equipamiento auxiliar
[I.10]	Degradación de los soportes de almacenamiento de la información.	Degradación como consecuencia del paso del tiempo	[D] disponibilidad	– [Media] soportes de información
[I.11]	Emanaciones electromagnética.	Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al	[C] confidencialidad	– [HW] equipos informáticos (hardware) – [Media] soportes de información – [AUX] equipamiento auxiliar – [L] instalaciones

		exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación		
[E]	– Errores y fallos no intencionados			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[E.1]	Errores de los usuarios.	Equivocaciones de las personas cuando usan los servicios, datos, etc.	[I] Integridad [C] confidencialidad [D] disponibilidad	– [D] datos / información [keys] claves criptográficas – [S] servicios – [SW] aplicaciones (software) – [Media] soportes de información
[E.2]	Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación.	[D] disponibilidad [I] integridad [C] confidencialidad	– [D] datos / información [keys] claves criptográficas – [S] servicios – [SW] aplicaciones (software) – [HW] equipos informáticos (hardware) – [COM] redes de comunicaciones – [Media] soportes de información

[E.3]	Errores de monitorización *(log)*.	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, etc.	[I] integridad	– [D.conf] datos de configuración.
[E.7]	Deficiencias en la organización.	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.	[D] disponibilidad	– [P] personal
[E.8]	Difusión de software dañino.	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	[D] disponibilidad [I] integridad [C] confidencialidad	– [SW] aplicaciones (software)
[E.9]	Errores de [re-] encaminamiento.	Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.	[C] confidencialidad	– [S] servicios – [SW] aplicaciones (software) – [COM] redes de comunicaciones
[E.10]	Errores de secuencia	Alteración accidental del orden de los mensajes transmitidos.	[I] integridad	– [S] servicios – [SW] aplicaciones (software) – [COM] redes de comunicaciones
[E.14]	Escapes de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí	[C] confidencialidad	–

		misma se vea alterada.		
[E.15]	Alteración accidental de la información	Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	[I] integridad	– [D] datos / información [keys] claves criptográficas – [S] servicios – [SW] aplicaciones (SW) – [COM] comunicaciones (tránsito).
[E.18]	Destrucción de información.	Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	[D] disponibilidad	– [D] datos / información [keys] claves criptográficas – [S] servicios – [SW] aplicaciones (SW) – [COM] comunicaciones (tránsito) – [Media] soportes de información – [L] instalaciones
[E.19]	Fugas de información	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.	[C] confidencialidad	– [D] datos / información [keys] claves criptográficas – [S] servicios – [SW] aplicaciones (SW) – [COM] comunicaciones (tránsito) – [Media] soportes de información – [L] instalaciones – [P] personal (revelación)
[E.20]	Vulnerabilidades de los programas	Defectos en el código que dan pie a una operación	[I] integridad [D] disponibilidad	– [SW] aplicaciones (software)

	(software)	defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	[C] confidencialidad	
[E.21]	Errores de mantenimiento / actualización de programas (software)	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.	[I] integridad [D] disponibilidad	– [SW] aplicaciones (software)
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	[D] disponibilidad	– [HW] equipos informáticos (hardware) – [Media] soportes electrónicos – [AUX] equipamiento auxiliar
[E.24]	Caída del sistema por agotamiento de recursos.	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	[D] disponibilidad	– [S] servicios – [HW] equipos informáticos (hardware) – [COM] redes de comunicaciones
[E.25]	Pérdida de equipos	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que	[D] disponibilidad [C] confidencialidad	– [HW] equipos informáticos (hardware) – [Media] soportes de información – [AUX] equipamiento auxiliar

		hospedan datos, además se puede sufrir una fuga de información.		
[E.28]	Indisponibilidad del personal.	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, etc.	[D] disponibilidad	– [P] personal interno
[A]	– Ataques intencionados			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[A.3]	Manipulación de los registros de actividad (log)		[I] integridad (trazabilidad)	– [D.log] registros de actividad
[A.4]	Manipulación de la configuración	Afecta la configuración de los activos. Es diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	[I] integridad [C] confidencialidad [D] disponibilidad	– [D.log] registros de actividad
[A.5]	Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, utilizando los privilegios de éste para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	[C] confidencialidad [A] autenticidad [I] integridad	– [D] datos / información [keys] claves criptográficas – [S] servicios – [SW] aplicaciones (software) – [COM] redes de comunicaciones
[A.6]	Abuso de privilegios de acceso	Cada usuario utiliza un nivel de privilegios para un determinado propósito. Cuando un usuario abusa de su nivel de privilegios	[C] confidencialidad [I] integridad [D] disponibilidad	– [D] datos / información [keys] claves criptográficas – [S] servicios – [SW] aplicaciones

		para realizar tareas que no son de su competencia, puede ocasionar problemas.		(software) – [HW] equipos informáticos (hardware) – [COM] redes de comunicaciones
[A.8]	Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	[D] disponibilidad [I] integridad [C] confidencialidad	– [SW] aplicaciones (software)
[A.9]	[Re]encaminamiento de mensajes	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido. Puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Un ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.	[C] confidencialidad	– [S] servicios – [SW] aplicaciones (software) – [COM] redes de comunicaciones
[A.10]	Alteración de secuencia	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la	[I] integridad	– [S] servicios – [SW] aplicaciones (software) – [COM] redes de comunicaciones

		integridad de los datos afectados.		
[A.11]	Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	[C] confidencialidad [I] integridad	– [D] datos / información [keys] claves criptográficas – [S] servicios – [SW] aplicaciones (software) – [HW] equipos informáticos (hardware) – [COM] redes de comunicaciones – [Media] soportes de información – [AUX] equipamiento auxiliar – [L] instalaciones
[A.12]	Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina tráfico	[C] confidencialidad	– [COM] redes de comunicaciones
[A.13]	Repudio	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción:	[I] integridad (trazabilidad)	– [S] servicios – [D.log] registros de actividad

		negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.		
[A.14]	Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.	[C] confidencialidad	– [COM] redes de comunicaciones
[A.15]	Modificación deliberada de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.	[I] integridad	– [D] datos / información [keys] claves criptográficas – [S] servicios (acceso) – [SW] aplicaciones (SW) – [COM] comunicaciones (tránsito) – [Media] soportes de información – [L] instalaciones
[A.18]	Destrucción de información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	[D] disponibilidad	– [D] datos / información [keys] claves criptográficas – [S] servicios (acceso) – [SW] aplicaciones (SW) – [Media] soportes de información – [L] instalaciones
[A.19]	Revelación de información	Revelación de información (divulgación, copia ilegal de software)	[C] confidencialidad	– [D] datos / información [keys] claves criptográficas

				– [S] servicios (acceso) – [SW] aplicaciones (SW) – [COM] comunicaciones (tránsito) – [Media] soportes de información – [L] instalaciones
[A.22]	Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza (alteración de programas)	[C] confidencialidad [I] integridad [D] disponibilidad	– [SW] aplicaciones (software)
[A.23]	Manipulación de los equipos	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza (sabotaje de hardware)	[C] confidencialidad [D] disponibilidad	– [HW] equipos – [Media] soportes de información – [AUX] equipamiento auxiliar
[A.24]	Denegación de servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada (saturación del equipo informático)	[D] disponibilidad	– [S] servicios – [HW] equipos informáticos (hardware) – [COM] redes de comunicaciones
[A.25]	Robo	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y	[D] disponibilidad [C] confidencialidad	– [HW] equipos informáticos (hardware) – [Media] soportes de información – [AUX] equipamiento auxiliar

		el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas con tratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.		
[A.26]	Ataque destructivo	Vandalismo, terrorismo, acción militar, etc. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal. (destrucción de hardware o de soportes)	[D] disponibilidad	– [HW] equipos informáticos (hardware) – [Media] soportes de información – [AUX] equipamiento auxiliar – [L] instalaciones
[A.27]	Ocupación enemiga	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.	[D] disponibilidad [C] confidencialidad	– [L] instalaciones
[A.28]	Indisponibilidad del personal	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, etc. (daños a la disponibilidad del personal)	[D] disponibilidad	– [P] personal interno

[A.29]	Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.	[C] confidencialidad [I] integridad [D] disponibilidad	– [P] personal interno
[A.30]	Ingeniería social	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	[C] confidencialidad [I] integridad [D] disponibilidad	– [P] personal interno

ANEXO N° 06

CATÁLOGO DE VULNERABILIDADES POTENCIALES USADO EN EL PLAN DE GESTIÓN DE RIESGOS

N°	Vulnerabilidad
01	Ausencia de personal
02	Acceso físico no autorizado
03	Acceso no autorizado a la documentación del sistema
04	Acceso no autorizado a la información
05	Acceso no autorizado a la información, redes y sistemas
06	Acceso no autorizado a las infraestructuras informáticas
07	Acceso no autorizado a las librerías fuente de los programas
08	Acceso no autorizado a los ordenadores
09	Acceso no autorizado a redes y sus servicios
10	Acceso no autorizado al equipamiento informático
11	Acceso no autorizado, inadecuado o corrupción del soporte en el tránsito
12	Activos no protegidos
13	Atribución incorrecta de privilegios de acceso
14	Código malicioso
15	Complicated user interface
16	Confianza de las organizaciones clave hacia la compañía.
17	Conformidad con estándares
18	Conformidad con la política de seguridad
19	Control mal implantado
20	Coordinación de actividades de seguridad
21	Cumplimiento de las obligaciones y deberes del outsourcing (externalización)
22	Derecho a auditar en contratos de terceras partes
23	Derechos de propiedad intelectual
24	Disponibilidad de las infraestructuras de procesamiento de la información
25	Disposición o reutilización de los medios de almacenaje sin una apropiada verificación
26	Externalización y uso de terceras partes contratadas
27	Clima extremo
28	Fallo del sistema
29	Falta de un acuerdo de intercambio de software e información
30	Falta de coordinación y organización de la seguridad
31	Falta de planes y procedimientos de continuidad de negocio

32	Falta de política de seguridad
33	Falta de responsabilidades, pruebas y formación en la continuidad de negocio
34	Falta de seguridad en el equipamiento informático
35	Falta de seguridad en los soportes informáticos
36	Falta de sensibilización
37	Falta de una gestión apropiada de las claves criptográficas
38	Falta de una política determinada en el uso de controles criptográficos
39	Gestión de contraseñas que es demasiado simple
40	Manejo inadecuado de la red
41	Uso inadecuado o descuidado del control de acceso físico al edificio
42	Procedimientos inadecuados de reclutamiento
43	Respuesta inadecuada del servicio de mantenimiento
44	Uso Incorrecto del hardware y software
45	Incorrecta clasificación, etiquetado o manejo de la información.
46	Incumplimiento de la legislación
47	Insuficiente mantenimiento / mala instalación de los medios de almacenaje.
48	Entrenamiento insuficiente de seguridad
49	Insuficiente seguridad construida dentro del sistema
50	falta de seguimiento
51	Falta de copias back-up
52	Falta de cuidado en la disposición
53	Falta de documentación
54	Falta del control del cambio eficaz
55	Falta de control eficiente del cambio de configuración
56	Falta de mecanismos de identificación y de autentificación tales como autentificación de usuario
57	Falta de identificación y autentificación del remitente y del receptor
58	Falta de mecanismos de supervisión
59	Falta de esquemas de reemplazo periódicos
60	Falta de protección física del edificio, puertas y ventanas;
61	Falta de políticas para el uso correcto de los medios de telecomunicación y mensajería
62	Falta de pruebas de envío y recibimiento del mensaje
63	Falta del conocimiento sobre seguridad
64	Localización en un área susceptible a la inundación
65	Nivel inapropiado de protección criptográfica
66	Dejar en sesión el sistema al salir del workstation.
67	Prueba insuficiente del software
68	Pobre cableado

69	Administración pobre de contraseñas
70	Prevención del uso no autorizado de las infraestructuras de procesamiento
71	Procesamiento de negocio correcto
72	Protección de datos y privacidad de la información personal
73	Protección de la información de la organización.
74	Recolección de evidencias
75	Regulación de los controles criptográficos
76	Responsabilidades no claramente definidas
77	Riesgos de comercio electrónico
78	Riesgos de los sistemas ofimáticos compartidos entre las organizaciones
79	Riesgos de los sistemas públicamente disponibles
80	Riesgos desde terceras partes
81	Riesgos provenientes de la informática móvil
82	Riesgos provenientes del teletrabajo
83	Riesgos relacionados con el outsourcing
84	Seguridad de Internet
85	Seguridad de la Intranet
86	Seguridad del comercio electrónico
87	Seguridad del teletrabajo
88	Seguridad en los negocios móviles
89	Sensibilidad a la radiación electromagnética
90	Únicos puntos de falla
91	Susceptibilidad a la humedad, al polvo
92	Susceptibilidad a las variaciones de la temperatura
93	Susceptibilidad a las variaciones del voltaje
94	Transferencia de passwords claramente
95	Especificaciones confusas o incompletas para los desarrolladores
96	Copiado incontrolado
97	Descarga y uso incontrolado de software
98	Líneas de comunicación desprotegidas
99	Password desprotegidos
100	Conexiones de red pública desprotegidas
101	Unprotected sensitive traffic
102	Almacenaje desprotegido
103	Unsupervised work by outside or cleaning staff
104	Saber bien los defectos en el software
105	Wrong allocation of access right

ANEXO N° 07

LISTADO DE OBJETIVOS DE CONTROL Y CONTROLES CLASIFICADOS POR DOMINIO, SEGÚN LA ISO/IEC 27002:2005

Control ISO	Requerimiento Objetivo de control	Control	Estrategia	Calificación
5. Política de seguridad				
5.1	**Política de Seguridad de la Información**			
5.1.1	Se tiene documento de la política de seguridad de la Información	Un documento de política de seguridad de la información debería ser aprobado por la Dirección y debería ser publicado y comunicado a todos los empleados y terceras partes.		
5.1.2	Se hace revisión y evaluación de este documento y se promulga su lectura y aplicación.	La política de seguridad de la información se debería revisar a intervalos planificados o en el caso de que se produzcan cambios significativos para asegurar la idoneidad, adecuación		
6. Organización de la Seguridad de la Información				
6.1	**Organización Interna**			
6.1.1	Compromiso de las Dirección con la seguridad de la información.	La Dirección deberá dar un activo soporte a la seguridad dentro de la organización a través de directivas claras, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de seguridad de la información.		
6.1.2	Coordinación de la Seguridad de la Información.	Las actividades relativas a la seguridad de la información deberían ser coordinadas por representantes de las diferentes partes de la organización con los correspondientes roles y funciones de trabajo.		

6.1.3	Asignación de responsabilidades sobre la seguridad de la información	Debería definirse claramente todas las responsabilidades de seguridad de la información.		
6.1.4	Proceso de Autorización de recursos para el procesamiento/tratamiento de información	Debería definirse e implantarse un proceso de autorización para la gestión de cada nuevo recurso de tratamiento de la información.		
6.1.5	Acuerdos de confidencialidad	Debería identificarse y revisarse de una manera regular los requisitos de los acuerdos de confidencialidad o no revelación que refleje las necesidades de la organización para la protección de la información.		
6.1.6	Contacto/Cooperación con las autoridades	Se debería mantener contactos adecuados con las autoridades que corresponda.		
6.1.7	Contacto con grupos de especial interés.	Se deberían mantener contactos apropiados con grupos de interés especial u otros foros especialistas en seguridad y asociaciones profesionales.		
6.1.8	Se realiza Auditoría interna - Revisiones independientes de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implantación debería revisarse de una manera independiente a intervalos planificados o cuando se producen cambios significativos en la implantación de la seguridad.		
6.2	**Seguridad de acceso de terceras partes**			
6.2.1	Identificación de riesgos de acceso de terceras partes.	Cuando el negocio requiera de partes externas, deberían identificarse los riesgos de la información de la organización y de los dispositivos de tratamiento de la información, así como la implantación de los controles adecuados antes de garantizar el		

		acceso.		
6.2.2	Consideraciones de seguridad en contratos con clientes	Todos los requisitos de seguridad que se hayan identificado deberían ser dirigidos antes de dar acceso a los clientes a los activos o a la información de la seguridad.		
6.2.3	Consideraciones de seguridad en contratos con terceros	Los acuerdos que comparten el acceso de terceros a recurso de tratamiento de información de la organización deben basarse en un contrato formal que tenga o se refiera a todos los requisitos de la seguridad que cumpla con las políticas y normas de seguridad de la organización. El contrato debe asegurar que no hay malentendidos entre la organización y los terceros. Las organizaciones deben verse compensadas hasta la indemnización de sus suministradores.		
7. Gestión de activos				
7.1	**Responsabilidad sobre los activos**			
7.1.1	Inventario de activos tecnológicos y de la información.	Todos los activos deberían ser claramente identificados y deberían prepararse y mantenerse un inventario de todos los activos importantes.		
7.1.2	Responsables/Propietarios de los activos tecnológicos.	Toda la información y los activos asociados con los recursos para el tratamiento de la información deberían ser propiedad de una parte designada de la organización.		
7.1.3	Uso aceptable de las activas tecnológicos.	Las reglas de uso aceptable de la información y los activos asociados con el tratamiento de la información, deberían ser identificadas,		

		documentadas e implantadas.		
7.2	**Clasificación de la información**			
7.2.1	Normas y directrices para clasificación de la información.	La información debería estar clasificada, según su valor, los requisitos legales, su sensibilidad y criticidad para la organización.		
7.2.2	Identificación, etiquetado y manejo de la información.	Debería desarrollarse un conjunto adecuado de procedimientos para marcar y tratar la información de acuerdo con el esquema de clasificación adoptado por la organización.		
8. Seguridad ligada a los Recursos Humanos				
8.1	**Seguridad en actividades previas en la contratación**			
8.1.1	Inclusión de la seguridad en las funciones y responsabilidades del trabajo.	Las funciones y responsabilidades de seguridad para los empleados, contratistas y usuarios de tercera parte deberían ser definidas y documentadas de acuerdo con la política de seguridad de la información de la organización. La comprobación de los antecedentes de todos los candidatos al puesto de trabajo, los contratistas o los usuarios de tercera parte deberían ser llevadas a		
8.1.2	Investigación del personal que va a ser contratado	De acuerdo con la legislación aplicable, las reglamentaciones y éticas de manera proporcional a los requisitos del negocio, la clasificación de la información a la que se accede y a los riesgos considerados.		
8.1.3	Términos y condiciones laborales.	Como parte de las obligaciones contractuales, los empleados, contratistas y usuarios de tercera parte deberían aceptar y firmar los términos y condiciones de su		

		contrato de trabajo, que deberían establecer sus responsabilidades, así como las de la organización en lo relativo a la seguridad de la información.		
8.2	**Seguridad en actividades durante el desempeño de las funciones**			
8.2.1	Responsabilidades de la Dirección	La Dirección debería requerir a los empleados, contratistas y de tercera parte, el aplicar la seguridad de acuerdo a lo establecido en las políticas y procedimientos de la organización.		
8.2.2	Conciencia y formación sobe la seguridad de la información: educación y entrenamiento	Todos los empleados de la organización y, cuando corresponda, los contratistas y los usuarios de tercera parte, deberían recibir una formación y concientización adecuadas y actualizadas de las políticas y procedimientos, según corresponda a su puesto de trabajo.		
8.2.3	Procesos disciplinarios	Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna brecha de seguridad.		
8.3	**Fin de contrato o cambio de funciones**			
8.3.1	Responsabilidades en la terminación del contrato	Las responsabilidades para llevar a cabo la finalización o cambio de puesto de trabajo deberían estar claramente definidas y asignadas.		
8.3.2	Devolución/restitución de activos tecnológicos	Todos los empleados, contratistas y usuarios de tercera parte deberían devolver los activos de la organización que tengan en posesión a la finalización de su empleo, contrato o acuerdo.		
8.3.3	Eliminación de permisos sobre los activos	Los derechos de acceso a la información y a los recursos de tratamiento de la información de		

		todos los empleados, contratistas y usuarios de tercera parte, debería ser retirada a la finalización de la contratación o del acuerdo, o adaptados según los cambios.		
9. Seguridad física y del entorno				
9.1	**Áreas seguras/restringidas**			
9.1.1	Perímetro de Seguridad Física	Debería usarse perímetros de seguridad (barreras tales como muros, puertas de entrada con control a través de tarjeta o mesas de recepción tripuladas) para proteger las áreas que contienen la información y los recursos de tratamiento de la información.		
9.1.2	Controles físicos de entrada	Las áreas seguras deberías estar protegidas por controles de entrada adecuados para asegurar que únicamente se permita el acceso al personal autorizado.		
9.1.3	Aseguramiento de oficinas, cuartos e instalaciones	Se debería diseñar y aplicar la seguridad física para las oficinas, despachos y recursos.		
9.1.4	Protección contra amenazas externas y ambientales	Se debería diseñar y aplicar una protección física contra el daño por fuego, inundación, terremoto, explosión, malestar social y otras formas de desastres naturales o provocadas por el hombre.		
9.1.5	Trabajo en áreas restringidas	Se debería diseñar e implantar la protección física y las directrices para trabajar en las áreas seguras.		
9.1.6	Acceso público	Deberían controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos donde pueda acceder personal no autorizado, y si es de carga, envíos y áreas posible, dichos puntos		

		deberías estar aislados de los recursos de tratamiento de la información para evitar accesos no autorizados.		
9.2	**Seguridad de los equipos**			
9.2.1	Ubicación, instalación y protección de equipos tecnológicos	Los equipos deberías estar situados o protegidos para reducir los riesgos de las amenazas y los riesgos del entorno, así como de las oportunidades de acceso no autorizado.		
9.2.2	Seguridad en el suministro de electricidad y servicios (utilities).	Los equipos deberías estar protegidos de los fallos de energía y de otras interrupciones causadas por fallos en las instalaciones de suministro.		
9.2.3	Seguridad en el cableado	El cableado eléctrico y de telecomunicaciones que transmiten datos a los servicios de soporte de la información debería estar protegido de interceptación o de daños.		
9.2.4	Mantenimiento de equipos	Los equipos deberías ser mantenido de una manera correcta para asegurar su continuidad, disponibilidad e integridad.		
9.2.5	Seguridad de equipos fuera de las áreas seguras	Se debería aplicar medidas de seguridad a los equipos fuera de los locales de la organización, teniéndose en cuenta los diferentes riesgos de trabajar fuera de los locales de la organización.		
9.2.6	Destrucción y reutilización de equipos	Todos los elementos del equipo que contengan medios de almacenamiento deberían ser comprobados para asegurar que todo dato sensible y software bajo licencia se ha borrado o sobrescrito, previamente a su utilización.		

9.2.7	Traslado de activos fuera de la organización	Los equipos, la información o el software no deberían sacarse fuera de las instalaciones sin previa autorización.		
10. Gestión de las comunicaciones y las operaciones				
10.1	**Procedimientos y responsabilidades operativas**			
10.1.1	Documentación de procesos operativos	Se debería implantar, mantener procedimientos operacionales y estar disponibles para todos los usuarios que lo necesiten.		
10.1.2	Control de Cambios	Se deberían controlar los cambios en los recursos y sistemas de tratamiento de la información.		
10.1.3	Segregación de funciones y tareas.	Las tareas y áreas de responsabilidad deberían segregarse para reducir la posibilidad de modificaciones no autorizadas y no intencionadas o el mal uso de los activos de la organización.		
10.1.4	Separación de los ambientes de Desarrollo, prueba y producción	Deberían separarse los recursos para el desarrollo, las pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema operativo.		
10.2	**Gestión de la provisión de servicios contratados con terceros**			
10.2.1	Entrega de servicios	Deberían asegurarse de que los controles de seguridad, los niveles de entrega y definiciones del servicio incluido en el acuerdo de entrega del servicio por tercera parte se implantan, se ponen en funcionamiento y son mantenidos por la tercera parte.		
10.2.2	Monitoreo y revisión de servicios de terceros.	Los servicios, informes y registros proporcionados por las terceras partes deberían ser controlados y revisados regularmente		
10.2.3	Administración de cambios a	Se deberían gestionar los cambios en		

	servicios de terceros.	la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio implicados y la revalorización de los riesgos.		
10.3	**Planificación y aceptación de sistemas**			
10.3.1	Gestión de capacidades	La utilización de los recursos deberían controlarse y ajustarse y se deberían hacer proyecciones de los requisitos de capacidad futura para asegurar el comportamiento requerido del sistema.		
10.3.2	Aceptación de sistemas	Debería establecerse un criterio e aceptación para los nuevos sistemas, las actualizaciones y las nuevas versiones; así como llevarse a cabo las pruebas adecuadas del (de los) sistema(s) durante el desarrollo y previamente a la aceptación.		
10.4	**Protección contra software malicioso y código móvil**			
10.4.1	Controles contra código malicioso	Se debería implantar procedimientos de concienciación del usuario adecuados; así como controles de detección, prevención y recuperación para proteger contra código malicioso.		
10.4.2	Controles contra código móvil	Cuando se autoriza el uso de código ambulante, la configuración debería asegurar que está operando un código ambulante autorizado de acuerdo a una política de seguridad claramente definida, y debería prevenirse la ejecución de código ambulante no autorizado.		

10.5	**Copias de seguridad**			
10.5.1	Copias de respaldo de la información.	Se debería hacer copias de seguridad de la información y del software y ser comprobadas regularmente de acuerdo con la política de copias de seguridad acordadas.		
10.6	**Gestión de la seguridad de red**			
10.6.1	Controles de la Red	Las redes deberían estar adecuadamente gestionadas y controladas, para estar protegidas de amenazas y para mantener la seguridad de los sistemas y aplicaciones que usan estas redes, incluyendo la información en tránsito.		
10.6.2	Seguridad de los Servicios de Red	Las características de seguridad, los niveles de servicio, los requisitos de gestión para todos los servicios de red deberían estar identificadas e incluidas en todo acuerdo de servicio de red, aunque estos servicios se proporcionen desde dentro de la organización o sean subcontratados.		
10.7	**Utilización de los soportes de información**			
10.7.1	Administración de medios removibles	Debería haber procedimientos para la gestión de los soportes desmontables.		
10.7.2	Destrucción de medios	Debería deshacerse de los soportes de una manera segura y fuera de peligro cuando no se vaya a requerir su uso durante más tiempo, mediante procedimientos formales.		
10.7.3	Procedimientos de manejo de la información.	Se debería establecer procedimientos para el tratamiento y el almacenamiento de la información para proteger esta información de revelación no		

		autorizada o mal uso.		
10.7.4	Seguridad de la documentación de los sistemas.	El sistema de documentación debería estar protegido contra accesos no autorizados.		
10.8	**Intercambio de información**			
10.8.1	Políticas y procedimientos del intercambio de información	Se debería establecer políticas de intercambio formal, procedimientos y controles para proteger el intercambio de la información mediante el uso de todos los tipos de servicios de comunicación.		
10.8.2	Acuerdos para el intercambio de información.	Se debería establecer acuerdos para el intercambio de información y software entre la organización y las partes externas.		
10.8.3	Medios físicos en movimiento	Los recursos que contienen información deberían estar protegidos contra el acceso no autorizado, el mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.		
10.8.4	Mensajería electrónica	La información implicada en el envío de mensajes electrónicos debería estar adecuadamente protegida.		
10.8.5	Sistemas de información de negocios.	Se debería desarrollar e implantar políticas y procedimientos para proteger la información asociada a la interconexión de sistemas de información entre organizaciones.		
10.9	**Servicios de comercio electrónico**			
10.9.1	Comercio electrónico	La información implicada en el comercio electrónico realizado a través de rede públicas debería protegerse de las actividades fraudulentas, los litigios contra contratos, y la revelación o modificación no autorizada de la		

		información.		
10.9.2	Transacciones en línea	La información implicada en las transacciones online debería estar protegida para evitar la transmisión incompleta, las rutas erróneas, la alteración no autorizada del mensaje, la revelación no autorizada, la duplicación no autorizadas del mensaje.		
10.9.3	Información de difusión pública	La integridad de la información que se hace disponible en el sistema públicamente disponible debería estar protegida para prevenir la modificación no autorizada.		
10.10	**Seguimiento/Monitoreo**			
10.10.1	Registros de auditoría	Se debería efectuar registros de auditoría de las actividades del usuario, excepciones e incidencias de información, y mantenerse durante un periodo acordado para ayudar en investigaciones futuras y en el seguimiento y monitorización del control de accesos.		
10.10.2	Seguimiento del uso de los sistemas	Se debería establecer procedimientos para el seguimiento del uso de los recursos de tratamiento de la información y revisarse regularmente los resultados del seguimiento de estas actividades.		
10.10.3	Protección de registros de monitoreo	Los dispositivos de registro y el diario de información deberán estar protegidos contra la manipulación y los accesos no autorizados.		
10.10.4	Registros de monitoreo de administradores y operadores	Las actividades de administrador del sistema y del operador del sistema deberán ser registradas.		
10.10.5	Registro de fallas y errores	Los fallos deberían ser registrados,		

		analizados y tomar las acciones adecuadas		
10.10.6	Sincronía de relojes	Los relojes de todos los sistemas de tratamiento de la información dentro de una organización o dominio de seguridad, deberían estar sincronizados con una precisión de tiempo acordada.		
11. Control de accesos				
11.1	**Requerimientos de negocio para control de acceso**			
11.1.1	Política de Control de Acceso	Se debería establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad para el acceso.		
11.2	**Gestión de acceso de los usuarios**			
11.2.1	Registro de usuarios	Debería haber un procedimiento de registro formal de usuarios y de retirada del registro para conceder y revocar el acceso a todos los sistemas y servicios de información.		
11.2.2	Administración de privilegios	La asignación y el uso de privilegios deberían estar restringidos y controlados.		
11.2.3	Administración de contraseñas de usuario (passwords)	La asignación de contraseñas debería ser controlada a través de un proceso formal de gestión.		
11.2.4	Revisión de los permisos asignados a los usuarios	La Dirección debería revisar los derechos de acceso de los usuarios a intervalos regulares y utilizando un procedimiento formal.		
11.3	**Responsabilidad de los usuarios**			
11.3.1	Uso de las contraseñas	Se debería requerir a los usuarios el seguir las buenas prácticas de seguridad en la selección y el uso de contraseñas.		
11.3.2	Equipos desatendidos	Los usuarios deberían asegurarse que el equipo desatendido tiene la		

		protección adecuada.		
11.3.3	Política de escritorios y pantallas limpias	Debería adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.		
11.4	**Control de acceso a la red**			
11.4.1	Políticas para el uso de los servicios de la red de datos.	Únicamente se debería proporcionar a los usuarios el acceso a los servicios para los que específicamente se les haya autorizado el uso.		
11.4.2	Autenticación de usuarios para conexiones externas.	Se debería utilizar los métodos apropiados de autenticación para el control de acceso a los usuarios en remoto.		
11.4.3	Identificación de equipos en la red.	Debería considerarse la identificación automática del equipo como un medio de autenticación de las conexiones para las posiciones y equipos específicos.		
11.4.4	Diagnóstico remoto y protección de la configuración de puertos	Se debería controlar acceso físico y lógico al diagnóstico y configuración de los puertos.		
11.4.5	Segregación en la red	Los grupos de servicio de información, de usuarios y de sistema de información deberían estar segregados en redes.		
11.4.6	Control de conexión a la red	Se debería restringir la capacidad de los usuarios a conectarse a la red en el caso de redes compartidas, especialmente para aquellas que traspasan las fronteras de la organización, en línea con la política de control de acceso y los requisitos de las aplicaciones de negocio.		

11.4.7	Control de enrutamiento de la red	Los controles de direccionamiento deberían estar implantados para las redes, para asegurar que las conexiones de las computadoras y los flujos de información no violen la política de control de acceso a las aplicaciones del negocio.		
11.5	**Control de acceso a los sistemas operativos**			
11.5.1	Procedimientos para inicio de sesión de las estaciones de trabajo	Se debería controlar el acceso al sistema operativo mediante un procedimiento de entrada seguro.		
11.5.2	Identificación y autenticación de los usuarios.	Todos los usuarios deberían tener un identificador de usuario (ID) para su uso personal y único. Se debería elegir una técnica adecuada de autenticación para la conformación de la identidad de un usuario.		
11.5.3	Sistema de administración de contraseñas.	Los sistemas para la administración de contraseñas deberían ser interactivos y asegurar la calidad de la contraseña.		
11.5.4	Uso de las utilidades del sistema	El uso de los programas que pueden ser capaces de invalidar los controles del sistema y de la aplicación, deberían estar restringidos y estrictamente controlados.		
11.5.5	Desconexión automática de sesión.	Las sesiones interactivas deberían cerrase después de un periodo de inactividad definido.		
11.5.6	Limitación en los periodos de tiempo de conexión a servicios y aplicaciones	Se debería usar restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones de alto riesgo.		
11.6	**Control de acceso a la información y aplicaciones**			
11.6.1	Restricción de acceso a los sistemas de información.	Debería restringirse el acceso de los usuarios y del personal de apoyo a la		

		información y a las funciones del sistema de aplicación, de acuerdo con la política de control de acceso definida.		
11.6.2	Aislamiento de sistemas sensibles	Los sistemas sensibles deberían tener un entorno de computadores dedicados y aislados.		
11.7	**Computación móvil y teletrabajo**			
11.7.1	Computación y comunicaciones móviles	Debería implantarse una política formal y debería adoptarse las apropiadas medidas de seguridad para proteger contra los riesgos de la utilización de computadores y comunicaciones móviles.		
11.7.2	Teletrabajo	Se deberían desarrollar e implantar procedimientos, planes operacionales y una política para las actividades de teletrabajo.		
12. Adquisición, desarrollo y mantenimiento de sistemas de información				
12.1	**Requisitos de seguridad de los sistemas de información**			
12.1.1	Análisis y especificaciones de los requerimientos de seguridad			
12.2	**Procesamiento correcto en aplicaciones**			
12.2.1	Validación de los datos de entrada	La introducción de datos en las aplicaciones debería validarse para garantizar que dichos datos son correctos y adecuados.		
12.2.2	Control del procesamiento interno.	Debería incorporarse comprobaciones de validación a las aplicaciones para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados.		
12.2.3	Integridad de los mensajes	Debería identificarse los requisitos para garantizar la autenticidad y proteger la integridad de los mensajes en las aplicaciones y		

		deberían identificarse e implantarse controles adecuados.		
12.2.4	Validación de los datos de salida.	Los datos resultantes de una aplicación deberían ser validados para garantizar que el procesamiento de la información almacenada es correcto y resulta adecuado a las circunstancias.		
12.3	**Controles criptográficos**			
12.3.1	Política para el uso de controles criptográficos	Debería desarrollarse e implementarse una política acerca del uso de controles criptográficos para proteger la información.		
12.3.2	Administración de claves/llaves.	Debería existir una gestión de las claves que apoye el uso de técnicas criptográficas por parte de la organización.		
12.4	**Seguridad de los ficheros del sistema**			
12.4.1	Control del software operacional (en producción)	Deberían existir procedimientos para controlar la instalación de software en los sistemas operativos.		
12.4.2	Protección de los datos en sistemas de prueba	Los datos de prueba deberían seleccionarse atentamente, protegerse y controlarse.		
12.4.3	Control de acceso a las librerías de código fuente	Debería restringirse el acceso al código fuente de los programas.		
12.5	**Seguridad en los procesos de desarrollo y soporte**			
12.5.1	Procedimientos para el control de cambios	La implementación de cambios debería estar controlada mediante el uso de procedimientos formales de control de cambios.		
12.5.2	Revisión técnica de aplicaciones después de cambios al sistema operativo	Cuando se realizan cambios en los sistemas debería revisarse y probarse las aplicaciones, sobre todas las críticas, para garantizar que no existen efectos adversos en las operaciones organizativas o la seguridad.		

12.5.3	Restricciones a cambios en paquetes de software	No debería estimularse las modificaciones a los paquetes de software, debería limitarse a los cambios necesarios y todos los cambios deberían estar estrictamente controlados.		
12.5.4	Fuga de información	Debería evitarse la oportunidad de fuga de información.		
12.5.5	Desarrollo de software por parte de Outsourcing	La externalización del desarrollo del software debería ser supervisada y monitorizada por la organización.		
12.6	**Gestión de vulnerabilidades técnicas**			
12.6.1	Control de vulnerabilidades técnicas	Debería obtenerse información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información que se estén utilizando. Asimismo, deberían evaluarse la exposición de la organización a dichas vulnerabilidades y deberían adoptarse medidas adecuadas para afrontar el riesgo asociado.		
13. Gestión de incidentes de seguridad de la información				
13.1	Comunicación de eventos y debilidades de seguridad de la información			
13.1.1	Reporte de eventos de Seguridad de la información.	Los eventos de seguridad de la información deberían comunicarse mediante canales adecuados de gestión lo antes posible.		
13.1.2	Reporte de debilidades de seguridad	Todos los trabajadores, contratistas y usuarios terceros de los sistemas y servicios de comunicación deberían estar obligados a anotar y comunicar cualquier punto débil que hayan observado o que sospechen que exista en los sistemas o servicios.		
13.2	**Gestión de incidentes de seguridad de la información y de su mejoramiento**			
13.2.1	Responsabilidades y	Debería establecerse		

	procedimientos	responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.		
13.2.2	Aprendizaje a partir de los incidentes de seguridad	Deberían existir mecanismos para permitir que los tipos, volúmenes y costes de los incidentes de seguridad de la información se cuantifiquen y se supervisen.		
13.2.3	Recolección de evidencia	Cuando una acción contra una persona u organización después de un incidente de seguridad de la información implique medidas legales (tanto civiles como penales), deberían recopilarse pruebas, que deberían conservarse y presentarse de manera que se ajusten a las normas establecidas en la jurisdicción pertinente con respecto a las pruebas.		
14. Gestión de la continuidad del negocio				
14.1	**Aspectos de seguridad de la información en la gestión de la continuidad del negocio**			
14.1.1	Inclusión de seguridad de la información en el proceso de administración de la continuidad del negocio	Debería desarrollarse y mantenerse un proceso controlado para la continuidad del negocio en toda la organización que trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.		
14.1.2	Continuidad del negocio y análisis de impacto (BIA)	Deberían identificarse los eventos que provocan interrupciones en los procesos del negocio; así como la probabilidad y los efectos de dichas interrupciones y sus consecuencias con respecto a la seguridad de la información.		
14.1.3	Desarrollo e implementación	Debería desarrollarse e implantarse		

	de planes de continuidad	planes para mantener o restaurar las actividades y garantizar la disponibilidad de la información en el nivel y la escala temporal requeridos después de una interrupción o un fallo de los procesos críticos de un negocio.		
14.1.4	Marco de planeación para la continuidad del negocio	Se debería mantener un único marco de referencia para los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, para dirigir de una manera coherente los requisitos de seguridad de la información, y para identificar prioridades para las pruebas y el mantenimiento.		
14.1.5	Pruebas, mantenimiento y revisión de los planes de continuidad del negocio.	Los planes de continuidad del negocio deberían probarse y actualizarse periódicamente para garantizar que están al día y que son efectivos.		
15. Conformidad				
15.1	**Cumplimiento con requerimientos legales**			
15.1.1	Identificación de la legislación aplicable	Todos los requisitos pertinentes, tanto legales como reglamentarios o contractuales, y el enfoque de la organización para cumplirlos, deberían definirse explícitamente, documentarse y mantenerse actualizados para cada sistema de información y la organización.		
15.1.2	Derechos de autor y propiedad intelectual	Deberían implantarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales acerca del uso de materiales con respecto a los cuales puedan existir derechos de		

		propiedad intelectual y acerca del uso de productos de software exclusivo.		
15.1.3	Salvaguardar los registros de la organización	Los registros importantes deberían estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, reglamentarios contractuales y empresariales.		
15.1.4	Protección de los datos y privacidad de la información personal	Debería garantizarse la protección de datos y la privacidad según se requiera en la legislación, las normativas y, si fuera aplicable, las cláusulas contractuales pertinentes.		
15.1.5	Prevención del mal uso de los componentes tecnológicos	Debería impedirse que los usuarios utilizaran las instalaciones de procesamiento de la información para fines no autorizados.		
15.1.6	Regulación de controles criptográficos	Los controles criptográficos deberían utilizarse de acuerdo con todos los contratos, leyes y normativas pertinentes.		
15.2	**Conformidad con políticas y normas de seguridad y conformidad técnica**			
15.2.1	Cumplimiento de los diferentes requerimientos y controles establecidos por la política de seguridad	Los gestores deberían asegurarse de que todos los procedimientos de seguridad, dentro de su área de responsabilidad, se realicen con el fin de cumplir las políticas y normas de seguridad.		
15.2.2	Chequeo del cumplimiento técnico	Debería comprobarse periódicamente que los sistemas de información cumplan las normas de implementación de seguridad.		
15.3	**Consideraciones sobre la auditoría de sistemas de información**			
15.3.1	Controles para auditoría del sistema	Los requisitos y actividades de la auditoría que impliquen comprobaciones en los sistemas		

		operativos, deberían planificarse cuidadosamente y acordarse, para minimizar los riesgos de interrupciones de los procesos.		
15.3.2	El acceso a las herramientas auditoría	Protección de las herramientas de los sistemas de información para evitar cualquier peligro uso indebido		

ANEXO N° 08

EXIGENCIAS DE LA NORMATIVA CIRCULAR Nº G-105-2002 CONSIDERADOS EN LOS ESTÁNDARES DE REFERENCIAS UTILIZADOS

Exigencia de la norma SBS		ISO/IEC 27001:2007	ISO/IEC 17799:2005	MagerIT
Establecer e implementar políticas y procedimientos necesarios para administrar los riesgos de TI (Art. N° 03)		X		
Cumplimiento de los criterios de control interno (Art. N° 03)	Eficacia		X	
	Eficiencia		X	
	Confidencialidad		X	X
	Integridad		X	X
	Disponibilidad		X	X
	Cumplimiento normativo		X	
Definir y mantener una estructura organizacional y procedimientos que les permita administrar adecuadamente los riesgos asociados a la tecnología de información (Art. N° 04)		X		
	Definición de una política de seguridad.	X		
	Evaluación de riesgos de seguridad a los que está expuesta la información			X

	Selección de controles y objetivos de control para reducir, eliminar o evitar los riesgos identificados		X	X
	Plan de implementación de los controles y procedimientos de revisión periódicos			X
	Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos		X	X
Responsabilidad de verificar que se mantengan las características de seguridad de la información en subcontrataciones (outsourcing) (Art. N° 06)	cumplimiento de la presente circular.		X	
	los proveedores del servicio exterior, aseguran el adecuado acceso a la información con fines de supervisión		X	
Administración de la seguridad de la información (Art. N° 07)	Seguridad lógica		X	
	Seguridad de personal		X	
	Seguridad física y ambiental		X	
	Clasificación de la seguridad		X	X
Administración de operaciones (Art. N° 08)			X	
Desarrollo y mantenimiento de sistemas informáticos - Requerimientos de seguridad (Art. N° 09)			X	
Procedimientos de respaldo (Art. N° 10)			X	
Planeamiento, criterios de diseño e implementación y pruebas de la continuidad de negocios (Art. N° 11, 12 y 13)		X		
Cumplimiento normativo (Art. N° 14)		X		
Privacidad de la información (Art. N° 15)		X		
Plan anual de trabajo para la evaluación de cumplimiento: Auditoría Interna y Externa (Art. N° 16 y 17)		X		
Información a la Superintendencia (Art. N° 18)		X	X	X
Sanciones en caso de incumplimiento (Art. N° 19)		X		X

EXIGENCIAS DE LA NORMATIVA RESOLUCIÓN S.B.S. N° 2116 -2009 CONSIDERADOS EN LOS ESTÁNDARES DE REFERENCIAS UTILIZADOS

Exigencia de la norma SBS		ISO/IEC 27001:2007	ISO/IEC 17799:2005	MagerIT
Definiciones básicas (Art. N° 02)	Apetito de riesgo			
	Evento de pérdida			X
	Tolerancia de riesgo			X
Identificación de riesgo operacional (Art. N° 03 y 4)	Procesos internos			X
	Personal			X
	Tecnologías de la información			X
	Eventos externos			X
Identificación de eventos de pérdida por riesgo operacional (Art. N° 05).	Fraude interno	X		
	Fraude externo	X		
	Relaciones laborales y seguridad en el puesto de trabajo		X	X
	Clientes, productos y prácticas empresariales	X		
	Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales.		X	X
	Pérdidas derivadas del incumplimiento involuntario o negligente		X	X
	Daños a activos materiales.		X	X
	Interrupción del negocio y fallos en los sistemas		X	X
	Ejecución, entrega y gestión de procesos		X	X
Definición de roles y responsabilidades (Art. N° 06, 07, 08 y 09)	Del Directorio	X		
	De la Gerencia	X		
	Comité de Riesgos	X		
Manual de gestión de riesgos operacional (Art. N° 10).				X
Metodología de gestión de riesgos operacional (Art. N° 11)				X
Base de datos de eventos de pérdida (Art. N° 12)			X	
Gestión de la continuidad del negocio y de la seguridad de la información (Art. N° 13)			X	
Requisitos para la Subcontratación de servicios (Art. N° 14).			X	
Informes para la Superintendencia (Art. N° 15)		X	X	X

ANEXO N° 09

CUADRO COMPARATIVO ENTRE LA ISO/IEC 27001 - ISO/IEC 17799 Y EL PLAN PROPUESTO PARA LA IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD COMO PARTE DEL SGSI

Criterio		ISO/IEC 27001	ISO/IEC 17799	Plan Propuesto	Aporte de la investigación
Identifica los objetivos de negocio considerados en el SGSI		Como norma internacional lo establece de carácter general como requisito de un SGSI	No forma parte de su alcance	Lo específica para el caso de estudio	Adecúa la norma al tipo de empresa.
Selecciona del ámbito de implantación apropiado para la implantación de las políticas de seguridad.		Como norma internacional lo establece de carácter general como requisito de un SGSI	Como norma internacional lo establece de carácter general como buena práctica para cada uno de sus objetivos de control	Lo específica para los procesos críticos del caso de estudio	Adecúa la norma al tipo de empresa
Determina niveles de madurez de las políticas de seguridad de la información.	Define documentos y formatos que especifique el ámbito de conformidad de la política	Lo define de manera general como requisito de un SGSI	Lo define de manera general sólo para algunos objetivos de control y controles	Si se ha considerado de manera específica para la evaluación de los controles actuales por activo de TI	Se ha elaborado formatos específicos para valorar las políticas y los controles
	Establece flujos de información claramente	No lo considera. Sólo indica que debe procedimentars	No lo considera. Sólo indica que debe	Establece criterios manera general para	No se ha procedimentado por que no es objetivo de la investigación

	definidos y documentados	e los procesos de TI	procedimentarse las buenas prácticas en sus guías de implementación	procedimentarse en el caso de estudio	
	Establece formas de inventario de activos de información	Lo define de manera general como requisito de un SGSI	Lo define de manera general para los objetivos de control y controles del dominio de clasificación de activos	Si lo establece	Se ha establecido una clasificación en la definición de la política relacionada con clasificación de activos
	Clasifican los activos de información	No lo considera	Lo considera de manera general en el dominio de clasificación de activos	Si lo establece	Se ha establecido una clasificación en la definición de la política relacionada con clasificación de activos
	Define una lista de controles.	No lo considera	Establece un listado completo por cada dominio y objetivo de control	Si lo establece	Se han identificado los controles específicos por cada activo en el caso de estudio.
	Está establecido un proceso de gestión para la continuidad de negocio	Lo establece como un requisito de mejoramiento continuo (ciclo PDCA)	No lo considera	Si lo establece	Se ha elaborado un procedimiento ara continuidad de procesos tomando como referencia las normas de la SBS y otras normas relacionadas con la continuidad de negocio

	Define programas de concienciación en seguridad	Lo define de manera general como requisito de un SGSI	Lo considera de manera general en el dominio Gestión de RRHH	No lo establece	Se establece como recomendación
	Identifica acciones correctivas y preventivas	Lo establece como un requisito de mejoramiento continuo (ciclo PDCA)	Lo considera de manera general en el dominio continuo de negocio	No lo establece como un proceso, pero si como controles específicos.	Se han establecido como controles específicos.
	Define mecanismos para medir la efectividad de los controles de las políticas de seguridad de la información	No define métricas, pero si establece que deben realizarse su seguimiento	No define métricas, pero si establece que deben realizarse su seguimiento	No se ha definido métricas, pero si se ha considerado evaluación de brechas	Se considera un proceso de evaluación de brechas

CUADRO COMPARATIVO ENTRE EL MODELO MAGERIT Y EL PLAN PROPUESTO PARA LA GESTIÓN DE RIESGOS DE TI

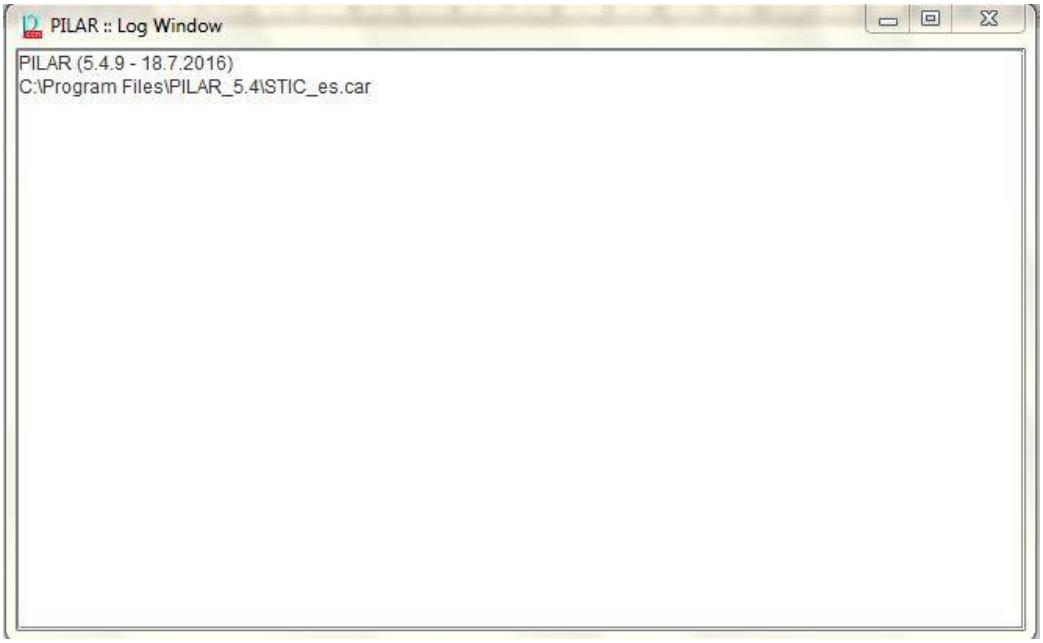
Criterio	Modelo MagerIT	Plan Propuesto	Aporte de la investigación
Determinación de los activos de TI que requieren protección	Define un listado general clasificado por tipo de activo	Utiliza la propuesta de MagerIT	Adecúa la propuesta de MagerIT para el caso de estudio
Identificación de vulnerabilidades	No lo considera	Si lo considera	Se ha elaborado un listado de vulnerabilidades y se considera su evaluación cuantitativa y cualitativa
Identificación de amenazas	Define un listado general clasificado por tipo de activo	Utiliza la propuesta de MagerIT	Adecúa la propuesta de MagerIT para el caso de estudio
Estimación del impacto de las amenazas	Establece criterios de evaluación cuantitativa y cualitativa para el impacto de las amenazas	Sí se realiza	Se ha elaborado criterios de valoración propios para el impacto de las amenazas en base a la evaluación de las características de la información: C, I, D
Estimación de la probabilidad de ocurrencia de las amenazas	Establece criterios de evaluación cuantitativa y cualitativa para la probabilidad de ocurrencia de las amenazas	Sí se realiza	Se ha elaborado criterios de valoración propios para la probabilidad de ocurrencia de las amenazas en base a la evaluación de las características de la información: C, I, D
Cálculo y clasificación del nivel de riesgo intrínseco.	Determina una forma de valoración del riesgo intrínseco	Sí se realiza	Se ha definido una fórmula básica para el cálculo del nivel de riesgo intrínseco
Implementación de las medidas de seguridad	Determina de manera general formas de implementación de salvaguardas	Sí se realiza	Se ha elaborado un listado de aplicabilidad de controles ajustado al caso de estudio
Identificación de la estrategia de	Determina de manera general las estrategias	Sí se realiza	Adecúa la propuesta de MagerIT para el caso de estudio

implementación de controles	de implementación de controles.		
Cálculo y clasificación de la brecha de seguridad: nivel de riesgo residual	Determina una forma de valoración del riesgo residual	Sí se realiza	Se ha elaborado una matriz de riesgos específica para realizar seguimiento de la efectividad de los controles en base a evaluación de brechas
Evaluación del grado de madurez de los controles	No lo contempla	Sí se realiza	Se ha elaborado una matriz de riesgos específica para evaluación del grado de madurez de los controles en base a un criterio propio

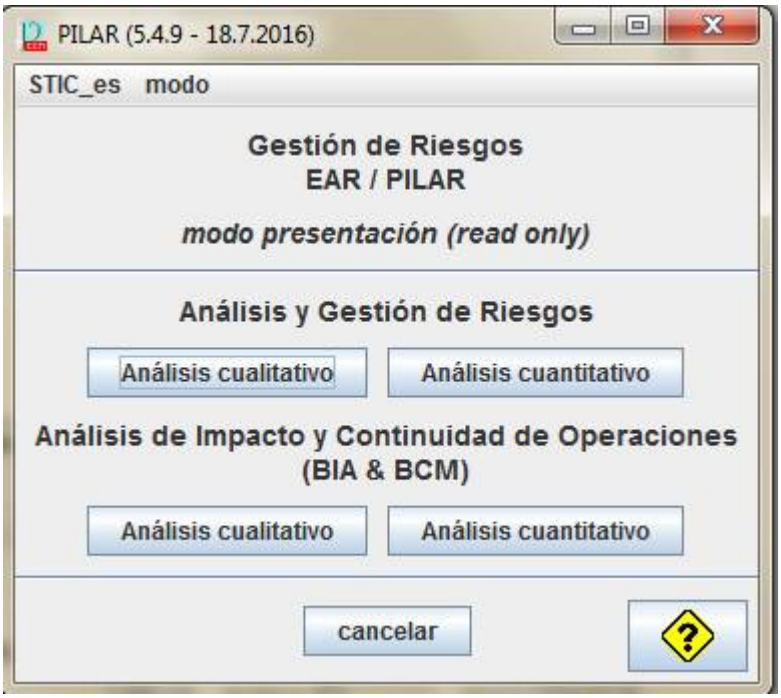
ANEXO N° 10

PROCESO DE INSTALACIÓN DEL SOFTWARE EAR/PILAR - ANÁLISIS Y GESTIÓN DE RIESGOS

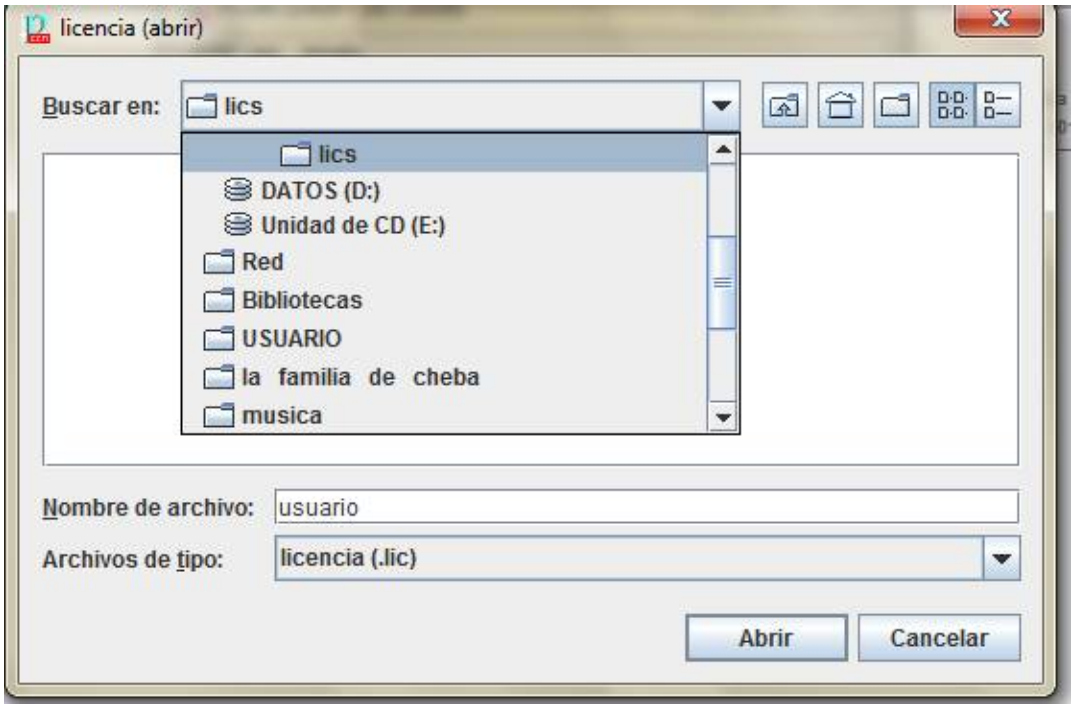
1. PILAR solicita un fichero CAR



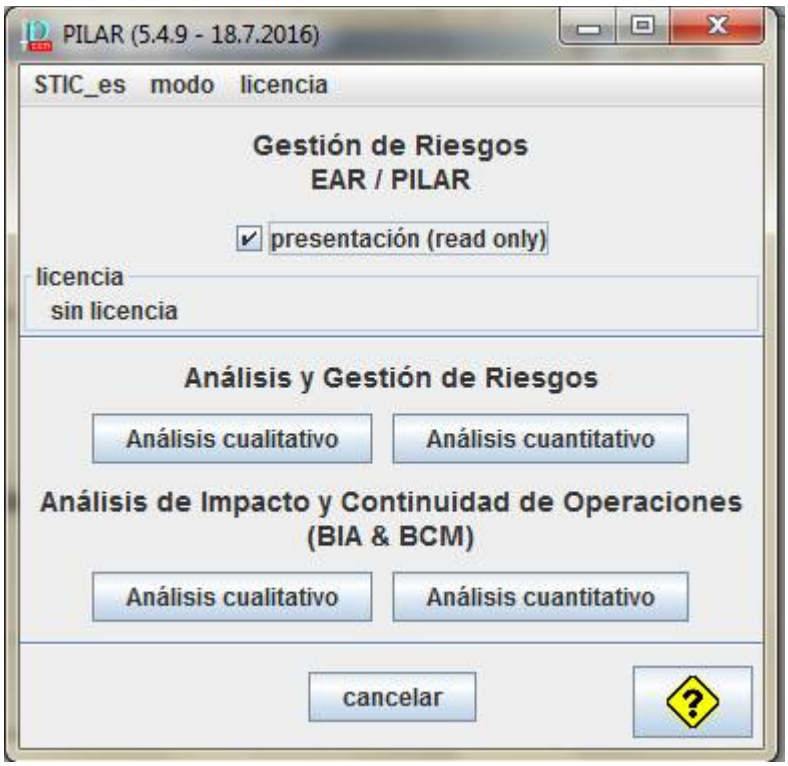
2. Cambie a modo de trabajo



3. PILAR solicita un fichero LIC



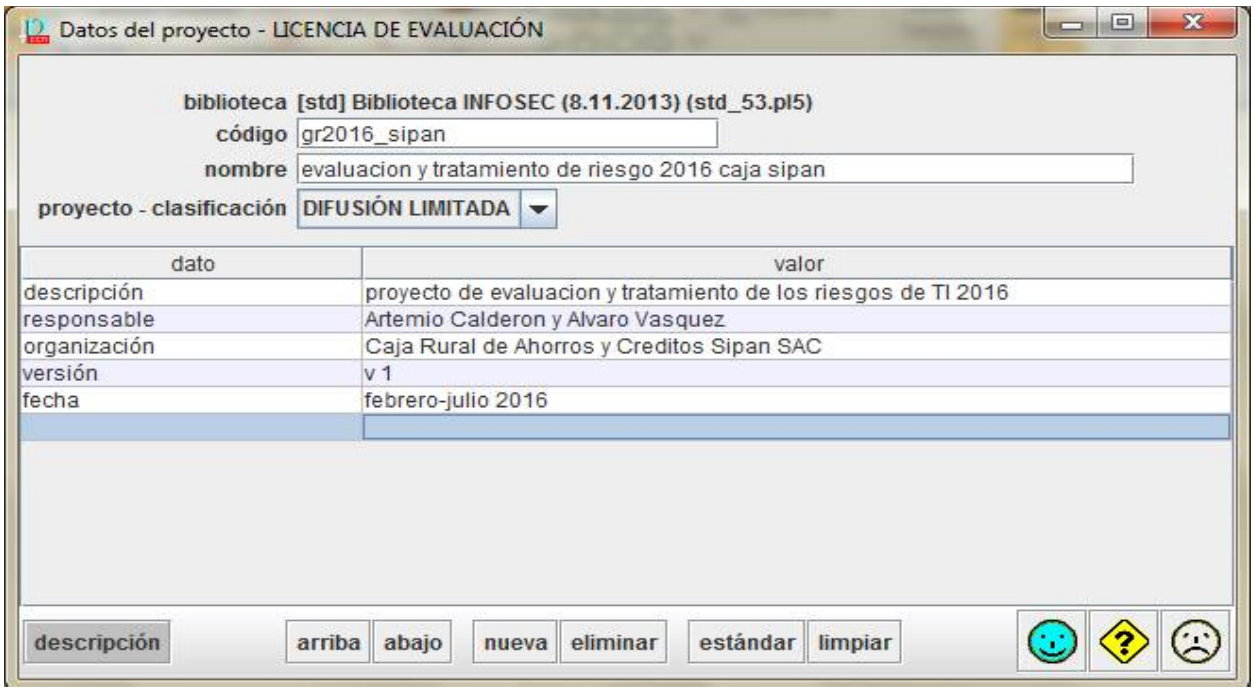
4. Listo para trabajar



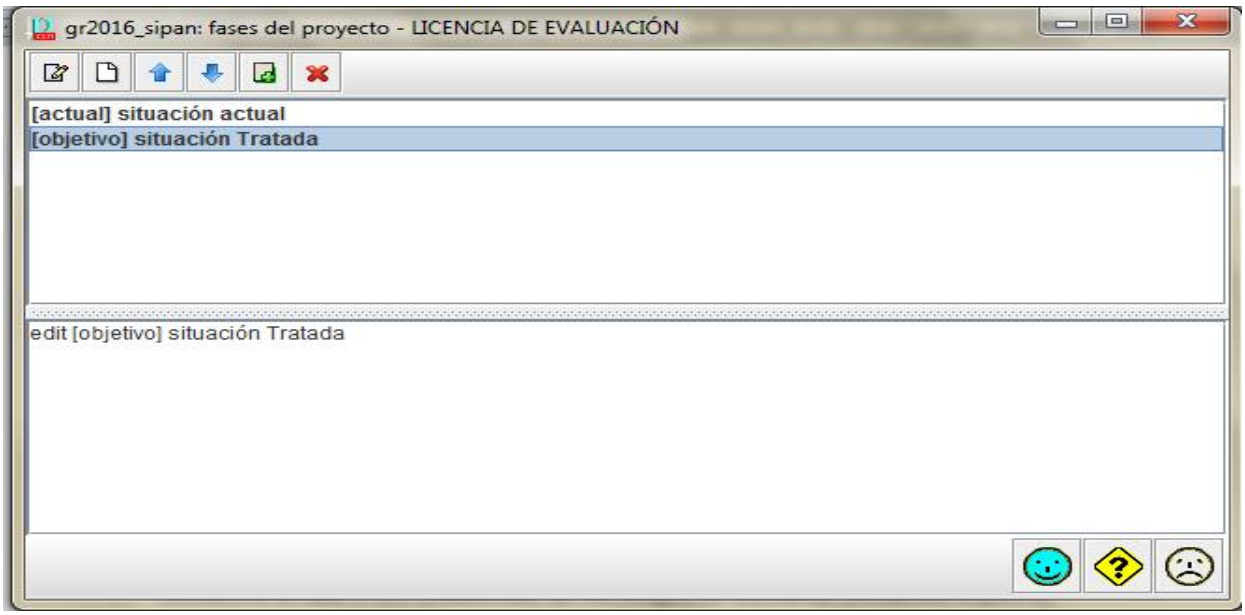
ANEXO N° 11

PANTALLAS DE SIMULACIÓN DEL PLAN DE GESTIÓN DE RIESGOS DE TI PROPUESTO EN EL SOFTWARE PILAR (5.4.9 - 18.7.2016)

1. Pantalla N° 01: Registro de datos del proyecto de gestión de riesgos de TI



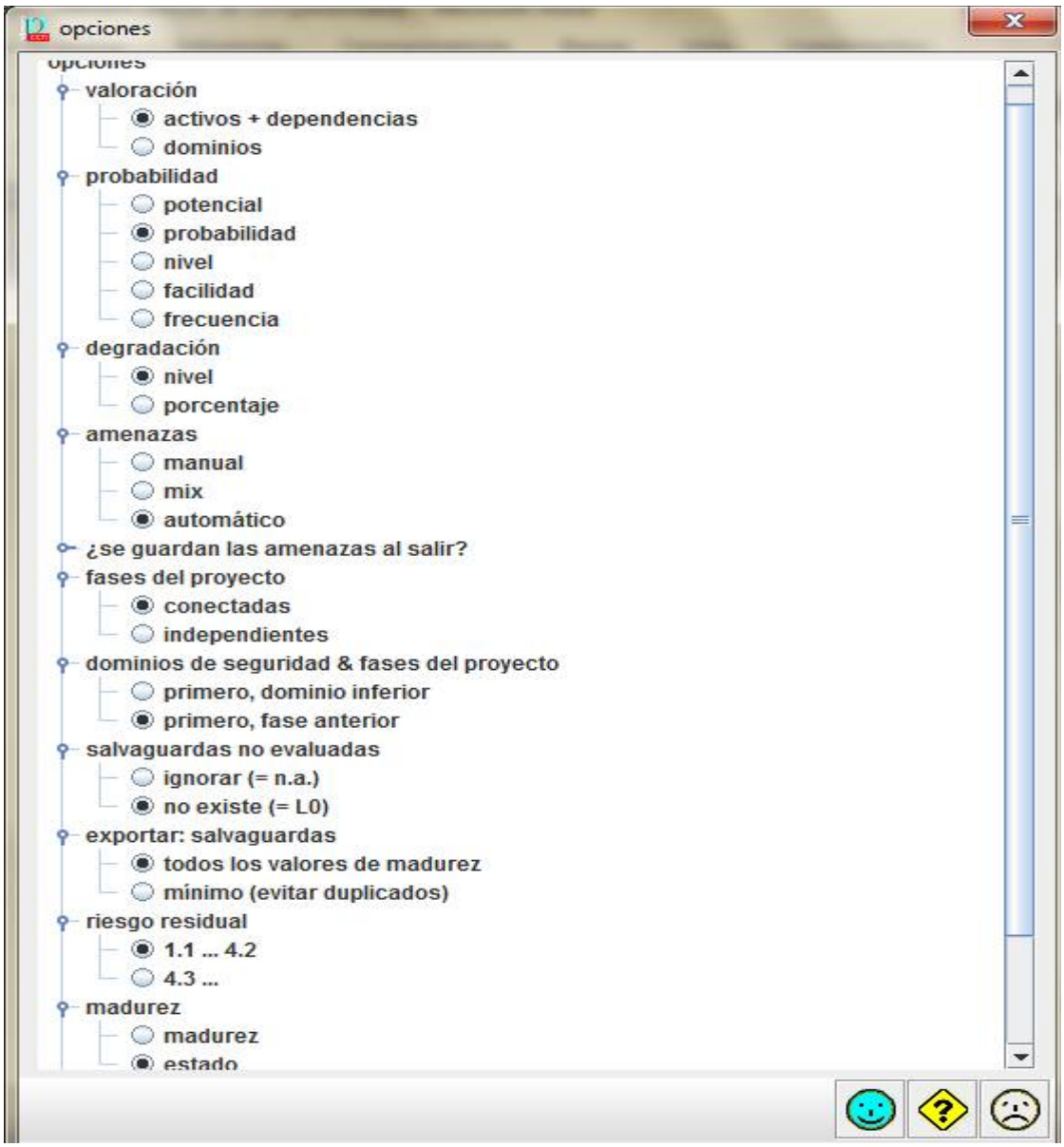
2. Pantalla N° 02: Definición de las fases del PGR-TI en el proyecto



Observación:

Se definieron las dos etapas que se desarrollaron en el PGR-TI: (1) Evaluación de riesgos de TI (Situación actual) y (2) Tratamiento de los riesgos no tolerables (Situación tratada)

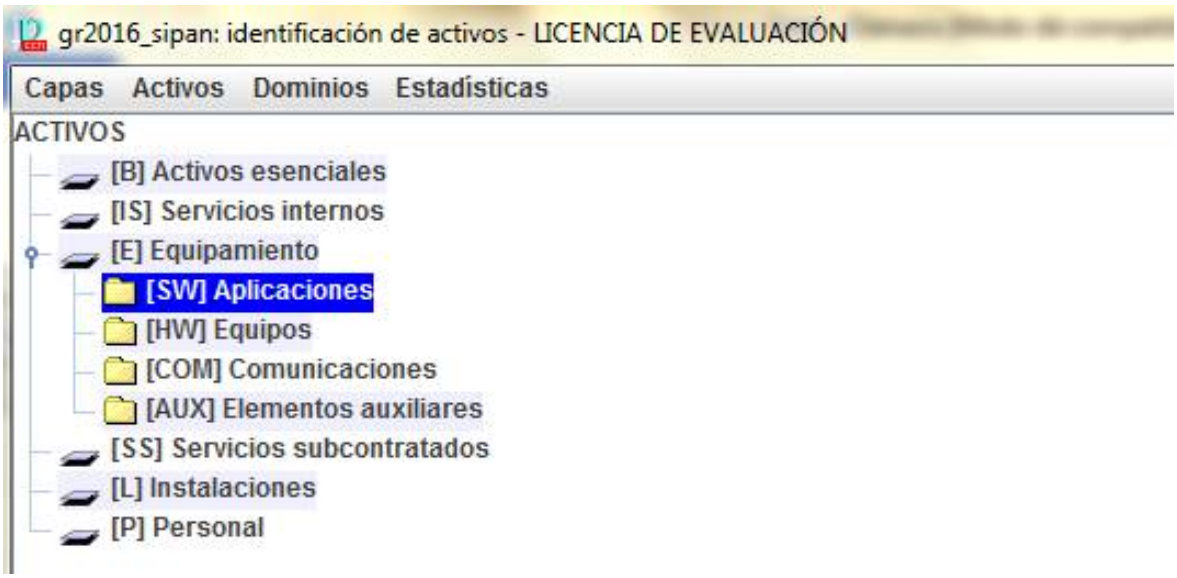
3. Pantalla N° 03: Ajuste de opciones y preferencias al PGR-TI



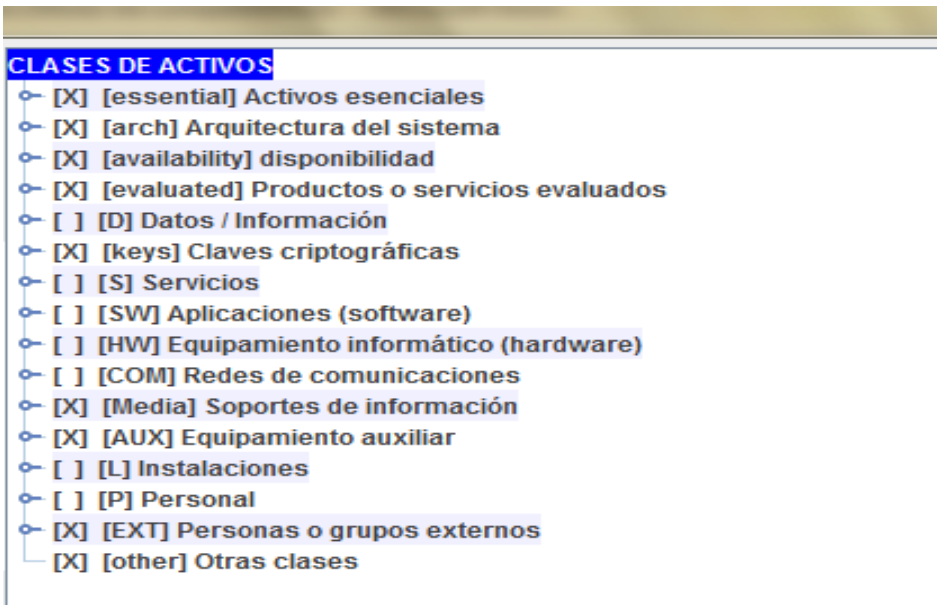
Observación: Este formulario permitió ajustar algunos parámetros del software PILAR para adecuarlo a la forma como evalúa el PGR-TI. Así tenemos:

- La valoración de los activos se debe realizar independientemente, uno por uno
- La probabilidad de ocurrencia debe ser evaluada en una escala de probabilidades: desde Raro a Casi Seguro
- Las fases del proyecto deben estar interconectadas para poder comparar el PGR-TI y lo que propone el software PILAR
- Los niveles de riesgos o degradación deben medirse en una escala por niveles, desde Muy Bajo hasta Muy Alto

4. Pantalla N° 04: Catálogo de Activos de PILAR



5. Pantalla N° 05: Catálogo de Tipos de Activos de PILAR



Observación: Estos formularios permiten seleccionar los activos de TI y sus correspondientes tipos, que serán considerados en la evaluación de riesgos. El software Pilar utiliza un catálogo de activos de TI según la Metodología MagerIT, el mismo que se utilizó en el trabajo de tesis (**Ver anexo N° 03**).

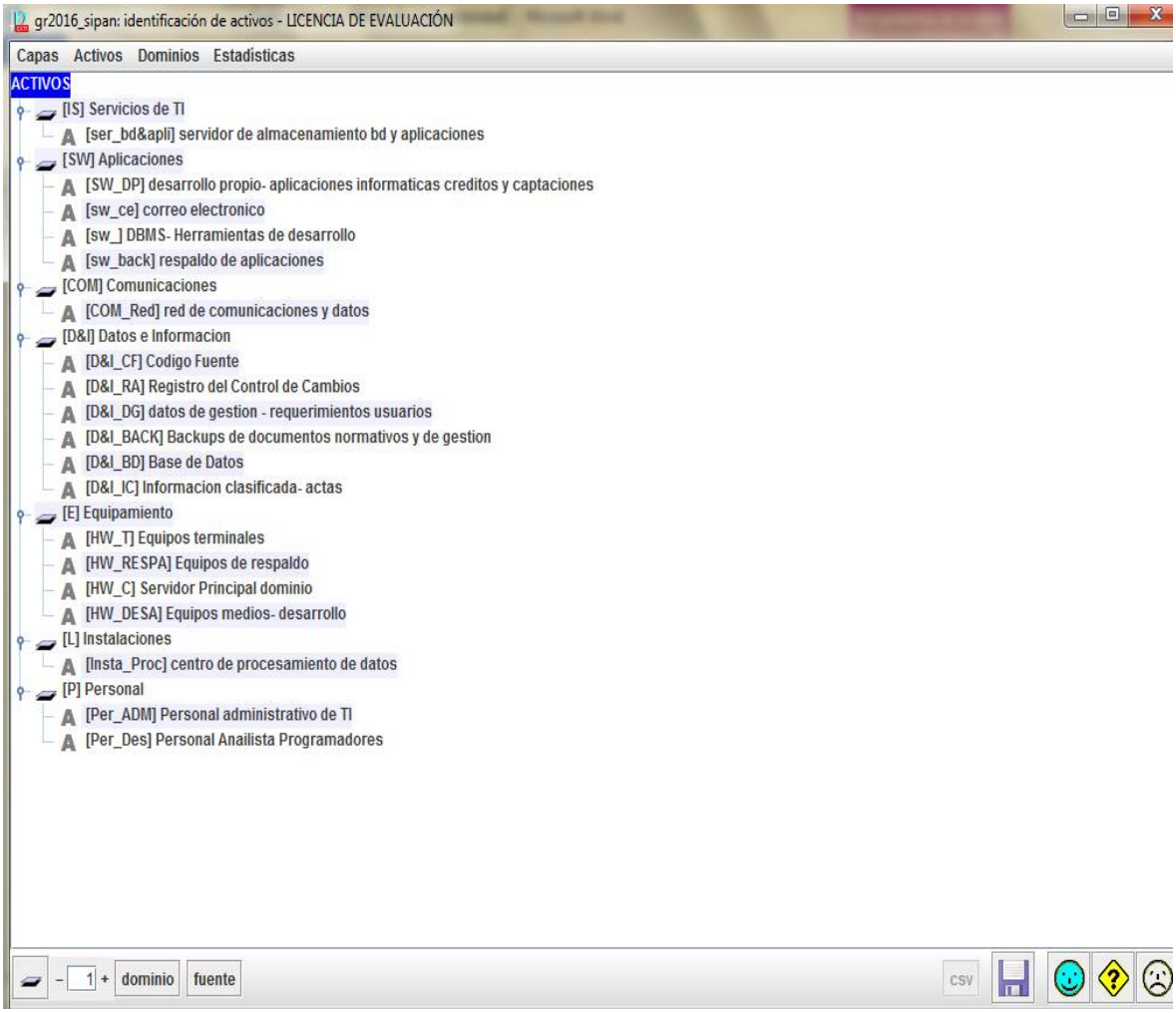
En la pantalla N° 05, los Tipos de Activos de TI que no se consideraron en la evaluación, ya han sido deshabilitados para el caso.

Los activos de TI y sus correspondientes tipos, seleccionados para el caso, de acuerdo al Catálogo de MagerIT, se muestran en la tabla siguiente:

Tipo de Activo		**Sub Clasificación**		**Descripción de aclaración**
[info]	Información	[clasificado]	Datos clasificados	Archivos de Actas de conformidad
[dato]	Datos o documentos	[files]	ficheros	Bases de Datos
		[backup]	copias de respaldo	Backups de documentos normativos y de gestión
		[int]	datos de gestión interna	Archivo de requerimientos informáticos (físico).
		[log]	registro de actividad	Registros de control de cambios de las aplicaciones.
		[source]	código fuente	Código fuente de las aplicaciones
[serv]	Servicios	[file]	Almacenamiento de ficheros.	Servidor principal de base de datos y aplicaciones
[sw]	Aplicaciones	[prp]	Desarrollo propio (in house)	Aplicaciones informáticas de créditos y captaciones
		[email_client]	Cliente de correo electrónico	Correo electrónico institucional.
		[dbms]	Sistema de gestión de bases de datos.	Herramientas de desarrollo.
		[backup]	Sistema de backup.	Backups o respaldos de desarrollo y mantenimiento.
		[host]	Grandes equipos	Servidor principal de dominio.
		[mid]	Equipos medios	Equipos de cómputo del Área de Desarrollo
		[pc]	Informática personal	Equipos de cómputo terminales de ventanilla y analistas de créditos

		[backup]	Equipamiento de respaldo	Backups de base de datos.
[com]	Comunicaciones	[X25]	X25 (red de datos)	Red de comunicaciones
[Inmueb]	Instalaciones	[data]	Cuarto de procesamiento de datos	Sala de servidores o Centro de Procesamiento Central
[pers]	Personal	[adm]	Administradores de sistemas.	Personal de área de TI.
		[des]	Desarrolladores / programadores.	Analistas de sistemas (Responsables de la implementación de requerimientos)

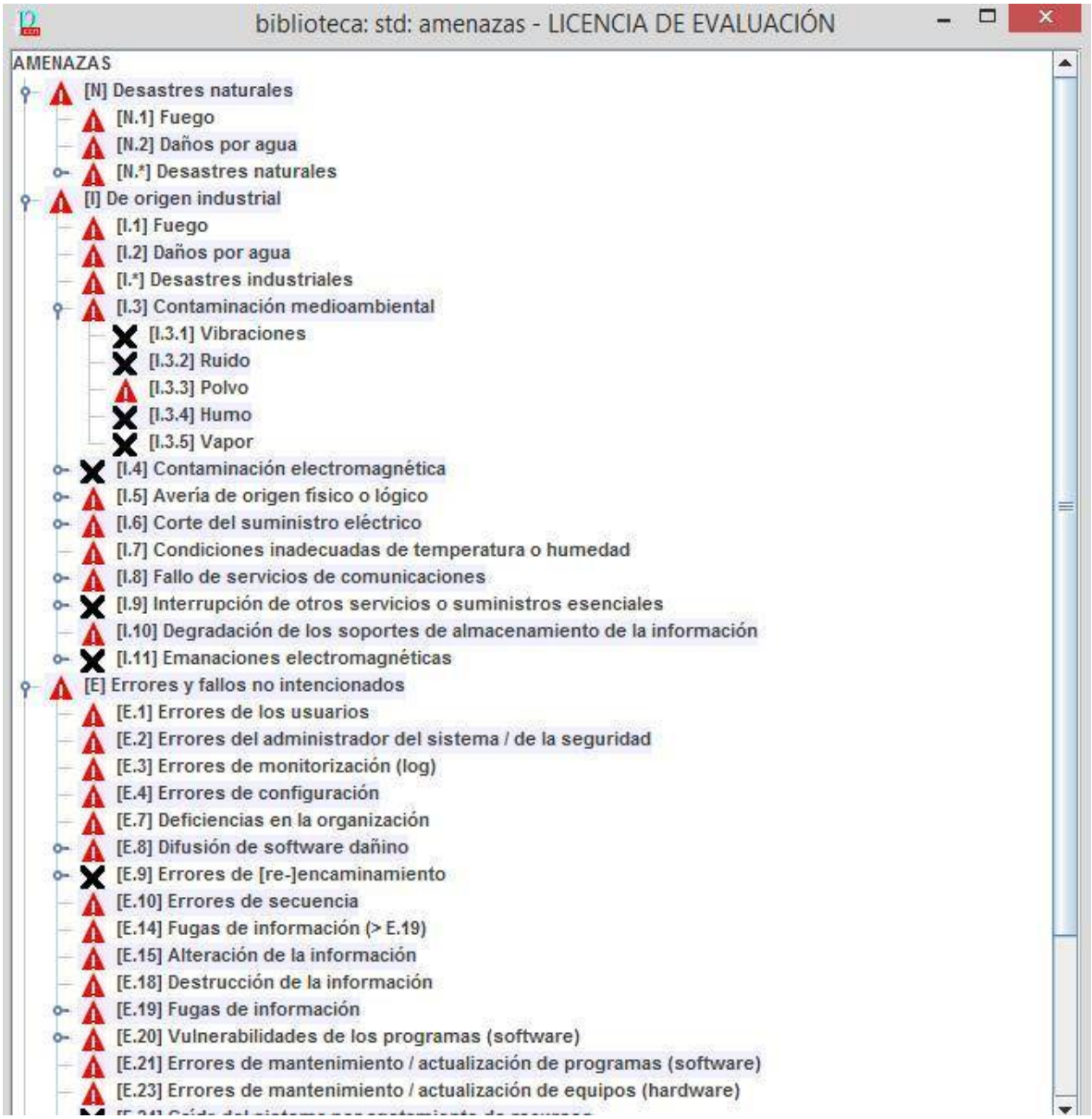
6. Pantalla N° 06: Catálogo de Activos de TI definidos para el caso (personalizados)



Observación: Este formulario muestra el resultado del catálogo de Activos de TI que serán

evaluados. Esta ajustado y personalizado para el caso de estudio de la Caja Sipán.

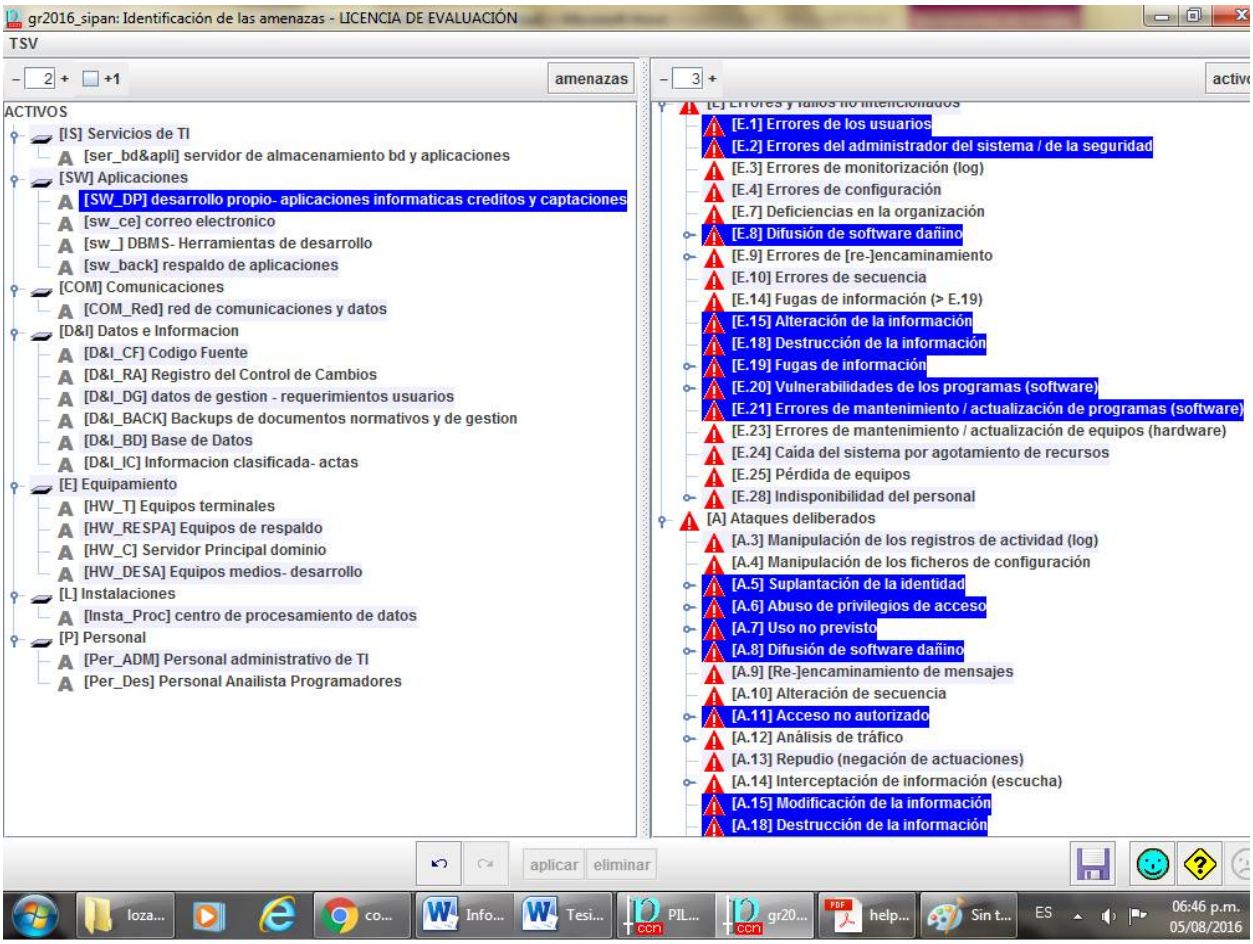
7. Pantalla N° 07: Catálogo de Amenazas de TI seleccionados para el caso de estudio



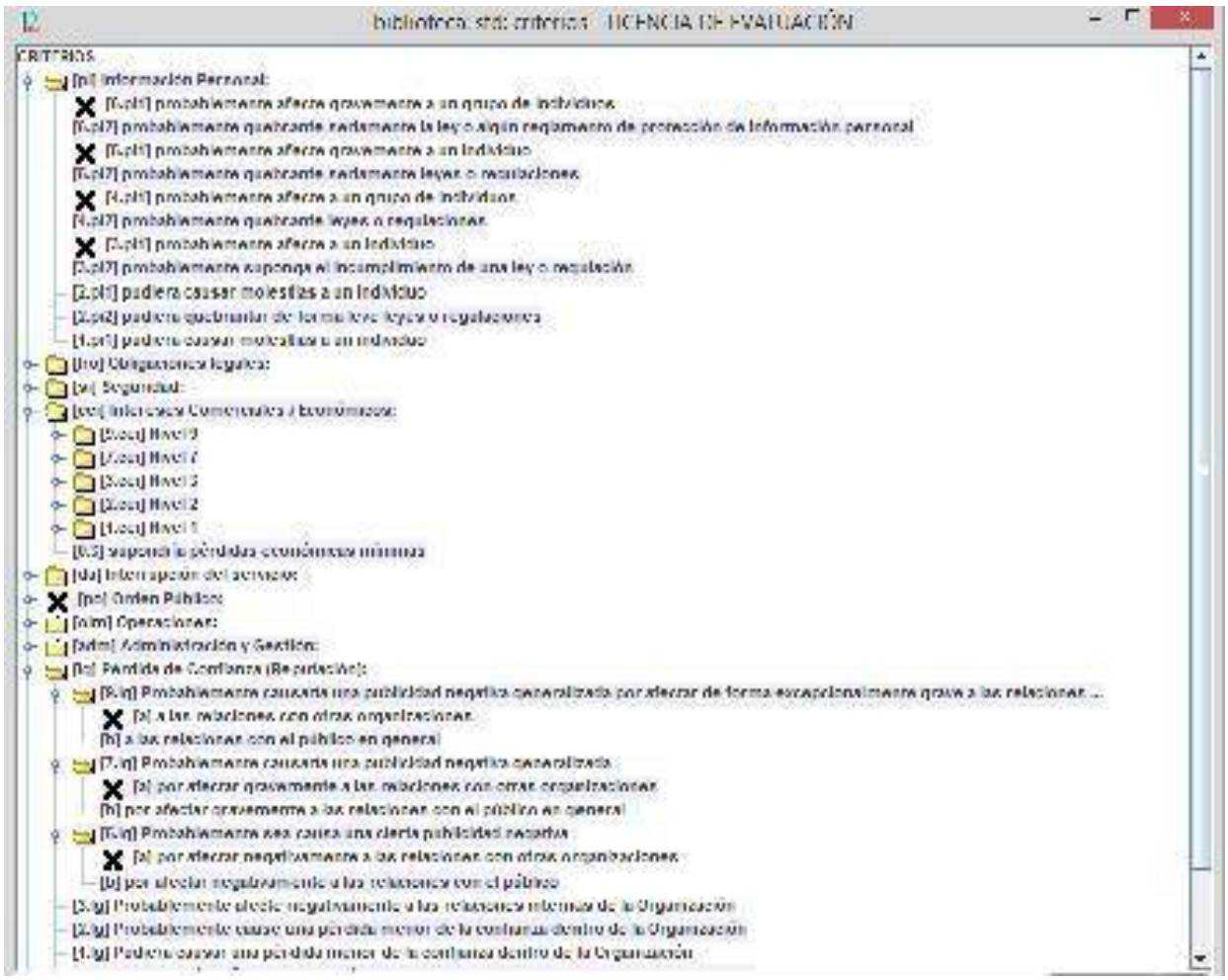
Observación: Este formulario muestra el resultado de la selección de las amenazas que se utilizaron para la evaluación de los niveles de riesgos de los activos de TI en el software PILAR.

Importante: Debe recordarse que en el trabajo de tesis se utilizó este mismo catálogo de la metodología Magerit, pero ajustado y personalizado al caso de estudio, por tanto sus definiciones no necesariamente son las mismas.

8. Pantalla N° 08: Selección Automática de Amenazas de TI para cada Activo de TI, según el software PILAR



9. Pantalla N° 09: Criterios de valoración de los activos de TI seleccionados para el caso de estudio

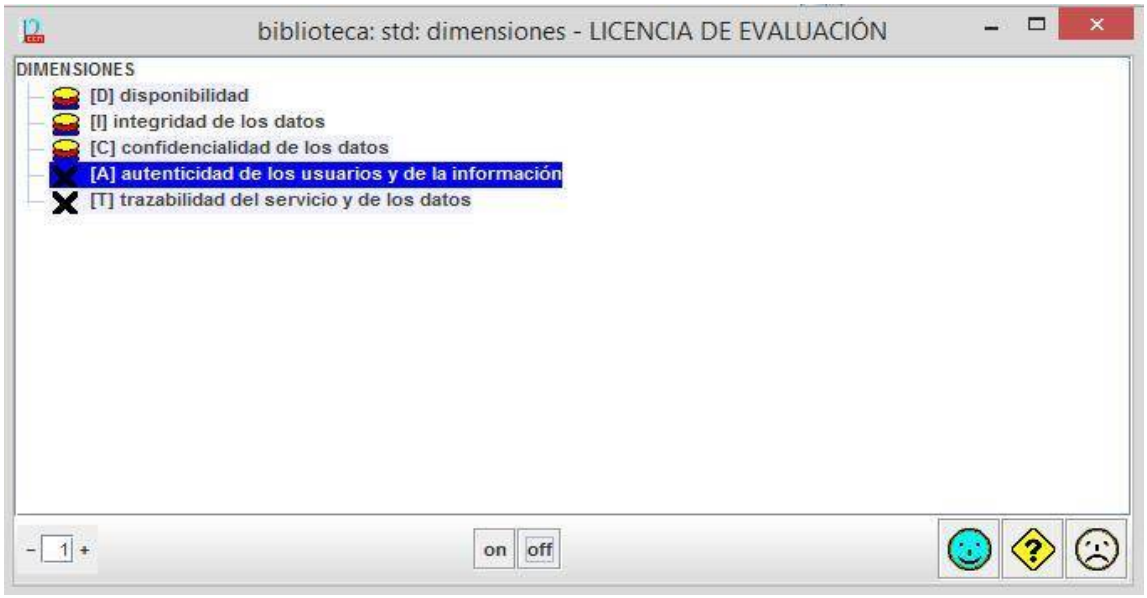


Observación: Este formulario muestra el resultado de la selección de criterios de valoración de activos de TI que se utilizaron para la evaluación de los niveles de riesgos de los activos de TI en el software PILAR.

Importante: Debe recordarse que en el trabajo de tesis NO se utilizó este catálogo de la metodología MagerIT. Se utilizó una escala de valoración de 5 puntos, desde Muy Baja afectación hasta Muy Alta Afectación. Sin embargo, para esta evaluación del software, se tuvo que considerar este catálogo (ajustado al caso de estudio), para comparar sus resultados con el PGR-TI propuesto. Los criterios de valoración que utiliza el software PILAR es el mismo del catálogo de la metodología MagerIT, es decir, utiliza una escala de 10 puntos.

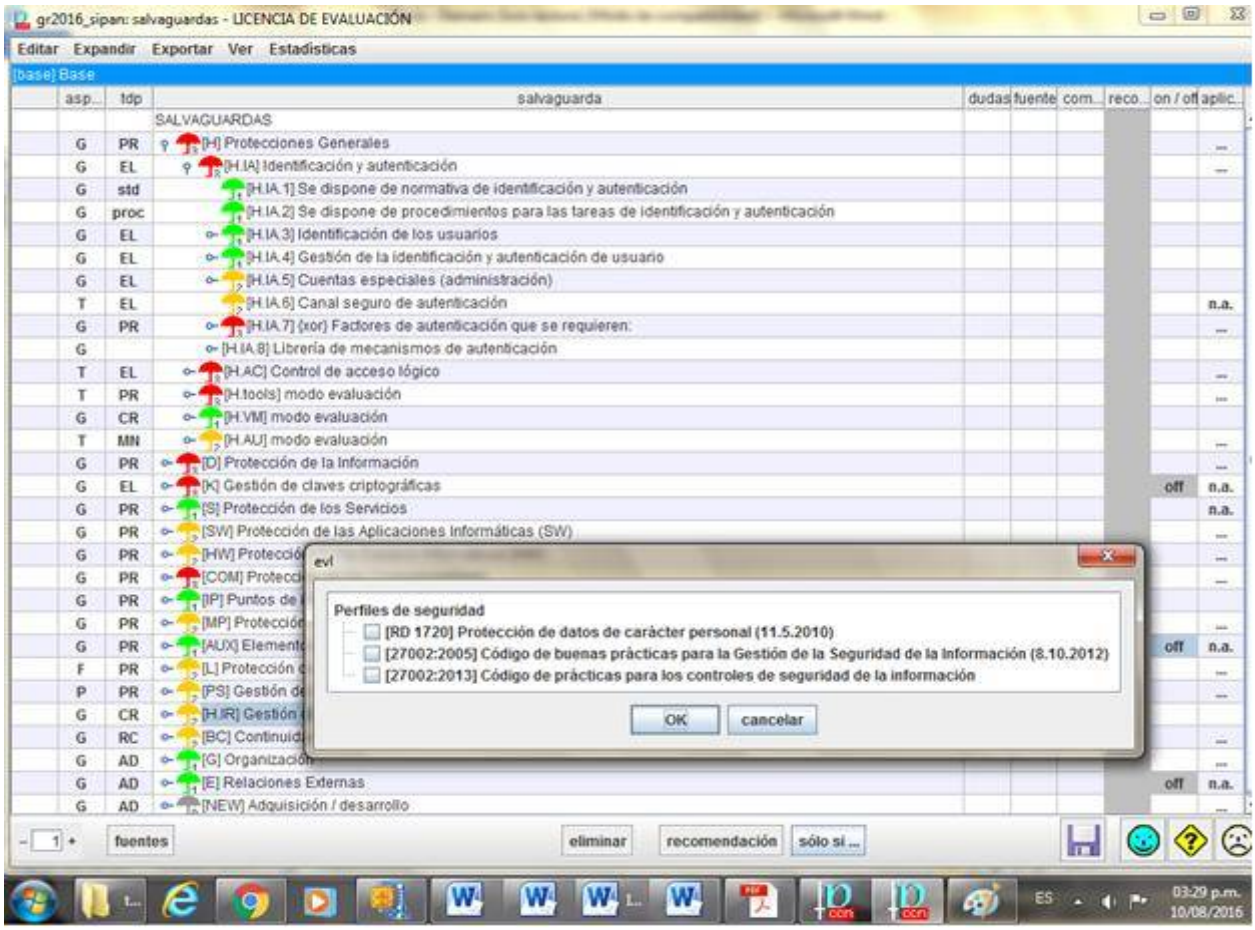
Por tanto, consideraremos cada par de puntos del software PILAR equivalente a un punto en el PGR-TI propuesto.

10. Pantalla N° 10: Dimensiones de evaluación de los activos de TI seleccionados para el caso de estudio.



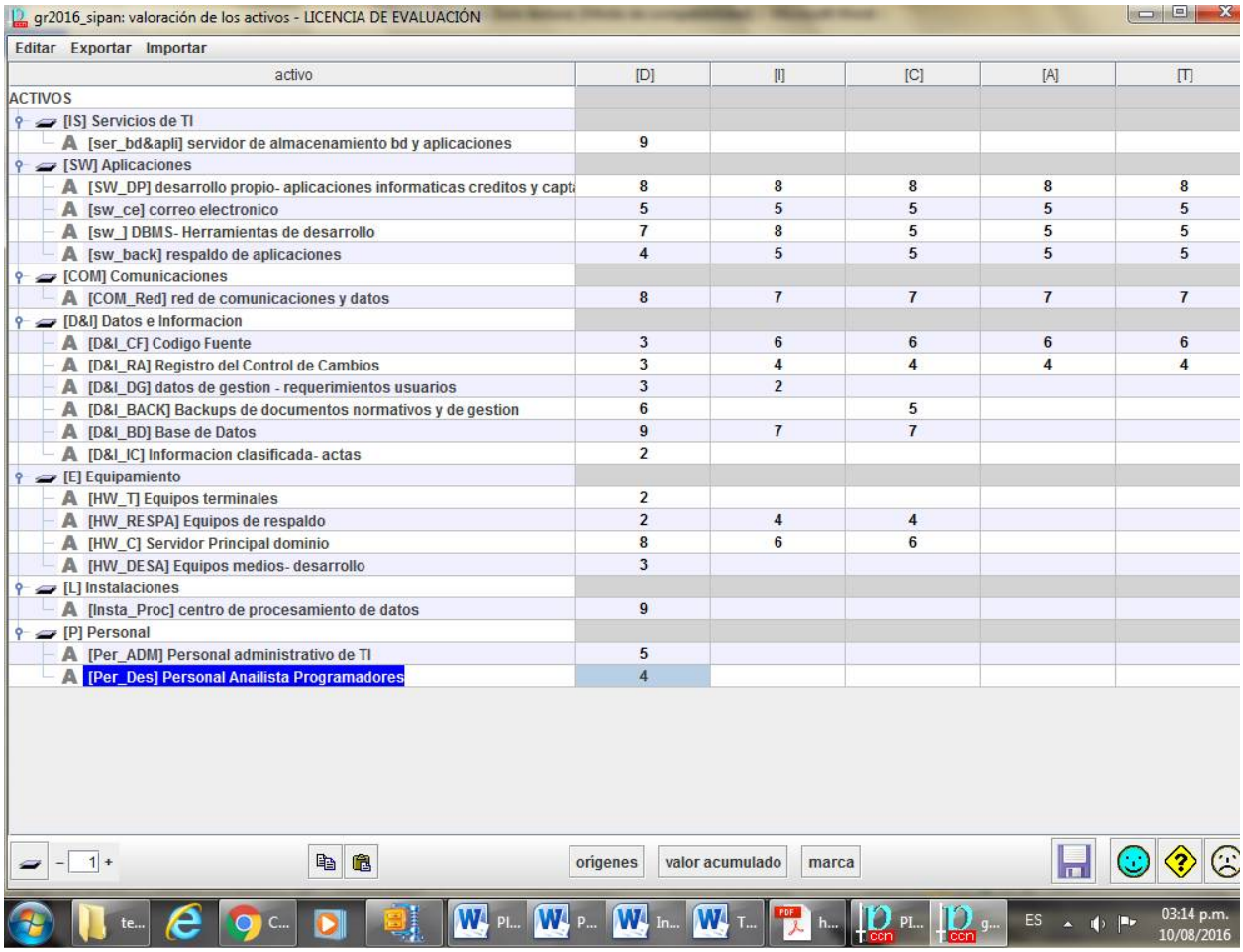
Observación: Sólo se seleccionaron las dimensiones de seguridad siguientes: Disponibilidad [D], Integridad [I] y Confidencialidad [C], para guardar concordancia con el trabajo de tesis y porque son las dimensiones exigidas por la SBS para ser evaluadas en los Sistemas de Gestión de Riesgos.

11. Pantalla N° 11: Selección de salvaguardas según perfil de seguridad



Observación: Las salvaguardas (controles) que se utilizaron en la evaluación del caso de estudio, fueron los que corresponden a los marcos de referencia ISO 27002:2005 (ISO 17799) e ISO 27002:2013.

12. Pantalla N° 12: Valoración de Activos de TI definidos para el caso de estudio



activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[IS] Servicios de TI					
[ser_bd&apli] servidor de almacenamiento bd y aplicaciones	9				
[SW] Aplicaciones					
[SW_DP] desarrollo propio- aplicaciones informaticas creditos y capt	8	8	8	8	8
[sw_ce] correo electronico	5	5	5	5	5
[sw_] DBMS- Herramientas de desarrollo	7	8	5	5	5
[sw_back] respaldo de aplicaciones	4	5	5	5	5
[COM] Comunicaciones					
[COM_Red] red de comunicaciones y datos	8	7	7	7	7
[D&I] Datos e Informacion					
[D&I_CF] Codigo Fuente	3	6	6	6	6
[D&I_RA] Registro del Control de Cambios	3	4	4	4	4
[D&I_DG] datos de gestion - requerimientos usuarios	3	2			
[D&I_BACK] Backups de documentos normativos y de gestion	6		5		
[D&I_BD] Base de Datos	9	7	7		
[D&I_IC] Informacion clasificada- actas	2				
[E] Equipamiento					
[HW_T] Equipos terminales	2				
[HW_RESPA] Equipos de respaldo	2	4	4		
[HW_C] Servidor Principal dominio	8	6	6		
[HW_DESA] Equipos medios- desarrollo	3				
[L] Instalaciones					
[Insta_Proc] centro de procesamiento de datos	9				
[P] Personal					
[Per_ADM] Personal administrativo de TI	5				
[Per_Des] Personal Anailista Programadores	4				

Observación: Para las valoraciones de los activos de TI se utilizaron los criterios de valoración de MAGERIT en base a 10 puntos. Por tanto, consideraremos cada par de puntos del software PILAR equivalente a un punto en el PGR -TI propuesto.

ANEXO N° 12

Tabla de costos para trabajar con el flujo de caja:

Nro.	Descripción	Dirección electrónica	COTIZACIÓN	Riesgo	Control
01	DIPLOMADO WINDOWS 2016 SERVER - ADMINISTRACION DE REDES CON CERTIFICACION OFICIAL MICROSOFT	https://auladiser.com/diplomado-windows-server-admon-de-redes-727	S/.2400.00	R3	C4
02	CONTRATAR OFICIAL DE SEGURIDAD DE LA INFORMACIÓN, esto permitirá controlar mejor los riesgos que se detallan en el cuadro de análisis de costo beneficio. CONTRATAR 02 TÉCNICOS DE SEGURIDAD DE LA INFORMACIÓNTÉCNICO EN SOPORTE INFORMÁTICO Y COMUNICACIONES, esto permitirá controlar mejor los riesgos que se detallan en el cuadro de gastos del análisis de costo beneficio, los	http://www.perucompras.gob.pe/userfiles/cms/convocatoria/perfil/detalle_cas_009_2018_cod_03.pdf http://www.ana.gob.pe/sites/default/files/convocatoria/PROCESO%20CAS%20N%C2%B0%20024-2018-ANA_0.pdf	S/.9000.00 S/.7000.00	R6 R8 R19 R22	C10 C13 C14 C15 C43 C46

	técnicos ayudaran en las acciones al OFICIAL DE SEGURIDAD DE LA INFORMACIÓN			R25 R31 R36 R37 R63 R65	C47 C51 C62 C63 C64 C69 C70 C71 C112 C113 C114 C116

				R71	C117 C118 C124
03	Contratar servicio de Protección integral frente a todo tipo de riesgos y amenazas para la Caja de ahorro y Crédito Sipán SA	http://www.movistar.com.pe/negocio/internet-seguridad/seguridad/-/tab/seguridad-gestionada	S/. 600.00	R9 R10	C16 C17 C18
04	MODULO DE BATERIA EXTERNA Módulo de baterías externas de 192V 3U rack/torre para sistemas UPS Tripp Lite selectos Amplía la autonomía de Sistemas UPS ..	http://www.tiendadecomputoperu.com/estabilizadores-baterias-c-39_1143.html	S/3,720.00	R11	C19
05	Contratar servicios de control de pruebas de operatividad de los equipos eléctricos para evaluar su funcionamiento	https://lima-lima.olx.com.pe/memoria-o-protocolo-de-pruebas-de-operatividad-y-mantenimiento-	S/. 3,450.00	R11	C20 C21

	Contratar servicios para el diseño del plan de mantenimiento al sistema eléctrico.	de-equipos-de-seguridad-certific-por-ingelectricista-iid-993787506 Ing. ANDRÉS AVENDAÑO CABRERA Ingeniero Electricista Colegiado Habilitado Registro CIP N° 66634 Ex Inspector INDECI N° 225570483 – ITS TELEFONOS: … 429-9949 ,… 99712-3030			
06	Contratar el servicio de COPIAS DE SEGURIDAD EN LA NUBE, está orientado a pymes, autónomos y usuarios de portátil. Permite externalizar las copias de seguridad de forma automática y sencilla.	http://www.gadae.com/backup.html	S/. 1,260.00	R29 R74	C56 C57 C58 C59 C127

07	Licencia del SQL Server SQL Server 2017 Ideal para Rendimiento confiable y completo para satisfacer los requisitos de base de datos y de Business Intelligence más exigentes. Proporciona los niveles de servicio y el rendimiento más altos para las cargas de trabajo de nivel 1 Adquisición de un Servidor Intel Xeon Gold 6126 - 2.6 GHz - 12 núcleos Intel Xeon Gold 6126 - 2.6 GHz - 12 núcleos 24 hilos-19.25 MB caché-LGA3647 Socket-para ProLiant DL380 Gen10 para el Centro de Cómputo alterno.	https://www.microsoft.com/es-es/sql-server/sql-server-2017-pricing#CP_StickyNav_1 http://www.tiendadecomputoperu.com/servidores-servidores-c-31_214.html?page=3&sort=3a	S/. 46,617.00 S/.12,540.00	R29	C60
08	Impresión de los formatos de control de confidencialidad para todos los trabajadores de la Caja de Ahorro y Crédito SA, así como las políticas de escritorio y pantallas limpias.	https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/	S/.500.00	R38 R59	C72 C105