UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

Modelo de gestión de riesgos de TI de acuerdo con las exigencias de la SBS, basados en las ISO/IEC 27001, ISO/IEC 17799, Magerit para la Caja de Ahorro y Créditos SIPAN SA

TESIS PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS Y COMPUTACIÓN

DÁMARIS FERNÁNDEZ FERNÁNDEZ

Chiclayo 19 de Agosto del 2015

“MODELO DE GESTIÓN DE RIESGOS DE TI DE ACUERDO CON LAS EXIGENCIAS DE LA SBS, BASADOS EN LAS ISO/IEC 27001, ISO/IEC 17799, MAGERIT PARA LA CAJA DE AHORRO Y CRÉDITOS SIPAN SA”

POR:

DÁMARIS FERNÁNDEZ FERNÁNDEZ

Presentada a la Facultad de Ingeniería de la Universidad Católica Santo Toribio de Mogrovejo para optar el título de:
INGENIERO DE SISTEMAS Y COMPUTACIÓN

APROBADA POR EL JURADO INTEGRADO POR

_____
Ing. Ricardo David Imán Espinoza
PRESIDENTE

_____
Ing. Huilder Juanito Mera Montenegro
SECRETARIO

_____
Ing. Hugo Enrique Saavedra Sánchez
ASESOR

DEDICATORIA:

A Dios por haberme llenado de bendiciones y guiado en el camino para lograr mis objetivos a lo largo de mi Formación profesional.
A las dos personitas que más amo en el mundo, mis hijos: Brian y Dárikson, que son mi fuerza y motivo para seguir adelante.

Agradecimiento:

A Dios por haberme guiado por el camino de la verdad
y el día de hoy permitirme lograr uno de mis mayores objetivos.
A mi asesor Ing. Hugo Saavedra Sánchez, por haberme
brindado su tiempo, apoyo y guía ´permanente.
Y finalmente a todos los docentes que me brindaron
sus conocimientos a lo largo de mi carrera universitaria.

INDICE GENERAL

INDICE DE TABLAS

INDICE DE GRÁFICOS

RESUMEN

La gestión de los riesgos de TI, conjuntamente con la gestión de la continuidad de los procesos del negocio, se constituye en "herramientas" estratégicas para asegurar la efectividad y la eficacia de los Sistemas de Gestión de la Seguridad de la Información en una organización; así como en mecanismo esencial para obtener la información necesaria en la toma de decisiones relacionada con la inversión oportuna y adecuada en la implementación de los controles de TI.

La falta de una metodología y de un software adecuado que de soporte a la gestión de riesgos de TI en entidades financieras de nuestro medio, no solo a través de "buenas prácticas", si no también que se ajusten a las exigencias de la Superintendencia de Banca y Seguro en sus normativas Resolución S.B.S N° 2116 -2009 - Reglamento para la Gestión del Riesgo Operacional y Circular Nº G-105-2002 - Riesgos de tecnología de información, constituye la justificación del presente trabajo de tesis.

Con esta investigación se demostró que con un modelo de gestión de riesgos implementado, tomando como referencia a los estándares ISO/IEC 27001, ISO 17799 y la metodología MagerIT, se puede lograr mayor efectividad en el cálculo de los niveles de riesgos de los diferentes activos de TI en la etapa de evaluación de los riesgos; así como también en el tratamiento de éstos, a través de la implantación y seguimiento de los controles, siempre en concordancia y en cumplimiento con los requerimientos mínimos de la SBS para estos fines. Para ello se tomó como caso experimental, la CRAC Sipán SAC.

PALABRAS CLAVES

Proceso crítico, vulnerabilidad, amenaza, impacto, nivel de riesgo, apetito de riesgo, control, matriz de riesgo, riesgo residual.

ABSTRACT

Managing IT risk, together with the management of the continuity of business processes, constitutes strategic "tools" to ensure the effectiveness and efficiency of the Systems Management Information Security in an organization; and essential to obtain the necessary information in making decisions related to the timely and adequate investment in implementing IT controls mechanism.

The lack of an adequate methodology and software that supports the management of IT risk with financial institutions in our country, not only through "best practices", but also to meet the requirements of the Superintendent of banking and Insurance's norm SBS Resolution No. 2116 -2009 - Rules for the Operational Risk Management and Circular No. G-105-2002 - Risks of information Technology, is the rationale for this thesis.

This research showed that a model risk management implemented with reference to ISO / IEC 27001, ISO 17799 standards and MAGERIT methodology can achieve greater effectiveness in the calculation of risk levels of different assets IT at the stage of risk assessment; as well as in the treatment of these, through the implementation and monitoring of controls, always in accordance and in compliance with the minimum requirements of the SBS for these purposes. This was taken as a test case, the CRAC Sipan SAC.

KEYWORDS:
Critical process, vulnerability, threat, impact, risk level, risk appetite, control, risk matrix, residual risk.

I. INTRODUCCIÓN

La globalización en las entidades financieras, junto con los avances de la tecnología financiera están haciendo las actividades bancarias, y en consecuencia, sus perfiles de riesgo, cada vez más complejos.

Según estudios de investigación realizados por la 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.

La Caja Rural de Ahorros y Créditos Sipán S.A.; es una sociedad anónima de derecho privado, con 602 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. Para cumplir con las exigencias de la SBS, en relación a la gestión de TI, de la seguridad y de riesgos de TI, se tiene que; sus dos principales procesos críticos son: créditos y captaciones o depósitos. El proceso de crédito, consiste en recopilar y revisar toda la información de los solicitantes de créditos mediante visitas domiciliarias o centro de negocio del cliente para otorgar créditos, normándolos y administrándolo correctamente. Otro punto de dicho proceso es evaluar y controlar las garantías que tiene que ser aceptada por la empresa para luego realizar el desembolso de los créditos aprobados. El proceso de captaciones o depósitos, consiste en la apertura de cuentas de ahorro, cuentas a plazo u órdenes de pago, así como también las operaciones realizables con dichas cuentas solicitados por los clientes

Orgánicamente cuenta con un Área de TI, con su jefatura, la Unidad Desarrollo, la Unidad de Producción y Soporte y la Unidad de Organización y Métodos. En la Unidad de Desarrollo laboran seis (06) analistas programadores. En la Unidad de Producción laboran dos (02) especialistas en infraestructura, redes y comunicaciones. En la Unidad de O&M trabaja una (01) persona.

Cuenta con una Unidad de Riesgos encargada de la evaluación y tratamiento de los riesgos -entre los cuales están los relacionados con TI- y de la planificación de la continuidad del negocio. Tiene una jefatura, un (01) oficial de seguridad de la información y dos (02) analistas de riesgos operativos.

La planificación del servicio y actividades de TI están expuestas en:

- Plan Estratégico Institucional Caja Sipán 2011 – 2014, aprobado por el Directorio: Sesión Nº 028 – 2011 de fecha 18.11.2011 (de ahora en adelante PEI)
- Plan Estratégico de Tecnologías de Información 2012 - 2016 (de ahora en adelante PETI)
- Plan Operativo del Área de Tecnología de la Información y Organización y Métodos – 2013 (de ahora en adelante POTI).

De acuerdo a los informes sobre la gestión de riesgos de TI, emitidos trimestralmente por la unidad de riesgos, los procedimientos actuales para evaluar y tratar los riesgos relacionados con TI evidencian lo siguiente:

- Existen problemas para definir los riesgos de TI de acuerdo a las categorías de información exigidas por la SBS
- Los procedimientos para la evaluación de riesgos de TI no están integrados al modelo en la gestión de riesgos corporativo
- Bajo nivel de concientización del personal en relación a la aplicabilidad de los controles de TI
- No se está cumpliendo totalmente con los requisitos y exigencias mínimas en la normativa de la SBS, en relación a la gestión de riesgos
- No existe un procedimiento adecuado para identificar y evaluar las amenazas vulnerabilidades, impactos, frecuencias
- No es efectivo el procedimiento para el monitoreo de las actividades de gestión de riesgos de TI
- Demoras en los procedimientos de recuperación de incidentes
- Bajo nivel de aplicabilidad del proceso para la evaluar los riesgos de TI actualmente
- Incoherencias en los resultados obtenidos con respecto a los cálculos actuales para determinar los niveles de riesgos inherentes de TI
- Falta de un procedimiento para determinar los controles adecuados, según los niveles de exposición a los riesgos y para el seguimiento de las brechas de seguridad
- El modelo actual no permite obtener toda la información requerida para elaborar los informes a la SBS en relación a la gestión de riesgos de TI
- Se está obteniendo información poco fiable para la toma de decisiones en relación a las inversiones de los controles de seguridad

Por lo tanto el problema central de la investigación es:
¿De qué manera se puede mejorar la gestión de riesgos de TI de acuerdo con las exigencias de la SBS, para la Caja de ahorros y Créditos SIPAN SA?

En consecuencia la hipótesis planteada fue: **Con la implementación de un modelo de gestión de riesgos TI de acuerdo con las exigencias de la SBS, basados en las ISO/IEC 27001, ISO 17799, Magerit se mejorará la gestión de riesgos relacionados con TI para la Caja de Ahorro y Créditos SIPAN SA**.

Expuesto que la presente tesis tenemos como objetivo general el Mejorar la gestión de riesgos de TI en la caja de ahorro y crédito SIPAN cumpliendo con las exigencias de la SBS, por medio de la implementación de un modelo de gestión de riesgos basados en las ISO/IEC 27001, ISO 17799, Magerit.

Objetivos Específicos:

- Mejorar el procedimiento para definir los riesgos de TI de acuerdo a las categorías de información exigidas por la SBS
- Lograr el alineamiento de los procedimientos de evaluación y tratamiento de riesgos de TI al modelo en la gestión de riesgos corporativo
- Mejorar el nivel de concientización del personal en relación a la aplicabilidad de los controles de TI
- Lograr el cumpliendo total de los requisitos y exigencias mínimas de la normativa de la SBS, en relación a la gestión de riesgos
- Mejorar el procedimiento para identificar y evaluar las amenazas vulnerabilidades, impactos, frecuencias
- Mejorar el procedimiento para el monitoreo de las actividades de gestión de riesgos de TI
- Optimizar los procedimientos de recuperación de incidentes para mejorar los tiempos de su registro y tratamiento
- Elevar el nivel de aplicabilidad del proceso para la evaluar los riesgos de TI actualmente
- Mejorar la efectividad de los resultados obtenidos con respecto a los cálculos actuales para determinar los niveles de riesgos inherentes de TI
- Mejorar la efectividad de los procedimientos para determinar los controles adecuados y para el seguimiento de las brechas de seguridad
- Obtener toda la información requerida para elaborar los informes a la SBS en relación a la gestión de riesgos de TI
- Obtener información fiable para la toma de decisiones en relación a las inversiones de los controles de seguridad

La presente tesis de justifica, en lo tecnológico, ya que con la sistematización de gestión de riesgos de TI/SI en base a estándares internacionales como la ISO/IEC 27001, ISO 17799, MagerIT, ha logrado mejorar la eficacia en la evaluación y tratamiento de riesgos, también nos ha permitido ahorrar tiempo en la detección oportuna de amenazas, además de una mejor administración de información estableciendo así un orden en la organización de acuerdo a controles establecidos y así hemos tomado las decisiones a tiempo, y han sido parametrizable y flexible, ajustado a las características de la organización y sobre todo manejable, todo esto con el fin de asegurar continuidad en el negocio y la disminución de daños en la Caja Rural de Ahorro y Crédito Sipán SAC.

En lo social, porque la propuesta metodológica permitió, a través de un conjunto de normas y procedimientos, administrar los incidentes de seguridad reduciendo los impactos negativos en los procesos, en las caídas de los activos tecnológicos, por tanto pérdida de imagen institucional.

En lo económico, porque esta investigación no sólo se limitó a obtener un enfoque respecto a los avances acerca del uso de metodologías para resolver o atenuar los

efectos de los diversos problemas o necesidades que puedan presentarse en la gestión de seguridad de la información, gestión de continuidad del negocio y gestión de riesgos operativos de TI, sino que, el modelo también nos brindó la suficiente información para que la dirección pueda tomar decisiones acertadas acerca de la "inversión" correcta en la implantación de controles como mecanismo de salvaguarda de sus activos tecnológicos, reduciendo así, gastos innecesarios en salvaguardas que no tienen efecto positivo o en controles que posteriormente no se pueden monitorear y maximizar los beneficios de la inversión en tecnología.

En lo científico, esta investigación permitió aportar una propuesta metodológica y un aporte a la ciencia ya que nos ayudará a demostrar que a través de la implementación de una herramienta automatizada basada en estándares internacionales mejoró la eficacia de la evaluación y tratamiento de los riesgos relacionados con TI/SI de una organización.

También está sirviendo de ayuda y orientación para realizar investigaciones posteriores que tengan como finalidad la Sistematización de la Gestión de Riesgos de seguridad de la información.

II. MARCO TEÓRICO

2.1. Antecedentes

Aguayo Yépez, Andrés Gustavo. Diciembre de 2011. Adaptación de un marco metodológico para la medición del riesgo operativo generado por puntos vulnerables de tecnologías de información con un enfoque de auditoria basado en riesgos en el ecuador. Tesis Maestría. Universidad Andina Simón Bolívar, Sede Ecuador.

Este estudio tiene como finalidad convertirse en un aporte cualitativo y técnico sobre las debilidades detectadas a través de la identificación de puntos vulnerables en las tecnologías de información y aquellas que hacen referencia específicamente a la gestión tecnológica como tal, que incrementa actualmente el riesgo operativo en las instituciones financieras, utilizando como guía de trabajo un enfoque de riesgos conforme lo requiere la norma, la legislación ecuatoriana y las mejores prácticas establecidas por el Comité de Basilea.

Porque está basada en normas exigidas por la SBS de su país, los estándares aplicables y aceptados para mejorar las prácticas de control y seguridad de las tecnologías de información propuestos por COBIT.

Ampuero Chang, Carlos Enrique. Noviembre de 2011. Diseño de un sistema de gestión de seguridad de información para una compañía de seguros. Tesis Pre-Grado. Universidad Católica - Lima-Perú.

En esta tesis el autor asevera que para poder desarrollar un SGSI es necesario tomar como base, la ISO 27001, ya que este estándar fue confeccionado para proveer un modelo para el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora de un SGSI. En el caso del desarrollo de la tesis, se utilizó tanto Cobit 4.1 como el estándar ISO/IEC 27001:2005 y el ISO/IEC 27002:2005 para armar el marco de control y poder definir los controles a seguir para el aseguramiento de la información de la compañía y el cumplimiento de la regulación impuesta por la SBS.

La relación con la investigación está en la implantación de un SGSI adecuado a las exigencias de la SBS, ente controlador de entidades financieras tipo cajas rurales.

Avalos Ruiz, Carlos. 22 de marzo del 2012. Análisis, diseño e implementación del sistema de Riesgo operacional para entidades financieras. Universidad Católica del Perú

Este proyecto pretende apoyar e impulsar el cumplimiento normativo dispuesto por la SBS y AFP’s en cuanto a la Gestión del Riesgo Operacional. La herramienta, permitirá a las entidades financieras cumplir de manera más rápida y eficiente los requisitos para alcanzar el método del estándar alternativo, lo cual le permitirá reducir el requerimiento patrimonial a causa del Riesgo Operacional. La misma que constituye en un motor de cambio para ayudarle a integrar la gestión del Riesgo Operacional en las diferentes áreas de su institución.

La relación con la investigación está en la implantación de un SGSI adecuado a las exigencias de la SBS, ente controlador de entidades financieras Y AFP.

2.2. Bases Teórico Científicas

2.2.1. La Superintendencia de Banca, Seguros y AFPs (SBS)

Las Cajas Rurales son empresas que gestionan la información a través de sistemas informáticos, por lo tanto ésta debe ser protegida ya que es un activo muy importante.

Para realizar esta propuesta la norma ISO 27001:2005 tiene como finalidad proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), entendiéndose por seguridad de la información "la preservación de la confidencialidad, integridad, y disponibilidad de la información" (ISO/IEC 17799:2005). La confidencialidad, que permite que tan solo accedan a la información personas autorizadas, la disponibilidad que hace que la información esté dispuesta en cualquier momento especialmente cuando los usuarios autorizados lo necesitan y la integridad, nos permite tener una información completa, exacta y valida.

El ente encargado de regular y supervisar las Cajas Rurales de Ahorro y Crédito es la Superintendencia de Banca y Seguro (SBS) que es un organismo que tiene dos tareas primordiales la regulación y la supervisión, también brinda mayor confianza y protección a los intereses del público.

La regulación porque establece reglas para que las empresas supervisadas puedan cumplirlas y la supervisión que consiste en verificar el cumplimiento de las normas, políticas y prácticas por parte de las empresas supervisadas.

Para la implementación de controles y de las medidas reactivas, correctivas y preventivas en la gestión de la información, que aseguren conseguir las tres características básicas de la seguridad de la información, las cajas rurales, frente a las exigencias de la SBS, deberán de aplicar o utilizar un marco metodológico que esté basado en estándares como: ISO/IEC 17799 y la ISO/IEC 27001 y otras.

La SBS ha determinado algunas normas específicas para tres ámbitos diferentes:

- Gestión de seguridad de la información: Circular N° G-140-2009 sobre Gestión de Seguridad de la Información, que establece criterios para gestionar la seguridad de la información y toma como referencia estándares internacionales como el ISO 17799 e ISO 27001.

- Gestión de continuidad del negocio: Circular N° G-139-2009 sobre Gestión de Continuidad del Negocio, que establece criterios para gestionar la continuidad de negocio financiero que forma parte de la gestión de riesgo operacional que tienen que enfrentar las empresas que son supervisadas por la SBS, las cuales toman como referencia los estándares internacionales como el BS-25999.

- Riesgos operativos de TI: Circular N° G-105-2002 sobre Riesgos de Tecnología de Información, que establece criterios para identificar y gestionar los riesgos relacionados con las tecnologías de información.

2.2.2. Definición de Riesgo de TI

De acuerdo a ISACA (2009) en los Lineamientos para la Gestión de Seguridad de TI publicadas por la Organización Internacional de Estandarización (ISO) en su (ISO/IEC PDTR 13335−1), riesgo es 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.

2.2.2.1. Proceso de Gestión de Riesgo

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

Sobre los procesos, se construyen controles con el objetivo de reducir la frecuencia de las amenazas o limitar el daño causado y llevar el nivel de riesgo a un nivel aceptable por la organización.

Dependiendo del tipo de riesgo, se puede optar por:

- Evitar el riesgo: por ejemplo eliminando el activo.
- Mitigar el riesgo: implementando controles para reducir la probabilidad y el impacto.
- Transferir el riesgo: por ejemplo contratando un seguro con cobertura para ese riesgo.
- Aceptar el riesgo: reconociendo que el riesgo existe y monitorizarlo.

Una vez que los controles han sido aplicados, el nivel de riesgo que queda es el riesgo residual. Como se establece en los Requerimientos de los Sistemas de Gestión de Seguridad de la

Información en la norma ISO 27001; la Dirección debe establecer el nivel de riesgo aceptable para la organización. Los riesgos que excedan de ese nivel deben ser reducidos.

2.2.2.2. Nivel de 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.

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

- La Política organizacional.
- Sensibilidad y criticidad de los activos involucrados.
- Niveles aceptables de los posibles impactos.
- Rentabilidad de la implementación.

2.2.3. Normas ISO relacionadas con la Gestión de Riesgos de TI

Las Normas ISO, ofrecen una visión ordenada y metodológica para implantar un programa de seguridad de la información, de forma tal de tener una guía que contemple todos los aspectos sobre el tema y que es producto de los representantes internacionales con mayores fortalezas en la disciplina.

El ISO 17799, al definirse como una guía en la implementación del sistema de administración de la seguridad de la información, se orienta a preservar los principios de confidencialidad, integridad y disponibilidad de la información. Estos principios en la protección de los activos de información constituyen las normas básicas deseables en cualquier organización, sean instituciones de gobierno, educativas e investigación. Es importante entender los principios y objetivos que dan vida al ISO 17799, así como los beneficios que cualquier organización, incluyendo las instituciones públicas, privadas y ambientes educativos pueden adquirir al implementarlo en sus prácticas de seguridad de la información.

El ISO 27001:2005, establece un Sistema de Gestión de la Seguridad de la Información (SGSI) conforme con el objetivo de hacer sostenibles en el tiempo todas las iniciativas en materia de seguridad de la información.

Todas las metodologías y estándares que respalden la gestión de riesgos de TI/SI, se aplican eficientemente si se ejecutan sus herramientas de manera automatizada, pero en la actualidad en nuestro mercado no existen o son pocos aplicables por sus costos elevados.

Por lo tanto, se hace necesario implementar un marco metodológico adecuado para la gestión de riesgos operativos relacionados con TI en la Caja Rural de Ahorro y Crédito Sipán SAC, que se ajuste a las exigencias de la SBS.

2.2.4. Norma ISO/IEC 27001

Hoy por hoy el mundo de la seguridad se debate en dos posturas de instituciones muy respetables, las cuales han regido el mundo de las normas internacionales en por muchos años, cada uno en diferentes lugares del mundo; y cada uno con una aproximación diferente. 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.

Lo primero que debemos aclarar es la procedencia de las dos organizaciones la ISO es bien conocida en el mundo como la organización que se encarga de fijar las normas aceptadas en Europa y en buena parte del mundo. Por su parte en USA, su contraparte en la materia es el NIST. Cada una tiene una postura frente al manejo de la seguridad informática que a lo largo de este artículo daremos a conocer para que el lector pueda tener una opinión informada al respecto.

Ante la necesidad de fijar un estándar en la industria la ISO adapto el estándar ingles que había sido promulgado con anterioridad el BS7799, que había tomado una gran fuerza como documento base en seguridad informática, documento el que poseía en su momento la versiones 7799-1 código de prácticas para la administración de seguridad en informática. Este documento es una guía general para encargados de seguridad en corporaciones Cuando fue publicado el estándar vigente a diciembre del 2001 servía como guía de implementación, pero no explica particularidades de los sistemas ni su implementación particular.

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 norma responde a la aplicación del modelo PDCA (Plan-Do-Check-Act) de mejora continua también existente en otras normas. La aplicación del proceso PDCA en el SGSI conforma un modelo de gestión de riesgos que guía la estrategia de “Corporate Governance”, incluyendo la gestión de riesgos de negocios. […] bajo el esquema común del modelo PDCA, la ISO 27001 también ofrece un interesante alineamiento con otras normas también de sistemas de gestión, como la ISO 9001 de Calidad y la ISO 14001 de Medio Ambiente, lo que se traduce en reducción de esfuerzos y costos en una implementación integrada.

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 o corrupción 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.
- Continuidad en las operaciones del negocio tras incidentes de gravedad.
- 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 los tópicos de 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 comercio electrónico.
- Aporta grandes beneficios para los bancos que requieren reducir riesgos operacionales, introducido por el Nuevo Acuerdo de Capitales Basilea II.
- Es consistente con lo establecido en regulaciones como la Ley Sarbanes-Oxley.

2.2.5. Norma ISO/IEC 17799

Tiene su origen en la norma BS7799-2 donde se detallan las especificaciones para la administración de seguridad en informática. Es una guía en la implementación de seguridad en organizaciones.

Según ISACA (2009), normativas como ISO/IEC 17799 asisten en la implantación y especialmente en la gerencia de día-a-día para enfrentar la proliferación de comunicación y discontinuidad de tecnología. Es por esta razón que componentes de esquemas como ISO asisten en la realización de seguridad tanto financieras como de red informática.

Una vez implantada la misma propicia mejoras concurrente con los avances en tecnología y proliferación de comunicación. La vulnerabilidad de sistemas es una situación que cambia a diario, no es una situación de semanas o meses, es de días u horas.

Para implantar ISO/IEC 17799 se requiere capacitar al personal no necesariamente y únicamente en aspectos tecnológicos pero en el trabajo de equipo y asegurar un avance del sistema de gerencia concurrente con la realidad tecnológica y comunicación. Esta capacitación incluye bases fundamentales de gerencia contemporánea incluyendo riesgos desde análisis de vulnerabilidad hasta mitigación o "Disaster Recovery".

En una secuencia lógica, los objetivos de cada dominio propuesto en la normativa ISO/IEC 17799 son:

1. Política de la Seguridad
   - Proporcionar a la dirección o gerencia la ayuda para la seguridad de la información.

2. Organización de la Seguridad
   - Manejar seguridad de la información dentro de la compañía.
   - Mantener la seguridad de los recursos de la organización, del tratamiento de la información y de los activos de la información alcanzados por terceros.
   - Mantener la seguridad de la información cuando el tratamiento de la información ha sido responsabilidad de un outsourcing (organización externa).

3. Seguridad del Personal
   - Reducir riesgos de error, hurto, fraude o el uso erróneo por parte del recurso humano.
   - Asegurarse de que los operadores estén enterados de amenazas y se preocupen de la seguridad de la información, y que estén equipados para utilizar la política corporativa de seguridad en el curso de su trabajo normal.
   - Reducir al mínimo el daño de incidentes y de mal funcionamiento de la seguridad y aprender de tales incidentes.

4. Clasificación y control del activo
   - Mantener la protección apropiada de activos corporativos y asegurarse de que los activos de la información reciben un nivel apropiado de protección.

5. Control de Acceso del Sistema
   - Controlar el acceso a la información.
   - Prevenir el acceso desautorizado a los sistemas de información.
   - Asegurar la protección de servicios network.
   - Prevenir el acceso desautorizado a los computadores.
   - Detectar actividades no autorizadas.
   - Asegurar la información al usar recursos móviles, el computador y servicios de telecomunicaciones de una red

6. Seguridad física y ambiental
   - Prevenir el acceso a personas no autorizadas a la información, que pudieran ocasionar daños o interferencia.
   - Prevenir la pérdida o daño en los activos y causaran interrupción a las actividades económicas.
   - Prevenir el hurto recursos con información y un mal tratamiento de ellos.

7. Desarrollo y Mantenimiento del Sistema
   - Asegurar la construcción de sistemas operacionales.
   - Prevenir la pérdida, modificación o el uso erróneo de los datos en sistemas o aplicaciones.
   - Proteger el secreto, la autenticidad y la integridad de la información.
   - Asegurar que los proyectos y actividades de ayuda se conduzcan de una manera correcta.

- Mantener la seguridad del software del sistema y de los datos de la aplicación.

8. Administración del Procesador y de la Red (Conectividad)
   - Asegurar la operación correcta y segura de los recursos que realizan tratamiento de información.
   - Reducir al mínimo el riesgo de fallas de los sistemas.
   - Proteger la integridad lógica del software y de la información.
   - Mantener la integridad, disponibilidad del tratamiento y de la comunicación de la información.
   - Asegurar y salvaguardar la información en redes y la protección de la infraestructura que se utiliza.
   - Prevenir las interrupciones de las actividades económicas y daños a los activos.
   - Prevenir la pérdida, modificación o el uso erróneo de la información intercambiada entre las organizaciones.

9. Hojas de operación (planning) de la Continuidad del Negocio
   - Evitar interrupciones a las actividades económicas y a los procesos críticos del negocio, evaluando los efectos de incidentes o de desastres importantes.

10. Conformidad
    - Maximizar la eficacia y reducir al mínimo la interferencia externa a los procesos o sistemas.
    - Evitar la ambigüedad de cualquier obligación criminal o civil, estatutos reguladores o contractuales que tengan relación con cualquier requisito de seguridad.
    - Asegurar la conformidad entre sistemas de seguridad y políticas o estándares de la organización.

2.2.6. Metodología de Gestión de Riesgo de TI

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 TI son:

2.2.6.1. Estimación de Riesgos

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.

2.2.6.2. Identificación de Riesgos

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 TI 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.

2.2.6.3. Análisis de Riesgos

Una vez hayan identificado los riesgos en la planificación, el paso siguiente es analizarlos para determinar su impacto, tomando así las posibles alternativas de solución. La explicación de Análisis de riesgos se extenderá posteriormente.

2.2.6.4. 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.

2.2.6.5. 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.

2.2.6.6. 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.

2.2.6.7. 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

2.2.6.8. 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.

2.2.6.9. 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.

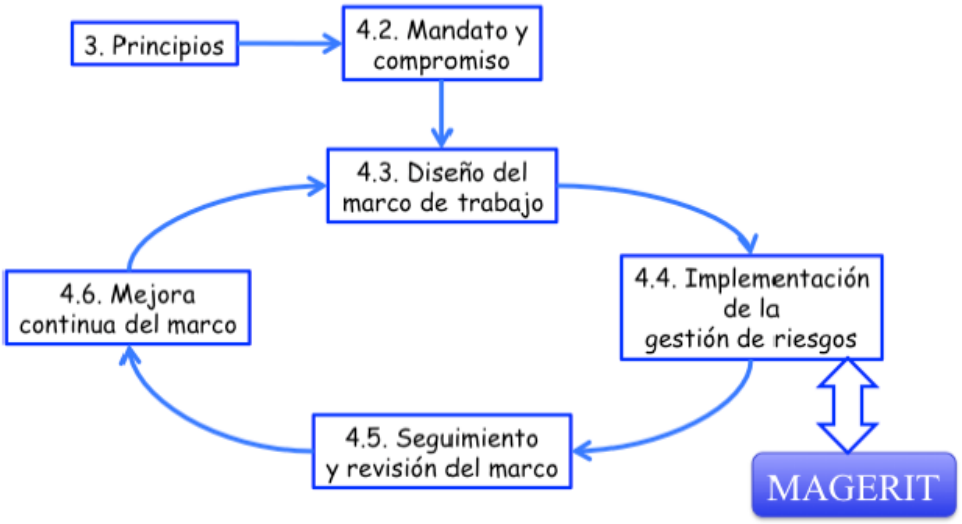
2.2.6.10. Monitorización de Riesgos

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.

2.2.7. Metodología MAGERIT

Siguiendo la terminología de la normativa ISO 31000, MAGERIT responde a lo que se denomina "Proceso de Gestión de los 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 (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012).

Gráfico N° 01: Alcance de MAGERIT según el Marco de trabajo para la gestión de riesgos propuesto por la ISO 31000



MAGERIT estudia los riesgos que soportan un sistema de información y el entorno asociable con él, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio. Recomienda las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados.

Para MAGERIT, las tareas de análisis y tratamiento de los riesgos no son un fin en sí mismas sino que se encajan en la actividad continua de gestión de la seguridad.

El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema. En coordinación con los objetivos,

estrategia y política de la Organización, las actividades de tratamiento de los riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la Dirección. Al conjunto de estas actividades se le denomina Proceso de Gestión de Riesgos.

Para ello, MAGERIT propone un catálogo, abierto a ampliaciones, que marca unas pautas en cuanto a:

- tipos de activos
- dimensiones de valoración de los activos
- criterios de valoración de los activos
- amenazas típicas sobre los sistemas de información
- salvaguardas a considerar para proteger sistemas de información

MAGERIT persigue dos objetivos:

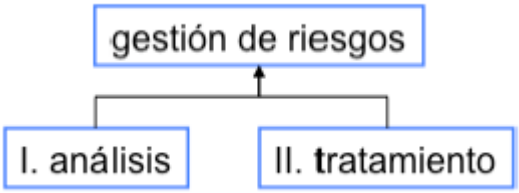
1. Por una parte, facilitar la labor de las personas que acometen el proyecto, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.
2. Por otra, homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

MAGERIT considera dos grandes tareas a realizar:

1. análisis de riesgos, que permite determinar qué tiene la Organización y estimar lo que podría pasar.
2. tratamiento de los riesgos, que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume.

Ambas actividades, análisis y tratamiento se combinan en el proceso denominado Gestión de Riesgos.

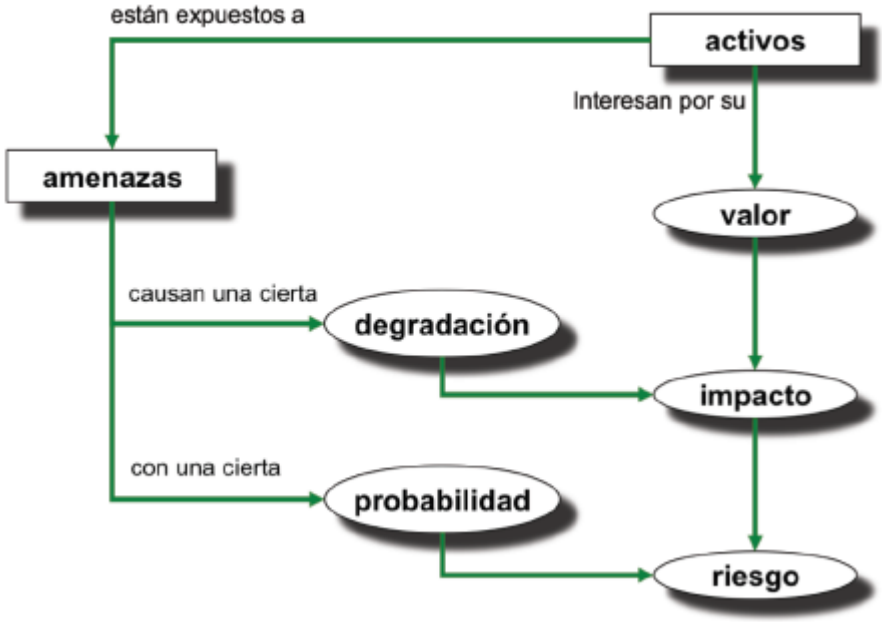
Gráfico N° 02: Etapas ara la Gestión de Riesgos según MAGERIT



Para el análisis de riesgos MAGERIT propone los pasos siguientes:

1. determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
2. determinar a qué amenazas están expuestos aquellos activos
3. determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
4. estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
5. estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza

Gráfico N° 03: Elementos del análisis de riesgos potenciales según MAGERIT



2.2.8. Apetito y tolerancia al riesgo

El apetito es el nivel de riesgo que la empresa quiere aceptar, aquél con el que se siente cómoda, su tolerancia será la desviación respecto a este nivel. Por otro lado, la capacidad de asumir riesgos, será el nivel máximo de riesgo que una organización puede soportar en la persecución de sus objetivos. Así, la tolerancia servirá como alerta para evitar que la empresa llegue al nivel establecido por su capacidad, algo que pondría en peligro la continuidad del negocio (Instituto de auditores internos de España, 2012)

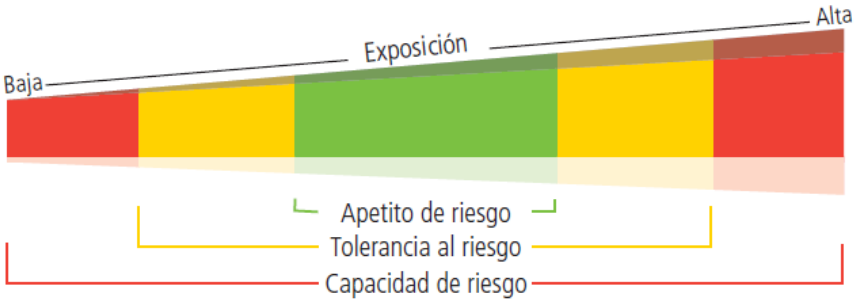
En ese sentido, podemos definir lo siguiente:

a. El apetito de riesgo: La cantidad de riesgo que una organización está dispuesta a buscar o aceptar en la búsqueda de sus objetivos a largo plazo.

b. Tolerancia al riesgo: Los límites de la asunción de riesgos, fuera de la cual la organización no está dispuesta a aventurarse en la búsqueda de sus objetivos a largo plazo.

c. Capacidad de riesgo: la capacidad de llevar los riesgos, y la madurez de gestión de riesgos para su gestión.

Gráfico N° 04: Determinación del apetito y la tolerancia al riesgo



2.2.9. Indicadores de riesgos clave (KRI)

Un indicador de riesgos clave (KRI) es una métrica para determinar qué tan posible es que la probabilidad de un evento, combinada con sus consecuencias, supere el apetito de riesgo de la organización (es decir, el nivel de riesgo que la compañía está preparada para aceptar), y tenga un impacto profundamente negativo en la capacidad de tener éxito de una organización.

Si una organización se especializa en ventas al por menor, por ejemplo, un indicador de riesgo clave podría ser el número de quejas de los clientes, porque el aumento de este KRI podría ser una indicación temprana de que hay que resolver un problema operativo.

El desafío para una organización no es solo identificar cuáles indicadores de riesgo deben ser identificados como claves (los más importantes), sino también comunicar esa información de tal manera que todo el mundo en la organización entienda claramente su significado.

Identificar indicadores de riesgos clave requiere la comprensión de las metas de la organización.

Cada KRI debería ser capaz de ser medido con precisión y reflejar de manera precisa el impacto negativo que tendría sobre los indicadores de desempeño clave de la organización (KPI). Los indicadores de rendimiento clave, que a menudo se confunden con los indicadores de riesgos clave, son las métricas que ayudan a una organización a evaluar el progreso hacia los objetivos declarados.

III. MATERIALES Y MÉTODOS

3.1. Diseño de investigación

De acuerdo al propósito del estudio **el diseño de la investigación es observacional**, porque dado las limitaciones que se tiene 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 modelo propuesto a través de las evaluaciones que realicen los actores directos de los procesos relacionados con la investigación al diseño y aplicabilidad del modelo propuesto. Los datos para la prueba del modelo en mayor porcentaje son retrospectivos (datos históricos) y para las mediciones en el tiempo los datos serán prospectivos (obtenidos a partir de los incidentes de seguridad y las evaluaciones posteriores a la construcción del modelo).

3.2. Hipótesis

Con la implementación de un modelo de gestión de riesgos TI de acuerdo con las exigencias de la SBS, basados en las ISO/IEC 27001, ISO 17799, Magerit se mejorará la gestión de riesgos relacionados con TI para la Caja de Ahorro y Créditos SIPAN SA.

3.3. Diseño de Contrastación

El modelo lógico de contrastación es del tipo cuasi experimental del tipo

G: X O

Dónde:

- el grupo de casos ha sido seleccionado intencionalmente y evaluado con una sola prueba: post prueba
- Se establece una línea base previa de tratamiento y se verifica equivalencias utilizando medias o desviaciones (grupo de control no equivalente): tabla de referencia para calificar los pesos de cada una de los indicadores medidos

X: Modelo de gestión de riesgos operativos de TI basados en las ISO/IEC 27001, ISO 17799, Magerit y en las exigencias de la SBS

O: La Observación postest consistirá en un cuestionario enviado al panel de personas seleccionadas para asignar pesos a los factores, variables y niveles del modelo propuesto, que se aplicará en el caso de estudio, con la finalidad de evaluar la efectividad del diseño y efectividad de la operación del modelo de gestión de riesgos propuesto (X).

3.4. Variables

a. Variable Independiente:
   Modelo de gestión de riesgos operativos de TI basados en las ISO/IEC 27001, ISO 17799, Magerit y en las exigencias de la SBS

b. Variable Dependiente:
   Gestión de riesgos relacionados con TI.

c. Variables – Operacionalización

Tabla N° 01: Operacionalización de variables

Variable	Perspectiva	Dimensión	Indicador
Gestión de riesgos de TI	efectividad del diseño del modelo	Estructuración de la metodología de análisis y tratamiento de riesgos	Efectividad en la definición de los riesgos de TI según las categorías de información
			Nivel de integración del modelo en la gestión de riesgos corporativo
			Grado de concientización
		Gobierno de los riesgos de TI	Cumplimiento normativo de las variables exigidas por la SBS
			Efectividad en la evaluación de los componentes del modelo de gestión de TI: amenazas, vulnerabilidades, impactos, frecuencias
			Efectividad del monitoreo de las actividades de gestión de riesgos de TI
			Tiempo de recuperación de incidentes (RTO)
	efectividad de la operación del modelo	Análisis y tratamiento de riesgos	Nivel de aplicabilidad del proceso implantado en el modelo propuesto para evaluar los riesgos de TI
			Efectividad los niveles de riesgos inherentes de TI
			Efectividad de la implantación de controles y seguimiento de las brechas de seguridad
		Gobierno de los riesgos de TI	Grado de satisfacción por la información resultante del modelo
			Grado de satisfacción del modelo para la toma de decisiones en relación a las inversiones de los controles de seguridad

3.5. Población y Muestra

Dado que el diseño de contrastación de la hipótesis es cuasi experimental, entonces la muestra ha sido seleccionada intencionalmente dado que son las personas de La Caja, que están directamente relacionados y que tienen la capacidad y autoridad para cumplir con las funciones de:

- Jefatura de TI
- Jefatura de la Unidad de Riesgos
- Oficialía de Seguridad de TI y de la Información
- Jefatura de la Unidad de Continuidad de negocio
- Auditor interno

La intención es que las personas que cumplen estas funciones sean los que evalúen el modelo de gestión propuesto.

3.6. Métodos y Técnicas recolección de Datos

En la investigación se emplearán múltiples técnicas e instrumentos de recolección de información: documentación (fichas de revisión de datos), entrevistas, encuestas y observaciones directas.

- **Documentación**, se revisarán los documentos estratégicos, administrativos y legales pertenecientes a la Caja, materia de estudio de caso, y se elaborarán fichas de revisión de datos, de cada documento, conteniendo información primordial de cada uno de ellos. Los documentos que se revisarán serán (en el caso de que existiesen):

  De la Jefatura de Tecnologías de la Información y Organización y Métodos

  a. Plan estratégico de TI
  b. Plan anual de TI
  c. Sistema de Gestión de Seguridad de la Información
  d. Manual de gestión de riesgos operativos de TI, con sus correspondientes informes y plan de pruebas

- **Entrevistas**, las entrevistas servirán para obtener información de los procedimientos actuales para la evaluación y seguimiento de los controles implantados para la protección y salvaguarda de los activos tecnológicos considerados en esta investigación. Serán conducidas en base a un protocolo determinado en los formatos tipo checklist preparados para este efecto (Ver Anexo N° 02). Se aplicará para el diagnóstico de los controles existentes. Básicamente se entrevistará, según sea el caso, a:

  - Jefatura de TI
  - Jefatura de la Unidad de Riesgos
  - Oficialía de Seguridad de TI y de la Información
  - Jefatura de la Unidad de Continuidad de negocio
  - Auditor interno

- **Observación directa**, para complementar el llenado de los formatos del Anexo N° 02 en el diagnóstico de los controles existentes.

- **Encuestas**. Se realizarán encuestas escritas, aplicando la técnica Delphi (juicio de expertos), donde los funcionarios indicados en las entrevistas, evaluarán la efectividad del diseño y de operación del modelo de gestión de riesgos de TI propuesto. Se ha seleccionado a los funcionarios indicados porque tienen la capacidad y autoridad para gestionar la seguridad de TI y de la información en las diferentes áreas de la Caja. La estructura de la encuesta se muestra en el Anexo N° 01. Se aplicará en el post test.

3.7. Técnicas de procesamiento de datos

Para el procesamiento de análisis de los datos se utilizó Microsoft Excel, a través del cual se obtuvieron los resultados de las encuestas.

3.8. Metodología

El modelo de Gestión de Riesgo propuesto, permitió determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo.

Para lograr ello, se identifica y evalúa los diferentes componentes, que los diferentes estándares y metodologías estudiadas, establecen como básicos en la gestión de riesgos de TI, como: los activos de TI, las amenazas, las vulnerabilidades, los impactos y las probabilidades; y así identificar, tanto el nivel de riesgo existente como el nivel de riesgo aceptable de la entidad financiera.

Finalmente, se evalúa y establece las recomendaciones sobre la eficiencia y madurez de los controles que éste tipo organizaciones implementan para gestionar sus riesgos de TI.

Así mismo, 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, las mismas que forman parte anexa de este trabajo de investigación (Ver Anexo N° 8).

En resumen, para el diseño del modelo de gestión de riesgos propuesto se ha tomado como referencia 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; así como de los estándares y metodologías que se han tomado como referencia.

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

1. Análisis de riesgos: donde se determinan los componentes de un sistema de TI que requiere protección y que le dan soporte a los procesos críticos. Esta etapa también contempla la identificación y estimación de sus vulnerabilidades que

lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.

2. Clasificación de los riesgos: donde se determina si los riesgos intrínseco y efectivo encontrados y sí los riesgos restantes o residuales son aceptables.
3. Implementación de controles: aquí se define e implementa las medidas de protección como controles o salvaguardas.
4. Control de eficiencia y madurez: analiza el funcionamiento, la efectividad y el cumplimiento de las medidas de protección para determinar y ajustar las medidas deficientes y sancionar el incumplimiento.

El modelo general de gestión de riesgos propuesto y la metodología para su aplicación están resumidos en los siguientes gráficos:

Gráfico N° 05: Modelo general del modelo de análisis de riesgos propuesto

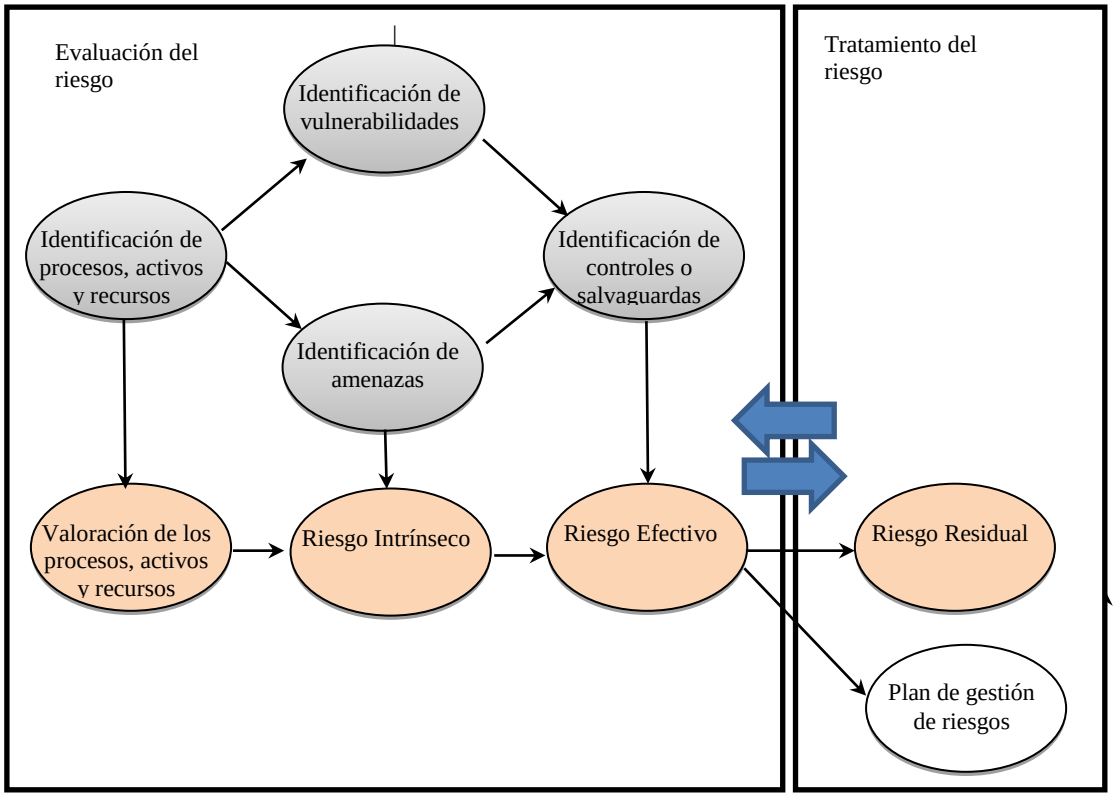
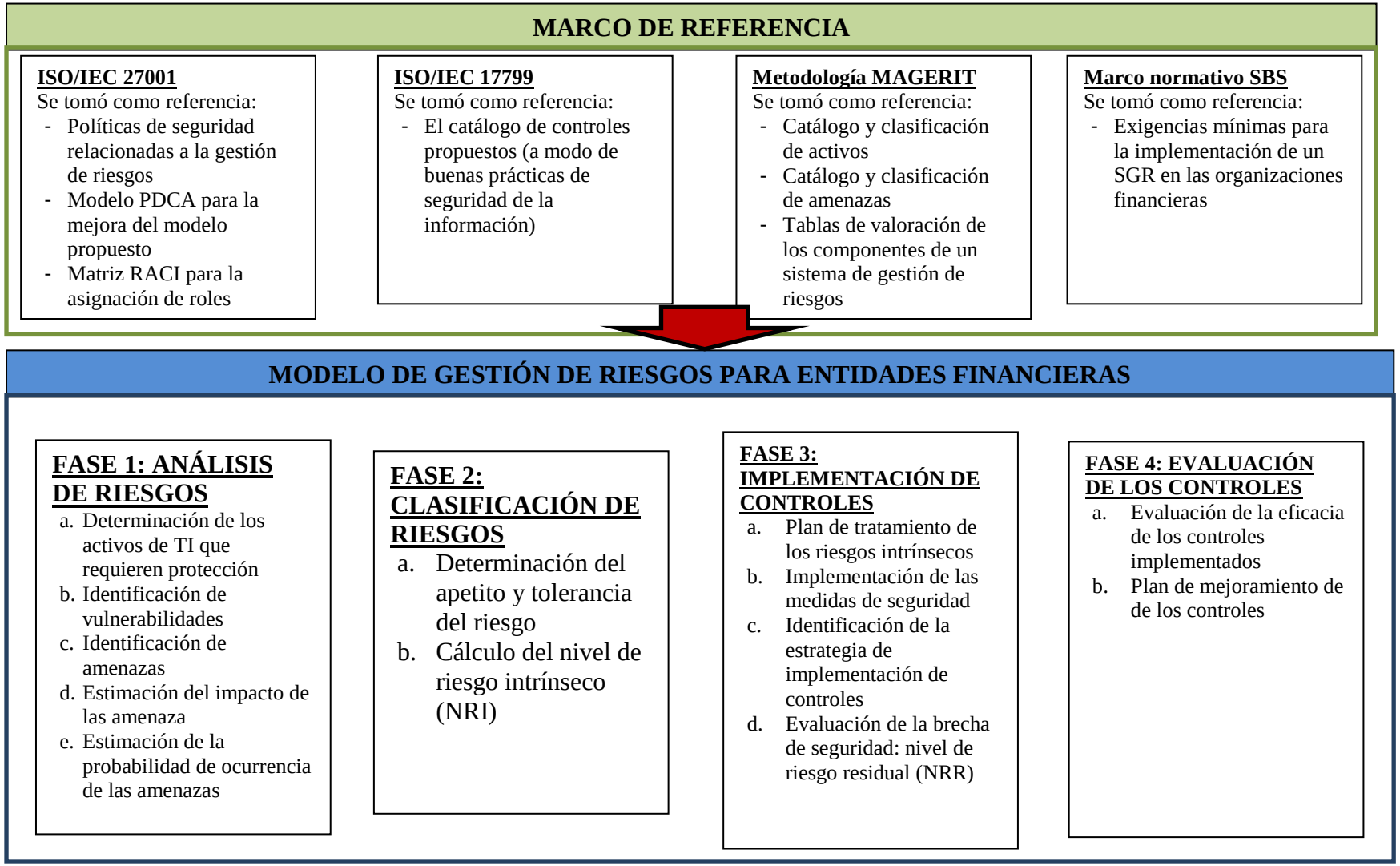


Gráfico N° 06: Metodología para la aplicación del modelo de análisis de riesgos propuesto



Fase 1: Análisis de riesgos de TI

En esta fase se identificarán los riesgos de seguridad de la información que podrían impedir que la organización financiera no logre sus objetivos, determinando su magnitud e identificando las áreas que requieren medidas de salvaguarda o controles en función del riesgo detectado: intrínseco y efectivo.

Esta fase contempla las siguientes actividades y tareas:

A. Identificación de activos de TI y definición de su criticidad
B. Identificación de amenazas por activo
C. Identificación de vulnerabilidades
D. Estimación del impacto de las amenazas
E. Estimación de la probabilidad de ocurrencia de la amenazas

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

Esta actividad busca identificar los activos relevantes dentro de los procesos críticos identificados de la entidad, caracterizándolos 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° 02: Ficha técnica de la actividad identificación de activos de TI y definición de su criticidad

<table>
<tr><th colspan="3">Tarea: Identificación de activos de TI</th></tr>
<tr><td colspan="3">Objetivo:
Identificar los activos que componen el sistema, determinando sus características, atributos y clasificación en los tipos determinados.</td></tr>
<tr><th>Entradas o insumos necesarios</th><th>Salidas</th><th>Técnicas</th></tr>
<tr><td>- 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</td><td>- Inventario de activos de TI a evaluar
- Clasificación de los activos de TI</td><td>- Diagramación de flujo de datos y diagramación de procesos de negocio
- 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)</td></tr>
<tr><th colspan="3">Tarea: Definición de la criticidad de los activos de TI</th></tr>
<tr><td colspan="3">Objetivos
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</td></tr>
<tr><th>Entradas o insumos necesarios</th><th>Salidas</th><th>Técnicas</th></tr>
<tr><td>- Inventario de activos de TI
- Descripción de los procesos críticos del negocio:
- Diagramas de flujo de datos</td><td>- Modelo de valor: Informe del valor de los activos de TI</td><td>- 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 criticidad de los activos de TI (ver Anexo n° 04)</td></tr>
</table>

a. Identificación de activos de TI

En este punto se identificarán los activos que dan soporte a los procesos de Créditos y Captaciones. Para ello se utilizará la clasificación propuesta por la ISO 27005:2008; específicamente la clasificación propuesta para activos de soporte de los activos primarios (procesos e información). Se podrá clasificar los activos de TI, según sus características, en los siguientes tipos:

- Dato: información que se genera, envía, recibe y gestionan dentro de la organización. Incluye los documentos que se gestionan dentro de sus procesos.
- Aplicación: software que se utilice como soporte en los procesos.
- Personal: actores que tienen posibilidades de acceso y manejo, de una u otra manera, de los activos de información.
- Servicio: servicios que alguna área de la organización suministra a otra área o entidades externas a la misma.
- Tecnología: hardware donde se procesa, almacena o transmite la información.
- Instalación: lugar donde se alojan los activos de información. Puede estar ubicado dentro de la entidad o fuera de ella.
- Equipamiento auxiliar: activos que no se hallan definidos en ninguno de los anteriores tipos.

Para obtener el inventario de activos de TI que se van a considerar en la evaluación de riesgos se debe analizar las entradas e insumos requeridos en la ficha técnica. Se podrá aplicar utilizar cualquiera de los dos enfoques que se indican a continuación, independiente o conjuntamente:

- Enfoque top-down (de arriba abajo), infiriendo los activos de información relacionados con los procesos críticos (créditos y captaciones) a partir de la descripción de los procesos.
- Enfoque bottom-up (de abajo arriba), identificando las principales aplicaciones, archivos, bases de datos, equipos, instalaciones, usuarios, etc. utilizados en los procesos.

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° 3:

Tabla N° 03: 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

Una vez inventariados los activos de TI es necesario identificar y documentar el valor que su seguridad representa para la entidad. Para ello, se asignará un conjunto de valores a cada activo teniendo en cuenta los diferentes requerimientos de seguridad que se consideren relevantes.

El valor que tienen los activos de información para una entidad financiera en el ámbito de la seguridad puede medirse desde diversos puntos de vista. Estos puntos de vista se denominan, en el marco de este modelo, requerimientos de seguridad o dimensiones de la seguridad, los cuales están definidos en el Anexo N° 04.

La valoración se deberá realizar mediante la ponderación de las pérdidas ocasionadas para la entidad financiera en caso de que falle o caiga el activo, debido a la materialización de una amenaza, de cada uno de los requerimientos de seguridad definidos para los diferentes activos de información, según las tablas de referencia del Anexo N° 04 en relación a: disponibilidad, integridad y confidencialidad.

Las escalas y criterios que se utilizarán para calificar cada una de las dimensiones de seguridad de TI de cada activo, se muestran en la tabla N° 04.

Tabla N° 04: Valores y criterios de referencia para la valoración de la criticidad de los activos de TI

	Valor	Criterio
Disponibilidad	**1**	No aplica/No es relevante
	2	Debe estar disponible al menos el 10% del tiempo
	3	Debe estar disponible al menos el 50% del tiempo
	4	Debe estar disponible al menos el 75% del tiempo
	5	Debe estar disponible al menos el 95% del tiempo

	Valor	Criterio
Integridad	**1**	No aplica / No es relevante
	2	No es relevante los errores que tenga o la información que falte
	3	Tiene que estar correcto y completo al menos en un 50%
	4	Tiene que estar correcto y completo al menos en un 70%
	5	Tiene que estar correcto y completo al menos en un 95%

	Valor	Criterio
Confidencialidad	**1**	No aplica / No es relevante
	2	Daños muy bajos, el incidente no trascendería del área afectada
	3	Daños bajos, el incidente no trascendería del área afectada
	4	Los daños serían relevantes, el incidente implicaría a otras áreas
	5	Los daños serían catastróficos, la reputación y la imagen de la institución se verían comprometidas

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

Tabla N° 05: Plantilla para la calificación de la criticidad de los activos de TI

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° 06: Niveles de valoración de la criticidad de los activos de TI

Rango	Nivel de criticidad	Descripción
1 – 5	1	Muy bajo
6 – 10	2	Bajo
11 – 15	3	Medio
16 – 20	4	Alto
21 – 25	5	Muy alto

B. Identificación de amenazas por activo

En esta actividad caracteriza el entorno al que se enfrenta el sistema, qué puede pasar, qué consecuencias se derivarían y cuán probable es que pase. Es decir, describe las amenazas a los que el sistema está expuesto.

Para la identificación de las amenazas significativas de cada activo de TI identificado, se tomará en consideración lo siguiente:

- 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° 07: 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° 08: Plantilla para la identificación de amenazas por activo

N°	Activo	Amenaza
1		
2		
3		

C. Identificación de vulnerabilidades por activo

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° 09: 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° 10: Plantilla para la identificación de las vulnerabilidades por cada Activo-Amenaza

N°	Activo	Amenaza	Vulnerabilidad
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
			Vulnerabilidad 2.2.3

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

Esta actividad 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° 11: 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 - Informes de vulnerabilidades - Historia o antecedentes de incidentes de seguridad de TI	- Mapa de riesgos: informe de amenazas posibles, caracterizadas por su frecuencia de ocurrencia y la degradación que causarían en los activos	- 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 - Valoración Delphi

a. 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° 12: 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

b. Estimación de la probabilidad de ocurrencia de una amenaza

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° 13: 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: Clasificación del riesgo de TI

a. Determinación del apetito y la tolerancia al riesgo

Para determinar el apetito y la tolerancia al riesgo en el modelo propuesto, se debe entender 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 14.

Tabla N° 14. 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
Relacionados con el personal de TI	Ausencia del personal
	Falta de habilidades y experiencia del personal
	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	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° 15. 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 16), tomando como referencia los niveles de riesgo definidos anteriormente.

Tabla N° 16: 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: implementación 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.

Los NRI cuya valoración sea "Muy Alta" o "Alta" son los que se tratarán mediante controles o salvaguardas para reducir la probabilidad que dichos riesgos identificados se materialicen o para reducir su impacto. Para las amenazas con NRI "Medio", "Baja" o "Muy Baja" se aplicará la estrategia de convivir con el riesgo.

A continuación se presenta los criterios de aceptación o no aceptación para dada uno de los niveles de los riesgos intrínsecos:

Tabla N° 17: 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

Luego, se determina el plan de tratamiento para cada uno de los riesgos encontrados no aceptables.

b. Implementación de las medidas de seguridad

Los controles que se seleccionarán para el tratamiento de los riesgos no aceptables, se obtendrán del Anexo N° 07 y que pertenecen al estándar ISO 17799 (ISO/IEC 27002), el cual contiene una lista bastante completa de objetivos de control y controles comúnmente relevantes para las organizaciones en general.

Para determinar los controles que se van a implementar se desarrollará la Declaración de la Aplicabilidad, donde 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.

IV. RESULTADOS

4.1. Identificación y clasificación de los Activos de TI de los procesos principales de la CRAC 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 Caja:

Tabla N° 18: 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 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	Bases de Datos
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 Actas de conformidad
13	Archivo de requerimientos informáticos (físico)
14	Analistas de sistemas (Responsables de la implementación de requerimientos)
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° 19: 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

4.2. 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° 05):

Tabla N° 20: 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

4.3. 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° 08):

Tabla N° 21: 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

4.4. 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° 10), el cual es el resultado del análisis de incidentes de seguridad de la información que tiene registrado La Caja:

Tabla N° 22: 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 / paralización de Operaciones)	No se mantiene un control o registro de acceso a las áreas restringidas
			Falta de un registro de acceso a la sala de servidores
			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 tranSACiones
			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 procesos, pérdida de información	Inadecuada segregación de funciones
			No existe un plan de capacitación adecuado

		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 tranSACiones 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-pagina 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 autorizado 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	Archivos 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	Falta de monitoreo de envío y recepción de

		a fuga a través de correos electrónicos y/o páginas web	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

4.5. 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° 23. 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° 24. 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

4.6. 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 Caja, 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° 11, 12, 14 y 15), se muestran en la siguiente tabla:

Tabla N° 25: 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	Medio
			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	R41	2	Bajo
		Pérdida de Activos de TI en la sala de servidores (costo de	No se mantiene un control o registro de acceso a las áreas restringidas	2	Menor	2	Improbable	R15	2	Bajo

		hardware / paralización de Operaciones)	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 realiza mantenimiento en la institución	2	Menor	3	Posible	R17	2	Bajo
			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	Medio
			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	Medio
			Falta de un lugar adecuado para su resguardo y protección de las copias de respaldo	2	Menor	2	Improbable	R30	2	Bajo
			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 destrucción de la información	Abuso de privilegios de accesos	4	Mayor	3	Posible	R36	3	Medio
			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	Medio
			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 computo	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 por parte del proveedor	No generación de copias de respaldo (cuentas creadas, permisos y configuración)	3	Moderado	3	Posible	R47	3	Medio
			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 del contraseñas de correo vía acceso-pagina web	3	Moderado	3	Posible	R50	3	Medio
10	Equipos de cómputo terminales de ventanilla y	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	4	Mayor	2	Improbable	R51	2	Bajo
			No se ha determinado la vida útil de los equipo	2	Menor	2	Improbable	R52	2	Bajo

	analistas de créditos		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 autorizado a la PC de Integración de Software	4	Mayor	2	Improbable	R61	2	Bajo
		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	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

	de la implementación de requerimientos)		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 través de correos electrónicos y/o páginas web	Falta de monitoreo de envío y recepción de correos	3	Moderado	2	Improbable	R70	2	Bajo
			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	R72	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 Desarrollo de Requerimientos	Copia de seguridad en lugares seguros	3	Moderado	3	Posible	R75	3	Medio
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

4.7. 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 Caja (es decir, el nivel de riesgo que la Caja 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 Caja.

De acuerdo a RMA[1] 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 modelo 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

Tabla N° 26: Indicadores de riesgo clave propuestos para el modelo 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 otra 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

[1] Risk Management Association

4.8. 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° 27: 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, este se 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	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

	mejoras en la seguridad de la información		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

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

Luego de definir las políticas de seguridad que La Caja 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 Caja.

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

Tabla N° 28: 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 backup	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 de auditoría al administrador de la BD, así como también las operaciones que realiza en la arquitectura de la BD	Elección de controles
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 autorizado	Evitar aumento del riesgo
			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 archivos comprimidos	Elección de controles
			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 creación de contraseñas	Evitar aumento del riesgo
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 funciones.	Evitar aumento del riesgo
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 generar 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 un complejidad en la contraseñas teniendo en caracteres y números, la contraseña cambia en cada respaldo	Evitar aumento del riesgo
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 proceso 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, asi mismo se generan tres copias de respaldo que son enviados al sitio alterno	Elección de controles
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

4.10. 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° 29: 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	Categoría	
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	Bajo	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 de respaldo en el centro de cómputo principal (CCP) en caso de caída del servidor primario							Riesgo aceptable
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	3	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 y certificación antes del pase a producción							Riesgo 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

4.11. Simulación del Modelo de Gestión de Riesgos de TI propuesto en el software PILAR v 5.4.4 - 3.12.2014

4.11.1. Objetivo de la simulación

El objetivo de la simulación es probar y demostrar que el Modelo de Gestión de Riesgos de TI (MGR-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, opte por la aplicación PILAR, ya que es el que más se ajusta a la metodología de mi modelo propuesto en mi tesis (Ver anexo N° 13).

4.11.2. 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/. La licencia de uso fue cedida por los dueños de los derechos comerciales de este producto.

4.11.3. Precisiones previas

El MGR-TI desarrollado en el trabajo de tesis:

- ha tomado 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 modelo ajustado a las exigencias de la SBS**.

- se ha basado 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 CRAC Sipán** para cumplir con las exigencias de la SBS.

V. DISCUSIÓN DE RESULTADOS

5.1. Caracterización de la discusión de resultados

De acuerdo a la descripción dada en el diseño de la investigación (ítem 3.1) observamos la necesidad de definir, desarrollar y proponer una metodología y una forma estructurada que permita evaluar objetivamente el diseño y la efectividad del modelo propuesto cuando se realizan las actividades de gestión de riesgos y evaluación de la continuidad de los procesos en la entidad tomada como caso de estudio.

Para atender y solucionar esta necesidad, se aplicó la siguiente metodología que permite relacionar variables cuantitativas y cualitativas a partir de los pesos asignados por las personas que tienen autoridad y desempeñan funciones de gestión de riesgos y de la continuidad de procesos en La Caja durante la evaluación, con el fin de valorar objetivamente la efectividad en el diseño y la efectividad del modelo propuesto. La metodología propuesta para evaluar el diseño y la efectividad del modelo propuesto es aplicable a todas las Cajas Rurales y su implementación depende del tamaño del negocio. Para efectos del ejercicio práctico que presentamos más adelante, la metodología se realizó en la CRAC Sipán SAC.

Para la aplicación de la metodología de evaluación del modelo propuesto se utilizó el Método Delphi. "Dos matemáticos norteamericanos, Norman Dalkey y Olaf Hermes, diseñaron en el año de 1963 la técnica que ellos bautizaron como "Delphi" con el propósito de establecer el consenso de expertos con respecto al acontecimiento de un hecho en el futuro. El nombre "Delphi" fue escogido en memoria de la ciudad de Delfos en la antigua Grecia, que era su centro religioso en el siglo IV antes de Cristo". (Trujillo, 2004).

Con el método "Delphi" obtuvimos la opinión y el conocimiento de las personas encargadas de las funciones de:

- Jefatura de TI
- Jefatura de la Unidad de Riesgos
- Oficialía de Seguridad de TI y de la Información
- Jefatura de la Unidad de Continuidad de negocio
- Auditor interno

Para su aplicación se consideró las siguientes características:

- Anonimato: Durante su aplicación ninguna de las personas que evaluaron el modelo supieron que los otros también estaban evaluando el modelo. Esto permitió que ninguna de los evaluadores del modelo sea influenciado por el conocimiento y experiencia de otro.
- Iteración y realimentación controlada: La iteración se consiguió al presentar el mismo cuestionario a todos los evaluadores de forma independiente.
- Respuesta del grupo: La información que se presenta a los evaluadores no es sólo el punto de vista de la mayoría, sino que se presentan todas las opiniones indicando el grado de acuerdo obtenido.

El procedimiento realizado fue el siguiente:

1. Se elaboró un cuestionario tomando como base las variables consideradas en el cuadro de "Variables de contrastación de hipótesis"

2. Conseguir su compromiso de colaboración. Las personas elegidas conocen del tema y del modelo propuesto. Sin embargo, se socializó y explicó de forma individual al panel de personas seleccionadas, la metodología y los modelos propuestos.

3. Se determinó el contexto y el horizonte temporal (tiempo de aplicación) para la aplicación del cuestionario. En este caso la metodología y modelos propuestos fueron utilizados durante tres (03) meses, entre noviembre del 2013 a enero del 2014.

4. Posteriormente, se les envío a través de correo electrónico, un archivo con los cuestionarios diseñados en hojas electrónicas, que contienen los niveles, factores y variables definidas a través de preguntas, para que cada uno de ellos comparta sus opiniones sobre la relevancia del modelo propuesto en este trabajo. La asignación de la relevancia por parte del "experto", se realiza respondiendo "sí" o "no" a cada factor y variable del cuestionario y la asignación de los pesos, la realiza mediante el análisis y aplicación del criterio profesional y su función dentro de La Caja, asignando o distribuyendo un peso porcentual utilizando la escala de (0% al 100%) para cada pregunta, rango, evento y nivel que conforman las variables.

5.2. Diseño del cuestionario enviado al panel de personas seleccionadas para asignar pesos a los factores, variables y niveles del modelo propuesto

a. Cuestionario para la Prueba de la Efectividad del Diseño:
Objetivo: Probar la efectividad del diseño del modelo propuesto determinando si los controles de la entidad son operados como fue prescrito por las personas que poseen la autoridad y competencias necesarias para desempeñar la gestión de la seguridad, el control y la gestión de riesgos y, si satisfacen los objetivos de control exigidos por la SBS para prevenir o detectar riesgos de TI. (Ver Anexo N° 01)

b. Cuestionario para la Prueba de la Efectividad del Operación:
Objetivo: Probar la efectividad de la operación del modelo propuesto determinando si está operando tal y como fue diseñado y si las personas que desempeñan la gestión de la seguridad, el control y la gestión de riesgos posee las competencias necesarias para desempeñar el control de manera efectiva. (Ver Anexo N° 01)

Para cada uno de los cuestionarios se utilizará la siguiente tabla de referencia para calificar los pesos de cada una de los indicadores de cada variable:

Tabla N° 30: Pesos para la calificación de los indicadores en los cuestionarios

Peso	Significado	Color
1	CLAVE	
2	RELEVANTE	
3	ESTÁNDAR	
4	IRRELEVANTE	

Leyenda

Clave: El indicador evaluado del modelo propuesto es importante considerarlo en el Sistema de Gestión de Seguridad de la Información de La Caja, porque cumple con los requisitos exigidos en la normativa la SBS y se adecúa a las funciones de la entidad.

Relevante: El indicador evaluado del modelo propuesto puede considerarse en el Sistema de Gestión de Seguridad de la Información de La Caja, porque cumple con los requisitos exigidos en la normativa la SBS.

Estándar: El indicador evaluado del modelo propuesto puede considerarse en el Sistema de Gestión de Seguridad de la Información de La Caja, con algunas modificaciones y mejoras para cumplir con los requisitos exigidos en la normativa la SBS y para que se adecúe a las funciones de la entidad.

Irrelevante: El indicador evaluado del modelo propuesto no cumple con los requisitos exigidos en la normativa la SBS por lo que no podría considerase en el Sistema de Gestión de Seguridad de la Información de La Caja.

5.3. Resultados obtenidos:

Los resultados del análisis Delphi se muestran en las siguientes tablas:

Tabla N° 31: Resultado de la evaluación de los factores y variables para probar la efectividad del diseño del modelo propuesto

			Jefe de TI		Jefe Unidad Riesgos		Oficialía de Seguridad Información		Jefe Continuidad procesos		Auditor Interno		TOTALES	
Variable		**Factor Relevante (indicador)**	**SI/NO**	**Peso**	**SI/NO**	**Peso**	**SI/NO**	**Peso**	**SI/NO**	**Peso**	**SI/NO**	**Peso**	**SI/NO**	**Peso**
Perspectiva: Gestión de riesgos de TI														
Estructuración de la metodología de análisis y tratamiento de riesgos	1	Se ha definido nítidamente las categorías – como disponibilidad, integridad y confidencialidad – en las que se pueden agrupar los riesgos de TI	SI	2	SI	2	SI	1	SI	2	SI	2	100%	2
	2	La gestión de riesgos de TI se integra en la gestión de riesgos general para todos los riesgos a nivel corporativo	SI	2	SI	2	SI	1	SI	2	NO	4	80%	2
	3	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	SI	2	SI	3	SI	2	SI	3	SI	2	100%	2
Gobierno de los riesgos de TI	4	Contempla todas las variables necesarias exigidas por la SBS para su evaluación	SI	2	SI	2	SI	2	SI	2	SI	3	100%	2
	5	Se ha establecido pautas para evaluar la magnitud de los riesgos de modo coherente	SI	2	SI	3	SI	3	SI	2	NO	4	80%	3
	6	Se cuenta con indicadores clave para monitorizar periódicamente la eficacia de nuestras actividades de gestión de riesgos de TI	SI	3	SI	3	SI	2	SI	2	SI	2	100%	2
		TOTAL (%)	100%		100%		100%		100%		67%		93%	2

Tabla N° 32: Resultado de la evaluación de los Factores y variables para probar la efectividad de la operación del modelo propuesto

			Jefe de TI		Jefe Unidad Riesgos		Oficialía de Seguridad Info		Jefe Continuidad procesos		Auditor Interno		TOTALES	
Variable		**Factor Relevante (indicador)**	**SI/NO**	**Peso**	**SI/NO**	**Peso**	**SI/NO**	**Peso**	**SI/NO**	**Peso**	**SI/NO**	**Peso**	**SI/NO**	**Peso**
Perspectiva: Gestión de riesgos de TI														
Análisis y tratamiento de riesgos	1	A partir del modelo propuestos se puede establecer un proceso formal y coherente para evaluar periódicamente potenciales riesgos de TI	SI	**2**	SI	**2**	SI	**2**	SI	**2**	SI	**2**	100%	**2**
	2	Se puede determinar con efectividad los niveles de riesgos inherentes de TI	NO	**2**	SI	**2**	SI	**2**	SI	**2**	SI	**2**	80%	**2**
	3	Se puede evaluar la efectividad de los controles y hacer seguimiento de las brechas de seguridad	SI	**2**	NO	**4**	SI	**2**	SI	**2**	NO	**4**	60%	**3**
Gobierno de los riesgos de TI	4	La información resultante del modelo es significativa para cumplir con los informes exigidos por la SBS en relación a la gestión de riesgos de TI	SI	**2**	SI	**2**	SI	**3**	SI	**2**	SI	**3**	100%	**2**
	5	La información resultante del modelo sirve para tomar decisiones con efectividad en relación a las inversiones e importancia de los controles de seguridad	NO	**4**	NO	**4**	NO	**4**	NO	**4**	NO	**4**	0%	**4**
		TOTAL (%)	60%		60%		80%		80%		60%		68%	**3**

De los resultados obtenidos se puede concluir lo siguiente:

Con respecto a la efectividad del diseño del modelo propuesto

a. aceptan en un 93% de los factores considerados para el diseño de la metodología de análisis y tratamiento de riesgos de TI propuesto, estableciendo que tiene un nivel de madurez de RELEVANTE, es decir, que la metodología de gestión de riesgos propuesta puede considerarse en el Sistema de Gestión de Seguridad de la Información de La Caja, porque cumple con los requisitos exigidos en la normativa la SBS.
b. aceptan el 100% de los factores considerados para el desarrollado las actividades iniciales de la gestión de la continuidad de procesos relacionados con TI, estableciendo que tiene un nivel de madurez de RELEVANTE, es decir, que el modelo propuesto puede considerarse en el Sistema de Gestión de Seguridad de la Información de La Caja, porque cumple con los requisitos exigidos en la normativa la SBS.

Con respecto a la efectividad de la operación del modelo propuesto

a. aceptan el 68% de los factores considerados para aplicar la metodología de análisis y tratamiento de los riesgos de TI en la gestión del sistema de seguridad de la información con el que cuenta La Caja, estableciendo que tiene un nivel de madurez de ESTANDAR, es decir, que la metodología propuesta puede aplicarse en el sistema de seguridad de la información con el que cuenta La Caja con algunos cambios para adecuarse a las exigencias de la SBS.
b. aceptan el 80% de los factores considerados para aplicar las actividades básicas de la gestión de la continuidad de los procesos de TI propuestas, en la gestión del sistema de seguridad de la información con el que cuenta La Caja, estableciendo que tiene un nivel de madurez de ESTANDAR, es decir, que pueden aplicarse con algunos cambios para adecuarse a las exigencias de la SBS.

VI. CONCLUSIONES

1. Con la definición de políticas de seguridad de la información, tangibilizados en procedimientos, reglamentos y controles debidamente formalizados, se ha logrado establecer un nivel de conocimiento, concientización y cultura en el personal de La Caja 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.

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

3. Se ha logrado implementar un modelo de gestión de riesgos de TI, que identifica, evalúa y trata nítidamente los activos de TI, 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 de riesgos de TI en La Caja, mediante la evaluación de brechas de efectividad de los controles de seguridad de la información.

4. 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 TI 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.

5. Queda demostrado que la metodología de gestión de riesgos y de continuidad de los procesos de TI, permite identificar los niveles de riesgos de tal forma que sirve de información para la toma de decisiones en relación la inversión para la implementación de los controles que sirvan de salvaguardas en la protección del proceso contra posibles amenazas y vulnerabilidades.

6. Se comprueba que los resultados obtenidos de la valoración cualitativa de los niveles de riesgo de TI, en el software comercial PILAR y en el desarrollo del caso de estudio con el MGR-TI propuesto son SIMILARES. Este es un indicador de que el MGR-TI propuesto funciona.

7. Las diferencias que podemos encontrar entre el sistema comercial y el MGR-TI son:

- Las escalas de valoración. Esto no es una deficiencia del modelo 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 MGR-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.

Recomendaciones:

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

2. 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.

3. Para lograr mejores resultados en la gestión de riesgos de TI y en la continuidad de procesos, La Caja 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.

VII. REFERENCIAS BIBLIOGRÁFICAS

Aguayo Yepez, A. G. (2011). Adaptación de un marco metodológico para la mitigación de riesgo operativo generado por vulnerabilidades de TI con un enfoque de aduditoria basado en riesgos en el Ecuador. *Tesis*. Ecuador: Universidad Andina San Simón.

Aldegani, G. M. (1997). *Seguridad informática.* Buenos Aires: MP Ediciones.

Ampuero Chang, C. E. (2011). Diseño d un sistema de gestión de seguridad de información para una compañía de seguros. *Tesis*. Lima, Perú: Pontificia Universidad Católica del Perú - PUCP.

Avalos Ruiz, C. (2012). Análisis, diseño e implementación del sistema de riesgo operacional para entidades financieras. *Tesis*. Lima, Perú: Pontificia Universidad Católica del Perú - PUCP.

Campos, J., & Herrera, F. (2007). Políticas de seguridad organizacional y control de activos según la Norma Técnica Peruana NTP-ISO/IEC 17799 en la Oficina Central de Informática de la Universidad Nacional Pedro Ruiz Gallo. *Tesis*. Lambayeque, Peru: Universidad Nacional Pedro Ruiz Gallo.

Córdova Rodriguez, N. E. (2009). Plan de seguridad para una entidad financiera. *Tesis*. Lima, Perú: Universidad Nacional Mayor de San Marcos.

Costas Santos, J. (2011). *Seguridad informática.* Bogotá: Editorial Ra-ma.

Gartner INC. (Abril de 2013). *Is Your IT Security Budget Immature?* Obtenido de Gartner WebSite: http://www.gartner.com/technology/metrics/

IBM. (Abril de 2013). *La gestión de riesgos de TI*. Obtenido de IBM Compañy WebSite: http://www.935.ibm.com/services/es/cio/pdf/gestion-riesgos-ti-unos-sistemas-informacion-maduros-pueden-generar-grandes-resultados.pdf

ISACA. (2012). *COBIT 5 - Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* ISACA - Information Systems Audit and Control Association. ISACA.

ISACA, Asociación de Auditoria y Control de Sistemas de Información. (2005). *Manual de preparación al examen CISA* (15ava ed.). Madrid.

ISACA, Asociación de Auditoria y Control de Sistemas de Información. (2009). Lineamientos para la gestión de la seguridad de TI. *Manual de preparación CISA 2009*. Lima, Perú.

Medina, A. (2007). *Seguridad informática.* Lima: Universidad Nacional Mayor de San Marcos.

ONGEI, Oficina Nacional de Gobierno Electrónico e Informática. (2004). Norma Técnica Peruana NTP/ISO/IEC 17799. *1era edición*. Lima, Perú.

ONGEI, Oficina Nacional de Gobierno Electrónico e Informática. (Abril de 2013). *Seguridad de la información*. Obtenido de http://www.ongei.gob.pe/eventos/Programas_docu/65/Programa_553.pdf

Peña, G., & Peña, L. (2005). Gestión de riesgo tecnológico. En *Mejores prácticas y estándares internacionales en gestión de riesgos y control interno.*

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

SBS, Superintendencia de Banca, Seguro y AFP. (2002). Resolución N° 006-2002. *Reglamento para la administración de riesgos de operación*. Lima, Perú.

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.

VIII. ANEXOS

ANEXO N° 01

TABLAS DE FACTORES Y VARIABLES DE EVALUACIÓN DEL MODELO PROPUESTO

Tabla Factores y variables para probar la efectividad del diseño del modelo 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 de la metodología de análisis y tratamiento de riesgos	Se ha definido nítidamente las categorías – 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 nuestras actividades de 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 modelo 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 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 la eficacia de nuestras actividades de gestión de seguridad de TI, gestión de riesgos de TI y continuidad de procesos		
Perspectiva: Gestión de riesgos de TI			
Análisis y tratamiento de riesgos	A partir del modelo propuestos se puede establecer un proceso formal y coherente para evaluar períodicamente 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 modelo es significativa para cumplir con los informes exigidos por la SBS en relación a la gestión de riesgos de TI		
	La información resultante del modelo sirve para tomar deciciones con efectividad en relación a las inversiones e importancia de los controles de seguridad		
Perspectiva: Continuidad de procesos			
Gobierno de la continuidad de procesos de TI	La información resultante del modelo es significativa para cumplir con los informes exigidos por la SBS en relación a la continuidad de procesos		
	A partir del modelo 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 ha 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 (microprocesador, memoria, fuente de poder, otros)	Se recomienda mejorar	La seguridad para la entrada y salida de paquetes a Internet de todas las agencias está basada en un 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 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, repotenciamiento 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

Nombre del Activo	Factor de Riesgo	Se protege?	Cómo? / Por qué?
Base de Datos	Copia no autorizada de o 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

Nombre del 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)

Nombre del Activo	Factor de Riesgo	Se protege?	Cómo? / Por qué?
Backup	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

Nombre del 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 par 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

Nombre del 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

Nombre del 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 las “altas” y “bajas” de los usuarios encontrándose casos en que personal ingresaba desde el terminal a su cargo con el ID de otro usuario. Por lo tanto en esos casos no es posible identificar las ocurrencias realizadas por usuarios físicos.

VIII. DOCUMENTACIÓN DEL SISTEMA

Nombre del 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 como "control de cambios". Falta implementar algunos 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

X. SISTEMA CONTABLE Y FINANCIERO ("SIPAN")

Nombre del 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. "Control de cambios"
	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 criptográficas	[info]	protección de la información	Claves públicas o privadas de 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
[serv]	Servicios	[www]	acceso a Internet	
		[telnet]	acceso remoto a cuenta local	
		[email]	correo electrónico	Servidor de correo electrónico
		[file]	almacenamiento de ficheros	Servidor de datos
		[ftp]	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	Toner
		[furniture]	mobiliario: armarios, etc	
		[safe]	cajas fuertes	
[Inmueb]	Intalaciones	[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

[D] disponibilidad
Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]
[I] integridad
Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
[C] confidencialidad
Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
[T] trazabilidad
Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]
[A] autenticidad
Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]

Tabla de definición de escala de 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	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones

		amenaza específica [E.31] para cubrir la Indisponibilidad 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	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones

		indisponibilidad 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 (electrónicos) - [AUX] equipamiento auxiliar
[I.7]	Condiciones	Deficiencias en la aclimatación de los locales,	[D] disponibilidad	- [HW] equipos

	inadecuadas de temperatura y/o humedad	excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, etc.		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,	[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 electromagnéticas	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 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:	[C] confidencialidad	- [HW] equipos informáticos (hardware) - [Media] media - [AUX] equipamiento auxiliar - [L] instalaciones

		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 (trazabilidad)	- [D.log] registros de actividad
[E.4]	Errores de configuración	Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su	[I] integridad	- [D.conf] datos de configuración

		configuración y ésta de la diligencia del ad ministrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.		
[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	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. 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	La información llega accidentalmente al		

	información	conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	[C] confidencialidad	
[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) - [Media] soportes de información - [L] instalaciones
[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 (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	[I] integridad [D] disponibilidad [C] confidencialidad	- [SW] aplicaciones (software)
[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	[D] disponibilidad [C] confidencialidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento

		pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.		auxiliar
[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 [A] 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 para realizar tareas que no son de su competencia, puede ocasionar problemas.	[C] confidencialidad [I] integridad [D] disponibilidad	- [D] datos / información - [keys] claves criptográficas - [S] servicios

				- [SW] aplicaciones (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 integridad de los datos afectados.	[I] integridad	- [S] servicios - [SW] aplicaciones (software) - [COM] redes de comunicaciones
[A.11]	Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente	[C] confidencialidad	- [D] datos / información - [keys] claves

		aprovechando un fallo del sistema de identificación y autorización.	[I] integridad	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 “monitorización de 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: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.	[I] integridad (trazabilidad)	- S] servicios - [D.log] registros de actividad
[A.14]	Interceptación de información	El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se	[C] confidencialidad	- [COM] redes de comunicaciones

	(escucha)	vea alterada.		
[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	Alteración intencionada del funcionamiento de los	[C]	- [SW] aplicaciones

	programas	programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza (alteración de programas)	confidencialidad [I] integridad [D] disponibilidad	(software)
[A.22]	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 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.	[D] disponibilidad [C] confidencialidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar
[A.26]	Ataque	Vandalismo, terrorismo, acción militar, etc.	[D] disponibilidad	- [HW] equipos

	destructivo	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)		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 MODELO DE GESTIÓN DE RIESGOS

N° Vulnerabilidad	
1	Ausencia de personal
2	Acceso físico no autorizado
3	Acceso no autorizado a la documentación del sistema
4	Acceso no autorizado a la información
5	Acceso no autorizado a la información, redes y sistemas
6	Acceso no autorizado a las infraestructuras informáticas
7	Acceso no autorizado a las librerías fuente de los programas
8	Acceso no autorizado a los ordenadores
9	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 (externalizació
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 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 y		
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 activos 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.		
8.1.2	Investigación del personal que va a ser contratado	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 cabo 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 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, envíos y áreas de carga	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 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, y también se deberían		

10.2.3	Administración de cambios a servicios de terceros	Se deberían gestionar los cambios en 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 a cerca 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 procedimientos	Debería establecerse 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 de planes de continuidad	Debería desarrollarse e implantarse 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	Protección de las herramientas para auditoría del sistema	El acceso a las herramientas de auditoría de los sistemas de información deberían estar protegidos para evitar cualquier posible peligro o uso indebido.		

ANEXO N° 08

NORMATIVAS DE LA SBS EN RELACIÓN A LA GESTIÓN DE RIESGOS

CIRCULAR Nº G-105-2002

Alcance
Artículo 1º.- Las disposiciones de la presente norma son aplicables a las empresas señaladas en los artículos 16° y 17° de la Ley General, al Banco Agropecuario, a la Corporación Financiera de Desarrollo S.A. (COFIDE), al Banco de la Nación, a la Fundación Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI) y a las derramas y cajas de beneficios que se encuentren bajo la supervisión de esta Superintendencia, en adelante empresas.

Definiciones
Artículo 2º .- Para efectos de la presente norma, serán de aplicación las siguientes definiciones:

a. Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.

b. Ley General: Ley N° 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros.

c. Proceso crítico: Proceso considerado indispensable para la continuidad de las operaciones y servicios de la empresa, cuya realización podría ser razonablemente desarrollada por la empresa supervisada.[2]

d. Reglamento: Reglamento para la Administración de los Riesgos de Operación aprobado por Resolución SBS N° 006-2002 del 4 de enero de 2002.

e. Riesgo de operación: Entiéndase por riesgo de operación a la posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación. 1

S, TECNOLOGÍA, PERSONAL,

f. Riesgos de tecnología de información: Los riesgos de operación asociados a los sistemas informáticos y a la tecnología relacionada a dichos sistemas, que pueden afectar el desarrollo de las operaciones y servicios que realiza la empresa al atentar contra la confidencialidad, integridad y disponibilidad de la información, entre otros criterios.

g. Seguridad de la información: Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad.

[2] Literales c. y e. sustituidos mediante Resolución SBS N° 240-2005 del 08/02/2005

h. Objetivo de control: Una declaración del propósito o resultado deseado mediante la implementación de controles apropiados en una actividad de tecnología de información particular.

Responsabilidad de la empresa
Artículo 3°.- Las empresas deben establecer e implementar las políticas y procedimientos necesarios para administrar de manera adecuada y prudente los riesgos de tecnología de información, incidiendo en los procesos críticos asociados a dicho riesgo, considerando las disposiciones contenidas en la presente norma, en el Reglamento, y en el Reglamento del Sistema de Control Interno aprobado mediante la Resolución SBS Nº 1040-99 del 26 de noviembre de 1999.

La administración de dicho riesgo debe permitir el adecuado cumplimiento de los siguientes criterios de control interno:

I. Eficacia. La información debe ser relevante y pertinente para los objetivos de negocio y ser entregada en una forma adecuada y oportuna conforme las necesidades de los diferentes niveles de decisión y operación de la empresa.
II. Eficiencia. La información debe ser producida y entregada de forma productiva y económica.
III. Confidencialidad. La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.
IV. Integridad. La información debe ser completa, exacta y válida.
V. Disponibilidad. La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida.
VI. Cumplimiento normativo. La información debe cumplir con los criterios y estándares internos de la empresa, las regulaciones definidas externamente por el marco legal aplicable y las correspondientes entidades reguladoras, así como los contenidos de los contratos pertinentes.

Estructura organizacional y procedimientos
Artículo 4°.- Las empresas deben definir y mantener una estructura organizacional y procedimientos que les permita administrar adecuadamente los riesgos asociados a la tecnología de información, consistente con su tamaño y naturaleza, así como con la complejidad de las operaciones que realizan.

Administración de la seguridad de información
Artículo 5º.- Las empresas deberán establecer, mantener y documentar un sistema de administración de la seguridad de la información, en adelante "Plan de Seguridad de la información - (PSI)". El PSI debe incluir los activos de tecnología que deben ser protegidos, la metodología usada, los objetivos de control y controles, así como el grado de seguridad requerido.

Las actividades mínimas que deben desarrollarse para implementar el PSI, son las siguientes:

a. Definición de una política de seguridad.
b. Evaluación de riesgos de seguridad a los que está expuesta la información

c. Selección de controles y objetivos de control para reducir, eliminar o evitar los riesgos identificados, indicando las razones de su inclusión o exclusión.
d. Plan de implementación de los controles y procedimientos de revisión periódicos.
e. Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría.
-

Las empresas bancarias y las empresas de operaciones múltiples que accedan al módulo 3 de operaciones a que se refiere el artículo 290º de la Ley General deberán contar con una función de seguridad a dedicación exclusiva.

Subcontratación (outsourcing)

Artículo 6º.- La empresa es responsable y debe verificar que se mantengan las características de seguridad de la información contempladas en la presente norma, incluso cuando ciertas funciones o procesos críticos puedan ser objeto de una subcontratación. Para ello se tendrá en cuenta lo dispuesto en la Primera Disposición Final y Transitoria del Reglamento. Asimismo, la empresa debe asegurarse y verificar que el proveedor del servicio sea capaz de aislar el procesamiento y la información objeto de la subcontratación, en todo momento y bajo cualquier circunstancia.

En caso que las empresas deseen realizar su procesamiento principal en el exterior, requerirán de la autorización previa y expresa de esta Superintendencia. Las empresas que a la fecha de vigencia de la presente norma se encontrasen en la situación antes señalada, deberán solicitar la autorización correspondiente. Para la evaluación de estas autorizaciones, las empresas deberán presentar documentación que sustente lo siguiente:

a) La forma en que la empresa asegurará el cumplimiento de la presente circular y la Primera Disposición Final y Transitoria del Reglamento.
b) La empresa, así como los representantes de quienes brindarán el servicio de procesamiento en el exterior, deberán asegurar adecuado acceso a la información con fines de supervisión, en tiempos razonables y a solo requerimiento.

Aspectos de la seguridad de información

Artículo 7°.- Para la administración de la seguridad de la información, las empresas deberán tomar en consideración los siguientes aspectos:

- 7.1 Seguridad lógica

Las empresas deben definir una política para el control de accesos, que incluya los criterios para la concesión y administración de los accesos a los sistemas de información, redes y sistemas operativos, así como los derechos y atributos que se confieren.

Entre otros aspectos, debe contemplarse lo siguiente:

a) Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios. Revisiones periódicas deben efectuarse sobre los derechos concedidos a los usuarios.

b) Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.
c) Controles especiales sobre utilidades del sistema y herramientas de auditoría.
d) Seguimiento sobre el acceso y uso de los sistemas y otras instalaciones físicas, para detectar actividades no autorizadas.
e) Usuarios remotos y computación móvil.

- 7.2 Seguridad de personal

Las empresas deben definir procedimientos para reducir los riesgos asociados al error humano , robo, fraude o mal uso de activos, vinculados al riesgo de tecnología de información. Al establecer estos procedimientos, deberá tomarse en consideración, entre otros aspectos, la definición de roles y responsabilidades establecidos sobre la seguridad de información, verificación de antecedentes, políticas de rotación y vacaciones, y entrenamiento.

- 7.3 Seguridad física y ambiental

Las empresas deben definir controles físicos al acceso, daño o interceptación de información. El alcance incluirá las instalaciones físicas, áreas de trabajo, equipamiento, cableado, entre otros bienes físicos susceptibles a riesgos de seguridad.

Se definirán medidas adicionales para las áreas de trabajo con necesidades especiales de seguridad, como los centros de procesamiento, entre otras zonas en que se maneje información que requiera de alto nivel de protección.

7.4 Clasificación de seguridad

Las empresas deben realizar un inventario periódico de activos asociados a la tecnología de información que tenga por objetivo proveer la base para una posterior clasificación de seguridad de dichos activos. Esta clasificación debe indicar el nivel de riesgo existente para la empresa en caso de falla sobre la seguridad, así como las medidas apropiadas de control que deben asociarse a las clasificaciones.

- Administración de las operaciones y comunicaciones

Artículo 8º.- Las empresas deben establecer medidas de administración de las operaciones y comunicaciones que entre otros aspectos contendrán lo siguiente:

- Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.
- Control sobre los cambios del ambiente de desarrollo al de producción.
- Separación de funciones para reducir el riesgo de error o fraude.
- Separación del ambiente de producción y el de desarrollo.
- Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.
- Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas.
- Seguridad sobre correo electrónico.
- Seguridad sobre banca electrónica.

- Desarrollo y mantenimiento de sistemas informáticos - Requerimientos de seguridad

Artículo 9º.- Para la administración de la seguridad en el desarrollo y mantenimiento de sistemas informáticos, se debe tomar en cuenta, entre otros, los siguientes criterios:

a) Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida.
b) Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida.
c) Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.
d) Controlar el acceso a las librerías de programas fuente .
e) Mantener un estricto y formal control de cambios, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios.

Procedimientos de respaldo
Artículo 10º.- Las empresas deben establecer procedimientos de respaldo regulares y periódicamente validados. Estos procedimientos deben incluir las medidas necesarias para asegurar que la información esencial pueda ser recuperada en caso de falla en los medios o luego de un desastre. Estas medidas serán coherentes con lo requerido en el Plan de Continuidad.

La empresa debe conservar la información de respaldo y los procedimientos de restauración en una ubicación remota, a suficiente distancia para no verse comprometida ante un daño en el centro principal de procesamiento.

- Planeamiento para la continuidad de negocios

Artículo 11º.- Las empresas, bajo responsabilidad de la Gerencia y el Directorio, deben desarrollar y mantener un "Plan de Continuidad de Negocios" (PCN), que tendrá como objetivo asegurar un nivel aceptable de operatividad de los procesos críticos, ante fallas mayores internas o externas.

Criterios para el diseño e implementación del Plan de Continuidad de Negocios
Artículo 12º.- Para el desarrollo del PCN se debe realizar previamente una evaluación de riesgos asociados a la seguridad de la información. Culminada la evaluación, se desarrollarán sub-planes específicos para mantener o recuperar los procesos críticos de negocios ante fallas en sus activos, causadas por eventos internos (virus, errores no esperados en la implementación, otros), o externos (falla en las comunicaciones o energía, incendio, terremoto, proveedores, otros).

Prueba del Plan de Continuidad de Negocios
Artículo 13º.- La prueba del PCN es una herramienta de la dirección para controlar los riesgos sobre la continuidad de operación y sobre la disponibilidad de la información, por lo que la secuencia, frecuencia y profundidad de la prueba del PCN, deberá responder a la evaluación formal y prudente que sobre dicho riesgo realice cada empresa.

En todos los casos, mediante una única prueba o una secuencia de ellas, según lo considere adecuado cada empresa de acuerdo a su evaluación de riesgos, los principales aspectos del PCN deberán ser probados cuando menos cada dos años.

Anualmente, dentro del primer mes del ejercicio[3], se enviará a la Superintendencia el programa de pruebas correspondiente, en que se indicará las actividades a realizar durante el ciclo de 2 años y una descripción de los objetivos a alcanzar en el año que se inicia.

- Cumplimiento normativo

Artículo 14º.- La empresa deberá asegurar que los requerimientos legales, contractuales, o de regulación sean cumplidos, y cuando corresponda, incorporados en la lógica interna de las aplicaciones informáticas.

Privacidad de la información

Artículo 15º .- Las empresas deben adoptar medidas que aseguren razonablemente la privacidad de la información que reciben de sus clientes y usuarios de servicios, conforme la normatividad vigente sobre la materia.

- Auditoría Interna y Externa

Artículo 16º.- La Unidad de Auditoría Interna deberá incorporar en su Plan Anual de Trabajo la evaluación del cumplimiento de lo dispuesto en la presente norma.

Asimismo, las Sociedades de Auditoría Externa deberán incluir en su informe sobre el sistema de control interno comentarios dirigidos a indicar si la entidad cuenta con políticas y procedimientos para la administración de los riesgos de tecnología de información, considerando asimismo, el cumplimiento de lo dispuesto en la presente norma.

Auditoría de sistemas

Artículo 17º.- Las empresas bancarias y aquellas empresas autorizadas a operar en el Módulo 3 conforme lo señalado en el artículo 290° de la Ley General, deberán contar con un servicio permanente de auditoría de sistemas, que colaborará con la Auditoría interna en la verificación del cumplimiento de los criterios de control interno para las tecnologías de información, así como en el desarrollo del Plan de Auditoría.

El citado servicio de auditoría de sistemas tomará en cuenta, cuando parte del procesamiento u otras funciones sean realizadas por terceros, que es necesario conducir su revisión con los mismos estándares exigidos a la empresa, por lo que tomará en cuenta las disposiciones indicadas en la Primera Disposición Final y Transitoria del Reglamento.

Las empresas autorizadas para operar en otros módulos, para la verificación del cumplimiento antes señalado, deberán asegurar una combinación apropiada de auditoría interna y/o externa, compatible con el nivel de complejidad y perfil de riesgo de la empresa. La Superintendencia dispondrá un tratamiento similar a las empresas pertenecientes al módulo 3, cuando a su criterio la complejidad de sus sistemas informáticos y su perfil de riesgo así lo amerite.

Información a la Superintendencia

[3] El plazo de remisión ha sido modificado a 90 días calendario siguientes al cierre de cada ejercicio, por la Circular G-130-2007 de fecha 07 de junio de 2007.

Artículo 18°.- El informe anual que las empresas deben presentar a la Superintendencia, según lo dispuesto en el Artículo 13° del Reglamento, deberá incluir los riesgos de operación asociados a la tecnología de información, como parte integral de dicha evaluación, para lo cual se sujetará a lo dispuesto en dicho Reglamento y a lo establecido en la presente norma.

Sanciones

Artículo 19°.- En caso de incumplimiento de las disposiciones contenidas en la presente norma, la Superintendencia aplicará las sanciones correspondientes de conformidad con lo establecido en el Reglamento de Sanciones.

Plan de adecuación

Artículo 20°.- En el Plan de Adecuación señalado en el segundo párrafo de la Cuarta Disposición Final y Transitoria del Reglamento, las empresas deberán incluir un sub-plan para la adecuación a las disposiciones contenidas en la presente norma.

Plazo de adecuación

Artículo 21°.- Las empresas contarán con un plazo de adecuación a las disposiciones de la presente norma que vence el 30 de junio de 2003

RESOLUCIÓN S.B.S. N° 2116 -2009
REGLAMENTO PARA LA GESTIÓN DEL RIESGO OPERACIONAL

CAPITULO I
DISPOSICIONES GENERALES

Artículo 1°.- Alcance
El presente Reglamento será de aplicación a las empresas señaladas en el artículo 16° de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP), en adelante empresas.

También será de aplicación a las Cajas Municipales de Ahorro y Crédito (CMAC), la Caja Municipal de Crédito Popular, el Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI), el Banco de la Nación, el Banco Agropecuario, la Corporación Financiera de Desarrollo (COFIDE), el Fondo MIVIVIENDA S.A., y las Derramas y Cajas de Beneficios bajo control de la Superintendencia, en tanto no se contrapongan con las normativas específicas que regulen el accionar de estas empresas.

Las empresas de servicios complementarios y conexos señaladas en el artículo 17° de la Ley General se sujetarán, para la gestión de su riesgo operacional, a lo establecido en sus normas específicas. Asimismo, podrán tomar en consideración las disposiciones señaladas en el presente Reglamento en función a su tamaño y complejidad.

Artículo 2°.- Definiciones
Para los efectos de la presente norma deben considerarse los siguientes términos:

a. Apetito por el riesgo: El nivel de riesgo que la empresa está dispuesta a asumir en su búsqueda de rentabilidad y valor.
b. Directorio: Toda referencia al directorio, entiéndase realizada también a cualquier órgano equivalente.
c. Evento: Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.
d. Evento de pérdida por riesgo operacional: El evento que conduce a una o varias pérdidas, cuyo origen corresponde al riesgo operacional.
e. Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada.
f. Proceso: Conjunto de actividades, tareas y procedimientos organizados y repetibles que producen un resultado esperado.
g. Reglamento de la Gestión Integral de Riesgos: Reglamento de la Gestión Integral de Riesgos aprobado mediante la Resolución SBS Nº 37-2008 del 10 de enero de 2008.
h. Riesgo legal: Posibilidad de ocurrencia de pérdidas financieras debido a la falla en la ejecución de contratos o acuerdos, al incumplimiento no intencional de las normas, así como a factores externos, tales como cambios regulatorios, procesos judiciales, entre otros.
i. Subcontratación: Modalidad de gestión mediante la cual una empresa contrata a un tercero para que éste desarrolle un proceso que podría ser realizado por la empresa contratante.

j. Superintendencia: Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.
k. Tolerancia al riesgo: El nivel de variación que la empresa está dispuesta a asumir en caso de desviación de los objetivos empresariales trazados.

Artículo 3°.- Riesgo operacional
Entiéndase por riesgo operacional a la posibilidad de ocurrencia de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.

Las empresas deben realizar una gestión adecuada del riesgo operacional que enfrentan, para lo cual observarán los criterios mínimos indicados en el presente Reglamento.

Artículo 4° Factores que originan el riesgo operacional

i) Procesos internos
Las empresas deben gestionar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, relacionados al diseño inapropiado de los procesos o a políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

ii) Personal
Las empresas deben gestionar apropiadamente los riesgos asociados al personal de la empresa, relacionados a la inadecuada capacitación, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, entre otros.

iii) Tecnología de información
Las empresas deben gestionar los riesgos asociados a la tecnología de información, relacionados a fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, problemas de calidad de información, la inadecuada inversión en tecnología, entre otros aspectos.

iv) Eventos externos
Las empresas deberán gestionar los riesgos asociados a eventos externos ajenos al control de la empresa, relacionados por ejemplo a fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, entre otros factores.

Artículo 5°.- Eventos de pérdida por riesgo operacional

Los eventos de pérdida por riesgo operacional pueden ser agrupados de la manera descrita a continuación:

a. Fraude interno.- Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas empresariales en las que se encuentra implicado, al menos, un miembro de la empresa, y que tiene como fin obtener un beneficio ilícito.

b. Fraude externo.- Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir la legislación, por parte de un tercero, con el fin de obtener un beneficio ilícito.

c. Relaciones laborales y seguridad en el puesto de trabajo.- Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamos por daños personales, o sobre casos relacionados con la diversidad o discriminación.

d. Clientes, productos y prácticas empresariales.- Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación empresarial frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto.

e. Daños a activos materiales.- Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.

f. Interrupción del negocio y fallos en los sistemas.- Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas.

g. Ejecución, entrega y gestión de procesos.- Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores.

En el Anexo N° 1, se incluye una categorización de los tipos de eventos de pérdida aplicable según el sector al que pertenece la empresa.

CAPITULO II
ROLES Y RESPONSABILIDADES

Artículo 6°.- Responsabilidades del Directorio
El Directorio tiene las siguientes responsabilidades específicas respecto a la gestión del riesgo operacional:

a) Definir la política general para la gestión del riesgo operacional.
b) Asignar los recursos necesarios para la adecuada gestión del riesgo operacional, a fin de contar con la infraestructura, metodología y personal apropiados.
c) Establecer un sistema de incentivos que fomente la adecuada gestión del riesgo operacional y que no favorezca la toma inapropiada de riesgos.
d) Aprobar el manual de gestión del riesgo operacional.
e) Conocer los principales riesgos operacionales afrontados por la entidad, estableciendo cuando ello sea posible, adecuados niveles de tolerancia y apetito por el riesgo.
f) Establecer un sistema adecuado de delegación de facultades y de segregación de funciones a través de toda la organización.
g) Obtener aseguramiento razonable que la empresa cuenta con una efectiva gestión del riesgo operacional, y que los principales riesgos identificados se encuentran bajo control dentro de los límites que han establecido.

Artículo 7°.- Responsabilidades de la Gerencia
La gerencia general tiene la responsabilidad de implementar la gestión del riesgo operacional conforme a las disposiciones del Directorio.

Los gerentes de las unidades organizativas de negocios o de apoyo tienen la responsabilidad de gestionar el riesgo operacional en su ámbito de acción, dentro de las políticas, límites y procedimientos establecidos.

Artículo 8°.- Comité de riesgos
Las funciones del Comité de Riesgos señaladas en el Reglamento de la Gestión Integral de Riesgos, son de aplicación a la gestión del riesgo operacional en lo que corresponda.

Artículo 9°.- Unidad de riesgos
De conformidad con el Reglamento de la Gestión Integral de Riesgos, las empresas podrán contar con una Unidad de Riesgos centralizada o con unidades especializadas en la gestión de riesgos específicos.

En ese sentido, la Unidad de Riesgos de la empresa o, de ser el caso, la unidad especializada de gestión del riesgo operacional deberá cumplir con las siguientes funciones:

a. Proponer políticas para la gestión del riesgo operacional.
b. Participar en el diseño y permanente actualización del Manual de gestión del riesgo operacional.
c. Desarrollar la metodología para la gestión del riesgo operacional.
d. Apoyar y asistir a las demás unidades de la empresa para la aplicación de la metodología de gestión del riesgo operacional.
e. Evaluación del riesgo operacional, de forma previa al lanzamiento de nuevos productos y ante cambios importantes en el ambiente operativo o informático.
f. Consolidación y desarrollo de reportes e informes sobre la gestión del riesgo operacional por proceso, o unidades de negocio y apoyo.
g. Identificación de las necesidades de capacitación y difusión para una adecuada gestión del riesgo operacional.
h. Otras necesarias para el desarrollo de la función.

Las empresas deberán asignar recursos suficientes para la gestión del riesgo operacional, que les permita un adecuado cumplimiento de las funciones señaladas en el presente artículo y asegurar una adecuada independencia entre el área que asuma las funciones de gestión del riesgo operacional señaladas en el presente artículo y aquellas otras unidades de negocio o de apoyo.

Los bancos, las financieras, las empresas de seguros y las AFP deberán contar con una función especializada en riesgo operacional. De acuerdo al tamaño y complejidad de las operaciones que realice la empresa, la Superintendencia podrá requerir la creación de una unidad especializada.

CAPITULO III
LA GESTIÓN DEL RIESGO OPERACIONAL

Artículo 10°.- Manual de gestión del riesgo operacional
Las empresas deberán contar con un manual de gestión del riesgo operacional, el cual deberá contemplar por lo menos los siguientes aspectos:

a. Políticas para la gestión del riesgo operacional.
b. Funciones y responsabilidades asociadas con la gestión del riesgo operacional del Directorio, la Gerencia General, el Comité de Riesgos, la Unidad de Riesgos (o la unidad especializada, si corresponde) y las unidades de negocio y de apoyo.
c. Descripción de la metodología aplicada para la gestión del riesgo operacional.
d. La forma y periodicidad con la que se deberá informar al Directorio y a la Gerencia General, entre otros, sobre la exposición al riesgo operacional de la empresa y de cada unidad de negocio.
e. El proceso para la aprobación de propuestas de nuevas operaciones, productos y servicios que deberá contar, entre otros aspectos, con una descripción general de la nueva operación, producto o servicio de que se trate, los riesgos identificados y las acciones a tomar para su control.

Artículo 11°.- Metodología para la gestión del riesgo operacional
La metodología definida por la empresa para la gestión del riesgo operacional, cuando sea tomada en su conjunto, deberá considerar los componentes señalados en el artículo 4° del Reglamento de la Gestión Integral de Riesgos.

Asimismo, deberán cumplirse los siguientes criterios:

a. La metodología debe ser implementada en toda la empresa en forma consistente.
b. La empresa debe asignar recursos suficientes para aplicar su metodología en las principales líneas de negocio, y en los procesos de control y de apoyo.
c. La aplicación de la metodología debe estar integrada a los procesos de gestión de riesgos de la empresa.
d. Deben establecerse incentivos que permitan una mejora continua de la gestión del riesgo operacional.
e. La aplicación de la metodología de gestión del riesgo operacional debe estar adecuadamente documentada.
f. Deben establecerse procedimientos que permitan asegurar el cumplimiento de su metodología de gestión del riesgo operacional.

Artículo 12°.- Base de datos de eventos de pérdida
Las empresas deberán contar con una base de datos de los eventos de pérdida por riesgo operacional.

Debe tenerse en cuenta que un evento puede tener como efecto una o más pérdidas, por lo cual las empresas deberán estar en capacidad de agrupar las pérdidas ocurridas por evento.

La base de datos deberá cumplir con los siguientes criterios:

a. Deben registrarse los eventos de pérdida originados en toda la empresa, para lo cual se diseñarán políticas, procedimientos de captura, y entrenamiento al personal que interviene en el proceso.

b. Debe registrarse, como mínimo, la siguiente información referida al evento y a las pérdidas asociadas:

- Código de identificación del evento.
- Tipo de evento de pérdida (según tipos de eventos señalados en el Anexo 1 del presente Reglamento).
- Línea de negocio asociada, según líneas señaladas en el Anexo 2 del presente Reglamento para las empresas del sistema financiero, Anexo 3 para las empresas de seguros y Anexo 4 para las AFP. Deberán considerarse los niveles 1 y 2 de los cuadros señalados en los anexos. Estos cuadros podrán ser actualizados por la Superintendencia mediante Circular.
- Descripción corta del evento.
- Descripción larga del evento.
- Fecha de ocurrencia o de inicio del evento.
- Fecha de descubrimiento del evento.
- Fecha de registro contable del evento.
- Monto(s) bruto(s) de la(s) pérdida(s), moneda y tipo de cambio.
- Monto(s) recuperado(s) mediante coberturas existentes de forma previa al evento, moneda, tipo de cambio y tipo de cobertura aplicada.
- Monto total recuperado, moneda y tipo de cambio.
- Cuenta(s) contable(s) asociadas.
- Identificación si el evento está asociado con el riesgo de crédito (para empresas del sistema financiero) o con el riesgo de seguros (para empresas del sistema de seguros).

En el caso de eventos con pérdidas múltiples, las empresas podrán registrar la información mínima requerida por cada pérdida, y establecer una forma de agrupar dicha información por el evento que las originó.

De otro lado, podrá registrarse información parcial de un evento, en tanto se obtengan los demás datos requeridos. Por ejemplo, podrá registrarse primero el monto de la pérdida, para posteriormente añadir las recuperaciones asociadas.

c. Deben definirse y documentarse criterios objetivos para asignar los eventos de pérdida a los tipos de evento señalados en el Anexo 1 del presente Reglamento, así como a las líneas de negocio señaladas en los Anexos 2, 3 y 4. Asimismo, deben definirse criterios específicos para aquellos casos en que un evento esté asociado a más de una línea de negocio.

d. Debe definirse un monto mínimo de pérdida a partir del cual se registrará un evento en la base de datos. Al respecto, se fija un monto mínimo de 3 000 nuevos soles para los bancos, las financieras, las compañías de seguros y las AFP, y de 1 000 nuevos soles para el resto de empresas. Las empresas podrán establecer un monto mínimo

inferior al indicado, teniendo en cuenta su volumen de operaciones y complejidad asociada. La Superintendencia podrá actualizar el monto mínimo definido por medio de Circular.

e. Debe definirse un monto mínimo de pérdida a partir del cual deberá contarse con un expediente físico o electrónico que contenga información adicional a la solicitada en el literal b. y que permita conocer el modo en que se produjo el evento, características especiales y otra información relevante, así como las acciones que hubiera tomado la empresa, incluyendo entre otras las mejoras o cambios requeridos en sus políticas o procedimientos. Dicho monto mínimo deberá ser aprobado por el Comité de Riesgos. La Superintendencia podrá establecer posteriormente un monto mínimo de carácter general.

Artículo 13°.- Gestión de la continuidad del negocio y de la seguridad de la información

Como parte de una adecuada gestión del riesgo operacional, las empresas deben implementar un sistema de gestión de la continuidad del negocio que tendrá como objetivo implementar respuestas efectivas para que la operatividad del negocio de la empresa continúe de una manera razonable, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la empresa.

Asimismo, las empresas deben contar con un sistema de gestión de la seguridad de la información, orientado a garantizar la integridad, confidencialidad y disponibilidad de la información.

Para ello, las empresas deberán aplicar las disposiciones que se establezcan en las normas específicas sobre estos temas.

Artículo 14°.- Subcontratación

Con el fin de gestionar los riesgos operacionales asociados a la subcontratación, las empresas deberán establecer políticas y procedimientos apropiados para evaluar, administrar y monitorear los procesos subcontratados. Dichas políticas y procedimientos deberán considerar:

a. El proceso de selección del proveedor del servicio
b. La elaboración del acuerdo de subcontratación
c. La gestión y monitoreo de los riesgos asociados con el acuerdo de subcontratación
d. La implementación de un entorno de control efectivo
e. Establecimiento de planes de continuidad

Los acuerdos de subcontratación deberán formalizarse mediante contratos firmados, los cuales deben incluir acuerdos de niveles de servicio, y definir claramente las responsabilidades del proveedor y de la empresa.

CAPITULO IV
REQUERIMIENTOS DE INFORMACION

Artículo 15°.- Informe a la Superintendencia
Las empresas deberán presentar a la Superintendencia informes anuales referidos a la gestión del riesgo operacional, a través del software IG-ROp, el cual se encontrará disponible en el "Portal del Supervisado". Dichos informes deberán ser remitidos a más tardar el 31 de enero del año siguiente al año de reporte. La Superintendencia podrá requerir, mediante Oficio, la actualización periódica de los informes.

El contenido mínimo del referido informe, así como los aspectos operativos del IG-ROp, relacionados con las instrucciones, responsables y demás aspectos necesarios para su adecuado funcionamiento, se establecen en el "Manual del IG-ROp", el cual estará publicado en el "Portal del Supervisado" de la SBS. Asimismo, en el Portal, se publicarán instrucciones adicionales para el adecuado uso del sistema.

Las empresas supervisadas deberán designar un funcionario responsable por la información a ser reportada a través del IG-ROp, y tomarán las medidas necesarias para asegurar la veracidad de dicha información. El funcionario responsable deberá corresponder a cualquiera de las siguientes clasificaciones: Director, Gerente o Funcionario Principal, según las disposiciones de la Circular G-119-2004, referida a las normas para el registro de Directores, Gerentes y Principales Funcionarios – REDIR.

Artículo 16°.- Información adicional
La Superintendencia podrá requerir a la empresa cualquier otra información que considere necesaria para una adecuada supervisión de la gestión del riesgo operacional de la empresa.

Asimismo, la empresa deberá tener a disposición de la Superintendencia todos los documentos mencionados por el presente Reglamento, así como los informes de auditoría o revisiones realizadas por la casa matriz en caso de ser aplicable.

CAPITULO V
COLABORADORES EXTERNOS

Artículo 17º.- Auditoría Interna
La Unidad de Auditoría Interna deberá evaluar el cumplimiento de los procedimientos utilizados para la gestión del riesgo operacional, así como de lo dispuesto en el presente Reglamento, de conformidad con lo establecido en el Reglamento de Auditoría Interna.

Artículo 18º.- Auditoría Externa
Las sociedades de auditoría externa deberán incluir en su informe sobre el sistema de control interno comentarios dirigidos a indicar si la entidad cuenta con políticas y procedimientos para la gestión del riesgo operacional, considerando el cumplimiento de lo dispuesto en el presente Reglamento.

Artículo 19º.- Empresas Clasificadoras de Riesgo
Las empresas clasificadoras de riesgo deberán tener en cuenta las políticas y procedimientos establecidos por la empresa para la gestión del riesgo operacional en el proceso de clasificación de las empresas supervisadas.

DISPOSICIONES FINALES Y TRANSITORIAS

Primera.- Autorizaciones especiales
Las empresas podrán solicitar a la Superintendencia exoneración específica de alguno de los requerimientos normativos indicados en este Reglamento, adjuntando la documentación de sustento correspondiente, para lo cual serán de aplicación los requisitos señalados en la Primera Disposición Final y Transitoria del Reglamento de la Gestión Integral de Riesgos, en lo que sea aplicable a la gestión del riesgo operacional.

Segunda.- Régimen simplificado para las Edpymes
Las Edpymes no están obligadas a implementar la base de datos de eventos de pérdida requerida en el artículo 12° del presente Reglamento. No obstante, la Superintendencia podrá exigir la aplicación de dicho artículo a aquellas Edpymes que considere apropiadas, teniendo en consideración su tamaño, complejidad y volumen de operaciones.

Tercera.- Sanciones
En caso de incumplimiento de las disposiciones contenidas en el presente Reglamento la Superintendencia aplicará las sanciones correspondientes de conformidad con lo establecido en el Reglamento de Sanciones.

Cuarta.- Transparencia
Como parte de la información que debe ser revelada en la Memoria Anual de las empresas, conforme a lo señalado en el Reglamento de la Gestión Integral de Riesgos, deben incluirse las características principales de la gestión del riesgo operacional implementada por la empresa.

Quinta.- Adecuación de las Administradoras Privadas de Fondos de Pensiones
En un plazo que no excederá de noventa (90) días calendario de haberse publicado el presente Reglamento, las AFP deberán remitir a la Superintendencia un plan de adecuación a las disposiciones contenidas en la presente norma.

Dicho plan deberá incluir un diagnóstico de la situación existente en la AFP respecto al cumplimiento de cada uno de los artículos del presente Reglamento, las acciones previstas para la total adecuación y el cronograma de las mismas, así como los funcionarios responsables del cumplimiento de dicho plan.

ANEXO N° 09

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		
Mantener y documentar un sistema de administración de la seguridad de la información - "Plan de Seguridad de la información - (PSI)" (Art. N° 05)	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	cumplimiento de la presente circular		X	
	los proveedores del		X	

características de seguridad de la información en subcontrataciones (outsourcing) (Art. N° 06)	servicio exterior, aseguran el adecuado acceso a la información con fines de supervisión			
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			X
	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.			X	

N° 12)			
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° 10

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

Criterio		ISO/IEC 27001	ISO/IEC 17799	Modelo 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 definidos y documentados	No lo considera. Sólo indica que debe procedimentarse los procesos de TI	No lo considera. Sólo indica que debe procedimentarse las buenas prácticas en sus guías de implementación	Establece criterios manera general para procedimentarse en el caso de estudio	No se ha procedimentado por que no es objetivo de la investigación
	Establece formas de inventario de	Lo define de manera general como requisito	Lo define de manera general para los	Si lo establece	Se ha establecido una clasificación en

	activos de información	de un SGSI	objetivos de control y controles del dominio "Clasificación de activos"		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 "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 para 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 "Continuidad de negocio"	No lo establece como un proceso, pero si como controles específicos	Se han establecido como controles específicos
	Define mecanismos para medir la	No define métricas, pero si establece que	No define métricas, pero si establece que	No se ha definido métricas, pero si	Se considera un proceso de evaluación de

	efectividad de los controles de las políticas de seguridad de la información	deben realizarse su seguimiento	deben realizarse su seguimiento	se ha considerado evaluación de brechas	brechas

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

Criterio	Modelo Magerit	Modelo 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 amenaza	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	Si se realiza	Se ha elaborado un listado de aplicabilidad de controles ajustado al caso de estudio
Identificación de la estrategia de implementación de controles	Determina de manera general las estrategias de implementación de controles	Sí se realiza	Adecúa la propuesta de Magerit para el caso de estudio

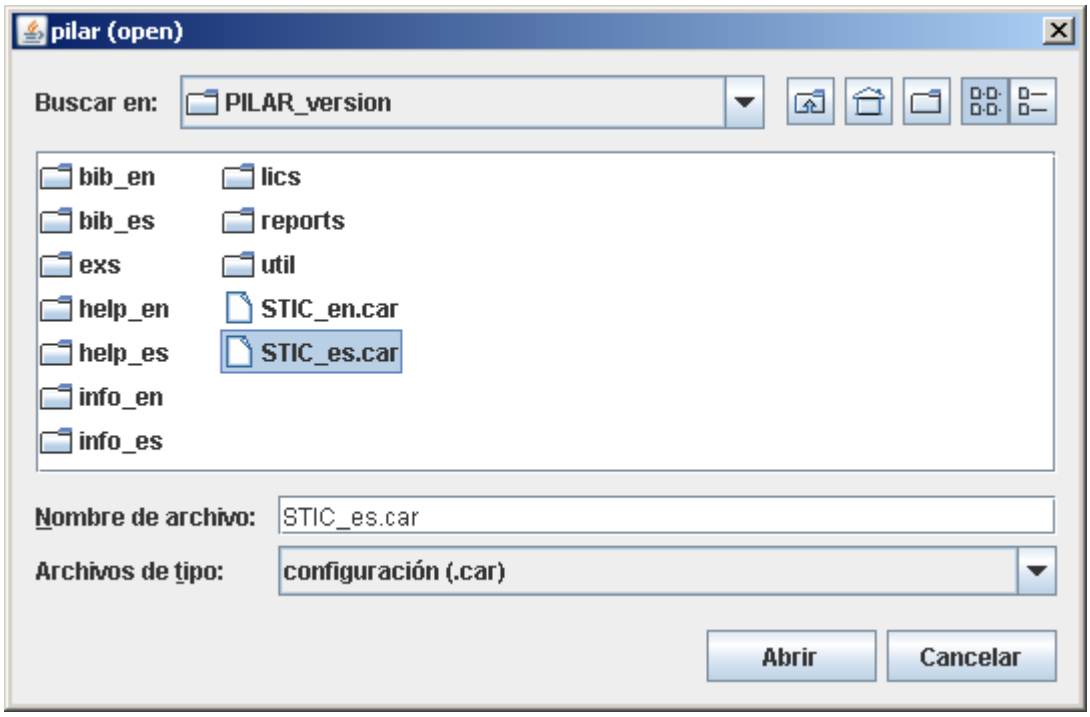
Cálculo y clasificación de la brecha de seguridad: nivel de riesgo residual	Determina una forma de valoración del riesgo residual	Sí se realiza	Se ha elaborado una matriz de riesgos específica para realizar seguimiento de la efectividad de los controles en base a evaluación de brechas
Evaluación del 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° 11

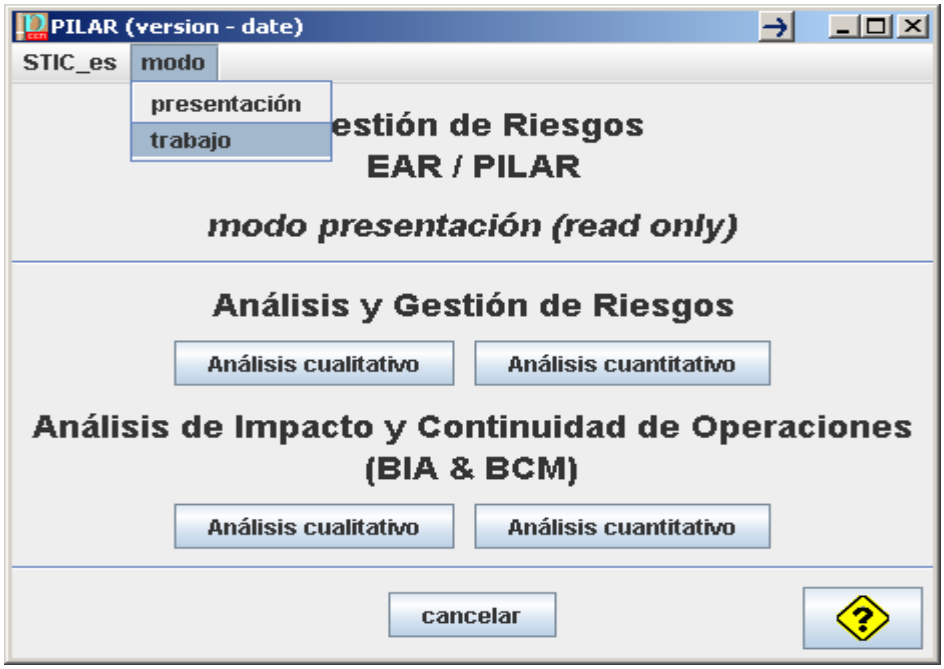
PROCESO DE INSTALACIÓN DEL SOFTWARE EAR/PILAR - ANÁLISIS Y GESTIÓN DE RIESGOS

1. PILAR solicita un fichero CAR

Lo encontrará en el directorio de la instalación:

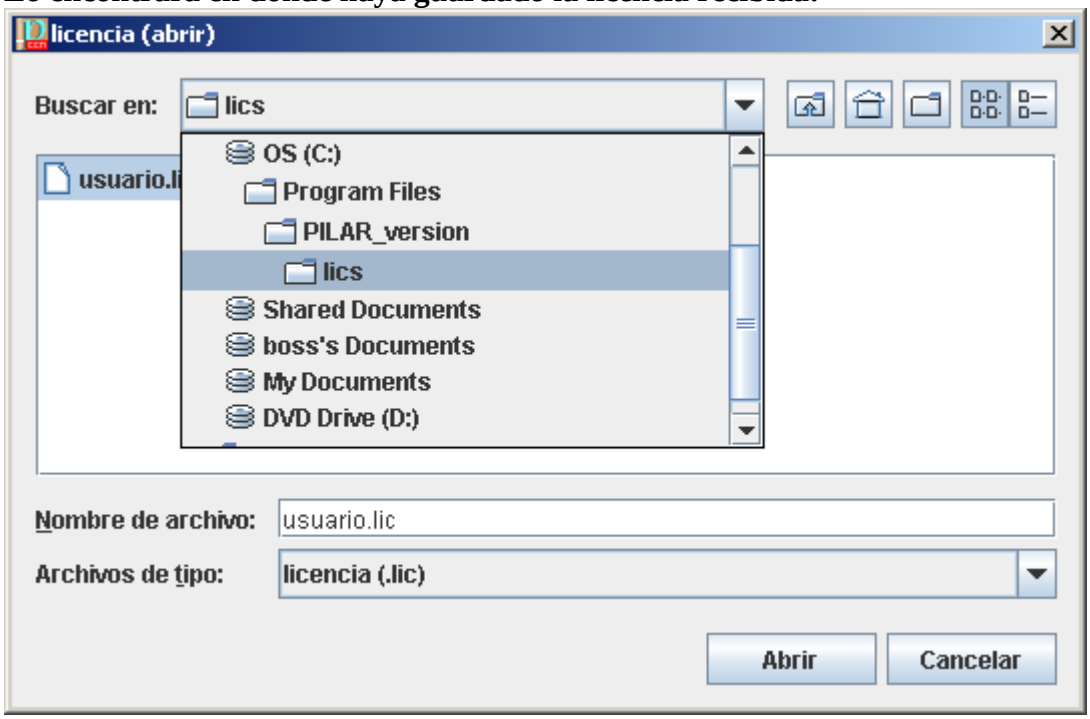


2. Cambie a modo de trabajo

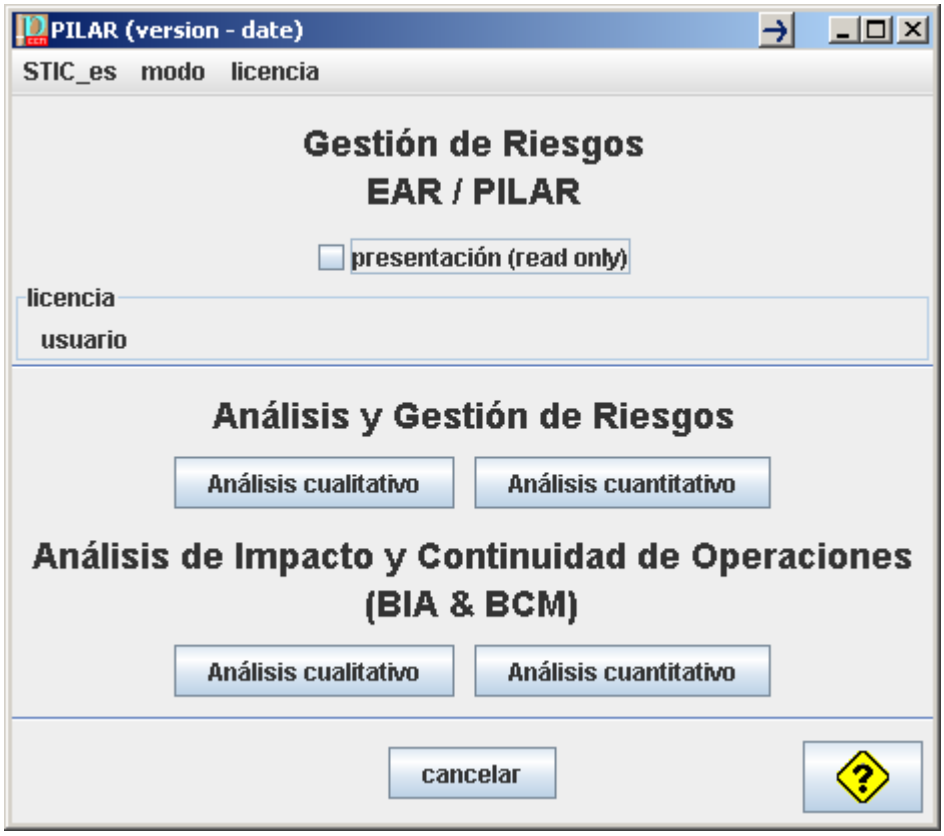


3. PILAR solicita un fichero LIC

Lo encontrará en donde haya guardado la licencia recibida:



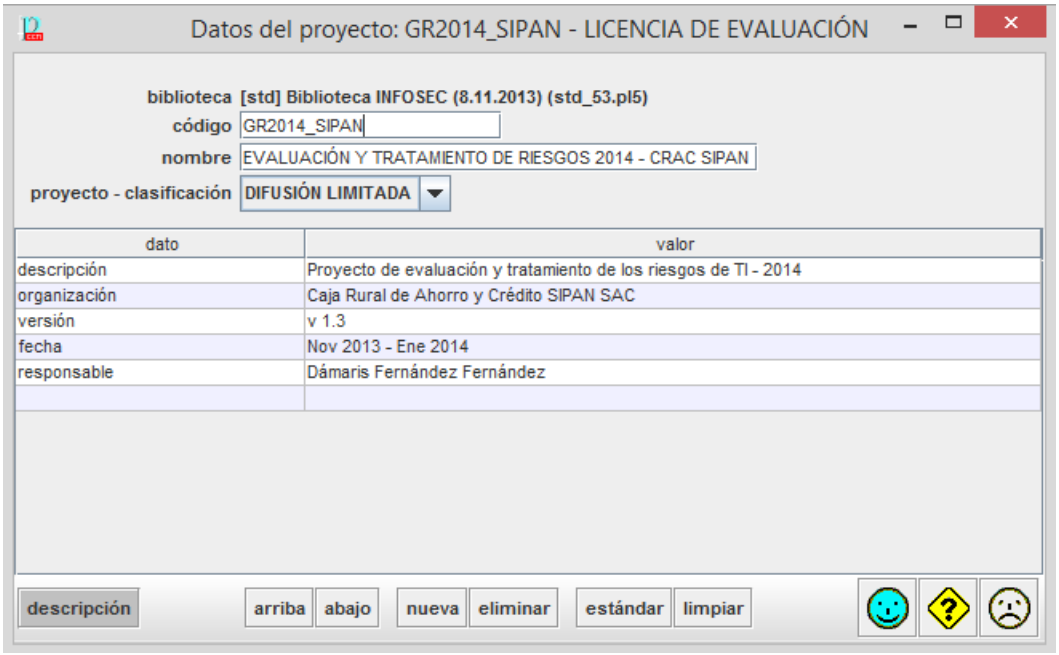
4. Listo para trabajar



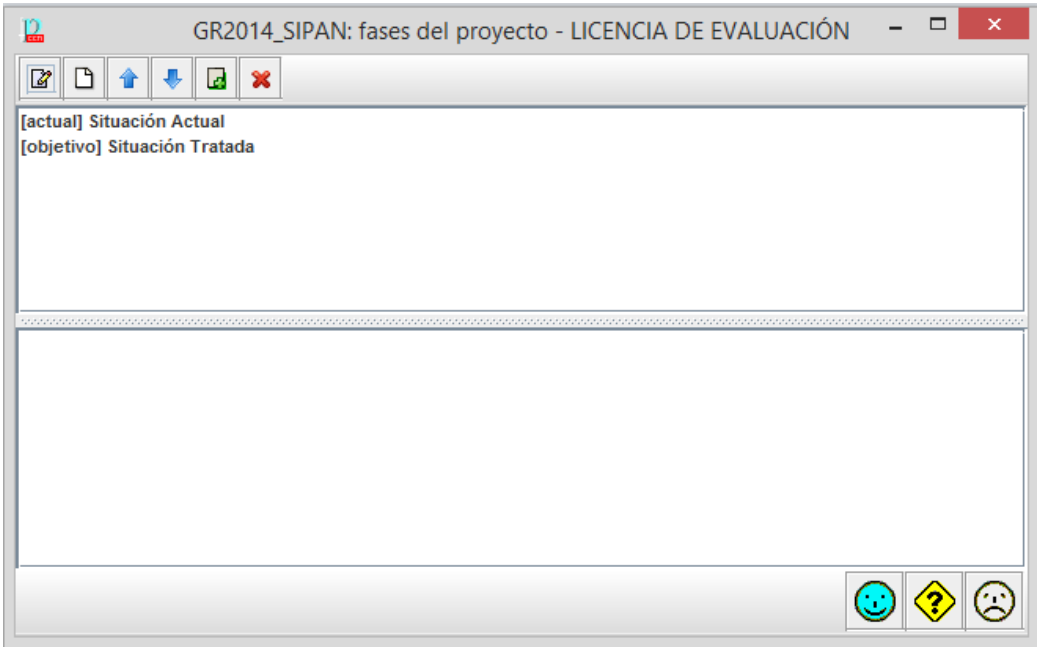
ANEXO N° 12

PANTALLAS DE SIMULACIÓN DEL MODELO DE GESTIÓN DE RIESGOS DE TI PROPUESTO EN EL SOFTWARE PILAR v 5.4.4 - 3.12.2014

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

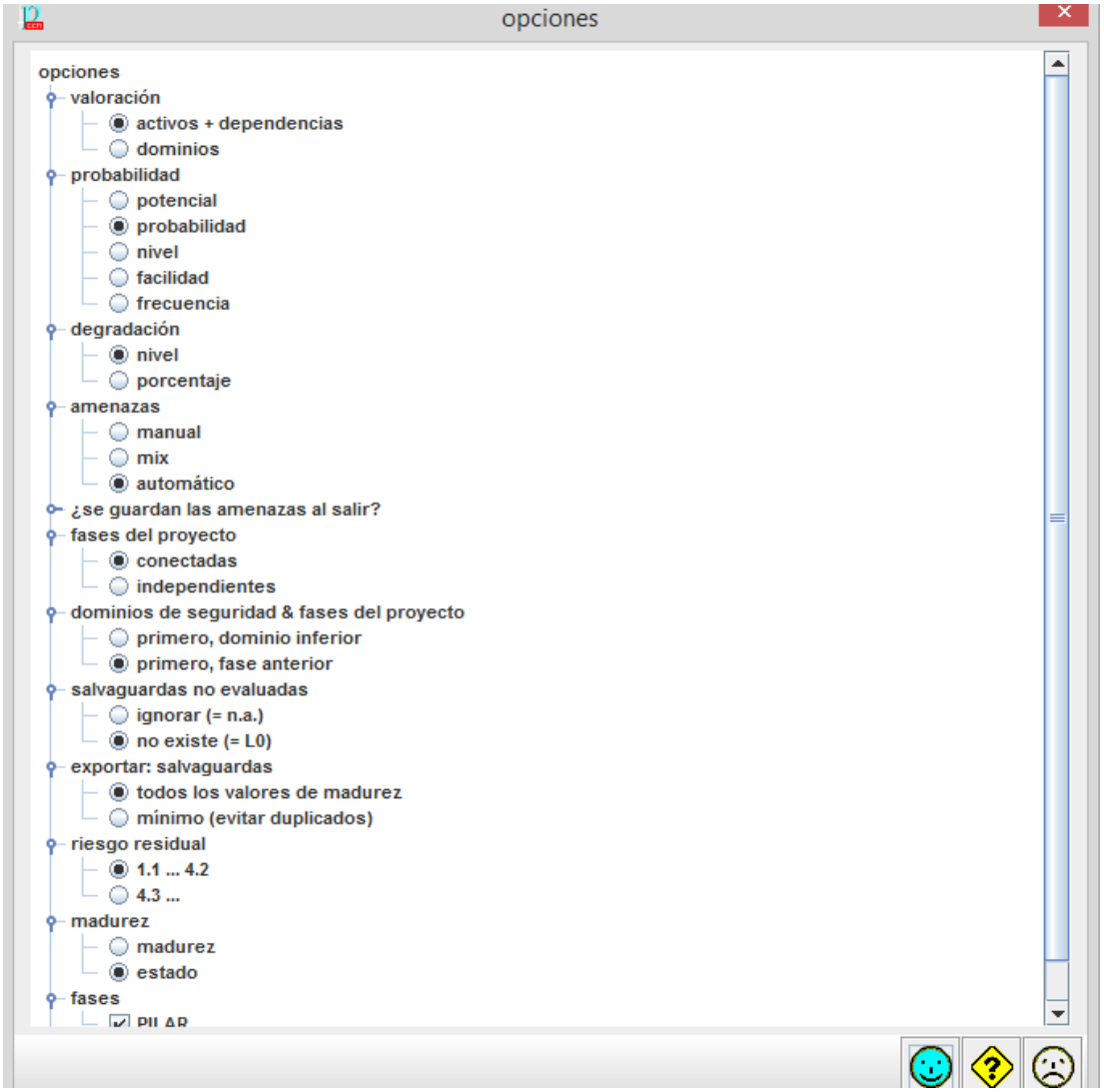


Pantalla N° 02: Definición de las fases del MGR-TI en el proyecto



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

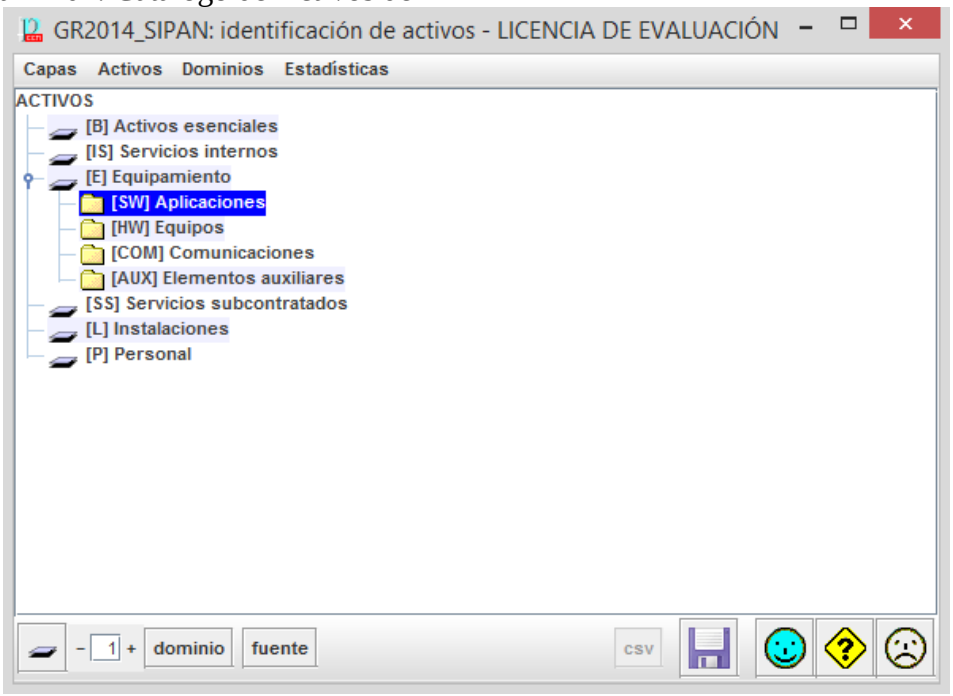
Pantalla N° 03: Ajuste de opciones y preferencias al MGR-TI



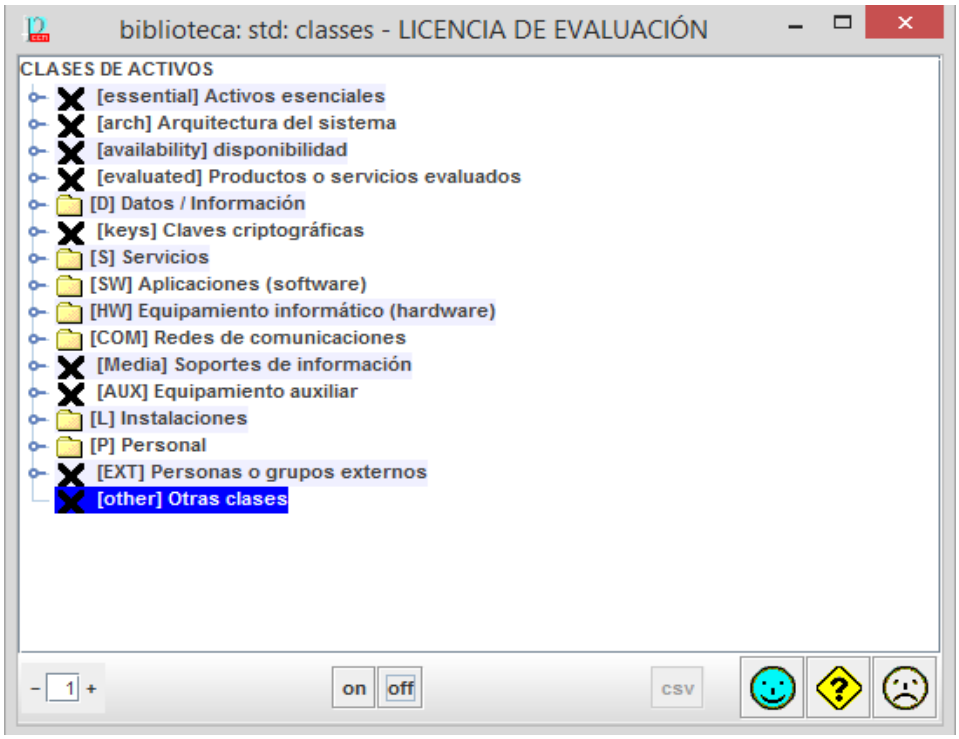
Observación: Este formulario permitió ajustar algunos parámetros del software PILAR para adecuarlo a la forma como evalúa el MGR-TI. Así tenemos:

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

Pantalla N° 04: Catálogo de Activos de PILAR



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



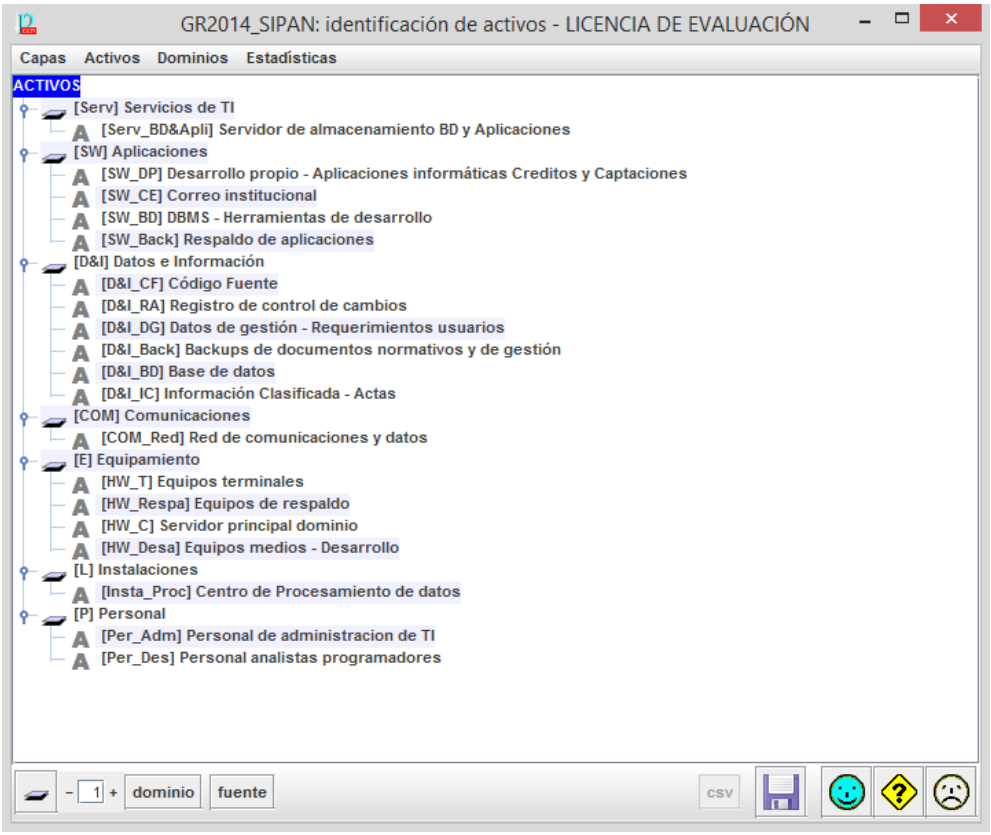
Observación: Estos formularios permiten seleccionar los activos de TI y sus correspondientes tipos, que serán considerados en la evaluación de riesgos. El software Pilar utiliza un catálogo de activos de TI según la Metodología Magerit, el mismo que se utilizó en el trabajo de tesis (**Ver anexo N° 03**).

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
[hw]	Equipos informáticos	[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

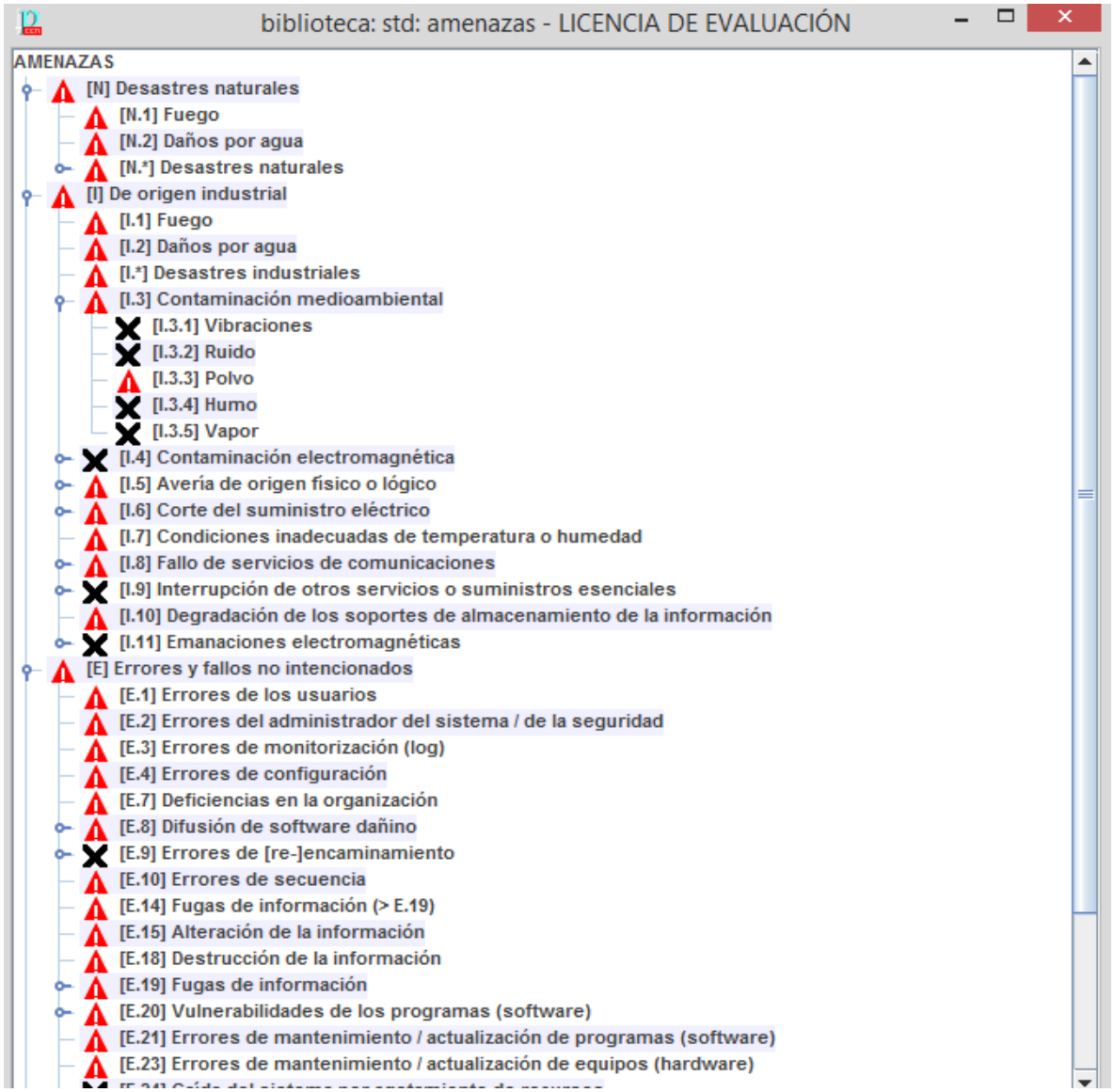
[com]	Comunicaciones	[X25]	X25 (red de datos)	Red de comunicaciones
[Inmueb]	Instalaciones	[data]	Cuarto de procesamiento de datos	Sala de servidores o Centro de Procesamiento Central
[pers]	Personal	[adm]	administradores de sistemas	Personal de área de TI
		[des]	desarrolladores / programadores	Analistas de sistemas (Responsables de la implementación de requerimientos)

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. Este listado está ajustado y personalizado para el caso de estudio (CRAC Sipán), de acuerdo al trabajo de tesis.

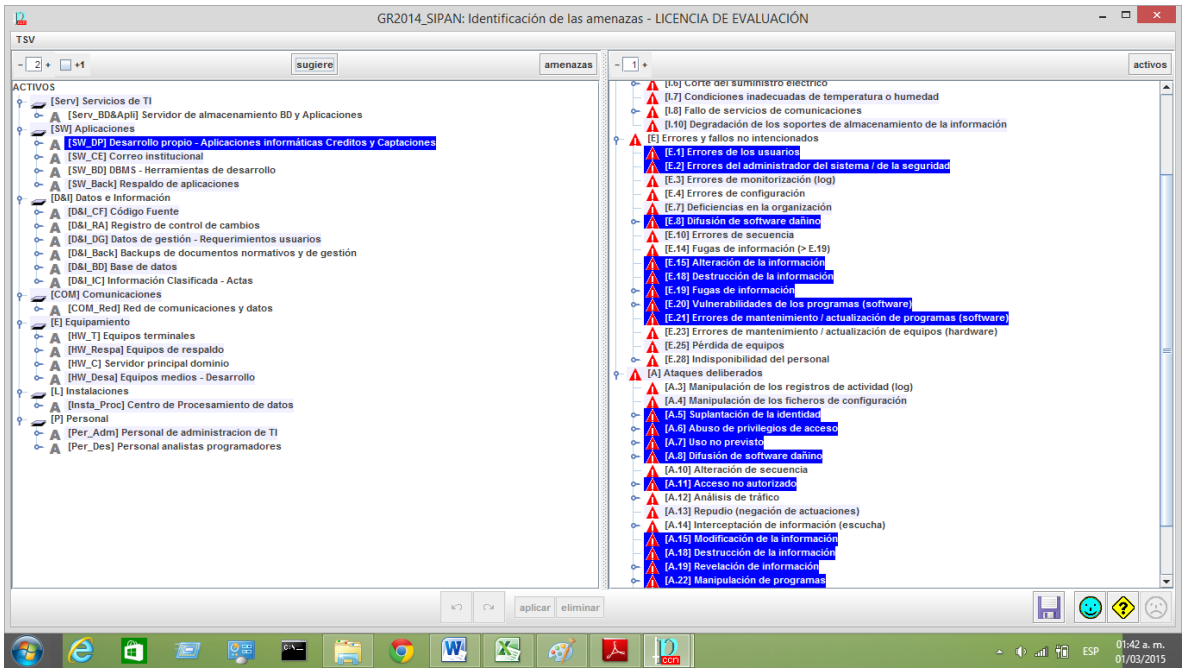
Pantalla N° 07: Catálogo de Amenazas de TI seleccionados para el caso de estudio



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.

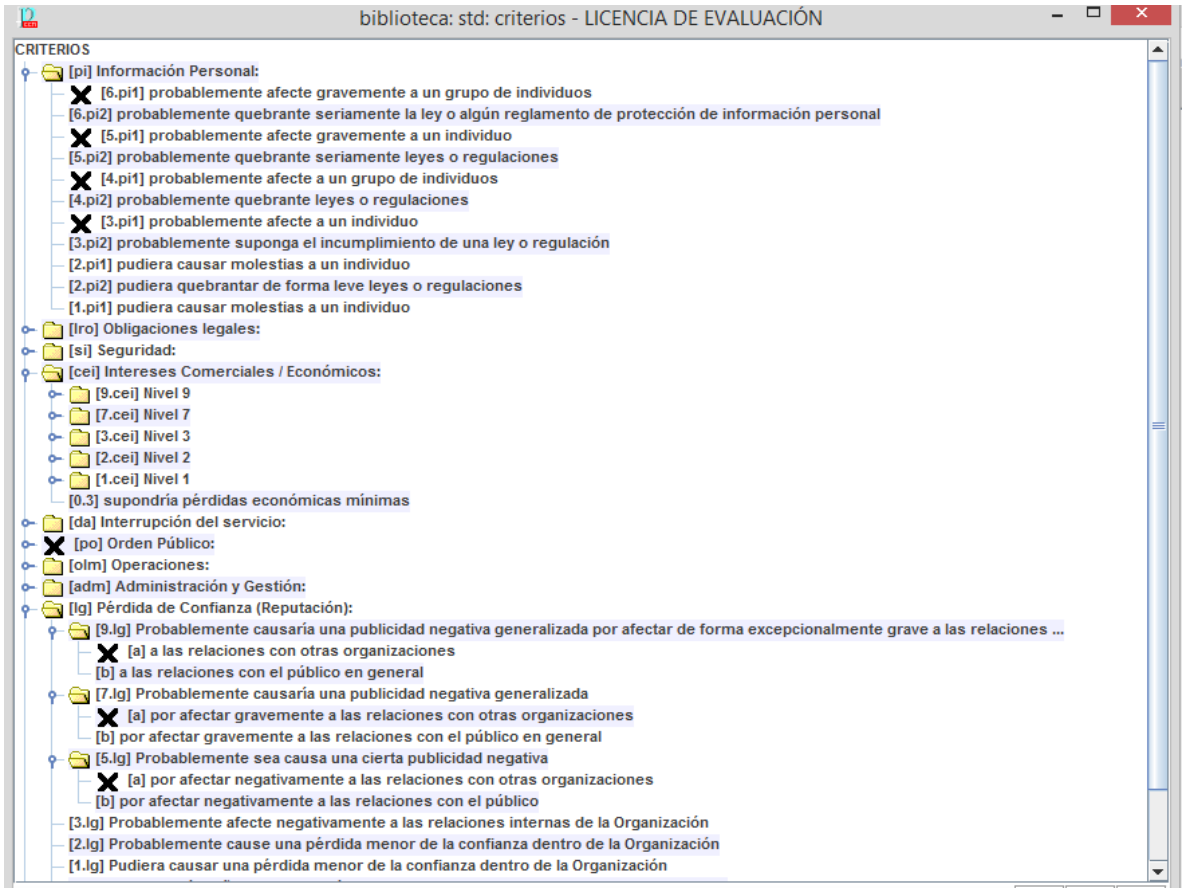
Importante: Debe recordarse que en el trabajo de tesis se utilizó este mismo catálogo de la metodología Magerit, pero ajustado y personalizado al caso de estudio, por tanto sus definiciones no necesariamente son las mismas.

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



Observación: Este formulario muestra la forma como se seleccionó (automática) las amenazas relacionadas con cada activo de TI que se ha definido para el caso de estudio. El ejemplo muestra la selección automática de las amenazas para el caso del activo "Aplicaciones informáticas de Créditos y Captaciones" (desarrollo propio)

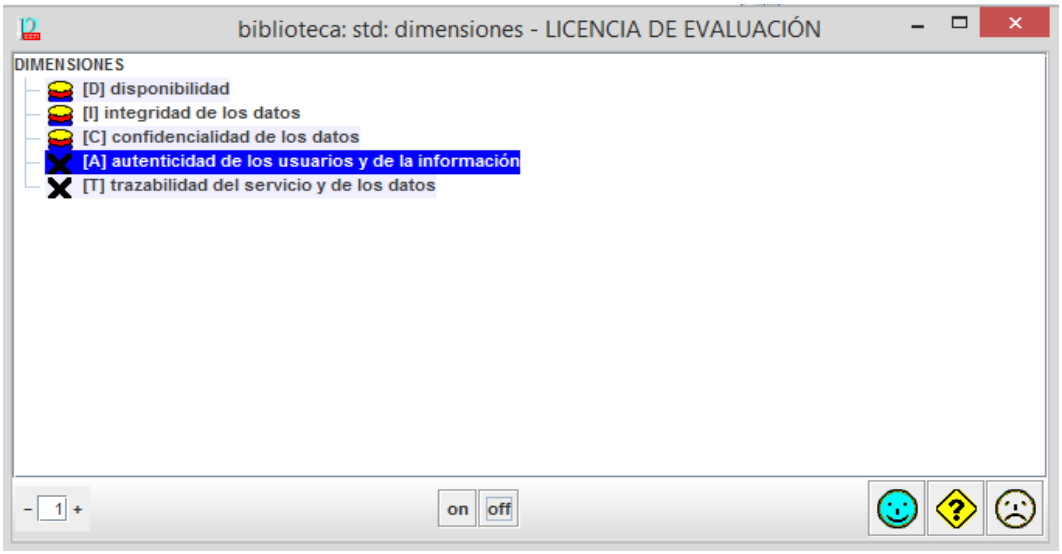
Pantalla N° 09: Criterios de valoración de los activos de TI seleccionados para el caso de estudio



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.

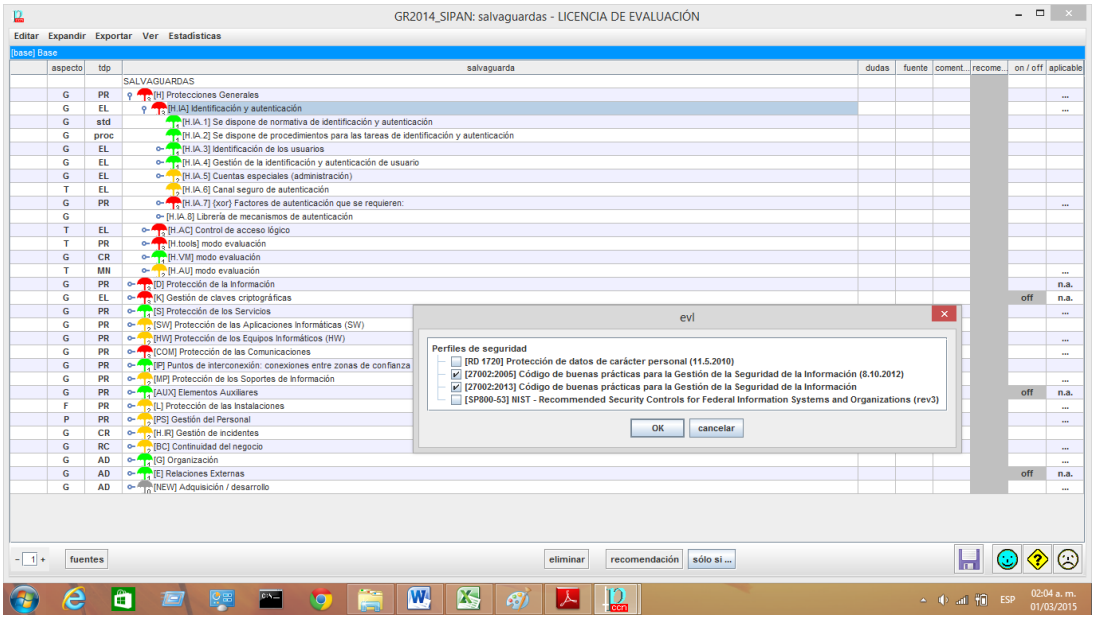
Importante: Debe recordarse que en el trabajo de tesis NO se utilizó este catálogo de la metodología Magerit. Se utilizó una escala de valoración de 5 puntos, desde Muy Baja afectación hasta Muy Alta Afectación. Sin embargo, para esta evaluación del software, se tuvo que considerar este catálogo (ajustado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

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



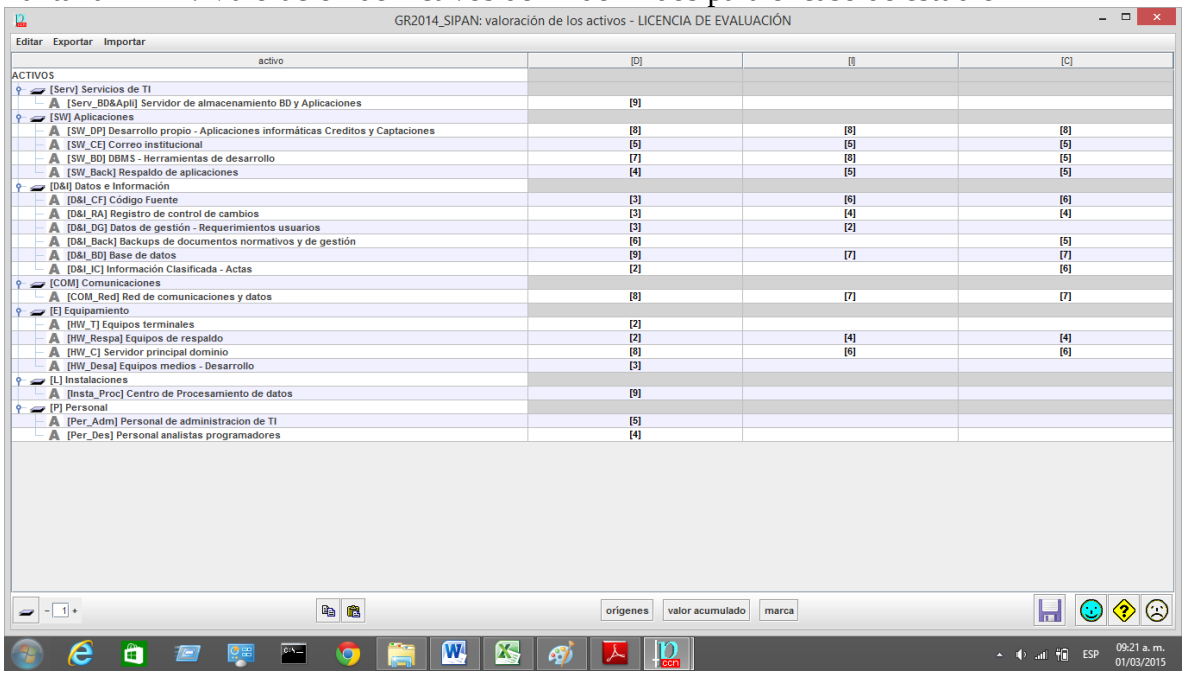
Observación: Sólo se seleccionaron las dimensiones de seguridad siguientes: Disponibilidad [D], Integridad [I] y Confidencialidad [C], para guardar concordancia con el trabajo de tesis y porque son las dimensiones exigidas por la SBS para ser evaluadas en los Sistemas de Gestión de Riesgos.

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.

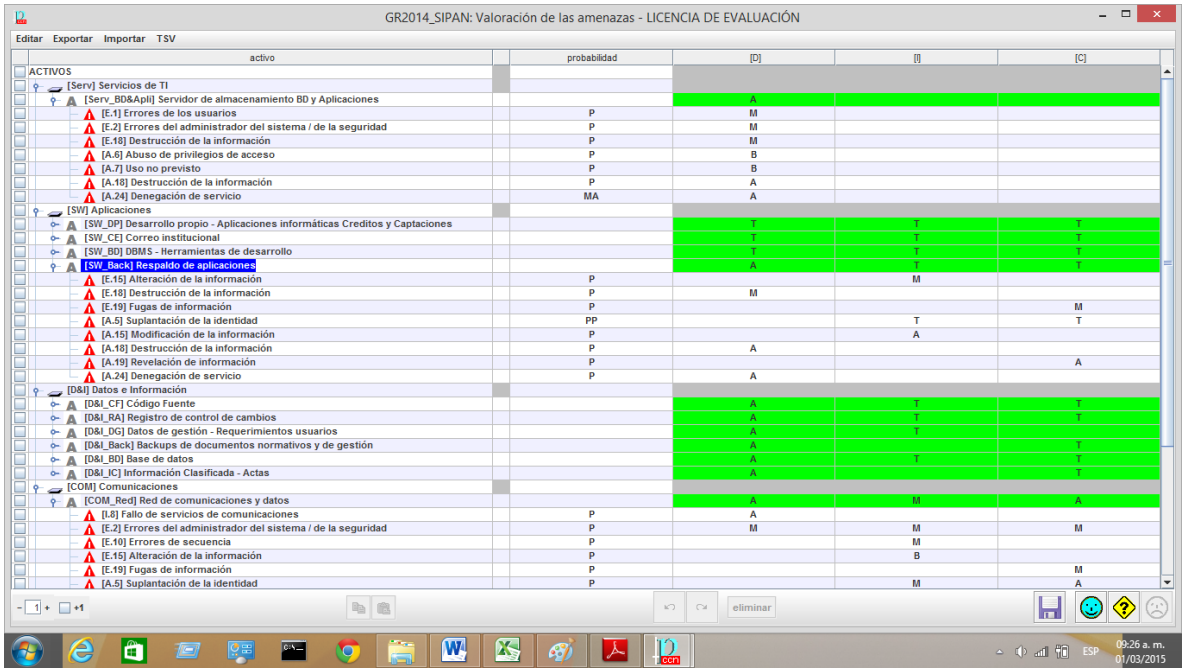
Pantalla N° 12: Valoración de Activos de TI definidos para el caso de estudio



activo	[D]	[I]	[C]
ACTIVOS			
[Serv] Servicios de TI			
[Serv_BD&Apli] Servidor de almacenamiento BD y Aplicaciones	[9]		
[SW] Aplicaciones			
[SW_DP] Desarrollo propio - Aplicaciones informáticas Creditos y Captaciones	[8]	[8]	[8]
[SW_CE] Correo institucional	[5]	[5]	[5]
[SW_BD] DBMS - Herramientas de desarrollo	[7]	[8]	[5]
[SW_Back] Respaldo de aplicaciones	[4]	[5]	[5]
[D&I] Datos e Información			
[D&I_CF] Código Fuente	[3]	[6]	[6]
[D&I_RA] Registro de control de cambios	[3]	[4]	[4]
[D&I_DG] Datos de gestión - Requerimientos usuarios	[3]	[2]	
[D&I_Back] Backups de documentos normativos y de gestión	[6]		[5]
[D&I_BD] Base de datos	[9]	[7]	[7]
[D&I_IC] Información Clasificada - Actas	[2]		[6]
[COM] Comunicaciones			
[COM_Red] Red de comunicaciones y datos	[8]	[7]	[7]
[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 de administracion de TI	[5]		
[Per_Des] Personal analistas programadores	[4]		

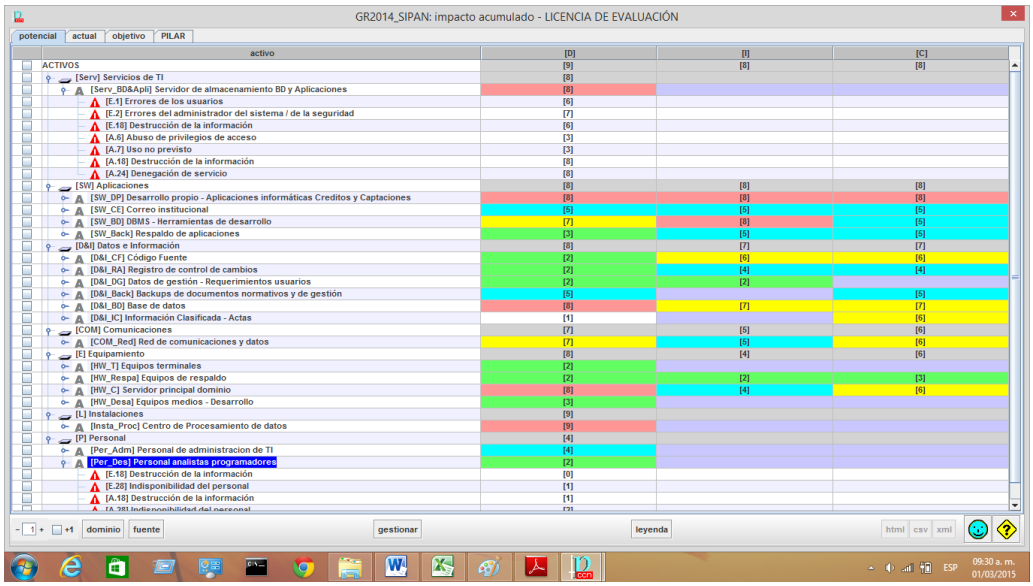
Observación: Para las valoraciones de los activos de TI se utilizaron los criterios de valoración de Magerit en base a 10 puntos. Por tanto, consideraremos cada par de puntos del software PILAR equivalente a un punto en el MGR-TI propuesto.

Pantalla N° 13: Valoración de las amenazas



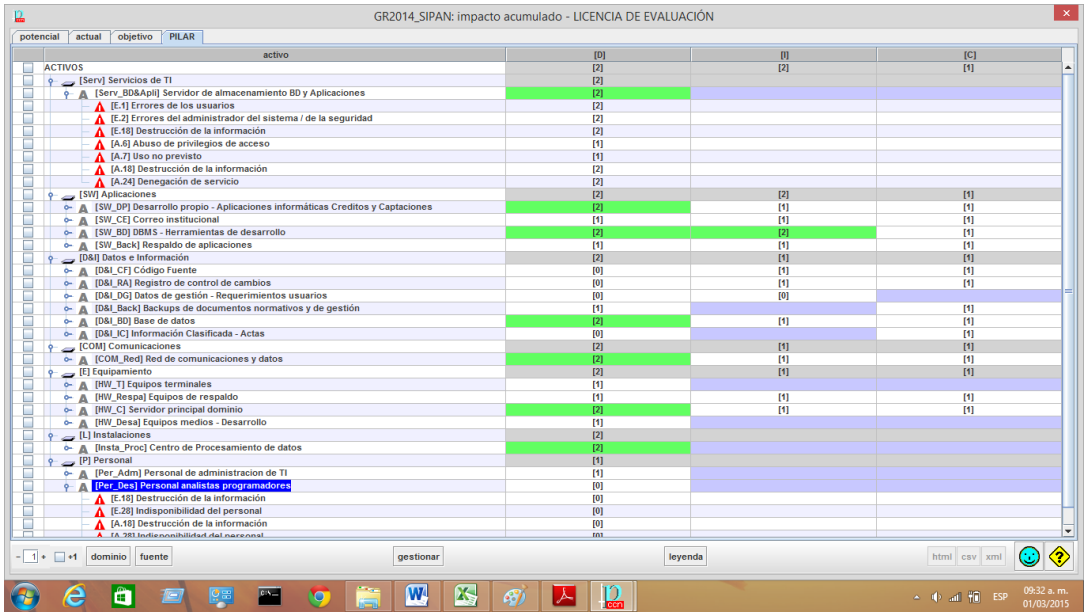
Observación: El formulario muestra los resultados obtenidos del cálculo automático que realiza PILAR para valorizar la probabilidad de ocurrencia de las amenazas y su impacto en cada una de las dimensiones de seguridad consideradas.

Pantalla N° 14: Cálculo de los niveles de riesgos potenciales



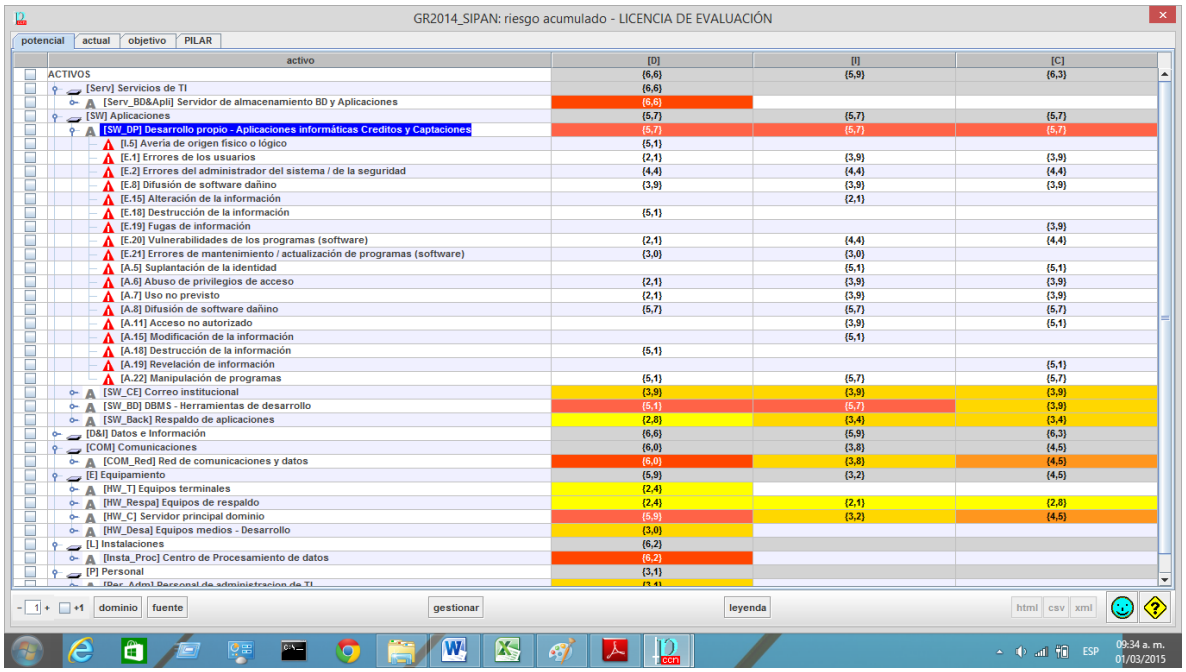
Observación: El formulario muestra los resultados obtenidos del cálculo automático de los riesgos potenciales, en base a los datos ingresados en las tareas anteriores

Pantalla N° 15: Cálculo de los niveles de riesgos objetivos que propone PILAR

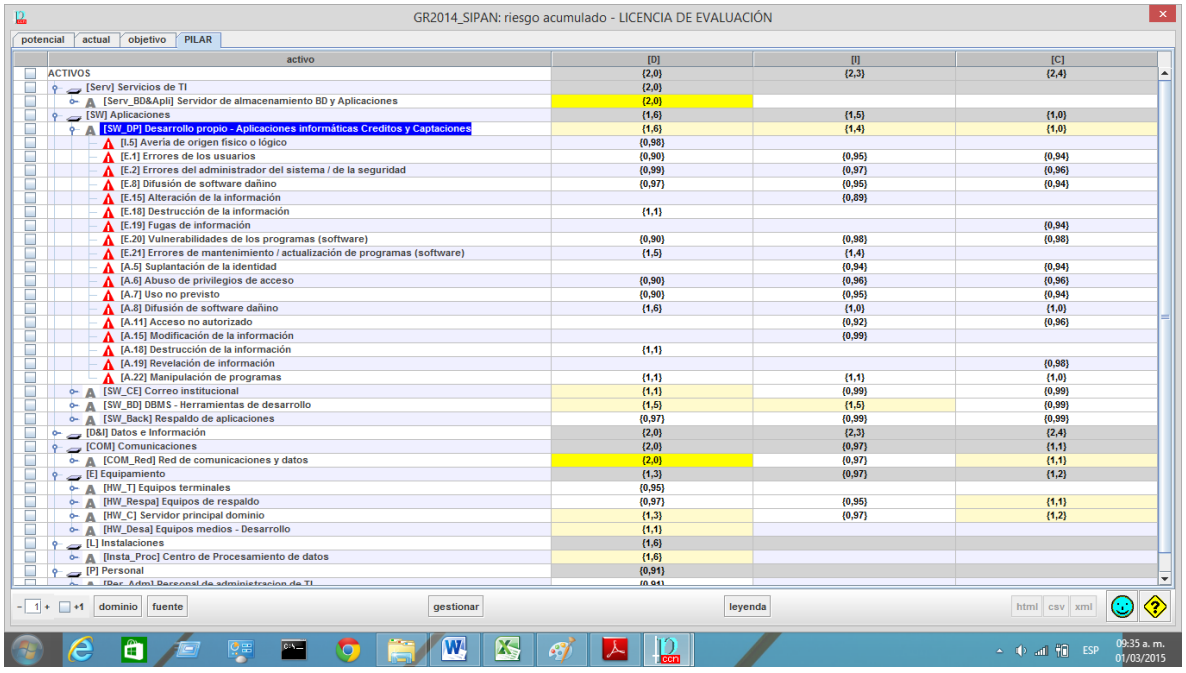


Observación: El formulario muestra los resultados obtenidos del cálculo automático de los riesgos objetivos, que PILAR recomienda alcanzar para lograr niveles de riesgos tolerables

Pantalla N° 16: Cálculo de los niveles de riesgos potenciales, medidas en los niveles de valoración



Pantalla N° 15: Cálculo de los niveles de riesgos objetivos que propone PILAR, , medidas en los niveles de valoración




niveles de criticidad
{9} - catástrofe
{8} - desastre
{7} - extremadamente crítico
{6} - muy crítico
{5} - crítico
{4} - muy alto
{3} - alto
{2} - medio
{1} - bajo
{0} - despreciable
OK

ANEXO N° 13

CUADRO COMPARATIVO DEL MODELO DE GESTIÓN DE RIESGOS ELABORADO EN MI TESIS CON APLICACIONES PARA GESTIÓN DE RIESGOS DE TI

		Aplicaciones para Gestión de Riesgos de TI									
	Características	**EAR/PILAR**	**CRAMM**	**COBRA**	**GlobalSGSI**	**GStool**	**Octave Automated Tool**	**Proteus**	**ISAMM**	**Migra Tool**	**Securia SGSI**
Matriz de gestión de riesgos excel	Metodología utilizada: MAGERIT	**MAGERIT**	**CRAMM**	**COBRA**	**ISO 31000**	**BSI Standard**	**OCTAVE y OCTAVE-S**		**ISAMM**	**MIGRA**	**ISO 27001**
	Es una aplicación específica para evaluación de riesgos (GRTI) o para implementar un SGSI	**GRTI**	**GRTI**	**GRTI**	**GRTI/SGSI**	**Modelador**	**GRTI**	**GRTI/SGSI**	**SGSI**	**GR**	**GRTI/SGSI**
	Su alcance incluye a instituciones financieras	**SI**	**NO**	**SI**	**SI**	**-----**	**SI**	**SI**	**SI**	**SI**	**SI**
	Permite gestionar riesgos de TI en sus dos fases principales: evaluación y tratamiento	**SI**	**SI**	**SI**	**SI**	**-----**	**SI**	**SI**	**SI**	**SI**	**SI**
	Utiliza el **método cualitativo** para evaluar los riesgos de TI	**SI**	**S/D**	**SI**	**SI**	**-----**	**SI**	**SI**	**NO**	**SI**	**SI**
	Define los activos de TI a evaluar de manera personalizada a una organización	**SI**	**NO**	**SI**	**Si**	**-----**	**SI**	**SI**	**N/D**	**SI**	**SI**
	Determina tablas de valoración de los elementos evaluables de manera personalizada a una organización	**SI**	**NO**	**S/D**	**SI**	**-----**	**SI**	**SI**	**NO**	**SI**	**SI**
	Las escalas de valoración pueden ser cambiadas en su interoretación en la cantidad de puntos de evaluación	**NO**	**NO**	**S/D**	**S/D**	**-----**	**NO**	**SI**	**NO**	**SI**	**SI**
	Define vulnerabilidades de los activos de Ti seleccionados	**NO**	**SI**	**SI**	**NO**	**-----**	**NO**	**SI**	**NO**	**SI**	**SI**
	Evalúa las amenazas a través de sus impactos y sus probabilidades de ocurrencia	**SI**	**SI**	**SI**	**SI**	**SI**	**SI**	**SI**	**SI**	**SI**	**SI**
	Permite definir niveles de toleracia de los niveles de riesgo de manera personalizada	**NO**	**S/D**	**NO**	**S/D**	**-----**	**NO**	**SI**	**NO**	**SI**	**SI**

	Calcula los niveles de riesgos y determina si está dentro o fuera de los niveles de tolerancia en base a colores de un mapa de calor	**SI**	**SI**	**SI**	**SI**	**-----**	**SI**	**SI**	**SI**	**SI**	**SI**
	Define los controles y salvaguardas en base a la ISO/IEC 27002 (ISO 17799)	**SI**	**SI**	**SI**	**SI**	**NO**	**SI**	**SI**	**SI**	**SI**	**SI**
	Caracteriza los controles en su implementación y ejecución: estrategia de implementación, situación actual	**NO**	**NO**	**NO**	**SI**	**-----**	**SI**	**SI**	**NO**	**SI**	**SI**
	Permite estimar brechas de seguridad (análisis GAP) a través del cálculo de nievles de riesgo residuales	**SI**	**NO**	**SI**	**SI**	**-----**	**SI**	**SI**	**SI**	**SI**	**SI**
	Necesita licencia	**NO**	**SI**	**SI**	**SI**	**SI**	**NO**	**SI**	**SI**	**SI**	**SI**
	Facilidad de uso y amigabilidad	**SI**	**NO**	**SI**	**SI**	**SI**	**SI**	**SI**	**SI**	**SI**	**SI**

N/D: No hay datos

Este factor se consideró importante para decidir su NO utilización

ANEXO N° 14

APLICACIONES PARA GESTIÓN DE RIESGOS

ISAMM (Information Security Assessment & Monitoring Method)
Última versión: S/D
Fabricante: Telindus
Procedencia: Bélgica
Web Oficial: http://www.telindus.com
Método de gestión de riesgos de TI que utiliza: ISAMM

Características principales:

- ISAMM Standard es una aplicación que permite verificar el cumplimiento de la norma ISO/IEC 27002, pero puede ser diseñado para cumplir con todo tipo de normas, leyes y reglamentos, políticas de propiedad, etc. Por tanto, ISAMM es un SGSI que contempla un método de gestión de riesgos, como una herramienta de apoyo.
- Para la evaluación de riesgos, utiliza una metodología cuantitativa, donde los riesgos evaluados se expresan a través de su Expectativa de Pérdida Anual (ALE), en unidades monetarias. La ALE se puede determinar para una amenaza o para un grupo de amenazas.

  Expectativa de pérdida anual (ALE) = [probabilidad] x [impacto medio]
- A través de ISAMM se puede desarrollar un plan de tratamiento de riesgos tomando en cuenta el Retorno de la Inversión (ROI) y un enfoque basado en las capacidades de justificación económica de ISAMM, permitiendo mostrar y simular el efecto de la reducción en el riesgo ALE para cada control implementado y compararlo con su costo de implementación.
- Utiliza como referencia para la implementación de controles a la norma ISO/IEC 27002 y considera a la norma ISO/IEC 27001 como un requisito clave para su uso.

Funcionalidad:

- Determinación del alcance
- Evaluación del cumplimiento y amenazas
- Cálculo del nivel de riesgos
- Presentación de informes
- Análisis Gap en el tiempo, por medio de la reutilización de la información obtenida de las evaluaciones de riesgos previas.

CRAMM (CCTA Risk Analysis and Management Method)
Última versión: 2003 (v5)
Fabricante: Insight Consulting
Procedencia: Reino Unido
Web Oficial: http://www.cramm.com , http://www.insight.co.uk
Método de gestión de riesgos de TI que utiliza: CRAMM

Características principales:

- CRAMM es un método de análisis de riesgos desarrollado por la organización del gobierno británico CCTA (Central de Comunicación y de la Agencia de Telecomunicaciones), ahora renombrado como Oficina de Comercio Gubernamental (OGC).
- Para aplicar este método se tiene que utilizar la aplicación del mismo nombre CRAMM. El método CRAMM es bastante difícil de utilizar sin la herramienta CRAMM.
- Las primeras versiones de CRAMM (método y herramienta) se basan en las mejores prácticas de las organizaciones del gobierno británico. En la actualidad es CRAMM método de análisis de riesgo preferido del gobierno del Reino Unido, pero CRAMM también se utiliza en muchos países fuera del Reino Unido.
- CRAMM es especialmente apropiado para grandes organizaciones, como los órganos de gobierno y la industria.
- Toma como referencia la norma ISO 17799

Funcionalidad:
- Examina la seguridad de los activos de SI, pero los reúne en unidades lógicas - modelos activos, que luego son objeto de análisis de riesgos.
- Se apoya en cuestionarios y las instrucciones:
- Identifica y valora los activos,
- Determina el riesgo de riesgos en base al análisis de las amenazas y vulnerabilidades,
- Define propuestas de medidas de seguridad.

Desventajas:
- se necesita que el personal evaluador tenga la capacidad de comprender la aplicación de la metodología CRAMM,
- imposibilidad de utilizar una licencia en varios equipos
- interfaz gráfica de usuario obsoleta
- no permite trabajo multiusuario, lo que hace difícil que una sola persona pueda realizar con eficacia todo el proceso de evaluación de riesgos, por su carácter especializado, complejo y dinámico. Por tanto, es difícil medir el nivel y localizar vulnerabilidades y debilidades de TI.

COBRA Tool
Última versión: Actualmente en proceso de mejora. No está disponible comercialmente
Fabricante: C & A Security Systems
Procedencia: Reino Unido
Web Oficial: S/D
Método de gestión de riesgos de TI que utiliza: ISO/IEC 17799

Características principales:
- Cobra Tool es una aplicación de software para el análisis de riesgos. Le permite a una organización utilizarlo como herramienta para la gestión de riesgos como parte

de la seguridad de los activos de TI, sin la necesidad de emplear a consultores externos.
- Está pensado principalmente para las organizaciones y las organizaciones comerciales que se centran en la norma ISO 17799, es decir, permite verificar el cumplimiento de la norma de seguridad ISO 17799, o de las propias políticas de seguridad de la organización.

Funcionalidad:
- Identifica las amenazas del sistema, las vulnerabilidades y exposiciones.
- Mide el grado de riesgo real para cada área o aspecto de un sistema, y vincula directamente éste al impacto potencial en el negocio.
- Ofrece soluciones detalladas y recomendaciones para reducir los riesgos.
- Proporciona informes técnicos.

GlobalSGSI
Última versión: GlobalSuite
Fabricante: Audisec Seguridad de la información S.L.
Procedencia: España
Web Oficial: http://www.globalsuite.es/es/
Método de gestión de riesgos de TI que utiliza: ISO 31000. Además se integra con ISO 27001, ISO 20000, ISO 22301, ISO 28000, ISO 9001, ISO 14001, etc.

Características principales:
- GlobalSGSI es una herramienta de gestión integral de la norma ISO 27001
- Cumple el ciclo PDCA completo, desde las fases de inicio y planificación del proyecto hasta el mantenimiento, pasando por el análisis de riesgos y el cuadro de mando.
- Tiene un módulo documental que permite tener centralizada y controlada toda la documentación del sistema de gestión.
- Contienen ayudas para la definición de las amenazas, vulnerabilidades y controles de seguridad
- Permite trabajo colaborativo
- Plataforma multidioma
- Su suite completa ayuda en la implantación, gestión, mantenimiento y despliegue de las normas, leyes y estándares internacionales mundialmente reconocidos como ISO 22301, ISO 27001, ISO 31000, ISO 20000, Leyes de Protección de Infraestructuras Críticas, Protección de Datos, Buenas Prácticas, Gobierno Corporativo, Balanced Score Card, etc.

Funcionalidad:
- Define el alcance
- Realiza análisis diferencial
- Permite realizar un inventario de activos
- Realiza análisis de riesgos

- Realiza el tratamiento de los riesgos
- Permite desarrollar la declaración de aplicabilidad
- Desarrolla cuadros de mando
- Permite realizar auditorías
- Gestión de incidencias
- Gestión de usuarios
- Documentación centralizada
- Informes y gráficos. Plantillas para mejor visualización

GStool
Última versión: v4.8. Debido a la falta de rentabilidad, se suspendió el desarrollo de gstools. La versión 4.x se siguen vendiendo, una actualización será posible hasta el final de 2016.
Fabricante: Bundesamt für Sicherheit in der Informationstechnik (BSI)
Procedencia: Alemania
Web Oficial:
https://www.bsi.bund.de/DE/Themen/weitereThemen/GSTOOL/Uebersicht/uebersicht_node.html
Método de gestión de riesgos de TI que utiliza: BSI Standard 100-3

Características principales😐
- GSTool forma parte de una serie de herramientas que la BSI ofrece para lograr un nivel adecuado de seguridad, donde también se incluyen normas propias de la BSI para la gestión de seguridad de la información y Catálogos Base para la Protección de TI. También incluye como referencia a la ISO 27001.
- Es un sistema de generación de informes, que permite analizar la información ingresada.
- Da soporte a los usuarios en el manual Básico de protección de TI, es decir, es una aplicación que permite la creación, gestión y actualización de los conceptos de seguridad de acuerdo con los lineamientos básicos de Protección de TI.
- Los usuarios tienen a su disposición un sistema de generación de informes, que les permite analizar la información y generar otros informes en formato papel o digital.
- Es una aplicación multicliente
- Es fácilmente actualizable a través de Internet, además permite la exportación de entornos de trabajo sin conexión a la red

Funcionalidad:
El GSTOOL apoya, en particular en las siguientes tareas de seguridad:
- Modelado de la seguridad de TI en base a conceptos básicos de seguridad
- Uso de la ISO 27001 y normas específicas de la BSI como referencia para protección informática
- Control básico de seguridad: implementación y medición
- Análisis de riesgos basado en la protección informática de referencia
- Análisis de costos
- Gestión de múltiples áreas de trabajo independientes

- Gestión histórica
- Requisitos de protección
- Informes e Información de Revisión (aprox. 50 formatos predefinidos)

Octave Automated Tool
Última versión:
Fabricante: Advanced Technology Institute (ATI)
Procedencia: USA
Web Oficial: http://oattool.aticorp.org/Tool_Info.html , http://www.aticorp.org
Método de gestión de riesgos de TI que utiliza: Octave y Octave-S

Características principales
- Esta herramienta ayuda al usuario durante la fase de recopilación de datos, organiza la información recopilada y finalmente produce informes de resultado de estudio.
- Puede ser aplicable para organizaciones gubernamentales, empresas privadas comerciales y no comerciales.
- Maneja una base de datos flexible que puede personalizarse y adaptarse a las necesidades del cliente. Para ello utiliza encuestas.
- Permite interoperabilidad con otras herramientas a través de interfaces e informes de exportación a través de MS Word y Excel y base de datos Oracle
- Ayuda en línea, necesita conocimiento del método OCTAVE

Funcionalidad:
- Identificación de riesgos
- Análisis de riesgos
- Evaluación de riesgos
- Tratamiento del riesgos
- Cálculo de los niveles de riesgos
- Determinación de la tolerancia del riesgo
- Contiene un catálogo de amenazas, riesgos y estrategias de protección

Proteus Enterprise
Última versión:
Fabricante: Information Governance Ltd - Infogov
Procedencia: Reino Unido
Web Oficial: http://www.infogov.co.uk/
Método de gestión de riesgos de TI que utiliza: BS ISO/IEC 17799, BS ISO 27001, BS 25999, SOX, Cobit, PCI DSS, etc.

Características principales
- Es una herramienta de Gobierno Corporativo basada en web, que da soporte completo a los procesos de cumplimiento normativo, seguridad de la información y gestión de riesgos.

- Permite implementar controles de cualquier norma o reglamento, como: BS ISO/IEC 17799, BS ISO 27001, BS 25999, SOX, Cobit, PCI DSS, etc.

Funcionalidad:

- Identificación de riesgos: usa técnicas de evaluación de riesgos tanto cualitativos como cuantitativos. Ambos están plenamente integradas con la gestión de activos, las amenazas, las contramedidas, planes de Tratamiento de Riesgos y Gestión de Incidentes
- Análisis de riesgos: se puede utilizar escalas de riesgo relativo y absoluto para adaptar el "apetito de riesgo" definido por las empresas.
- Evaluación de riesgos: 5 tipos: física, Información, Servicio, Aplicación y de grupo (combinación). Las amenazas pueden ser heredados de forma automática a través de relaciones de activos, localización y perfil activo.
- Inventario de activos y evaluación: Con la información de la ubicación de los activos y referencias cruzadas entre las áreas de la organización, incluyendo áreas externas y terceros, se puede importar datos e integrarlos en un solo catálogo de activos.
- Evaluación del riesgo: a través de un proceso genérico de 5 etapas, utilizando como referencia la BS ISO 27001, IRAM u otras metodologías.
- Tratamiento del riesgo: permite elaborar "Planes de Acción" integrados con el Cumplimiento, Evaluación de Riesgos, Análisis de Impacto del Negocio, Continuidad del Negocio y Gestión de Incidentes.
- Aceptación del riesgo: Cada proceso se captura automáticamente como una marca de tiempo en PDF, y lleno de cierre de sesión y la aceptación es compatible a través de correo electrónico y la gestión del flujo de trabajo.
- La comunicación del riesgo: Cada aspecto del sistema se puede informar a través de archivos PDF seguros, Business Objects completamente personalizables de informes, y a través de la información de un tablero gráfico de gestión opcional Proteus RISKview ™

Migra Tool
Última versión:
Fabricante: AMTEC/Elsag Datamat S.p.A.
Procedencia: Italia
Web Oficial: http://www.elsagdatamat.com/
Método de gestión de riesgos de TI que utiliza: metodología MIGRA

Características principales

- Herramienta web basada en la metodología MIGRA para apoyar al responsable de la seguridad durante todo el proceso de diseño y mantenimiento de un sistema de protección eficaz y eficiente, que contemple tanto la seguridad de los activos como la de los bienes tangibles.

Funcionalidad:

- Proporciona la información necesaria para la toma de decisiones; así como para poder justificar dichas decisiones y comprender sus consecuencias, en relación a la seguridad.
- Generar un modelo de la organización adecuada para el análisis de seguridad
- Evaluar la idoneidad y la eficacia de las medidas de seguridad frente a las amenazas y los requisitos de la política de seguridad normativos o de organización
- Identifica y asigna funciones y responsabilidades de seguridad
- Consolida e intercambia conocimientos técnicos de seguridad sobre las amenazas y contramedidas
- Realiza análisis de riesgo cualitativo
- Realiza análisis de cumplimiento en relación con la legislación, las reglas, normas o políticas internas
- Proporciona indicadores de riesgo
- Realiza análisis What-if
- Gestión de la producción y los informes operativos
- La herramienta consta de 5 módulos principales: - la base de conocimientos (que proporciona total ISO 27001: 2005 de conformidad) - la herramienta de modelado de escenarios - el análisis del riesgo y la conformidad del motor - el qué-si el motor - el motor generador de informes.

Securia SGSI
Última versión:
Fabricante: Centro Europeo de Empresas e Innovación de Albacete
Procedencia: España
Web Oficial: http://www.ceeialbacete.com/
Método de gestión de riesgos de TI que utiliza: ISO/IEC 27001

Características principales
- Cubre el proceso automático de implantación, puesta en funcionamiento, mantenimiento y mejora continua de un SGSI según la norma internacional ISO/IEC 27001.

Funcionalidad:
- Módulo de Análisis y Gestión de Riesgos
    - Inventario de procesos y activos
    - Valoración de impacto de activos
    - Identificación de amenazas y vulnerabilidades
    - Cálculo del riesgo
    - Decisión de criterios de aceptación
    - Toma de decisiones de actuación
    - Generación y seguimiento de las contramedidas
    - Evaluación del nivel de seguridad

- Módulo de gestión de incidencias: asegura que eventos y puntos débiles de la seguridad de la información, asociados con los sistemas de información se comunican de forma que sea posible emprender su resolución mediante la aplicación de acciones correctivas.
- Módulo de mejora continua: gestión de acciones preventivas y de mejora para adaptarlo a nuevas situaciones y en la previsión de nuevos fallos, situaciones de riesgo, etc.
- Módulo de gestión documental