UNIVERSIDAD NACIONAL "PEDRO RUIZ GALLO"

FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS

Escuela Profesional de Computación e Informática

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

AUDITORÍA EN EL USO DE TECNOLOGÍA DE INFORMACIÓN PARA OPTIMIZAR LA SEGURIDAD DE LA CAJA SIPÁN S.A

PRESENTADO POR:

BACH. CAMPOS MUÑOZ ANGEL EDUARDO

BACH. RIOS DAMIÁN CARLOS ALBERTO

ASESOR: ING. CHAYAN COLOMA, ALEJANDRO

LAMBAYEQUE – PERÚ 2016

UNIVERSIDAD NACIONAL "PEDRO RUIZ GALLO"

FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS

Escuela Profesional de Computación e Informática

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

AUDITORÍA EN EL USO DE TECNOLOGÍA DE INFORMACIÓN PARA OPTIMIZAR LA SEGURIDAD DE LA CAJA SIPÁN S.A

BACH. CAMPOS MUNOZ
ANGEL EDUARDO
AUTOR

BACH. RIOS DAMIAN
CARLOS ALBERTO
AUTOR

UNIVERSIDAD NACIONAL "PEDRO RUIZ GALLO"

FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS

Escuela Profesional de Computación e Informática

AUDITORÍA EN EL USO DE TECNOLOGÍA DE INFORMACIÓN PARA OPTIMIZAR LA SEGURIDAD DE LA CAJA SIPÁN S.A

PRESENTADO POR:

BACH. CAMPOS MUÑOZ ANGEL EDUARDO

BACH. RIOS DAMIÁN CARLOS ALBERTO

Aprobado por los Miembros del Jurado:

ING. LUIS ALBERTO REYES LESCANO
PRESIDENTE

ING. GILBERTO CARRION BARCO
SECRETARIO

ING. PERCY JAVIER CELIS BRAVO
VOCAL

DEDICATORIA

Cuando contemplo el cielo, y la luna y las estrellas que tú mismo hiciste,
No puedo menos que pensar: « ¿Qué somos los mortales para que pienses en nosotros y nos tomes en cuenta?» (Salmos 8:3-4)

Dedico este trabajo con todo mi amor.
A ti DIOS que me diste la oportunidad de vivir y las fuerzas para terminar este proyecto.

DEDICATORIA

Este trabajo está dedicado a Dios, por darme a mis padres Luisa y Carlos Ernesto que han sido los pilares más importantes en mi vida personal y profesional. A mi amada esposa Ely por siempre creer en mí.
.

AGRADECIMIENTO

A mi madre que con su apoyo incondicional me motivó.

A mi esposa e hijos que son la fuerza que me impulsa.

AGRADECIMIENTO

Gracias a Dios por permitirme tener y disfrutar a mi familia, A mi familia por apoyarme en cada decisión y proyecto. Gracias a la vida porque cada día me demuestra lo hermosa que es la vida y lo justa que pueda llegar a ser, gracias a mi familia por permitirme cumplir con excelencia en el desarrollo de esta tesis. Gracias.

RESUMEN

El objetivo del informe fue elaborar la auditoría en el uso de tecnología de información para la Caja Sipán S.A, utilizando como marco metodológico de referencia lo estipulado como "buenas prácticas" en la Norma Técnica Peruana 17799, basada en la NTP ISO/IEC 17799:2007, así como lo indicado en Circular G-139-2009 – SBS, Circular G-140-2009 – SBS, Resolución S.B.S.N° 2116 - 2009, Reglamento de gestión operacional de la institución.

Se Analizó el Sistema de Gestión de la Seguridad de la Información actual, cuyo resultado ayudo a encauzar y determinar una adecuada acción gerencial, la definición de prioridades para gestionar los riesgos de seguridad de la información y la implantación de los controles seleccionados para protegerse contra dichos riesgos. Los procedimientos metodológicos y requisitos de éstos sistemas cumplen con las normatividades de la SBS para estos casos: Circular Nº G- 140 -2009: Gestión de la seguridad de la información y Resolución S.B.S. N° 2116 -2009: Reglamento para la gestión del riesgo operacional.

Palabras claves:

Auditoría, seguridad, información, gestión operacional, tecnología de información

ABSTRACT

The objective was to develop the audit report on the use of information technology to the SA box Sipán using methodological framework stipulated as " good practices" in the International Standard 17799 , based on ISO NTP / IEC 17799: 2007, and as indicated in Circular G - 139-2009 - SBS Circular G - 140-2009 - SBS , Resolution SBSN ° 2116 -2009 , regulation of operational management of the institution.

Is achieved implement a Management System of Information Security, the results helped channel and determine an appropriate managerial action, the definition of priorities for managing security risks information and implementation of selected controls protect against these risks. The methodological procedures and requirements of these systems comply with the SBS normativities for these cases: Circular No. 140 -2009 G: Management of Information Security and Resolution SBS N ° 2116 -2009: Regulations for the management of operational risk.

Keywords:

Auditing, security, information, operational management, information technology

INDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

El informe ha sido estructurado tomando como referencia lo indicado en Circular G-139-2009 – SBS, Circular G-140-2009 – SBS, Resolución S.B.S.N° 2116 -2009 (Reglamento de gestión operacional); así como lo estipulado como "buenas prácticas" en la Norma Técnica Peruana 17799, basada en la NTP ISO/IEC 17799:2007; especificando como objetivo central Elaborar la auditoría en el uso de tecnología de información para optimizar la seguridad de la Caja Sipán S.A y como objetivos específicos:

- Analizar la estructura orgánica del área de TI de la Caja Sipán
- Evaluar la estructura de gestión de la seguridad de la información y de la gestión de TI.
- Calcular el valor de criticidad de riesgo Gestión de TI para la Caja Sipán

La Caja Sipán soporta sus procesos de gestión de la información interna y la de sus clientes de manera automatizada; es decir que existe dependencia de los sistemas informáticos para realizar, controlar y registrar sus operaciones y transacciones, implicando ello, que la Caja puede ser vulnerable ante amenazas que atenten contra la seguridad de su información; generando posibles riesgos e inseguridades procedentes de una amplia variedad de fuentes como: fraudes basados en informática, espionaje, vandalismo, sabotaje, daños por virus informáticos, ataques de intrusión o denegación de servicios, mal desarrollo de sistemas, caídas de los equipos tecnológicos críticos, etc.; que puedan estar impidiendo asegurar la continuidad del negocio o maximizando los daños a la organización o minimizando el retorno de las inversiones y las oportunidades de negocio.

Por tanto, el presente proyecto se justifica toda vez que contempla la valoración de riesgos asociados a cada una de las deficiencias, debilidades o vulnerabilidades que afectaría, si ocurriesen los sucesos o eventos o riesgos que se indican.

Se han realizado los estudios siguientes relacionados con el tema de investigación Buenas prácticas para auditar redes inalámbricas aplicadas a las empresas de rubro hotelero de la Ciudad de Chiclayo de Santa María Becerra, Franck Jhonathan, Metodología táctica para la implantación de sistemas de información basada en métrica y COBIT de Pedro Daniel Camacho Gomez y Wilmer Nilton Ramos Arrieta, y Auditoría Informática orientada a los procesos críticos de crédito generados en la Cooperativa de Ahorro Y Crédito "Fortuna" aplicando el marco de trabajo COBIT de Karolay Michell Coronel Castro

CAPÍTULO I: DATOS GENERALES DE LA ORGANIZACIÓN

1.1. Descripción de la organización

Caja Sipán es una sociedad anónima de derecho privado, con 564 accionistas de la región, 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.

Su funcionamiento, como Caja Rural Cruz de Chalpón, fue autorizado por la Superintendencia de Banca y Seguros mediante Resolución N° 213-95 de fecha 06.03.1995 e inició sus operaciones el 27 de Marzo de 1995, con fecha 21 de marzo del 2006 la Superintendencia autorizó el cambio de nombre a Caja Sipán, nombre previamente registrado en INDECOPI.

La actividad crediticia y de negocios en general se desarrolla a través de sus Oficinas ubicadas en la ciudad de Chiclayo, capital del Departamento de Lambayeque, en el norte del Perú a 770 kilómetros de Lima, contando con seis agencias para la atención de clientes, dos ubicadas en la ciudad de Chiclayo, una en la ciudad de Jaén del departamento de Cajamarca, una en la ciudad de Chepén una en la ciudad de Trujillo del departamento de La Libertad y otra en Nueva Cajamarca departamento de San Martin.

1.2. Misión, visión y objetivos de la organización

1.1.1. Misión

“Facilitamos el progreso económico y social de la población emergente, sin exclusión alguna, con servicios financieros innovadores y responsables, que respondan a sus necesidades y sueños”

1.1.2. Visión

"Nuestros clientes se sienten satisfechos, con el acceso y uso a servicios financieros mediante sus dispositivos digitales y, con una cálida atención al acompañarlos en su desarrollo".

1.1.3. Objetivos de la organización

Uno de sus principales objetivos es capacitar al personal y conseguir fuentes de financiamiento nacional e internacional con el objeto de contribuir al desarrollo regional dado a que Lambayeque tiene un potencial de crecimiento bastante alto en el país.

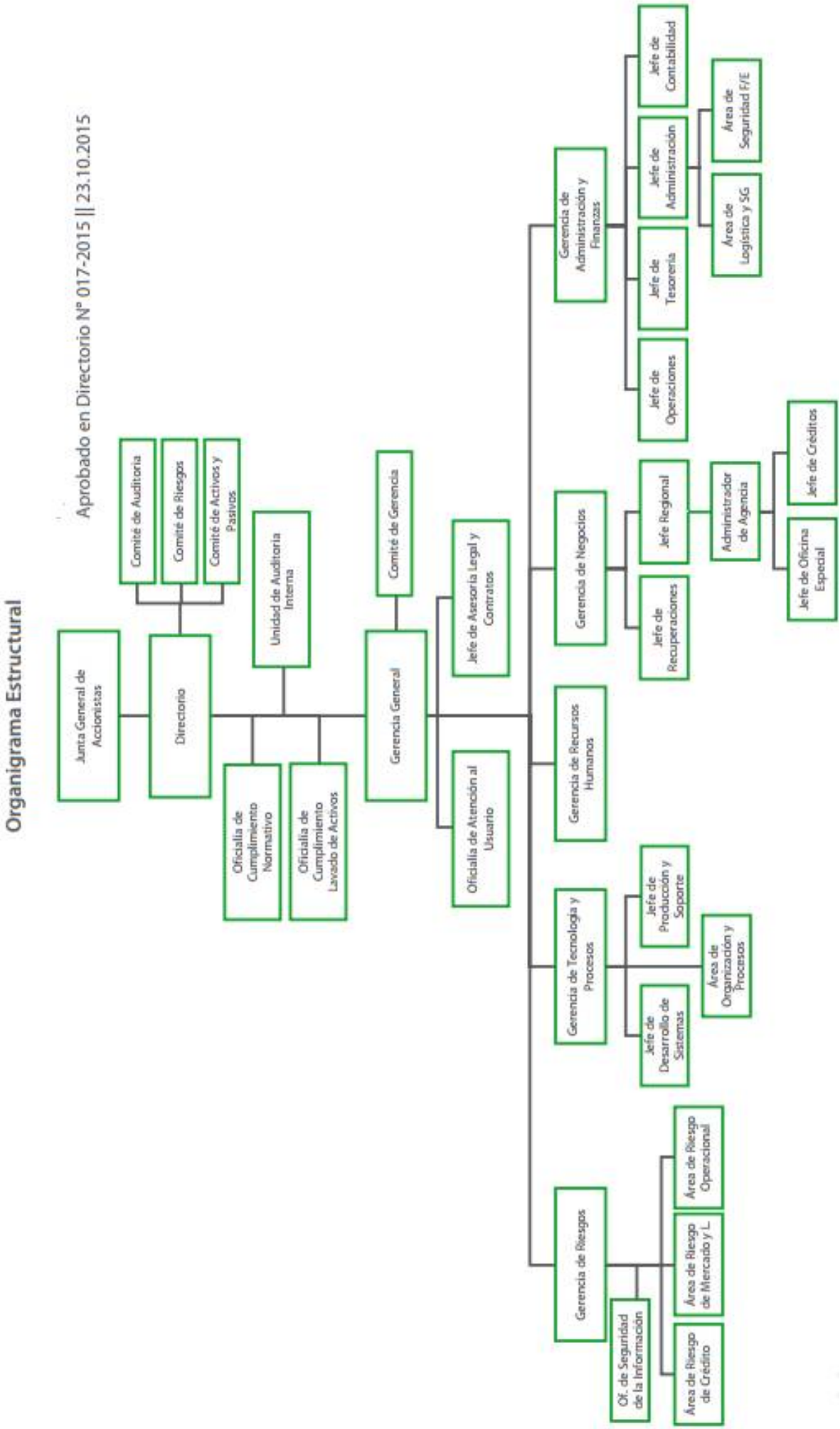
1.3. Estructura orgánica

Directorio

Presidente	:	Sr. Julio Del Castillo Vargas
Vicepresidente	:	Sr. Olivio Huancaruna Perales
Director	:	Sr. Víctor Raúl Rojas Díaz
Director	:	Sr. Roger Cangahuala Janampa
Director	:	Sra. Nancy Goyburo
Director	:	Sr. Guillermo Fajardo
Director	:	Sr. Marcos Gasco Arrobas

Funcionarios

Gerente General	:	Nancy Goyburo R.
Gerente de Administración y Finanzas	:	Walter Segura Oblitas.
Gerente de Negocios	:	Sergio Flores Ramirez
Gerente de Recursos Humanos	:	Sonia Chiu Cabrera
Gerente de Riesgos	:	Luz Tatiana Zuñiga
Gerente de Tecnología y Procesos (e)	:	Ivette Yep Tello
Gerente de Auditoría Interna	:	Magali Montenegro Requejo
Jefe de Asesoría Legal y de Contratos	:	Ledy Linares Cubillas.
Jefe de Operaciones	:	Gulliana Gamarra Pacheco
Contador General	:	Rosa Milagros Taype
Adm. Agencia Chiclayo	:	Martín Urbina Romain
Adm. Agencia Moshoqueque	:	.
Adm. Agencia Jaén	:	Roger Campos Martinez
Adm. Agencia Chepén	:	Saul Vasquez Tacilla
Adm. Agencia Trujillo	:	Jean Narvaez Moreno
Adm. Agencia Nueva Cajamarca	:	Jhony Alegria Saavedra


Organigrama Estructural
Aprobado en Directorio N° 017-2015 || 23.10.2015
Junta General de Accionistas
Directorio
Comité de Auditoria
Comité de Riesgos
Comité de Activos y Pasivos
Unidad de Auditoria Interna
Oficialia de Cumplimiento Normativo
Oficialia de Cumplimiento Lavado de Activos
Gerencia General
Comité de Gerencia
Jefe de Asesoría Legal y Contratos
Oficialia de Atención al Usuario
Gerencia de Administración y Finanzas
Jefe de Contabilidad
Jefe de Administración
Área de Seguridad F/E
Área de Logística y SG
Jefe de Tesorería
Jefe de Operaciones
Gerencia de Negocios
Jefe Regional
Administrador de Agencia
Jefe de Créditos
Jefe de Oficina Especial
Jefe de Recuperaciones
Gerencia de Recursos Humanos
Gerencia de Tecnología y Procesos
Jefe de Producción y Soporte
Área de Organización y Procesos
Jefe de Desarrollo de Sistemas
Gerencia de Riesgos
Área de Riesgo Operacional
Área de Riesgo de Mercado y L.
Área de Riesgo de Crédito
Of. de Seguridad de la Información

CAPÍTULO II: PROBLEMÁTICA DE LA INVESTIGACIÓN

2.1. Realidad problemática

La Caja Sipán soporta sus procesos de gestión de la información interna y la de sus clientes de manera automatizada; es decir que existe dependencia de los sistemas informáticos para realizar, controlar y registrar sus operaciones y transacciones, implicando ello, que la Caja puede ser vulnerable ante amenazas que atenten contra la seguridad de su información; generando posibles riesgos e inseguridades procedentes de una amplia variedad de fuentes como: fraudes basados en informática, espionaje, vandalismo, sabotaje, daños por virus informáticos, ataques de intrusión o denegación de servicios, mal desarrollo de sistemas, caídas de los equipos tecnológicos críticos, etc.; que puedan estar impidiendo asegurar la continuidad del negocio o maximizando los daños a la organización o minimizando el retorno de las inversiones y las oportunidades de negocio.

2.2. Formulación del problema

2.3. Justificación e importancia de la investigación

El presente proyecto se justifica toda vez que contempla la valoración de riesgos asociados a cada una de las deficiencias, debilidades o vulnerabilidades que afectaría, si ocurriesen los sucesos o eventos o riesgos que se indican

2.4. Objetivos de la investigación

2.4.1. Objetivo general

Elaborar la auditoría en el uso de tecnología de información para optimizar la seguridad de la Caja Sipán S.A.

2.4.2. Objetivos específicos

- Analizar la estructura orgánica del área de TI de la Caja Sipán S.A.
- Evaluar la estructura de gestión de la seguridad de la información y de la gestión de TI.
- Calcular el valor de criticidad de riesgo Gestión de TI para la Caja Sipán S.A.

2.5. Limitaciones de la investigación

- El trabajo ha sido limitado a optimizar la seguridad de la Caja Sipán.
- La falta de acceso a documentos estratégicos de la organización, por ser de carácter confidencial.
- La falta de documentación física, reportes y control de incidencias por parte del área de sistemas.

CAPÍTULO III: MARCO METODOLÓGICO

3.1. Tipo de investigación

Descriptiva

3.2. Hipótesis

La elaboración de la auditoría en el uso de tecnología de información optimizará la seguridad de la Caja Sipán S.A.

3.3. Variables

3.3.1. Variable independiente

Auditoría en el uso de tecnología de información

3.3.2. Variable dependiente

Seguridad de la Caja Sipán S.A.

3.4. Diseño y Contrastación de Hipótesis

Si se elabora la auditoría en el uso de tecnología de información entonces optimizará la seguridad de la Caja Sipán S.A.

Para el análisis y discusión de los resultados se realizaron encuestas a expertos, definidos por cinco funcionarios de alto nivel de la Caja Sipán S.A:

Experto 1: Sr. Julio Del Castillo Vargas (Presidente)

Experto 2: Sr. Olivio Huancaruna Perales (Vice Presidente)

Experto 3: Sr. Víctor Raúl Rojas Díaz (Director)

Experto 4: Sr. Roger Cangahuala Janampa (Director)

Experto 5: Ing. Hobbier Siccha Ayvar (Jefe Sistema)

CAPÍTULO IV: MARCO TEÓRICO

4.1. Antecedentes de investigación

4.1.1. Antecedentes en el contexto internacional

TITULO : Auditoría Informática orientada a los procesos críticos de crédito generados en la Cooperativa de Ahorro Y Crédito "Fortuna" aplicando el marco de trabajo COBIT

AUTOR : Karolay Michell Coronel Castro

AÑO : 2012, Loja Ecuador

RESUMEN

La presente investigación se enfoca al desarrollo del proceso de una auditoría informática para evaluar y determinar el nivel de cumplimiento de los procesos críticos de crédito de la Cooperativa de Ahorro y Crédito "Fortuna", en base al marco de referencia COBIT. El proceso abarca la recopilación de la mayor cantidad de evidencia técnica mediante la aplicación dos herramientas: IDEA para análisis de la base de datos y NESSUS para escaneo de vulnerabilidades de equipos, también se aplicó la metodología de los modelos de madurez del COBIT, la cual por medio de una matriz de evaluación permitió la verificación del cumplimiento de los procesos de crédito, todo esto con el fin de emitir un informe de hallazgos, que muestre las falencias existentes en dichos procesos, tanto manuales como sistematizados. Finalmente se plantea un plan de acción el cual pretende facilitar la toma de decisiones por parte de los directivos de institución, el cual asociado a la introducción y consolidación de la auditoría informática establecerá una cultura de seguridad en el tratamiento de la información en todos los procesos de negocio.

4.1.2. Antecedentes en el contexto nacional

TITULO : Metodología táctica para la implantación de Sistemas de Información basada en métrica y COBIT

AUTOR: Pedro Daniel Camacho Gomez

Wilmer Nilton Ramos Arrieta

AÑO : LIMA - 2010

RESUMEN

El propósito de este trabajo es proponer una metodología para la implantación de un sistema de información basándose en los lineamientos de METRICA (metodología de planificación, desarrollo y mantenimiento de sistemas de información) y en COBIT (Objetivos de Control para la información y Tecnologías relacionadas) el cual es un conjunto de mejores prácticas para el manejo de información. Sintetizando ambos

Conjuntos de conocimientos orientados a procesos nos enfocaremos específicamente en la implantación delas soluciones informáticas. El punto de partida para dar uso de la metodología es cuando las organizaciones decidan por el cambio de un sistema de información existente o a la implementación de uno nuevo, eligen en base a dos opciones: unas optan por el desarrollo propio y otras por la adquisición de un software existente en el mercado que puede incluir o no la personalización respectiva. La elección a tomar, ya sea de desarrollo propio o la adquisición de un software el paso siguiente es lograr su implantación. Es aquí donde surgen los problemas en la mayoría de organizaciones el cual es dar inicio del funcionamiento de un proyecto tecnológico utilizando solo la experiencia llevándolo al fracaso porque no se dispone de una metodología apropiada para lograr cumplir con los objetivos. La metodología propuesta fue pensada para ayudar a todas aquellas personas que día a día trabajan en alguna área de tecnología, y por más esfuerzos que hacen, pocas veces logran que sus proyectos de implantación satisfagan las necesidades del negocio.

4.1.3. Antecedentes en el contexto local

TITULO: Buenas prácticas para auditar redes inalámbricas Aplicadas a las empresas del rubro hotelero de la Ciudad de chiclayo.

AUTOR : Santa Maria Becerra, Franck Jhonathan

AÑO : Chiclayo 30 de Octubre de 2012

RESUMEN

Al presentar esta investigación, se propone buenas prácticas para el desarrollo de auditorías de redes inalámbricas aplicadas a las empresas del rubro hotelero. La propuesta está basada en el estudio de las empresas del rubro hotelero de la ciudad de Chiclayo con el fin de mejorar la disponibilidad, confiabilidad e integridad de la información, cotejando metodologías existentes que ayuden auditar redes inalámbricas, y desarrollando la propuesta de las buenas prácticas. En base a las metodologías COBIT 4.1, NTP – ISO – IEC 27001, NTP – ISO – IEC 27002, Osstmm Wireless 2.9, ENISA, RED-M, Information networks planning and design (INPD) y metodología para administrar redes 3.0., se elaboraron buenas prácticas para auditar redes inalámbricas. Como parte de las buenas prácticas se encuentra, los dominios Diseño, Administración y Seguridad, y cada una presenta sus buenas prácticas, a la vez cada de estas tiene su objetivo, actividades o tareas, herramientas de apoyo y un Checklist para auditar la red inalámbrica.

4.2. Desarrollo de la temática

4.2.1. Auditoría informática

(Acha, 1994) Define auditoría informática como “un conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un sistema informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existente en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente”.

4.2.1.1. Alcance

El alcance de la auditoría define con precisión el entorno y los límites en que va a desarrollarse la auditoría informática y se complementa con los objetivos de ésta. El alcance se concretará expresamente en el informe final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas

4.2.1.2. Tipos de auditoría informática

Existen diferentes tipos de auditorías,

TIPO	DESCRIPCION
Auditoría de las bases de datos	Controles de acceso, de actualización, de integridad y calidad de los datos.
Auditoría de la seguridad	Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.
Auditoría de la seguridad lógica	Comprende los métodos de autenticación de los sistemas de información.
Auditoría de la seguridad en producción	Errores, accidentes y fraudes.

TABLA 1 - TIPOS DE AUDITORÍA INFORMÁTICA

4.2.1.3. Pruebas y herramientas para efectuar una auditoría informática

Al elaborar una auditoría informática el auditor puede realizar las siguientes pruebas:

- Pruebas clásicas: Consiste en probar las aplicaciones/sistemas con datos de prueba, observando la entrada, la salida esperada, y la salida obtenida. Existen paquetes que permiten la realización de estas pruebas.

- Pruebas sustantivas: Aportan al auditor informático las suficientes evidencias y que se pueda formar un juicio. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican así mismo la exactitud, integridad y validez de la información.

- Pruebas de cumplimiento: Determinan si un sistema de control interno funciona adecuadamente según la documentación, según declaran los auditados y según las políticas y procedimientos de la organización.

Las principales herramientas de las que dispone un auditor informático son:

- Observación
- Realización de cuestionarios
- Entrevistas a auditados y no auditados
- Flujogramas
- Listas de chequeo

4.2.2. Proceso de una auditoría informática

El proceso de una auditoría informática se resume en las fases y etapas que se muestran en la siguiente figura:

(Mario G. Piattini, 2001)

PROCESO DE UNA AUDITORIA INFORMATICA

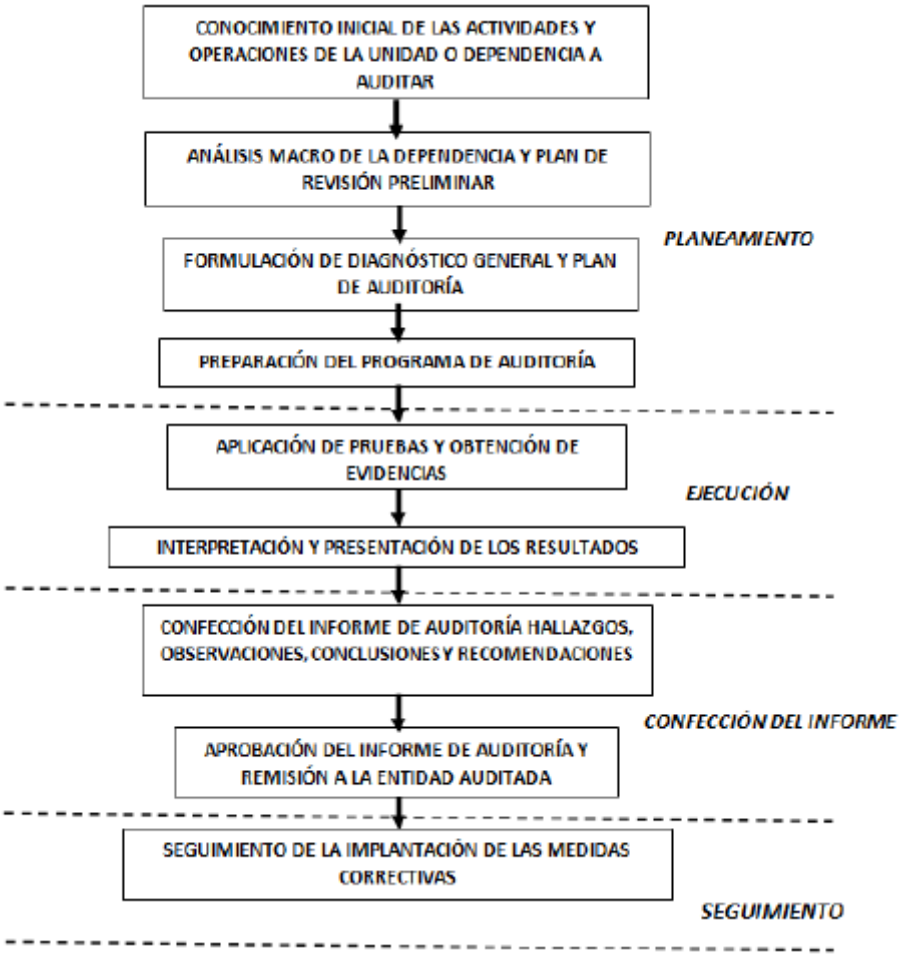


FIGURA 1 - PROCESO DE UNA AUDITORÍA INFORMÁTICA

Todo proceso posee una metodología para ser realizado, es así que el método de trabajo del auditor pasa por las siguientes etapas:

Planificación de la auditoría informática

Los ámbitos que deben ser cubiertos dentro de la planificación de la auditoría son:

- Comprensión de la empresa
- Riesgo y materialidad de auditoría
- Objetivos de control y objetivos de auditoría
- Procedimientos de auditoría

Ejecución de la auditoría informática

Para el desarrollo adecuado de una auditoría por lo general se debe llevar una apropiada documentación que de modo general incluye:

- Tema de auditoría: Donde se identifica el área a ser auditada.
- Objetivos de auditoría: Donde se indica el propósito del trabajo de auditoría
- Alcances de auditoría: Se detalla los sistemas específicos o unidades de organización que se han de incluir en la revisión en un período de tiempo determinado.
- Planificación previa: Donde se identifica los recursos y destrezas que se necesitan para realizar el trabajo así como las fuentes de información para pruebas o revisión y lugares físicos o instalaciones donde se va auditar.
- Procedimientos de auditoría

Finalización de la auditoría informática

- Preparación y redacción del informe final

- Redacción de la carta de introducción o carta de presentación del informe final y seguimiento de las medidas correctivas.

4.2.3. Estándares de auditoría informática

El auditor de procesos TI tiene una variada gama de herramientas y/o marcos de trabajo que pueden asistirle al momento de aplicar la auditoría que corresponda, dando una visión objetiva para que el auditor decida qué marco es el mejor para usarse en base al medio donde realice su trabajo y dependiendo de la función que cumple la organización.

La siguiente tabla resume en un cuadro comparativo los marcos de trabajo que se han considerado más importantes:

ÁREA	CobiT	ITIL	ISO 27000
Funciones	Mapeo de procesos IT	Mapeo de la Gestión de Niveles de Servicio de IT	Marco de referencia de seguridad de la Información
Áreas	4 Procesos y 34 Dominios	9 Procesos	10 Dominios
Creador	ISACA	OGC	ISO International Organization for Standardization
¿Para que se Implementa?	Auditoria de Sistemas de Información	Gestión de Niveles de Servicio	Cumplimiento del estándar de seguridad
¿Quienes lo evalúan?	Compañías de contabilidad, Compañías de consultoria en IT	Compañías de Consultoria en IT	Compañías de Consultoria en IT, Empresas de Seguridad, Consultores de seguridad en redes

TABLA 2 - CUADRO COMPARATIVO DE MARCOS DE TRABAJO

4.2.4. Auditoría informática en el sector bancario

4.2.4.1. Necesidad y beneficios de la auditoría informática en las entidades financieras

Una de las características de cualquier actividad auditora está relacionada con las funciones de control. Por ello la participación de la auditoría informática en el sector financiero la constituye la revisión de las aplicaciones informáticas con el objeto de asegurar que cumplan con los criterios funcionales y operativos definidos por la entidad financiera. Los sistemas de información de bancos y entidades financieras tienen entre sus características particulares la de construir fuentes de datos para múltiples agentes externos. La importancia de la auditoría informática debe garantizar el correcto funcionamiento de los sistemas, no solo desde la perspectiva de la gestión de la propia empresa sino también desde la óptica de los clientes.

La auditoría informática en las entidades financieras suele aportar con la detección de procesos obsoletos, ineficaces o redundantes, que no añaden valor a la actividad de negocio y que sin embargo suponen un coste. El auditor informático tiene la oportunidad de analizar la información, los procesos operativos relacionados con los productos y tratamientos informáticos.

4.2.4.2. Auditoría informática en la protección de datos personales

Una entidad financiera dispone de diversa información patrimonial y personal de cada uno de sus clientes. Los datos que posee la entidad pueden ser, sus datos personales (nombre, dirección, teléfono), también puede disponer de datos profesionales (actividad a la que se dedica, empresa para la que trabaja), además posición completa de sus cuentas

(saldos), valor tasado de su vivienda en caso de que le haya otorgado un préstamo, nivel de endeudamiento, etc.

La sensibilidad de la información manejada por una entidad financiera es mayor si se tiene en cuenta la totalidad de sus clientes y productos, ya que tienen información más completa y valiosa y por tanto más sensible, que disponer exclusivamente de las cuentas de un único cliente.

Los principales riesgos a los que hace frente la gestión de la información son:

- Difusión no autorizada, intencionada o no, hacia destinos improcedentes. La confidencialidad es un tema de especial preocupación en cualquier entidad financiera ya que en una entidad bancaria interviene la confianza depositada por el cliente.
- Obtención de información errónea, por accidente o por manipulación indebida, y como consecuencia de la normativa a la que está sometida la actividad bancaria perjudicando a los clientes.

4.2.4.3. Actividades de auditoría en relación con la protección de datos personales

Con respecto a la realización de la auditoría, esta debería verificar el cumplimiento de los controles en las áreas siguientes:

- Controles de procedimientos y normas operativas.
- Controles relacionados con la seguridad física.
- Controles relativos a la seguridad lógica.
- Controles de respaldo.

4.3. Selección de la metodología a utilizar en la investigación

4.3.1.1. Metodologías de auditoría informática

La metodología es necesaria para que un equipo de profesionales alcance un resultado homogéneo tal como si lo hiciera uno sólo. Por ello, resulta habitual el uso de metodologías en las empresas auditoras/consultoras profesionales (desarrolladas por los más expertos) para conseguir resultados similares (homogéneos) en equipos de trabajo diferentes (heterogéneos).

Las metodologías que se puede encontrar en la auditoría informática son dos familias distintas:

- Las auditorías de controles generales: Cuyo objetivo es dar una opinión sobre la fiabilidad de los datos del ordenador para la auditoría financiera. El resultado externo es un escueto informe como parte del informe de auditoría, donde se destacan las vulnerabilidades encontradas. Están basadas en pequeños cuestionarios estándares que dan como resultado informes muy generalistas.

- Las metodologías de los auditores internos: Están formuladas por recomendaciones de plan de trabajo y de todo el proceso que se debe seguir, por tanto, están basadas en profesionales de gran nivel de experiencia y formación, capaces de dictar recomendaciones técnicas, operativas y jurídicas, que exigen una gran profesionalidad y formación. De la misma forma se describe en forma de cuestionarios genéricos, con una orientación de los controles a

revisar. El auditor interno debe crear sus metodologías necesarias para auditar los distintos aspectos o áreas en el plan auditor.

4.3.1.2. Criterios de selección de metodología

4.3.1.3. COBIT - metodología seleccionada

El marco de referencia de COBIT 5 consta de objetivos de control de TI de alto nivel y de una estructura general para su clasificación y presentación, que han sido basadas en tres niveles de actividades de TI al considerar la administración de sus recursos, estos son:

- Actividades: las actividades y tareas son las acciones requeridas para lograr un resultado medible. Las actividades tienen un ciclo de vida, mientras que las tareas son más discretas.
- Procesos: son conjuntos de actividades o tareas con delimitación o cortes de control.
- Dominios: es la agrupación natural de procesos denominados frecuentemente como dominios que corresponden a la responsabilidad organizacional.

Por lo tanto, el marco de referencia conceptual puede ser enfocado desde tres puntos estratégicos: criterios de información, recursos de TI y procesos de TI.

Estos tres puntos estratégicos son descritos en el cubo COBIT que se ilustra en Figura

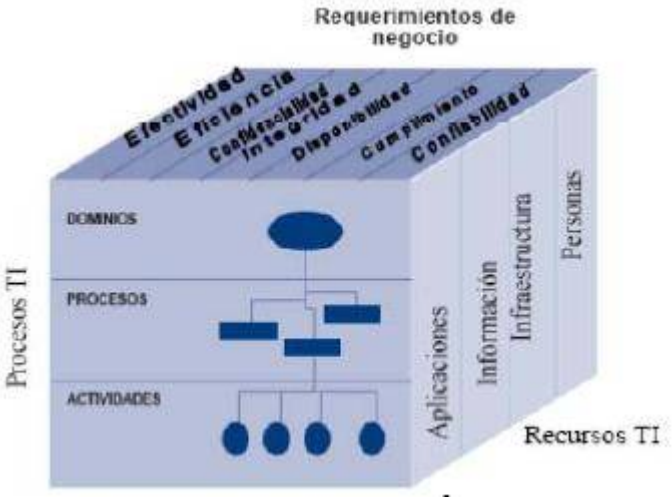


FIGURA 2 - CUBO COBIT

Para lograr la alineación de las mejores prácticas con los requerimientos del negocio, se recomienda que COBIT se utilice al más alto nivel, brindando así un marco de control general basado en un modelo de procesos de TI que debe ser aplicable en general a toda empresa.

4.3.1.3.1. Dominios

COBIT presenta treinta y cuatro objetivos generales, uno para cada uno de los procesos de las TI, estos procesos están agrupados en cuatro dominios como lo muestra la figura

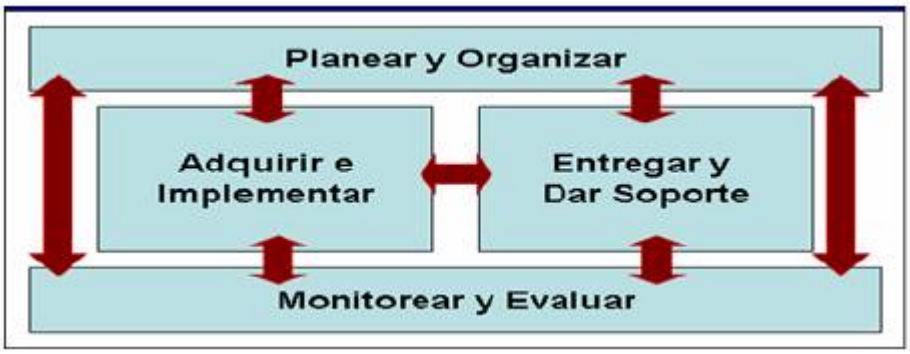


FIGURA 3 - DOMINIOS COBIT

PLANEAR Y ORGANIZAR (PO)

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada.

Este dominio considera los siguientes objetivos de alto nivel o procesos:

- PO1 Definir un plan estratégico de tecnología de información
- PO2 Definir la arquitectura de Información
- PO3 Determinar la dirección tecnológica
- PO4 Definir la organización y de las relaciones de TI
- PO5 Manejar la inversión en Tecnología de Información
- PO6 Comunicar la dirección y aspiraciones de la gerencia
- PO7 Administrar recursos humanos
- PO8 Asegurar el cumplimiento de requerimientos externos
- PO9 Evaluar riesgos
- PO10 Administrar proyectos
- PO11 Administrar calidad

ADQUIRIR E IMPLEMENTAR (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración en los procesos del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

Este dominio considera los siguientes objetivos de alto nivel o procesos:

- AI1 Identificar soluciones
- AI2 Adquirir y mantener software de aplicación
- AI3 Adquirir y mantener arquitectura de tecnología
- AI4 Desarrollar y mantener procedimientos relacionados con TI
- AI5 Instalar y acreditar sistemas
- AI6 Administrar cambios

ENTREGAR Y DAR SOPORTE (DS)

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales.

Este dominio considera los siguientes objetivos de alto nivel o procesos:

- DS1 Definir niveles de servicio
- DS2 Administrar servicios prestados por terceros
- DS3 Administrar desempeño y capacidad

- DS4 Asegurar servicio continuo
- DS5 Garantizar la seguridad de sistemas
- DS6 Identificar y asignar costos
- DS7 Educar y entrenar a los usuarios
- DS8 Apoyar y asistir a los clientes de TI
- DS9 Administrar la configuración
- DS10 Administrar problemas e incidentes
- DS11 Administrar datos
- DS12 Administrar instalaciones
- DS13 Administrar operaciones

MONITOREAR Y EVALUAR (ME)

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

Este dominio considera los siguientes objetivos de alto nivel o procesos:

- M1 Monitorear los procesos
- M2 Evaluar lo adecuado del control Interno
- M3 Obtener aseguramiento independiente
- M4 Proporcionar auditoría independiente.

En resumen, los Recursos de TI necesitan ser administrados por un conjunto de procesos agrupados en forma natural, con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos.

COBIT es considerada una herramienta completa ya que permite administrar los sistemas de información a un nivel más alto que los estándares existentes para el mismo propósito.

Se ha determinado que por las características y ambiente de aplicación de COBIT, ésta es la herramienta más útil para fundamentar el presente proyecto, ya que, independientemente de la misión de la organización a ser auditada, la plataforma en la que se basa el desarrollo de las tecnologías de la información, el servicio o producto que ofrezca, el tipo de administración que predomine; el marco de referencia COBIT no es sólo una guía para auditores o técnicos profesionales en procesos TI, sino también para gerentes y todos quienes están involucrados en el cumplimiento de los objetivos del negocio, pues en ambos aspectos, gerencial y tecnológico, su implementación será fundamental para que el gobierno de TI se desarrolle como debe ser.

OBJETIVOS DE CONTROL

Un objetivo de control de TI es una declaración del resultado o fin que se desea lograr al implantar procedimientos de control en una actividad de TI en particular. Los objetivos de control de COBIT son los requerimientos mínimos para un control efectivo de cada proceso de IT. Ya que los objetivos de control de TI de COBIT están organizados por procesos de TI, el marco de trabajo brinda vínculos claros entre los

requerimientos de gobierno de TI, los procesos de TI y los controles de TI.

Cada uno de los procesos de TI de COBIT tiene un objetivo de control de alto nivel y un número de objetivos de control detallados.

Los objetivos de control detallados se identifican por dos caracteres que representan el dominio (PO, AI, DS y ME) más un número de proceso y un número de objetivo de control.

Además de los objetivos de control detallados, cada proceso COBIT tiene requerimientos de control genéricos que se identifican con PCn (Control de Proceso número). Estos se deben

tomar como un todo junto con los objetivos de control del proceso para tener una visión completa de los requerimientos de control

MODELOS DE MADUREZ

Los modelos de madurez para el control de los procesos de TI consisten en desarrollar un método de puntaje de modo que una organización pueda calificarse a sí misma desde inexistente hasta optimizada (de 0 a 5). Este método ha sido derivado del modelo de madurez que el Software Engineering Institute definió para la madurez de la capacidad de desarrollo de software. Contra estos niveles, desarrollados para cada uno de los treinta y cuatro procesos de TI de COBIT, la administración puede mapear o cruzar:

- El estado actual de la organización - dónde está la organización actualmente

- El estado actual de la industria (la mejor de su clase en) - la comparación
- El estado actual de los estándares internacionales - comparación adicional
- La estrategia de la organización para mejoramiento - dónde quiere estar la organización.

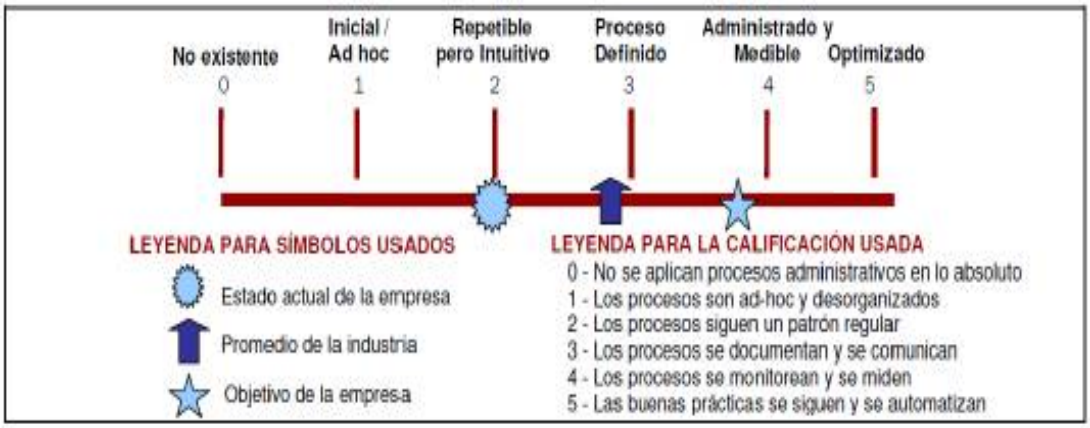


FIGURA 4 - NIVELES DE MADUREZ COBIT

0 Inexistente. Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.

1 Inicial. Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

2 Repetible. Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo.

Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

3 Definido. Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

4 Administrado. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

5 Optimizado. Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

En resumen, los modelos de madurez brindan un perfil genérico de las etapas a través de las cuales evolucionan las empresas para la administración y el control de los procesos de TI, este perfil es:

- Un conjunto de requerimientos y los aspectos que los hacen posibles en los distintos niveles de madurez
- Una escala donde la diferencia se puede medir de forma sencilla
- Una escala que se presta a sí misma para una comparación práctica
- La base para establecer el estado actual y el estado deseado
- Soporte para un análisis de brechas para determinar qué se requiere hacer para alcanzar el nivel seleccionado
- Tomado en conjunto, una vista de cómo se administra la TI en la empresa.

4.4. Sistema de Seguridad de la Información

La norma técnica peruana NTP-ISO/IEC 17799 ofrece todas las recomendaciones necesarias para poder gestionar un Sistema de Seguridad de la Información (SSI), al igual que la norma internacional ISO 27001, ofreciendo los requisitos necesarios para que los responsables del área en concreto puedan iniciar, implantar, mantener y mejorar la seguridad en las organizaciones.
La norma **ISO/IEC 17799** persigue que se proporcione una base común con la que poder llevar a cabo normas de seguridad dentro de las empresas y convertirse en una práctica eficaz de gestión de la seguridad.

La norma técnica peruana **ISO/IEC 17799** es una guía práctica que desarrolla los estándares organizacionales de la seguridad y genera prácticas efectivas durante la gestión de la Seguridad de la Información. Además, incrementa la confianza a la hora de establecer relaciones entre diferentes organizaciones. Todas las recomendaciones que genera esta norma tienen que ser utilizadas de acuerdo con la legislación aplicable a esta materia.

La **información** es un activo que tiene un elevado valor para las empresas, lo que requiere que se genere una protección adecuada. Hay que tener en cuenta el aumento en la seguridad dentro de las organizaciones. El resultado de este

creciente aumento es que la **información** se encuentra más expuesta a un alto número de amenazas y vulnerabilidades.

La **información** es adoptada de varías formas diferentes. Puede encontrarse en formato papel, almacenada electrónicamente, enviada por correo electrónico, en formato vídeo o a través de una conversación hablada personalmente. Es por todo esto, que la **información** tiene que estar debidamente protegida, sea cual sea el formato en la que no la encontremos.

4.5. El **Sistema de Seguridad de la Información** (SSI) ayuda a proteger la **información** de un amplio rango de amenazas diferentes con el que asegurar la continuidad del negocio, disminuir los daños generados en la organización y maximizar el retorno de la inversiones y las oportunidades de negocio.

4.5.1. El **Sistema de Seguridad de la Información** se consigue implementando un conjunto adecuado de controles, que puede ser políticas de seguridad, procedimientos, estructuras organizativas y funciones de software y hardware. Los controles necesarios son establecidos, implementados, monitoreados, revisados y mejorados en lo que sea necesario, con lo que se asegura que se cumplan todos los objetivos específicos de seguridad y negocios de la organización.

Esta norma **ISO/IEC 17799** cuenta con unos términos específicos, los cuales es necesario conocer para poder entender lo que expone la norma, durante este post vamos a ver todos los términos y a definirlos para su mejor comprensión:

Activo: es algo que tenga un gran valor para la organización.

Control: es la herramienta de gestión del riesgo, en el que se incluyen las políticas, las pautas, las estructuras organizacionales, que sean de naturaleza administrativa, técnica o legal.

Pauta: describe de forma clara lo que se debe hacer y cómo se debe hacer, persiguiendo el fin de alcanzar todos los objetivos planteados en la política de seguridad.

Instalaciones de proceso de información: Sistemas de información, servicio o infraestructuras en las que se localice de forma física.

Seguridad de la Información: es la preservación de la confidencialidad, la integridad y la disponibilidad de la información, además de otras muchas propiedades como puede ser la autenticidad, la falta de rechazo, la contabilidad y la confiabilidad que puede ser considera también.

Evento de Seguridad de la Información: es una ocurrencia que se encuentra identificada por un sistema, servicio o red en el que se indica una posible fisura en la política de seguridad de **información** o algún posible fallo en las situaciones relevantes para la seguridad.

Incidente de Seguridad de la Información: se encuentra indicado por diferentes eventos que no son esperados o no deseados, y que tienen una gran probabilidad de poner en un compromiso las operaciones de negocios y las amenazas de Seguridad de la Información.

Política de Seguridad: es un documento en el que se expresa los objetivos que tiene una organización a la hora de implementa un Sistema de Seguridad de la Información. Se encuentra firmada por la gerencia de la empresa y tiene que estar disponible para todo el mundo que desee verla.

Riesgo: es la combinación de probabilidad de que ocurra un incidente y las consecuencias de éste.

Análisis del riesgo: utilización sistemática de la **información** para identificar todas las fuentes que puedan generar algún riesgo.

Evaluación del riesgo: es el proceso general de análisis y evaluación de riesgo.

Valoración del riesgo: es el proceso mediante el cual se compara el riego estimado con el riesgo dado.

Gestión del riesgo: son actividades coordinadas para dirigir y controlar una organización considerando el riesgo que puede producir.

Tratamiento del riesgo: es el proceso por el que se selecciona e implementa las medidas para modificar el riesgo.

Terceros: es la persona que se reconoce por ser independiente por las partes involucradas concerniente al tema en cuestión.

Amenaza: causa potencial de un incidente no deseado lo que puede resultar dañando al sistema o a la organización.

Vulnerabilidad: es la debilidad presentada por un activo o grupo de activos que pueden ser explotados por una o más amenazas.

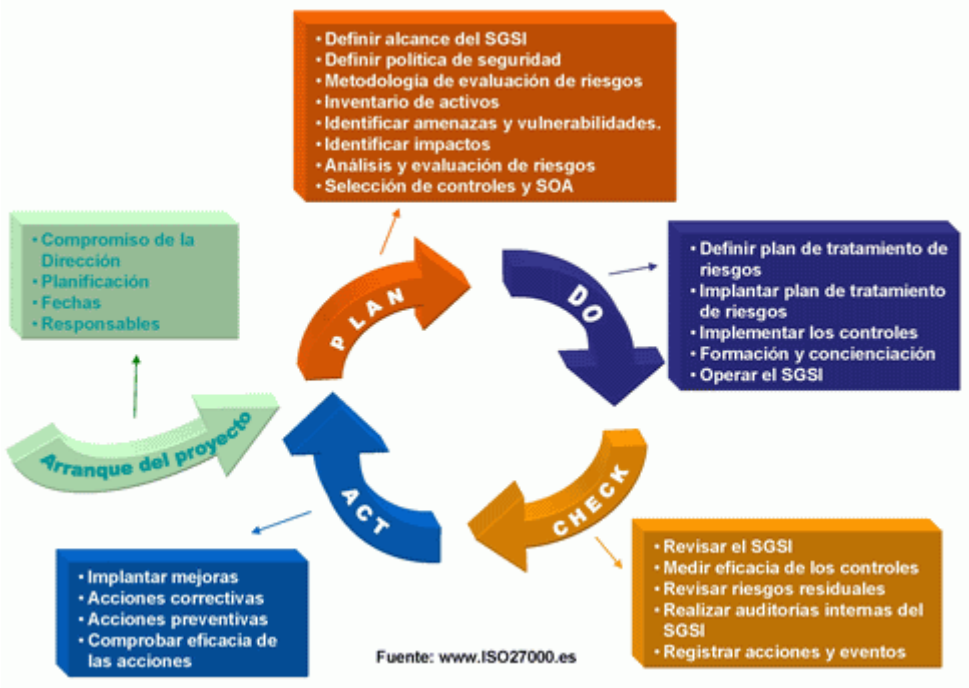
4.6. Estandares ISO 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

El ISO-27000 se basa en la segunda parte del estándar británico BS7799 (BS7799:2). Está compuesta a grandes rasgos por:

- ISMS(Information Security Management System).
- Valoración de Riesgo.
- Controles.

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares.



- **ISO 27000:** En fase de desarrollo. Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. Esta norma será gratuita, a diferencia de las demás de la serie, que tendrán un coste.
- **ISO 27001:** Es la norma principal de requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Fue publicada el 15 de Octubre de 2005 y sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última.

  En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en

dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

- **ISO 27002:** Cambio de nomenclatura de ISO 17799:2005 realizada el 1 de Julio de 2007. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.
- **ISO 27003:** En fase de desarrollo; probable publicación a finales de 2008. Contendrá una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.
- **ISO 27004:** Proporciona directrices para la medición de la seguridad de la información; se acopla bien con ISO 27001 ya que explica cómo determinar si el SGSI ha alcanzado los objetivos.
- **ISO 27005:** proporciona directrices para la gestión de riesgos de seguridad de información. Es un muy buen complemento para ISO 27001 ya que brinda más información sobre cómo llevar a cabo la evaluación y el tratamiento de riesgos, probablemente la etapa más difícil de la implementación. ISO 27005 ha surgido de la norma británica BS 7799-3.
- **ISO 27006:** Publicada en Febrero de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.
- ISO 22301 define los requerimientos para los sistemas de gestión de continuidad del negocio, se adapta muy bien con ISO 27001 porque el punto A.17 de esta última requiere la implementación de la continuidad del negocio aunque no proporciona demasiada información.

- ISO 9001 define los requerimientos para los sistemas de gestión de calidad. Aunque a primera vista la gestión de calidad y la gestión de seguridad de la información no tienen mucho en común, lo cierto es que aproximadamente el 25% de los requisitos de ISO 27001 y de ISO 9001 son los mismos: control de documentos, auditoría interna , revisión por parte de la dirección, medidas correctivas, definición de objetivos y gestión de competencias. Esto quiere decir que si una empresa ha implementado ISO 9001 le resultará mucho más sencillo implementar ISO 27001.

Familia de normas 27000	
Norma ISO/IEC	**Título**
ISO 27000	Gestión de la Seguridad de la Información: Fundamentos y vocabulario.
ISO 27001	Especificaciones para un **SGSI**.
ISO 27002	Código de Buenas Prácticas.
ISO 27003	Guía de Implantación de un **SGSI**.
ISO 27004	Sistema de Métricas e Indicadores.
ISO 27005	Guía de Análisis y Gestión de Riesgos.
ISO 27006	Especificaciones para Organismos Certificadores de **SGSI**.
ISO 27007	Guía para auditar un **SGSI**.
ISO 2701X	Guías sectoriales.
ISO 27XXX	Futuras normas.

4.6.1. ISO 27001

- ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.
- ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una

organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

- ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento; aquí se puede ver la cantidad de certificados en los últimos años:

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

¿Cómo funciona la ISO 27001?

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI).

Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, anti-virus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc.

¿Por qué ISO 27001 es importante para su empresa?

Hay 4 ventajas comerciales esenciales que una empresa puede obtener con la implementación de esta norma para la seguridad de la información:

Cumplir con los requerimientos legales – cada vez hay más y más leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información. La buena noticia es que la mayoría de ellos se pueden resolver implementando ISO 27001 ya que esta norma le proporciona una metodología perfecta para cumplir con todos ellos.

Obtener una ventaja comercial – si su empresa obtiene la certificación y sus competidores no, es posible que usted obtenga una ventaja sobre

ellos ante los ojos de los clientes a los que les interesa mantener en forma segura su información.

Menores costos – la filosofía principal de ISO 27001 es evitar que se produzcan incidentes de seguridad, y cada incidente, ya sea grande o pequeño, cuesta dinero; por lo tanto, evitándolos su empresa va a ahorrar mucho dinero. Y lo mejor de todo es que la inversión en ISO 27001 es mucho menor que el ahorro que obtendrá.

Una mejor organización – en general, las empresas de rápido crecimiento no tienen tiempo para hacer una pausa y definir sus procesos y procedimientos; como consecuencia, muchas veces los empleados no saben qué hay que hacer, cuándo y quién debe hacerlo. La implementación de ISO 27001 ayuda a resolver este tipo de situaciones ya que alienta a las empresas a escribir sus principales procesos (incluso los que no están relacionados con la seguridad), lo que les permite reducir el tiempo perdido de sus empleados.

¿Dónde interviene la gestión de seguridad de la información en una empresa?

Básicamente, la seguridad de la información es parte de la gestión global del riesgo en una empresa, hay aspectos que se superponen con la ciberseguridad, con la gestión de la continuidad del negocio y con la tecnología de la información:

¿Cómo es realmente ISO 27001?

ISO/IEC 27001 se divide en 11 secciones más el anexo A; las secciones 0 a 3 son introductorias (y no son obligatorias para la implementación), mientras que las secciones 4 a 10 son obligatorias, lo que implica que una organización debe implementar todos sus requerimientos si quiere cumplir con la norma. Los controles del Anexo A deben implementarse sólo si se determina que corresponden en la Declaración de aplicabilidad.

De acuerdo con el Anexo SL de las Directivas ISO/IEC de la Organización Internacional para la Normalización, los títulos de las

secciones de ISO 27001 son los mismos que en ISO 22301:2012, en la nueva ISO 9001:2015 y en otras normas de gestión, lo que permite integrar más fácilmente estas normas.

Sección 0 – Introducción – explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión.

Sección 1 – Alcance – explica que esta norma es aplicable a cualquier tipo de organización.

Sección 2 – Referencias normativas – hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.

Sección 3 – Términos y definiciones – de nuevo, hace referencia a la norma ISO/IEC 27000.

Sección 4 – Contexto de la organización – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI.

Sección 5 – Liderazgo – esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.

Sección 6 – Planificación – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.

Sección 7 – Apoyo – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.

Sección 8 – Funcionamiento – esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la

evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.

Sección 9 – Evaluación del desempeño – esta sección forma parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.

Sección 10 – Mejora – esta sección forma parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

Annexo A – este anexo proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 secciones (secciones A.5 a A.18).

¿Cómo implementar ISO 27001?

Para implementar la norma ISO 27001 en una empresa, usted tiene que seguir estos 16 pasos:

1) Obtener el apoyo de la dirección
2) Utilizar una metodología para gestión de proyectos
3) Definir el alcance del SGSI
4) Redactar una política de alto nivel sobre seguridad de la información
5) Definir la metodología de evaluación de riesgos
6) Realizar la evaluación y el tratamiento de riesgos
7) Redactar la Declaración de aplicabilidad
8) Redactar el Plan de tratamiento de riesgos
9) Definir la forma de medir la efectividad de sus controles y de su SGSI
10) Implementar todos los controles y procedimientos necesarios
11) Implementar programas de capacitación y concienciación
12) Realizar todas las operaciones diarias establecidas en la documentación de su SGSI
13) Monitorear y medir su SGSI

14) Realizar la auditoría interna

15) Realizar la revisión por parte de la dirección

16) Implementar medidas correctivas

Documentación obligatoria

ISO 27001 requiere que se confeccione la siguiente documentación:

- Alcance del SGSI (punto 4.3)
- Objetivos y política de seguridad de la información (puntos 5.2 y 6.2)
- Metodología de evaluación y tratamiento de riesgos (punto 6.1.2)
- Declaración de aplicabilidad (punto 6.1.3 d)
- Plan de tratamiento de riesgos (puntos 6.1.3 e y 6.2)
- Informe de evaluación de riesgos (punto 8.2)
- Definición de roles y responsabilidades de seguridad (puntos A.7.1.2 y A.13.2.4)
- Inventario de activos (punto A.8.1.1)
- Uso aceptable de los activos (punto A.8.1.3)
- Política de control de acceso (punto A.9.1.1)
- Procedimientos operativos para gestión de TI (punto A.12.1.1)
- Principios de ingeniería para sistema seguro (punto A.14.2.5)
- Política de seguridad para proveedores (punto A.15.1.1)
- Procedimiento para gestión de incidentes (punto A.16.1.5)
- Procedimientos para continuidad del negocio (punto A.17.1.2)
- Requisitos legales, normativos y contractuales (punto A.18.1.1)

Y estos son los registros obligatorios:

- Registros de capacitación, habilidades, experiencia y calificaciones (punto 7.2)
- Monitoreo y resultados de medición (punto 9.1)
- Programa de auditoría interna (punto 9.2)
- Resultados de auditorias internas (punto 9.2)
- Resultados de la revisión por parte de la dirección (punto 9.3)
- Resultados de medidas correctivas (punto 10.1)
- Registros sobre actividades de los usuarios, excepciones y eventos de seguridad (puntos A.12.4.1 y A.12.4.3)

Por supuesto que una empresa puede decidir confeccionar otros documentos de seguridad adicionales si lo considera necesario.

CAPÍTULO V: DESARROLLO DE LA PROPUESTA

Procedimiento de investigación

Se realizaron tres exámenes para el estudio:

- Identificación y evaluación de la estructura de gestión de la seguridad de la información (Comité de gestión) y de la gestión de TI.
- Identificación, análisis y evaluación de los planes, procedimientos y ejecución de las políticas de gestión de tecnologías de información y de la seguridad de la información.
- Evaluación de la efectividad de los controles y procedimientos de TI.

Examen o prueba aplicada:

Identificación y evaluación de la estructura de gestión de la seguridad de la información (Comité de gestión) y de la gestión de TI.

A.1. Técnicas aplicadas

- Revisión y análisis documental
- Confrontación documental
- Entrevistas y descargo de los funcionarios de las Áreas de TI, Unidad de riesgos – Oficial de seguridad de la información
- Muestreo y seguimiento de proyectos de TI

A.2. Hallazgos potenciales

- Se evidencia que orgánicamente existe y funciona un Comité de Riesgos como órgano staff asesor al Directorio de la Caja. Se reúne periódicamente de manera mensual.

- Se evidencia que las funciones específicas del Comité de Riesgos en relación a la seguridad de la información están definidas en el SGRO.

- Se evidencia que orgánicamente existe y funciona una Unidad de Riesgos como unidad de línea, dependiente de la Gerencia General de La Caja.

- Se evidencia que funcionalmente existe y se cumple con el cargo de Oficial de Seguridad de la información asignado a la Unidad de Riesgos (designado el 23 de agosto 2010 en Acta 018-2010), que desarrolla funciones de asegurar que las actividades de seguridad de la información sean ejecutadas en cumplimiento con las políticas de seguridad y los objetivos de control especificados en su SGSI.

- Se evidencia que orgánicamente existe y funciona el Área de TI & Organización y Procesos como órgano staff, dependiente de la Gerencia General de la Caja, que desarrolla funciones de gestión de las TI, descritas en el PETI, y de seguridad de la información, descritas en el SGSI.

- En relación a la estructura orgánica del Área de Tecnologías de Información está conformada por una Gerencia de Tecnologías y Procesos, cuyo responsable es Ing. en Computación e Informática. Dependiendo de esta jefatura se encuentran las jefaturas de:

    a. Desarrollo y Sistemas, cuyo responsable es Ing. en Computación e Informática, el cual está encargado en el puesto. Cuenta además con dos (02) analistas programadores que cumple con perfiles de puesto adecuado, contratados por recibo de honorarios.

b. Producción y Soporte, cuyo responsable es Ing. en Computación e Informática. Cuenta con el apoyo de un operador de sistemas que cumple con el perfil de puesto.

c. Organización y Procesos, cuyo responsable es un profesional encargado.

- Se evidencia que el personal del Área de TI está capacitado y cuenta con la experiencia y conocimiento de los procesos de la Caja a los cuales les brinda soporte tecnológico; así como en las políticas, procedimientos y objetivos de control de seguridad de la información.

- Se evidencia que NO se ha cumplido con el plan de capacitación del personal del Área de TI, pese a que está contemplado en el Plan operativo.

A.3. Conclusiones de auditoría

- La estructura orgánica definida en el SGSI es concordante con lo estipulado en el Art. N° 4 del Circular G-140-2009-SBS en relación a contar con una estructura organizacional que les permita implementar y mantener el sistema de gestión de la seguridad de información.

- La estructura orgánica definida en el SGRO es concordante con lo estipulado en la normatividad Resolución S.B.S. N° 2116 -2009 en relación a la gestión de los riesgos operativos relacionados con TI.

- La estructura orgánica del Área de TI es adecuada para la segregación de

funciones en relación a la seguridad de la información, entre las unidades de desarrollo de sistemas y las de producción y soporte. Además, su ubicación en la estructura organizativa le permite una interacción directa, ejecutiva y estratégica con la Gerencia General para la toma de decisiones y la planificación de proyectos relacionados con TI.

- Las funciones y esfuerzos del recurso humano del Área de TI están dedicados a atender los requerimientos rutinarios de las unidades usuarias de la Caja y observaciones de la SBS, sin posibilidad de desarrollar nuevos proyectos estratégicos de TI para la Caja.

- Se considera como amenaza el contar con personal contratado por recibo de honorarios en la Unidad de desarrollo de sistemas, por cuanto NO asegura la continuidad de la ejecución de los proyectos pendiente y los nuevos.

- Se considera como factor de desmotivación del personal y de una amenaza de continuidad de la ejecución de los proyectos pendiente y los nuevos, el no contar con personal capacitado, sobre todo con respecto a las tecnologías de información relacionadas con los proyectos y servicios que brinda el Área de TI como soporte a los procesos del negocio.

A.4. Recomendaciones de auditoría

- En la elaboración del nuevo PETI, la Gerencia General debe coordinar con la Jefatura del Área de TI con la finalidad de asegurar que la planificación de los nuevos proyectos estratégicos de TI cuente con una

estructura organizativa que supere los inconvenientes actuales de que el esfuerzo del recurso humano con el que cuenta el área de TI esté totalmente dedicado a cumplir tareas rutinarias y sin posibilidad de dedicarse a proyectos que generen nuevo valor agregado. Para poder cumplir con nuevos proyectos de TI debe evaluarse la posibilidad de ampliación del recurso humano del Área de TI, outsourcing (subcontratación especializada) o tercerizar servicios.

- La Gerencia general debe ordenar a quien corresponda la regularización de pase a planilla del personal de la Unidad de desarrollo de sistemas para mitigar la amenaza de la NO continuidad de la ejecución de los proyectos pendiente y los nuevos. Así mismo, se debe regularizar la situación de "encargatura" del Jefe de la Unidad de desarrollo de sistemas.

- La Gerencia general debe ordenar a quien corresponda la ejecución del Plan de capacitación para el personal del Área de TI, relacionado con las tecnologías, proyectos y servicios que brinda el Área de TI como soporte a los procesos del negocio.

A.5. Valoración de la criticidad de riesgos asociados a este factor

Criterio de seguridad que afecta				Valoración de criticidad de riesgos relacionados
Integridad de la información	Confidencialidad de la información	Disponibilidad de la información	Gestión de TI	
			X	2

TABLA 3 - VALORACIÓN DE LA CRITICIDAD DE RIESGO

Examen o prueba aplicada:

Identificación, análisis y evaluación de los planes, procedimientos y ejecución de las políticas de gestión de tecnologías de información y de la seguridad de la información.

B.1. Técnica aplicada

- Revisión y análisis documental
- Confrontación documental
- Entrevistas y descargo de los funcionarios de las Áreas de TI, Unidad de riesgos – Oficial de seguridad de la información
- Muestreo y seguimiento de casos

B.2. Hallazgos potenciales

<u>Con respecto a Sistema de gestión de seguridad de la información</u>

- Se evidencia la elaboración de un plan de trabajo 2011 considerando y organizando actividades para verificar la implementación y efectividad de las políticas y controles de seguridad de la información descritos en el SGSI, concordante con el requerimiento mínimo señalado en el Art. N° 5 del circular G-140-2009-SBS.
- Se evidencia la formalización y normalización mediante reglamentos operativos específicos de los siguientes procedimientos relacionados con la seguridad de la información:

  - Altas, bajas y modificación de usuarios de los sistemas (fecha aprobación: 30/12/2010, última modificación: 17/01/2011), donde se define el procedimiento para las altas, bajas y modificación de datos de los usuarios de los sistemas de la Caja. Incluye también el procedimiento de altas para usuarios externos

  - Administración de perfiles de usuarios (fecha aprobación: 13/04/2011), como parte de la seguridad lógica se especifica el procedimiento de creación de perfiles de usuario y otorgamiento de códigos de usuario

  - Atención de requerimientos de usuarios (fecha aprobación: 13/04/2011), donde se especifica el procedimiento cómo las áreas usuarias deben realizar sus solicitudes de cambios operativos y funcionales al SIIF y SIG.

- Certificación de módulos – adecuaciones de sistemas (fecha aprobación: 13/04/2011) donde se establece la forma como se realizan las pruebas y posterior certificación para poner en producción los nuevos módulos implementados o los adecuados o modificados.

- Respaldo de la información (fecha aprobación: 30/03/2011) donde se establece la frecuencia, procedimiento, etiquetado y rotulado y almacenamiento de las copias de respaldo de la información

- Uso del correo electrónico institucional (fecha aprobación: 13/04/2011) donde se especifica los estándares para la especificación de los nombres de las cuentas de correo electrónico, espacio asignado, políticas de uso del correo electrónico, altas y bajas de cuentas, procedimientos de envió de archivos adjuntos

- Se evidencia el cumplimiento de las actividades programadas en el plan de trabajo 2011 del SGSI, por parte de la Oficial de seguridad de la información, concluyendo en la remisión de informes trimestrales hacia la Jefatura de Riesgos y la Gerencia General, donde se detalla los resultados de las mismas y las recomendaciones correspondientes.

Con respecto a los riesgos operativos relacionados con TI

- Se evidencia la elaboración de un plan de trabajo para la evaluación de riesgos operacionales 2011, en las que se considera evaluación de los riesgos operacionales relacionados con TI, elaborado por el Oficial de Seguridad de la Unidad de Riesgos.

- Se evidencia de la aplicación de un procedimiento metodológico para la evaluación de riesgos operativos relacionados con TI, que contempla:

  - Identificación de procesos críticos
  - La identificación y medición de riesgos: probabilidad de ocurrencia
  - Análisis de impacto de ocurrencia (BIA)
  - Planes de acción para mitigar riesgos: definición de controles
  - Capacitación en gestión de riesgos
  - Monitoreo y seguimiento de la implementación de controles y evaluación de su efectividad

- Se evidencia la elaboración de matrices de riesgos y matrices para cerrar brechas, en las que se ha identificado y evaluado cada uno de los riesgos relacionados con los siguientes sub procesos del Área de TI:

  - Gestión de proyectos y desarrollo de software
  - Gestión de la infraestructura tecnológica y redes
  - Mantenimiento de equipos
  - Soporte
  - Organización y Procesos

- Se evidencia el cumplimiento de las actividades programadas en el plan de trabajo 2011 sobre la Gestión de riesgos operativos de TI, por parte de la Oficial de seguridad de la información, concluyendo

en la remisión de informes trimestrales hacia la Jefatura de Riesgos y la Gerencia General, donde se detalla los resultados de las mismas y las recomendaciones correspondientes.

Con respecto a la gestión de TI

- Se evidencia en el PETI la definición de un plan de trabajo donde se observa el desarrollo de proyectos, adecuaciones de los sistemas SIIF y SIG ante los requerimientos de distintas Áreas usuarias (cambios funcionales y operativos) y observaciones de la SBS, auditoria interna y auditoria externa, para un horizonte de tres (03) años 2009 - 2011.
- Se evidencia retrasos e incumplimientos significativos en el desarrollo de los proyectos descritos en el PETI y POTI, como:
  - Implementación de mensajería SMS y correo electrónico a clientes para campañas, promociones, notificaciones de vencimientos y otros.
  - Tarjetas de ahorro con código de barra para cuentas de captaciones
  - Banca electrónica, otros
- Se evidencia la existencia de una planificación de trabajo en el POTI 2011 en la que se especifica las actividades programadas referentes a:

Desarrollo de sistemas

- Atención de requerimientos operativos y funcionales de las áreas usuarias en el SIIF
- Optimización e incorporación de nuevos reportes al Sistema de Información Gerencial (SIG); e implementación de consultas y reportes de captaciones.
- Implementación de recomendaciones de SBS, auditoría externa, auditoría interna y unidad de riesgos
- Adecuaciones a los sistemas informáticos para la generación de la Central de Riesgo por Operación CRO SBS

Producción y soporte

- Implementación de un Centro de Cómputo Alterno
- Actualización de software ofimático, de servidor
- Renovación del parque informático

Organización y Procesos

- Formalización de procesos de TI: Desarrollo y Producción

▪ Se evidencia que la ejecución del plan de trabajo descrito en el POTI 2011 y el seguimiento del mismo es controlado mediante una cartera de actividades clasificadas y codificadas por dependencia solicitante, donde la prioridad de atención de requerimientos la tienen la SBS, Riesgos y los declarados como nuevos y urgentes (prioridad 1), que hace que la planificación inicial sea modificada, ocasionando retrasos o postergaciones en la atención de requerimientos de otras áreas y en el desarrollo de proyectos estratégicos relacionados con el PETI. A continuación se muestran una estadística de la situación de atención de requerimientos a la fecha de la presente auditoria.

		Estado			
Dependencia Solicitante	**Prioridad**	**Culminado**	**En Proceso**	**Pendiente**	**Total por dependencia**
Atención al Usuario	3			1	1
Auditoría	2	1			1
	4			2	2
Contabilidad	1	3			3
	2	2			2
	3	5	1		6
	4			6	6
Gerencia	3	1			1
Gerencia de Administración	1	1			1
	3		1		1
Legal	3		1	1	2
	4			2	2
Logística	4			1	1
Negocios	1	3			3
	3	2	2		4
	4		1	4	5
Operaciones	1	2			2
	2	2			2
	3	1	3		4
	4			5	5
Producción	1	1			1
	2	1			1
Recuperaciones	1	1			1

	2	2			2
	3	3			3
	4			1	1
Riesgos	1	1			1
	2	4			4
	3	5			5
	4			5	5
SBS	1		1		1
Servicio de Créditos	4			3	3
TI	1	1			1
	3		1		1
	4			1	1
Total general		**42**	**11**	**34**	**87**

TABLA 4 - SITUACIÓN DE ATENCIÓN DE REQUERIMIENTOS DE LA AUDITORIA EXTERNA

- Se evidencia que se ha formalizado los procedimientos críticos de las unidades del Área de sistemas, como sigue:

Desarrollo de sistemas

- Manual de procedimientos de desarrollo de software, en el que se describe en detalle los procesos de la unidad de Desarrollo de Sistemas en cuanto a: Atención de requerimientos de usuario, Implementación de nuevos módulos y modificación de los sistemas informáticos de la Caja, Integración de módulos de los

sistemas informáticos desarrollados/modificados, Pruebas en ambiente de desarrollo, Generación de versiones de sistemas informáticos.

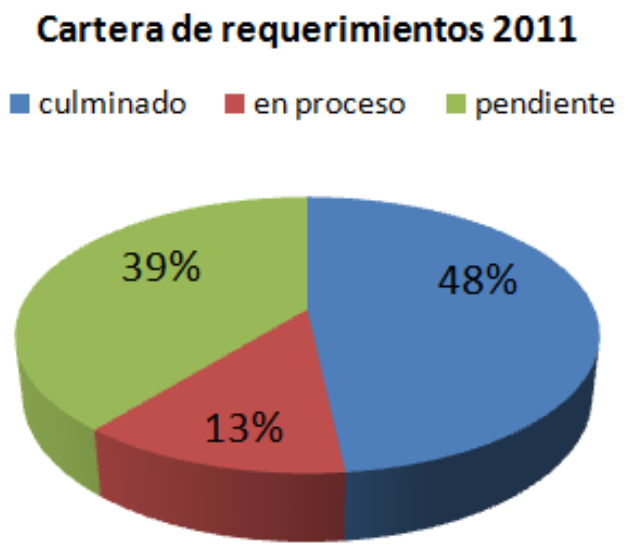


FIGURA 5 - CARTERA DE REQUERIMIENTOS

- Manual de procedimientos para la generación de base de datos de desarrollo (fecha de aprobación: 25/07/2011), en el que se establecen los procedimientos para la obtención de una base de datos para el trabajo de programación y pruebas de la División de Desarrollo, de tal manera que su personal no pueda acceder o manipular información real de los clientes de la Caja, sus cuentas de activos o pasivos y cualquier otra que vulnere el principio de confidencialidad de la información.

Producción y soporte

- Manual de procedimientos de actualización de inventario de hardware y software (fecha de aprobación: 13/04/2011), cuya

finalidad inventariar los recursos tecnológicos con los que cuenta la organización para su mejor aprovechamiento, evitar el uso de software ilegal, llevar un correcto control de inventarios, además identificar y establecer las necesidades existentes respecto a herramientas tecnológicas en las áreas de la Caja.

- Manual de configuración de comunicaciones
- Manual de configuración del Active Directory
- Manual de configuración del ISA Server
- Manual de procedimiento de cierre diario de las operaciones
- Manual de procedimiento de cierre mensual de las operaciones

Con respecto a Organización y Procesos

- Se evidencia la definición de un plan de trabajo 2011 en el POTI para la Unidad de Organización y Procesos.

- Se evidencia que se ha formalizado el procedimiento de Actualización de la normatividad (fecha de aprobación: 13/04/2011) en un reglamento específico con la finalidad de que sirva como guía al personal de todas las Gerencias, Áreas y Agencias, para solicitar actualización de la normatividad que le compete por optimización de la normatividad vigente y/o nuevas normas emitidas por las entidades supervisoras y reguladoras.

B.3. Conclusiones de auditoría

- Se ha logrado que el Sistema de gestión de la seguridad de la información y la gestión de riesgos operativos relacionados con TI, la gestión del área de TI, con la implementación de normativas, controles y procedimientos formalizados, tengan las siguientes características:

  - Desde el punto de vista de ingeniería: se ha logrado niveles aceptables de validación, verificación, integración de productos y desarrollo de requisitos (Nivel 3 en la clasificación CMMI)

  - Desde el punto de vista de la gestión de proyectos: se ha logrado niveles aceptables de gestión de riesgos, gestión de proveedores integrada, equipos de trabajo integrados (Nivel 3 en la clasificación CMMI)

  - Desde el punto de vista de gestión de procesos: se ha logrado niveles aceptables de formación organizativa, definición de procesos organizativos y un enfoque en el proceso organizado (Nivel 3 en la clasificación CMMI)

  - Desde el punto de vista de soporte: se ha logrado niveles aceptables de gestión de la configuración, aseguramiento de la calidad de los procesos y de los productos y medición y análisis (Nivel 2 en la clasificación CMMI)

- Los procesos de desarrollo de sistemas y producción y soporte están

institucionalizados debido a que se ha logrado seguir de forma rutinaria, como parte de la cultura de la organización, el establecimiento de políticas y metodologías propias de trabajo, planes, recursos, asignación de responsabilidades y autoridad, formación, comprobar la implantación y cumplimiento

- Falta implementar un procedimiento de Medición y control en base a indicadores de rendimiento de las actividades y tareas en los procesos de desarrollo de sistemas y producción y soporte del Área de TI.

- Las actividades y tareas desarrolladas por el área de TI se han orientado básicamente a atender requerimientos de modificaciones y adecuaciones del SIIF y SIG relacionados con la normatividad y observaciones de la SBS, auditoría interna y externa y de las diferentes áreas usuarias de la Caja, dejando en estado de "pendiente" los proyectos de TI relacionados con nuevos productos y servicios de TI para operaciones electrónicas que coloque a la institución en una posición competitiva con respecto a la banca comercial y otros competidores directos. Por tanto, se concluye que el Área de TI está dedicada todavía a actividades y tareas a nivel operativo y no de nivel estratégico y de generación de valor agregado a los servicios que brinda la Caja.

- En los reglamentos y controles NO se evidencia la descripción objetivos de control sobre el registro de incidentes relacionados con TI, procedimientos de revisión y evaluación de los controles y políticas de seguridad de la información descrita en respuesta a los cambios del ambiente organizacional, nuevos productos de negocio,

condiciones legales o cambios en la infraestructura tecnológica.

B.4. Recomendaciones de auditoría

- Incluir en el Reglamento de Administración de perfiles de usuarios una matriz anexa en la que se especifique los niveles de acceso de los usuarios a los módulos y opciones de los sistemas SIIF y SIG según su perfil de puesto de trabajo, que permita a la Unidad de Riesgos realizar las verificaciones de cada ocurrencia de alta, baja o modificación de usuarios, la que deberá ser actualizada permanentemente, teniendo en cuenta que las opciones que se agrupan para un perfil pueden ser modificadas por nuevas opciones que se agreguen al sistema informático o por solicitud de algunas jefaturas para la mejor operatividad del personal a su cargo.

- El SGSI debe completarse con lo siguiente:
  - Debe especificarse objetivos de control para el "registro de incidentes relacionados con TI", que permita posteriormente la evaluación de posibles vulnerabilidades y amenazas a cargo del área de Gestión de riesgos y del Oficial de seguridad, en base a estadísticas y las frecuencias de ocurrencia por tipo de incidente.

  - Procedimientos de revisión y evaluación de los controles y políticas de seguridad de la información descritos en respuesta a los cambios del ambiente organizacional, nuevos productos de negocio, condiciones legales o cambios en la infraestructura tecnológica.

- El Área de TI debe implementar un procedimiento de Medición y control en base a indicadores de rendimiento de las actividades y tareas en los procesos de desarrollo de sistemas y producción y soporte del Área de TI.

B.5. Valoración de la criticidad de riesgos asociados a este factor

Criterio de seguridad que afecta				Valoración de criticidad de riesgos relacionados
Integridad de la información	**Confidencialidad de la información**	**Disponibilidad de la información**	**Gestión de TI**	
			X	**3**

TABLA 5 - CRITERIO DE SEGURIDAD SOBRE DESARROLLO DE SISTEMAS

Examen o prueba aplicada

Evaluación de la efectividad de los controles y procedimientos de TI.

C.1. Técnica aplicada

- Revisión y análisis documental
- Confrontación documental
- Entrevistas y descargo de los funcionarios de las Áreas de TI, Unidad de riesgos – Oficial de seguridad de la información
- Muestreo y seguimiento de casos (expedientes de atención de requerimientos y certificación de módulos)
- Pruebas sustantivas de escritorio para determinar niveles de acceso

C.2. Hallazgos potenciales

Con respecto al desarrollo de software

- Se evidencia que el proceso de desarrollo de software esta formalmente definido y estandarizado en base a un manual de procedimientos de desarrollo de software. El procedimiento de desarrollo de software está definido en un modelo de ciclo de desarrollo de software propio que establece las actividades, tareas y formatos a utilizar en cada fase del ciclo.

- Se evidencia que se aplica con efectividad el control y administración de los requerimientos solicitados por las áreas usuarias en aplicación de su correspondiente reglamento. El procedimiento contempla:

  - La gestión adecuadamente de las autorizaciones antes de efectuar las atenciones a los requerimientos
  - La evaluación técnica de la factibilidad de la atención al requerimiento
  - La determinación del nivel de priorización para la atención del requerimiento
  - El llenado de los formatos correspondientes al detalle de los requerimientos y los vistos buenos de los usuarios solicitantes
  - Conformidad de usuarios

- Se evidencia que la Unidad de desarrollo de sistemas realiza un control de cambios del código fuente y de las estructuras de la base de datos, cuando se atiende un requerimiento de actualización o modificación del SIIF y SIG, generándose un expediente por cada requerimiento atendido. El expediente de control contempla:

  - Con respecto al código fuente se registra los cambios sobre los objetos del sistema: la descripción de cambio, la fecha, el analista programador responsable, la librería a la que pertenece el objeto y se indica si el objeto es nuevo o modificado.

  - Con respecto a la estructura de datos se registra los cambios en la estructura de datos: descripción de la estructura modificada (base de datos, tabla, columnas)

  - Carga de data. Cuando es necesario se deja registro de los datos nuevos que han sido agregados a las tablas y base de datos, para dar funcionalidad a las modificaciones realizadas sobre el sistema.

  - Los scripts de actualización de base de datos

  - La documentación que certifica las pruebas de la funcionabilidad y operatividad de los cambios realizados
  - El manual de usuario o la actualización del mismo

- Se evidencia que la Unidad de desarrollo de sistemas realiza la

gestión de bibliotecas de versiones. Cuando los cambios son sustantivos, a criterio de la Jefatura de Desarrollo de sistemas se genera un expediente de la nueva versión, consolidando todos los cambios en el código fuente y estructuras de datos que incluye la nueva versión y se informa a la Jefatura de TI. Los expedientes de cambios y versiones es administrada únicamente por el Jefe de la Unidad de desarrollo.

- Se evidencia que existe una adecuada segregación funcional con respecto a la seguridad de la información de la Unidad de Desarrollo con respecto a la Unidad de Producción y soporte. Se evidencia con:

  - La Unidad de desarrollo de sistemas trabaja en una red de datos que física y lógicamente es independiente de la red de datos institucional.
  - La Unidad de desarrollo de sistemas trabaja con una copia actualizada de la base de datos institucional de manera independiente.

<u>Con respecto a producción y soporte</u>

- Se evidencia que se aplica con efectividad el control y procedimiento certificación de módulos-adecuaciones. El procedimiento contempla:

  - Las pruebas unitarias y pruebas integrales de acuerdo al tipo de requerimiento. Las pruebas se documentan.
  - Simulación de pase a producción (con datos reales) en un ambiente preparado para esta finalidad
  - Certificación de manuales de usuario del módulo y/o adecuación

- Se evidencia que los diferentes módulos del SIIF y del SIG cuentan con sus correspondientes "Manuales de Usuario" los cuales se actualizan cada vez que ocurre una modificación de los sistemas en atención de requerimientos. Estos manuales en formatos PDF.

- Se evidencia la definición de perfiles de usuario para determinar los niveles de acceso a los diferentes módulos y opciones del sistema de la Caja mediante códigos de usuario y sus password. Utilizando diferentes códigos de usuario y sus password se comprobó la efectividad del cumplimiento de los niveles de acceso según el tipo de usuario al SIIF y SIG. Las opciones que no corresponden al nivel de acceso de acuerdo al usuario aparecen deshabilitadas o no se tiene acceso.

- Se evidencia la definición de perfiles de usuario para determinar los niveles de acceso al sistema de red datos de la Caja mediante códigos de usuario y sus password y configuración del sistema operativo. Se realizaron pruebas verificándose que:

  - El acceso a los terminales está definido y limitado por usuario y área (grupo), mediante procedimientos de autentificación de usuario (login de usuario y password).

  - Existe acceso limitado y controlado a Internet, con posibilidades de acceso a sitios Web autorizados: sitio Web institucional, instituciones financieras, algunos diarios, SUNAT, SUNARP,

EsSalud y otros con extensión .org).

- Se han deshabilitado los puertos USB, lectoras/reproductores de CD o DVD y otras posibilidades de lectura/escritura de data y programas a las terminales; a excepción de personal autorizado por administración.
- Existe imposibilidad de instalación de programas en general.
- Existe imposibilidad de modificación de parámetros del sistema: fecha, hora y otros; así como acceso a entornos de configuración del computador.
- Existe imposibilidad de cambios de propiedades de conexión LAN (IP).
- Existe imposibilidad de agregar nuevos dispositivos externos conectados a los terminales.
- Se han desinstalado y deshabilitado aplicaciones que posibiliten distracciones en el trabajo o para manipulación de información de la base de datos (acceso, consulta, modificaciones).
- La opción ejecutar está deshabilitada
- La opción de acceso al sistema operativo DOS está deshabilitada

- No existe posibilidad de acceso a la red de datos mediante el explorador

- No existe posibilidad de acceso a la unidad C:\ mediante el explorador

- Se ha deshabilitado las opciones importación de datos de aplicativos como MS Excel

- Se evidencia que las posibilidades de modificación de los parámetros del SIIF es nula desde el sistema. Las modificaciones de parámetros del sistema son responsabilidad del jefe de la Unidad de Producción y Soporte, en coordinación con los jefes de área, según sea el caso.

- No se encontró documentación sobre procedimientos para el registro de incidencias de seguridad, como: fallos del sistema de información y pérdidas de servicio, denegación de servicio, errores que resultan de datos del negocio inexactos o incompletos, intentos de accesos no autorizados.

- Se evidencia que se ha automatizado el registro de pistas de auditoría, para posteriores seguimiento de incidencias y con posibilidades de recuperación de la información. La estrategia implementada registra en una sola tabla el usuario que registró la transacción, fecha, hora, tabla y campo se modificó, el tipo de operación que se realizó (insert, update, delete), valor anterior del campo, valor actual del campo. Las consultas de las pistas de

auditoría está implementado en el Módulo de Controles con acceso restringido sólo para el personal autorizado de Auditoría.

- Se evidencia que se aplica con efectividad el control y procedimiento de creación de respaldos de la información. El procedimiento contempla:

  - Periodicidad de la generación de los respaldos de información
  - Responsables de la generación de los respaldos de información
  - Etiquetado de los respaldos de información
  - Procedimiento de almacenamiento de los respaldos de información
  - Procedimiento de recuperación de los respaldos de información

- Se evidencia que la Caja ha implementado Acuerdo de confidencialidad entre los trabajadores y la institución, de tal forma que éstos reconozcan que en el cumplimiento de sus funciones acceden a información confidencial oral, escrita, visual o electrónica, propiedad de la Caja, la cual no puede ser divulgada de manera parcial o total su contenido a ningún tercero o a demás personal de la Caja que no tenga vínculo y responsabilidad directa con dicha información, salvo en los casos en que sea necesario hacerlo, pero con la debida aprobación y autorización. Específicamente a TI, la información confidencial corresponde al funcionamiento, infraestructura, hardware, software, datos, usuarios, comunicaciones y seguridad informática.

C.3. Conclusiones de auditoría

- Se ha logrado un nivel aceptable de cumplimiento y efectividad de los controles y procedimientos de seguridad en el proceso de desarrollo de sistemas.

- Se ha logrado un nivel aceptable de cumplimiento y efectividad de los controles y procedimientos de seguridad en el proceso de puesta en producción de los sistemas y de infraestructura de soporte, faltando implementar un procedimiento específico para el registro de incidentes relacionados con TI.

C.4. Recomendaciones de auditoría

- El Oficial de seguridad de la información, en coordinación con la Jefatura de TI, deberán implementar y reglamentar un procedimiento para el registro de incidencias de seguridad, que incluya: fallos del sistema de información y pérdidas de servicio, caídas de los equipos de core (servidor, switch, router), caídas de estaciones de trabajo, denegación de servicio, errores que resulten de datos del negocio inexactos o incompletos, intentos de accesos no autorizados y otros relacionados con la TI.

C.5. Valoración de la criticidad de riesgos asociados a este factor

Criterio de seguridad que afecta				Valoración de criticidad de riesgos relacionados
Integridad de la información	**Confidencialidad de la información**	**Disponibilidad de la información**	**Gestión de TI**	
X	**X**	**X**	**X**	**2**

TABLA 6 - VALORACIÓN DE CRITICIDAD SOBRE SOPORTE

Resultados y discusión

Para el análisis y discusión de los resultados se realizaron encuestas a expertos, definidos por cinco funcionarios de alto nivel de la Caja Sipán:

Experto 1: Sr. Julio Del Castillo Vargas (Presidente)

Experto 2: Sr. Olivio Huancaruna Perales (Vice Presidente)

Experto 3: Sr. Víctor Raúl Rojas Díaz (Director)

Experto 4: Sr. Roger Cangahuala Janampa (Director)

Experto 5: Ing. Hobbier Siccha Ayvar (Jefe Sistema)

Los resultados de las encuestas las mostramos en la siguiente tabla (Escala del 1 al 5):

Preguntas	Experto 1	Experto 2	Experto 3	Experto 4	Experto 5	Promedio
¿En qué porcentaje cree Ud. Mejorará la organización del área de TI?	4	4	5	4	4	**4.2**
¿En qué porcentaje cree Ud. Mejorará la seguridad de datos?	4	4	4	4	4	**4**
¿En qué porcentaje cree Ud. Mejorará la ejecución de procesos del área de TI?	5	5	5	5	5	**5**
4.4						

TABLA 7 - RESULTADOS DE ENCUESTAS DE AUDITORÍA

Escala:

Efectividad	Puntaje
Muy alta	5
Alta	4
Media	3
Baja	2
Muy baja	1

La elaboración de la auditoría en el uso de tecnología de información optimizará la seguridad de la Caja Sipán S.A. tendrá una aceptación superior o igual a 4 en la escala planteada.

CAPÍTULO VI: COSTOS Y BENEFICIOS

6.1. Análisis de costos

- **Remuneración**

Detalle	Cantidad	Unidad	P.Unit (S./)	Total (S./)
Personal Auditor	2	Personas	15.000	30.000
TOTAL				**30.000**

- **Gastos Materiales**

Detalle	Cantidad	Unidad	P.Unit (S./)	Total (S./)
Papel A4	1	Millar	13.00	13.00
Tinta de impresora HP	2	cartuchos	90.00	180.00
Útiles de escritorio (lapiceros, folder, etc)			40.00	40.00
Computadora	1	Unidad	2000.00	2000.00
Impresora	1	Unidad	800.00	800.00
CD's	5	Unidad	2.00	10.00
Fotocopias	500	Unidad	0.05	50.00
TOTAL				**3093.00**

- **Gastos Servicios**

Detalle	Cantidad	Unidad	P.Unit (S./)	Total (S./)
Luz	3	Mes	20.00	60.00
Agua	3	Mes	10.00	30.00
Internet	3	Mes	100.00	300.00
Teléfono	3	Mes	30.00	90.00
Transporte público local	60	Pasaje	4.00	240.00
Viáticos	2		1000.00	2000.00

TOTAL	**2720.00**

- **Totales**

Detalle	**Totales**
Remuneración	30000.00
Bienes	3093.00
Servicios	2720.00
TOTAL	**s/.35813.00**

6.2. Beneficios

Los problemas tecnológicos, administrativos y las dificultades operacionales pueden detectarse antes de que suceda por lo que le permite a la organización evitar mayores costos a causa de las deficiencias detectadas.

Tal es así que la auditoría en el uso de tecnologías de información representa una herramienta Gerencial para auxiliar a la organización en el cumplimiento de los objetivos deseados. Al realizar una Auditoría en el Uso de tecnologías de Información la empresa podrá tener un mejor manejo de la información haciendo un óptimo uso a sus recursos y por ende el crecimiento de la misma, permitiéndose así:

- Recomendar ciertas medidas para mejorar la situación presente.
- Descarga a la dirección de obligaciones importantes dedicándose a asuntos no delegables.
- Extiende la función auditora a toda la empresa.
- Asegura información detallada y objetiva.
- Obliga a la empresa a replantear situaciones en una fuente continua y saludable de nuevas ideas y aplicaciones. Por lo que podemos resumir que mediante esta auditoría se le ayuda a la gerencia a reducir costos, aumentar las utilidades y aprovechar mejor los recursos tecnológicos, materiales y financieros.
- Mejora la imagen pública.
- Confianza en los usuarios sobre la seguridad y control de los servicios de TI.
- Optimiza las relaciones internas y del clima de trabajo.
- Realiza un control de la inversión en un entorno de TI, a menudo impredecible.

CAPÍTULO VII: CONCLUSIONES

- Se realizó el levantamiento de información para conocer la estructura orgánica del área de Tecnología de Información de la Caja Sipán, determinando que existe un Comité de Riesgos como órgano staff asesor al Directorio de la Caja; además de un Área de Tecnologías de Información con jefe encargado, jefe de desarrollo y mantenimiento, responsable de producción y soporte técnico, y jefe de organización y método; concordante con lo estipulado en el Art. N° 4 del Circular G-140-2009-SBS y en la normatividad Resolución S.B.S. N° 2116 - 2009

- Se evaluaron la estructura de gestión de la seguridad de la información y de la gestión de Tecnología de Información de la Caja Sipán, determinando la existencia de un plan de trabajo 2011, donde se consideran y organizan actividades para verificar la implementación y efectividad de las políticas y controles de seguridad de la información concordante con el requerimiento mínimo señalado en el Art. N° 5 del circular G-140-2009-SBS.

- Se ha logrado implantar un Sistema de Gestión de la Seguridad de la Información y un Sistema para Gestión de Riesgos Operativos relacionados con Tecnología de Información para la Caja Sipán, cuyos resultados de sus evaluaciones están ayudando a encauzar y determinar una adecuada acción gerencial, las definición de prioridades para gestionar los riesgos de seguridad de la información y la implantación de los controles seleccionados para protegerse contra dichos riesgos. Los procedimientos metodológicos y requisitos de éstos sistemas cumplen con las normatividades de la SBS para estos casos: Circular Nº G- 140 -2009: Gestión de la seguridad de la información y Resolución S.B.S. N° 2116 -2009: Reglamento para la gestión del riesgo operacional

CAPÍTULO VIII: RECOMENDACIONES

Los problemas de seguridad de la información y las dificultades operacionales pueden detectarse antes de que suceda por lo que le permite a la organización evitar mayores costos a causa de las deficiencias detectadas. Tal es así que la auditoría en el uso de tecnologías representa una herramienta para auxiliar a la organización en el cumplimiento de los objetivos deseados. Al realizar una Auditoría en el uso de tecnologías la empresa podrá tener un mejor manejo de la información haciendo un mejor uso a sus recursos y por ende el crecimiento de la misma.

- Se recomienda cumplir con el plan operativo de capacitación del personal del Área de TI.

- Se recomienda realizar auditorías específicas para cada proceso o recurso de tecnología de información como por ejemplo de base de datos, de comunicaciones, de seguridad física, de seguridad lógica, de los programas.

- Se recomienda realizar la auditoría en el uso de tecnologías de información con una frecuencia de una vez al año

- Se recomienda encargar la realización de la auditoría a un grupo de profesionales externos, con la finalidad de asegurar la integridad de los resultados de la auditoría.

CAPÍTULO IX: REFERENCIAS BIBLIOGRÁFICAS

Castro, K. M. (2012). *Auditoría Informática orientada a los procesos críticos de crédito generados en la Cooperativa de Ahorro Y Crédito "Fortuna" aplicando el marco de trabajo COBIT.* Loja Ecuador.

Framework, C. (2010). *Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Estados Unidos: ISACA.

Marcillo, G. F. (2012). *Auditoría informática de la cooperativa de ahorro y crédito "Alianza del Valle" LTDA aplicando COBIT 4.0.*

Michel, C. J. (2009). *Auditoria de seguridad de redes inalámbricas de área local Wireless local área Network (WLAN).* La Paz – Bolivia.

Acha Iturmendi, J. (1994). *Auditoría Informática en el empresa.* Madrid: Parainfo.

Mario G. Piattini, E. d. (2001). *Auditoria informática, un enfoque práctico, 2da Edición.* Mexico: Editorial Alfa Omega.

ANEXO Nº 01

Resultados de la evaluación de parches y services Pack de los sistemas operativos en los equipos de cómputo de las diferentes agencias

(Se utilizó los programas Caín & Abel y Nessus)

a. Oficina Principal – Chiclayo

ID	Equipo	Dirección IP	Dirección Mac	Sistema Operativo	Service Pack	Nombre NetBios
1	Router	192.168.1.1		CISCO IOS 12.4		
2	PC	192.168.1.2	00:21:5e:30:4f:92	Microsoft Windows Server 2008	SP 2	ADDS-PRI
3	PC	192.168.1.3	00:21:5e:30:4e:9c	Microsoft Windows Server 2008	SP 2	ADDS-SEC
4	PC	192.168.1.4	00:0d:60:17:3b:a7			BACKUP
5	PC	192.168.1.7	00:21:5e:30:4c:62	Microsoft Windows Server 2008	SP 1	PRUEBAS
6	PC	192.168.1.8		Microsoft Windows Server 2008	SP 1	SBD-SIPAN-1
7	PC	192.168.1.9	00:21:5e:30:49:c8	Microsoft Windows Server 2008	SP 1	SBD-SIPAN-2

ID	Equipo	Dirección IP	Dirección Mac	Sistema Operativo	Service Pack	Nombre NetBios
1	Router	192.168.50.1		CISCO IOS 12.4		
2	PC	192.168.50.25	00:22:64:83:04:52	Microsoft Windows XP	SP 2 & SP 3	GERENTE-NEG
3	PC	192.168.50.101	00:1e:4f:a7:6e:03	Microsoft Windows XP	SP 2 & SP 3	ANA-PRI-1
4	PC	192.168.50.103	00:1e:4f:a7:6e:e2	Microsoft Windows XP	SP 2 & SP 3	ANA-PRI-3
5	PC	192.168.50.104	00:1e:4f:a7:62:96	Microsoft Windows XP	SP 2 & SP 3	ANA-PRI-12
6	PC	192.168.50.106	00:1e:4f:a7:6a:d9	Microsoft Windows XP	SP 2 & SP 3	ANA-PRI-6
7	PC	192.168.50.107	00:1e:4f:a7:5f:ab	Microsoft Windows XP	SP 2 & SP 3	ANA-PRI-7
8	PC	192.168.50.108	00:1e:4f:a7:60:ed	Microsoft Windows XP	SP 2 & SP 3	ANA-PRI-8

9	PC	192.168.50.109	00:1e:4f:a7:68:98	Microsoft Windows XP	SP 2 & SP 3	ANA-PRI-9
10	PC	192.168.50.110	00:1e:4f:a7:64:60	Microsoft Windows XP	SP 2 & SP 3	ANA-PRI-10
11	PC	192.168.50.111	00:1e:4f:a7:68:a2	Microsoft Windows XP	SP 2 & SP 3	ANA-PRI-11
12	PC	192.168.50.113	00:1e:4f:a7:62:e8	Microsoft Windows XP	SP 2 & SP 3	ANA-PRI-13
13	PC	192.168.50.116	00:19:b9:3e:e0:eb	Microsoft Windows XP	SP 2 & SP 3	JEF-OPE
14	PC	192.168.50.117	00:1e:4f:a6:6f:20	Microsoft Windows XP	SP 2 & SP 3	CAJ-GEN
15	PC	192.168.50.118	00:19:b9:3e:e1:30	Microsoft Windows XP	SP 2 & SP 3	AUX-OPE-1
16	PC	192.168.50.119				AUX-OPE-2
17	PC	192.168.50.120	00:1e:4f:a7:5f:f2	Microsoft Windows XP	SP 2 & SP 3	AUX-OPE-3
18	PC	192.168.50.122				AUX-PLA-2
19	PC	192.168.50.123				JEF-SER-CRE
20	PC	192.168.50.124				ASI-SER-CRE

ID	Equipo	Dirección IP	Dirección Mac	Sistema Operativo	Service Pack	Nombre NetBios
1	Router	192.168.60.1		CISCO IOS 12.4		
2	PC	192.168.60.28	00:25:b3:76:9b:14	Microsoft Windows XP	SP 2 & SP 3	GERENTE-ADM
3	PC	192.168.60.100	00:11:95:e3:58:23	Microsoft Windows XP	SP 2 & SP 3	AUX-ADM
4	PC	192.168.60.101	00:1e:4f:a7:4a:62	Microsoft Windows XP	SP 2 & SP 3	ASI-ADM
5	PC	192.168.60.106	00:1e:4f:a7:64:fa	Microsoft Windows XP	SP 2 & SP 3	AUX-CON
6	PC	192.168.60.108	00:11:95:fd:4d:30	Microsoft Windows XP	SP 2 & SP 3	AUX-CON-2
7	PC	192.168.60.119	00:11:95:f5:70:d9	Microsoft Windows XP		LEGAL
8	PC	192.168.60.131	00:1e:4f:a7:5e:91	Microsoft Windows XP	SP 2 & SP 3	ASI-CON
9	PC	192.168.60.171	00:1c:23:df:1c:b3	Microsoft Windows XP	SP 2 & SP 3	ASI-LEG
10	PC	192.168.60.180	00:1e:4f:a7:5f:af	Microsoft Windows XP	SP 2 & SP 3	JEF-AUD
11	PC	192.168.60.181	00:1e:4f:a7:b5:3f	Microsoft Windows XP	SP 2 & SP 3	AUD-JUN

12	PC	192.168.60.192	00:1e:4f:a6:76:dd	Microsoft Windows XP	SP 2 & SP 3	ASI-LOG

ID	Equipo	Dirección IP	Dirección Mac	Sistema Operativo	Service Pack	Nombre NetBios
1	Router	192.168.70.1	00:24:51:26:31:c3	CISCO IOS 12.4		
2	PC	192.168.70.2	00:26:6c:42:07:40	Windows 7 Professional		GER-GENERAL
3	PC	192.168.70.101	00:01:6c:91:e5:3a	Microsoft Windows XP	SP 2 & SP 3	JEFE-PYS
4	PC	192.168.70.103	00:1e:4f:a7:68:6b	Microsoft Windows XP	SP 2 & SP 3	ANALISTA-OYM
5	PC	192.168.70.145	00:19:b9:3e:e0:bd	Microsoft Windows XP	SP 2 & SP 3	ANA-RIE-CRE
6	PC	192.168.70.146	00:1e:4f:a7:6e:84	Microsoft Windows XP	SP 2 & SP 3	ANA-RIE-OPE
7	PC	192.168.70.163	00:22:64:83:73:a8	Microsoft Windows XP	SP 2 & SP 3	GERENTE-RIESGOS
8	PC	192.168.70.200	00:15:e9:a9:89:33	Microsoft Windows XP	SP 2 & SP 3	PRA-RIE
9	PC	192.168.70.202	00:1e:4f:a7:6e:8b	Microsoft Windows XP	SP 2 & SP 3	SEC-GER
10	PC	Desconectado para el uso del punto de red				

ANEXO Nº 02

LISTADO DE RIESGOS OPERATIVOS RELACIONADOS CON TECNOLOGÍA INFORMATICA

En el siguiente formato contiene el listado de los posibles riesgos relacionados con Tecnología de la Información que afectan directamente los procesos críticos de TI de la Caja y que deberías ser evaluados: probabilidad de ocurrencia, identificación de amenazas y vulnerabilidades relacionadas, tiempos máximos de recuperación, contramedidas.

SERVIDORES, CONCENTRADORES Y EQUIPOS DE COMUNICACIÓN CENTRALES

Activo o recurso tecnológico	Riesgo asociado
Servidores y concentradores centrales y de borde	Accesos no autorizados
	Corte de luz, Sistema ininterrumpido de energía (UPS) descargado o variaciones de voltaje
	Destrucción o fallo de un componente crítico del equipo (microprocesador, memoria, fuente de poder, otros)
	Errores de configuración
	Factores ambientales no adecuados. (ventilación, protección contra incendios, acondicionamiento racks, otros)
	Límite de vida útil – Máquinas obsoletas (antigüedad del equipo, repotenciamiento de componentes)
	Mal mantenimiento
	Robo
	Afectación por virus

II. BASE DE DATOS

Nombre del Activo	Factor de Riesgo
Base de Datos	Copia no autorizada de o a un medio de datos externos
	Errores de software (motor y contenedor de base de datos)
	Falta de espacio de almacenamiento
	Pérdida o falla de backups
	Pérdida de confidencialidad en datos privados y de sistema
	Directorios compartidos
	Accesos no autorizados
	Afectación de virus
	Sabotaje

III. SOFTWARE BACKOFFICE Y SISTEMAS OPERATIVOS

Nombre del Activo	Factor de Riesgo
Software de BackOffice y sistemas operativos instalados en servidores y terminales	Aplicaciones sin licencias
	Error de configuración
	Mala Administración de control de accesos
	Pérdida de datos
	Afectación de virus

IV. BACKUP (SISTEMA DE RESPALDO)

Nombre del Activo	Factor de Riesgo
Backup	Copia no autorizada del backup
	Errores de software para recuperación de información de backup (restore)
	Falla o deterioro del medio de almacenamiento externo del backup
	Falta de espacio de almacenamiento
	Mala integridad de los datos resguardados al recuperar la información de un backup
	Medios de datos no están disponibles cuando son necesarios
	Pérdida o robo de backups
	Sabotaje

V. CABLEADO Y CONCENTRADORES SECUNDARIOS

Nombre del Activo	Factor de Riesgo
Cableado y concentradores	Conexión de cables inadmisible (modificación de conexiones y mal etiquetado)
	Daño o destrucción, de cables o equipamiento, inadvertido (mala ubicación, por limpieza, impedimento de libre tránsito, otros)

	Factores ambientales
	Accesos no autorizados.
	Longitud de los cables de red excedidos a las normas

VI. RED

Nombre del Activo	Factor de Riesgo
Red	Mantenimiento no adecuado de puertos. (restricciones de acceso a ciertos puertos, perfiles de acceso)
	Configuración inadecuada de componentes de red
	Errores de operación (mala estandarización de velocidades de transmisión y ancho de banda, otros)
	Mal uso de servicios de red

VII. USUARIOS

Nombre del Activo	Factor de Riesgo
Usuarios	Acceso no autorizado a datos
	Borrado, modificación o revelación de claves de acceso a la información y aplicaciones, desautorizada o inadvertida
	Condiciones de trabajo adversas (ergonomía, ubicación de equipos, otros)
	Destrucción negligente de datos por parte de los usuarios

	Documentación deficiente (manual de usuario)
	Entrada sin autorización a ambientes
	Entrenamiento de usuarios inadecuado
	Falta de controles y log de las transacciones realizadas por los usuarios.
	No cumplimiento con las medidas de seguridad del sistema
	Desvinculación del personal con la institución

VIII. DOCUMENTACIÓN DEL SISTEMA

Nombre del Activo	Factor de Riesgo
Documentación de programas, hardware, procedimientos administrativos locales, manuales, etc.	Acceso no autorizado a datos de documentación
	Borrado, modificación o revelación desautorizada de información
	Copia no autorizada de un medio de documentación del sistema
	Descripción de archivos y programas inadecuado
	Documentación insuficiente o faltante, funciones no documentadas
	Factores ambientales (almacén de documentación)
	Mantenimiento y actualización inadecuado o ausente de la documentación

X. SIIF/SIG

Nombre del Activo	Factor de Riesgo
SIIF y SIG	Modificaciones inoportunas y no documentadas
	Funcionalidad del sistema (no atiende todos los requerimientos de los usuarios y áreas)
	Acceso a los programas fuentes no controlado
	Validación en los procesos de captura y registro de transacciones
	Sabotaje (eliminación de programas)

OBSERVACIÓN:

Adicionalmente se debe considerar los riesgos relacionados con desastres naturales e incendios.