UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE INGENIERIA MECANICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

“IMPLANTACIÓN DE UN PROCESO DE AUDITORÍA DE SEGURIDAD DE INFORMACIÓN BAJO LA NORMA ISO/IEC 27002 EN UNA ENTIDAD FINANCIERA DE PUNO – 2016”

TESIS

PRESENTADO POR:

MAX YONEL PUMA AROSQUIPA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

PUNO – PERÚ

2017

UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

IMPLANTACIÓN DE UN PROCESO DE AUDITORÍA DE SEGURIDAD DE INFORMACIÓN BAJO LA NORMA ISO/IEC 27002 EN UNA ENTIDAD FINANCIERA DE PUNO – 2016

TESIS PRESENTADA POR:

MAX YONEL PUMA AROSQUIPA

Fecha de sustentación: 14 - jul – 2017

PARA OPTAR EL TITULO PROFESIONAL DE INGENIERO DE SISTEMAS

APROBADA POR EL JURADO FIRMANTE CONFORMADO POR:

PRESIDENTE DEL JURADO :.....

M.Sc. EDGAR HOLGUIN HOLGUIN

PRIMER JURADO :.....

M.Sc. FREDY HERIC VILLASANTE SARAVIA

SEGUNDO JURADO :.....

M.Sc. ADOLFO CARLOS JIMÉNEZ CHURA

DIRECTOR / ASESOR :.....

Mg. ELMER COYLA IDME

PUNO – PERÚ
2017

Área : Seguridad Informática
Línea : Desarrollo, Gestión, Seguridad y Auditoría de Sistemas de Información
Tema : Auditoría de Seguridad de Información

DEDICATORIA

Hay un grupo de personas que sin quererlo y tal vez sin imaginarlo han contribuido a este trabajo que pone fin a una etapa de mí, no solo en las influencias académicas han sido importantes por eso quiero darle crédito a la gran cantidad de personas excelentes que me rodean como mis padres Martin y Gertrudes, mis hermanos Logand y Caterin quienes inculcaron los valores de esfuerzo, perseverancia por lograr mis objetivos. Gracias por acompañarme en momentos del presente trabajo.

AGRADECIMIENTO

Mi agradecimiento primeramente a quien ha forjado mi camino y el sendero correcto, a Dios por bendecirme para llegar hasta donde he llegado, porque hiciste realidad este sueño anhelado. A la Universidad Nacional del Altiplano por darme la oportunidad de estudiar y ser un profesional. A mi directora de tesis, Mg. Elmer Coyla Idme por su esfuerzo y dedicación. También me gustaría agradecer a mis profesores durante toda mi carrera profesional porque todos han aportado con un granito de arena a mi formación, De igual manera agradecer a mi jurado dictaminador de Tesis de Grado, M.Sc. Edgar Holguin Holguin, M.Sc. Fredy Heric Villasante Saravia y M.Sc. Adolfo Carlos Jimenez Chura por su visión crítica de muchos aspectos cotidianos de la vida y por su rectitud en su profesión como docente e investigador.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

En este estudio de la Caja Los Andes de la región de Puno, se examina la importancia de una auditoría de seguridad de información por medio de la implantación de un proceso de auditoría de seguridad de información, que cuenta con 26 actividades y en ellas se toman las buenas prácticas y controles de la norma ISO/IEC 27002. En donde se logró observar los principales beneficios con las que cuenta la Gerencia de Auditoría Interna de la Caja Los Andes como es; la disminución significativa del gasto que ocasión, al ya no contratar una consultara sino utilizar el proceso implementado que es ejecutado por el auditor interno, así mismo, se logra reducir con el proceso el tiempo de ejecución de la auditoria realizado en 156 horas, que normalmente en años pasados las consultoras lo hacían en 176 horas hábiles a más. El proceso permitirá al auditor interno tener la forma de cómo realizar la auditoría de seguridad de información, las herramientas necesarias, pautas técnicas, actividades fundamentadas en los objetivos de control de la norma ISO/IEC 27002, una estructura de custodia de papeles de trabajo, ficha de control de tiempos y un informe, además, la caja Los andes estará cumpliendo con lo dispuesto por la Superintendencia de Banca, Seguros y AFP de realizar auditorías continuas respecto a la seguridad de información.

PALABRAS CLAVE: Seguridad de Información; Proceso de Auditoría; Auditoría Interna; Entidades Financieras; Norma ISO/IEC 27002.

ABSTRACT

In this study of the Caja Los Andes in the Puno region, the importance of an information security audit is examined by means of the implementation of an information security audit process, which has 26 activities and is taken the good practices and controls of the ISO / IEC 27002 standard. It is possible to observe the main benefits that the Internal Audit Department of the Caja Los Andes will have as it is; The significant reduction of the expense that occasion, to no longer hire a consult but to use the process implemented that is executed by the internal auditor, likewise, it is possible to reduce with the process the execution time of the audit performed in 156 hours, which normally In past years the consultants did it in 176 hours more. The process will allow the internal auditor to have the form of how to perform the audit of information security, the necessary tools, technical guidelines, activities based on the control objectives of ISO / IEC 27002, a structure of custody of working papers, Time control tab and a report, in addition, the box The Andes will be complying with the provisions of the Superintendence of Banking, Insurance and AFP to carry out continuous audits regarding information security.

KEYWORDS: Information Security; Audit Process; Internal Audit; Financial Institutions; Standard ISO/IEC 27002.

CAPITULO I

1. INTRODUCCIÓN

Un proceso de auditoría de seguridad de información se hace necesaria en las entidades financieras de la región de Puno porque permite verificar una adecuada protección frente a las posibles intrusiones que son derivadas de las vulnerabilidades del sistema de gestión de la seguridad de la información (SGSI) y poder ver el estado actual de la seguridad de información dentro de la organización, asimismo, ver si se consideran la normativa vigente como es la Norma ISO/IEC 27002, la evaluación de riesgos e incidentes, ver si cumplen con sus políticas, controles de seguridad de información y la actualización constante, porque según los diagnósticos las políticas pueden quedar desfasadas con los cambios de la tecnología y versiones de algunas normas o estándares.

La entidad financiera de Puno administra una gran cantidad de información que debe ser accedida por diferentes personas en lugares distintos lo que genera riesgos. Afortunadamente, la entidad financiera es una entidad regulada por la Superintendencia de Banca, Seguros y AFP (SBS) la cual establece la norma "Circular G-140-2009 Gestión de la seguridad de la información", que indica que las empresas deberán establecer, mantener, documentar y verificar un sistema de gestión de seguridad de la información (SGSI).

Para la verificación del cumplimiento de la norma, cada año contratan a terceros para realizar la auditoría de seguridad de información, que en los últimos años fue ocasionando gastos. Para dar una solución a esta problemática se implantará el proceso de auditoría de seguridad de información que permitirá al auditor tener la forma de cómo realizar una auditoría de seguridad de información en la entidad financiera a la vez ya no será necesario contratar consultorías para dicha actividad.

1.1. Descripción del problema.

En todas las entidades financieras reguladas por la SBS (Superintendencia de Banca y Seguros) se exige el cumplimiento de la norma Circular G-140-2009 (Gestión de la seguridad de la información, 2009) con la finalidad de

establecer criterios mínimos de seguridad de información, la SBS ha considerado conveniente establecer las siguientes disposiciones, las cuales indica tomar como referencia al estándar internacional ISO/IEC 27002, disponiéndose su publicación en virtud de lo señalado en el Decreto Supremo N° 001-2009-JUS, en dicho circular hace referencia de que la entidad financiera debe realizar actividades de Auditoría Interna y dichos resultados serán de gran ayuda en las visitas de control programadas por la SBS a dicha entidad.

Es así que en todas las entidades reguladas por la SBS tienen un sistema de gestión de seguridad de información que son gestionadas por un oficial de seguridad de información o una jefatura encargada de realizar dicho trabajo. Muchas de las entidades financieras realizan gastos contratando consultoras para cumplir con lo dispuesto en la circular G-140 y la entidad financiera de Puno no es ajeno a este hecho ya que el incumplimiento a la norma puede generar multas.

Uno de los mayores desafíos de la empresa independientemente de su tamaño, es la implantación de un proceso de auditoría de seguridad información que garantice un control de nivel óptimo del sistema de gestión de seguridad de información y reducir los costos que se realiza en este tipo de actividades.

Tomando en cuenta los aspectos mencionados se plantea la siguiente interrogante:

¿De qué manera el proceso de auditoría de seguridad de información basada en la norma ISO/IEC 27002 reduce costos en la Auditoria de seguridad de información realizada por la Gerencia de Auditoria Interna, Caja Los Andes, Puno-2016?

1.2. Antecedentes de investigación.

Si revisamos años atrás la preocupación en entidades fue la de implantar un sistema de gestión de seguridad de información como la investigación de (Blanco, 2009) que trata de la implementación de un SGSI basada de la

norma técnica peruana NTP/ISO 17799 en la empresa de generación eléctrica San Gabán S.A. que ha reducido el número de incidentes de seguridad, además indica que el 50% fue por desconocimiento del personal interno sobre procesos, que recomienda que se deba sensibilizar al personal sobre seguridad de la información e implantar procesos.

También en ese entonces la auditoría venia tomando gran importancia como en la investigación de (Zurita, 2009) que trata de la implantación de Auditoría informática en instituciones públicas de la ciudad de Puno, que dicha implantación mejora significativamente la gestión de la información en las instituciones públicas y se recomienda realizar auditorías que mejor si ya se tienen procesos establecidos para realizarla, pero en la actualidad el problema viene embarcando en si una Auditoría de seguridad de información es efectiva y si es necesario realizar inversiones en seguridad, en gran parte para resolver sus vulnerabilidades y el prestigio de la empresa.

Por ello ahora la preocupación es la efectividad de los procesos con que cuentan las entidades, se menciona algunas investigaciones realizadas como el trabajo de (Benavides, Enriquez, & Solarte, 2015), Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001, recomendando que del proceso de auditoría de seguridad de la información, el proceso debe ser continuo y que debe ser realizado por los entes de control interno de cada organización, y periódico por empresas auditoras externas que permitan hacer la evaluación y seguimiento del sistema de control de seguridad informático para el diseño, implementación e implantación de un SGSI adecuado a sus necesidades. Con esto podemos recalcar que es necesario un proceso de auditoría de seguridad de información en la Caja Los Andes.

También hay investigaciones que se enfocan a la respuesta a incidentes de seguridad informática como el trabajo de (Muñoz & Rivas, 2015) que investiga el Estado Actual de la Gestión de Crisis de la Seguridad Informática. Estos equipos brindan ayuda necesaria para mantener en una organización la privacidad de los datos, integridad y disponibilidad que son propiedades fundamentales para reforzar la infraestructura de información y

calidad de control de incidentes. Que concluye, aun cuando existen diferentes maneras de proteger sus datos, el principal problema es la desinformación que tienen las organizaciones, por lo tanto, se identifica la necesidad de desarrollar métodos y procesos para tener un nivel alto de seguridad de información.

En las investigaciones anteriormente mencionados nos brindan gran información, pero respecto a temas de Auditoría tenemos trabajos de investigación de (Mejías, 2016) Metodología para Auditorías de Ciberseguridad, que se centra en la revisión de plataformas y redes de comunicación que albergan los sistemas de la organización, concluyendo que gracias a la metodología, el auditor puede identificar los procedimientos y puntos más importantes a la hora de realizar una auditoría basados en los estándares fijados por COBIT y los estándares de ISO 27001. En esta metodología da a conocer que es necesario conocer dichos procedimientos la cual implantaremos en la Caja Los Andes.

De estos estudios la idea principal es que sirva como uso interno dentro de la entidad y sean de control interno, y de esta manera adaptar el diseño del informe final a las normas y procedimientos de la organización para enfrentar al mundo de la ciberseguridad que está en constante evolución. Es por ello que la necesidad de darle la importancia a este tipo de auditorías más aun tener procesos ya que la seguridad absoluta no existe solo queda minimizar el riesgo.

Todos los trabajos mencionamos anteriormente nos direcciona de mejor forma la necesidad de implantación de un proceso de auditoría de seguridad de información en la entidad financiera de Puno.

1.3. Justificación del problema.

La entidad financiera tiene un SGSI, pero no cuenta con un proceso para realizar la auditoría de seguridad de información, para suplir dicha actividad se realizó la contratación de una Consultora, al que se le pagó un monto considerable. Por tanto, se propone implantar un proceso de auditoría de seguridad de información.

Asimismo, la entidad financiera realiza operaciones mediante el uso de aplicaciones Core Bancario (Intercambio en tiempo real centralizado), sistemas de información, dispositivos tecnológicos e internet, implicando que sus activos de información estén en el ciberespacio. Esta operativa implica que se encuentra expuesta a sufrir lo que denominamos ciberataques procedentes de las redes de comunicación externas o internas buscando las vulnerabilidades de los sistemas con ataques que evitan prestar el servicio en el ciberespacio y ataques dirigidos a alterar la información, robarla, cometer fraude e incidentes mal intencionados hacia la empresa. Con el proceso a implantar se verificará la existencia de dichas vulnerabilidades.

Debido a los continuos y recientes ataques que se producen en las grandes empresas y tomando en cuenta el fácil acceso a la tecnología, ya no es necesario salir de casa o de la oficina para cometer crímenes financieros lo que incrementa la vulnerabilidad empresarial, algunas empresas han tenido pérdidas multimillonarias y, por consiguiente, hay una tendencia importantes para invertir en los presupuestos de la entidad financiera en seguridad de información o ciberseguridad y ésta es cada vez más protagonista en los planes estratégicos de las empresas. El problema es mundial y muchos tocan este tema en la actualidad como la revista Centro de Estudios EY. (Gómez & Noreña, 2016). Indica "*Desarrollar un plan de respuesta a ataques cibernéticos que englobe y aúne todas las partes del negocio, para contar con una estructura de respuesta centralizada.*"

Ante lo comentado anteriormente, las empresas realizan cada vez auditorías más intensas sobre seguridad de información más aún la Entidad Financiera que deben cumplir con las normas dadas por la SBS, en caso de no cumplir dicha norma se sanciona con multa no menor de 0,5 ni mayor de cien (100) UITs. Por ello, será de utilidad para el auditor o a quien se disponga a realizar una auditoría de seguridad de información la implantación de un proceso que el objetivo será analizar y diagnosticar el estado del SGSI.

Una vez implantada se debe dar respuesta a preguntas como las siguientes ¿La implantación del proceso redujo costos? ¿La unidad auditada es resistente? ¿La política de privacidad de la unidad auditada es correcta? ¿Son

seguros los sitios web y las aplicaciones que se utilizan? ¿Se están gestionando eficientemente las amenazas?

1.4. Objetivo de la investigación.

1.4.1. Objetivo General.

Implantar el proceso de auditoría de seguridad de la información basada en la norma ISO/IEC 27002 para reducir costos de auditoría de seguridad de información realizada por la Gerencia de Auditoría Interna, Caja Los Andes, Puno-2016.

1.4.2. Objetivos Específicos.

a) Realizar el análisis situacional de los trabajos realizado por las consultoras sobre Auditoría de seguridad de información.
b) Diseñar, definir el esquema y las actividades del proceso de auditoría de seguridad de información.
c) Evaluar la disminución del costo de ejecución de la Auditoría de seguridad de información luego de implementar el proceso propuesto.

CAPITULO II

2. REVISIÓN DE LITERATURA

2.1. Marco Teórico.

2.1.1. Funcionamiento de la norma ISO 27002.

La norma ISO/IEC 27002 que es el "Estándar Internacional de Sistemas de Gestión de Seguridad de la Información", publicado desde hace más de doce años, cuyo fundamento es la Norma Británica BS7799 que data de 1995. Ahí se establece Política de seguridad, Aspectos organizativos para la seguridad, Clasificación y control de activos, Seguridad ligada al personal, Seguridad física y del entorno, Gestión de comunicaciones y operaciones, Control de accesos, Desarrollo y mantenimiento de sistemas, Gestión de incidentes de seguridad de la información, Gestión de continuidad de negocio, Conformidad y "Conjunto de recomendaciones sobre qué medidas tomar en la empresa para asegurar los Sistemas de Información.", el cual nos provee de una serie de dominios por medio de los cuales se logra la integración de las actividades y los objetivos que se deben considerar para lograr una correcta y exitosa implementación y mejora continua de los procesos. A diferencia de:

La ISO/IEC 27001 fundamenta en el modelo propuesto por W. Edwards Deming con el ciclo que lleva el mismo nombre, también conocido como PDCA (Plan-Do-Check-Act), ayuda a la organización no solo a obtener una certificación en materia de seguridad de la información para los procesos de negocio que conforman la organización, sino que debido a su fundamento en el ciclo Deming, vea Figura 1 para el entendimiento del ciclo (Pérez, 2013), que propicia que sea un proceso iterativo, de fácil y eficiente monitoreo con respecto de donde estamos y a dónde queremos llegar en un tiempo específico, así es posible adoptar un enfoque proactivo y flexible del cumplimiento regulatorio de corto al largo plazo.

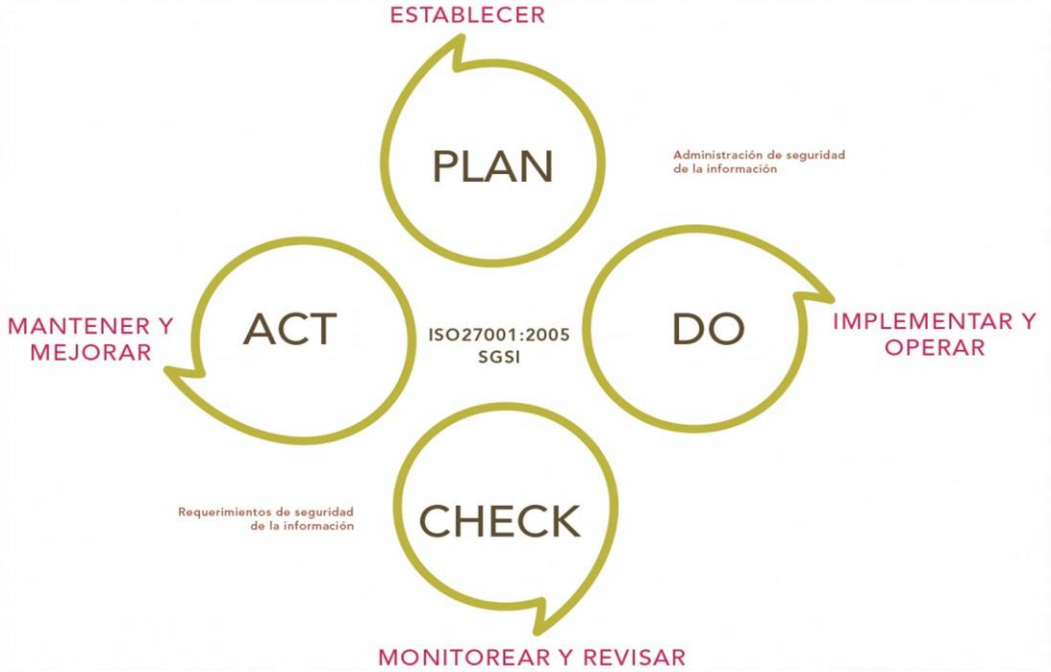

Figura 1: Ciclo Deming

Fuente: Obtenida de (Pérez, 2013)

2.1.1.1. Información.

La información es un conocimiento explícito extraído por la humanidad o sistemas expertos es y será susceptible de riesgo, es decir, siempre existirán mayores factores de amenaza y vulnerabilidades que atenten contra su integridad, confidencialidad y/o disponibilidad, ya que representan el activo más importante de cualquier organización. Sin embargo, para tomar medidas al respecto es necesario no considerarla como un activo aislado, sino inherente, que está relacionada con un componente de tecnologías de información, ya que son aquellas las que nos procuran y facilitan su uso, manejo y administración.

2.1.1.2. Confidencialidad de datos.

Es cuando un usuario o empleado de la empresa garantice seguridad al momento de ingresar a la información, no divulgando dicha información a personas ajenas a la empresa; con ello se busca

conseguir una seguridad donde los que puedan acceder a los datos son los administradores del sistema o la misma gerencia.

2.1.1.3. Disponibilidad de datos.

La disponibilidad de datos es el acceder a la información de la empresa al tiempo o la hora que sea con el fin que los usuarios alteren, actualicen, respalden los datos útiles y no tener pérdidas financieras o de personal.

2.1.1.4. Integridad de datos.

La integridad de datos hace referencia a que los datos no pueden ser alterados por ningún tipo de personal, solo por la alta dirección, para ello deben de tener un tipo de seguridad que ayude al manejo debido de los datos para beneficio propio de la empresa.

2.1.2. Sistema de gestión de la seguridad de la información.

(Benavides et al., 2015) Es una práctica que está incorporándose con mayor frecuencia a las organizaciones que sí consideran la seguridad de la información como un área estratégica, este sistema podrá ayudar a las organizaciones a minimizar los impactos adversos y manejar los riesgos, este modelo tiene varios objetivos como alineación estratégica, reducción de riesgos a un nivel aceptable, uso efectivo y eficiente de recursos, mediciones para asegurar el logro de los objetivos y servicios que presta la organización con apoyo de TI.

2.1.3. Responsabilidad del oficial de seguridad de información

(Sanchez, 2015) El oficial de seguridad de información, es la persona responsable de cumplir y hacer cumplir el Plan de Seguridad de Información. Tiene la función de brindar los servicios de seguridad de información en la organización, a través de la planeación y coordinación de los procesos de seguridad informática, así como difundir la cultura de seguridad informática entre todos los miembros de la Empresa. Algunas funciones específicas:

- No divulgar ni transferir a terceros, y bajo ningún motivo la información procesada, información técnica, estrategias de marketing, base de datos procesados o sin procesar, sobre relación de clientes y/o proveedores, etc., de propiedad de la entidad financiera que sean conocidas como consecuencia directa e indirecta de sus funciones.
- El Oficial de Seguridad de Información tiene como principal función la responsabilidad de la verificación y control periódico del plan de seguridad de información.
- Asesorar en el buen funcionamiento del proceso de seguridad de información y ser capaz de guiar y aconsejar a los usuarios de la entidad sobre cómo desarrollar procedimientos para la protección de los recursos asociados a la seguridad de información.
- Guiar a la administración de la organización ante incidentes de seguridad de información mediante un plan de respuesta a incidentes, con el fin de atender rápidamente este tipo de eventualidades.
- Responsable de proponer y coordinar la realización de un análisis de riesgos en seguridad de la información.
- Desarrollar procedimientos de seguridad que fortalezcan políticas de seguridad de información.

2.1.4. Auditoría interna.

La Auditoría Interna es un órgano autónomo y objeto de aseguramiento, control y consulta, concebida para agregar valor y mejorar las operaciones de la entidad financiera, apoyando a cumplir con los objetivos, aportando un enfoque sistemático y disciplinado en la evaluación y mejora de la eficacia de la gestión de riesgos y del gobierno corporativo.

2.1.5. Auditor de tecnologías de información.

El auditor de tecnologías de información realiza las labores de Auditoría relacionadas a las tecnologías, seguridad y sistemas de

información, así como verificar la implementación de las medidas correctivas, cautelando que su trabajo aporte valor a la empresa. Algunas funciones:

- Evaluar el nivel de ejecución de las medidas de continuidad del negocio, seguridad (de la información, de las personas, físico, ambiental), plan de contingencias, plan estratégico y operativo del área de sistemas.
- Evaluar si es adecuada la administración de las operaciones y comunicaciones que realiza el área de sistemas.
- Evaluar el desarrollo y mantenimiento de los sistemas informáticos.
- Evaluar la performance del software informático con el que opera la entidad, determinando los riesgos existentes y hallazgos de ser el caso.

2.1.6. Activos de Información

(Mejías, 2016) Son los bienes de una organización, que se encuentran relacionadas de manera directa o indirecta con la actividad informática, entre los cuales se encuentran:

- Información mecanizada, es decir, no tienen documentos fuentes que los generen.
- Medios de comunicación que se utilizan para la transmisión de datos, tales como: redes, correo electrónico, etc.
- Medios magnéticos y ópticos de almacenamiento de información como: discos, USB, DVD, CD, etc.
- Programas y aplicaciones de la empresa, ya sea desarrollados por la misma, o adquiridos por terceros.
- Manuales, procedimientos y reglamentaciones afines al área informática.

2.1.7. Vulnerabilidad.

Las vulnerabilidades son errores que permiten realizar acciones desde afuera, sin permiso del administrador del equipo, incluso se puede suplantar a un usuario en común Actualmente existen muchas amenazas que tratan de acceder remotamente a ordenadores, ya sea para hacerlos servidores ilegales o robar información privada.

2.1.8. Seguridad de la información.

(ISO/IEC 27002, 2013) La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades.

2.1.8.1. Seguridad física.

Mediante la seguridad física se evita el acceso no autorizado, daños o intromisiones en las instalaciones y a la información de la organización; ya que los servicios de procesamiento de información deben ubicarse en áreas seguras y protegidas en un perímetro de seguridad definido por barreras y controles de entrada adecuados.

2.1.8.2. Seguridad física del edificio.

Aquí se intenta minimizar el riesgo que personas ingresen a algunos recursos informáticos específicos, con el objetivo de asegurar los activos. Así mismo, se trata de que el centro de procesamiento de datos esté ubicado en un lugar seguro, sin vulnerabilidades de accesos a los mismos.

Deberían existir políticas de seguridad bien planteadas, diseñadas y desarrolladas que cubran la gran mayoría de aspectos respecto a la seguridad física, así mismo deberían existir planes de

seguridad que ayuden a tomar decisiones seguras para cuando exista un acceso físico no autorizado a algún recurso informático de la empresa.

2.1.8.3. Control de accesos.

Todos los sitios en donde se encuentren sistemas de procesamiento de datos informáticos o de almacenamiento, deben estar protegidos de accesos no autorizados, utilizando tecnologías de autenticación, monitoreo, registro de entradas y salidas, guardias de seguridad, detectores metálicos, etc.

2.1.8.4. Seguridad en el acceso a la información.

En la seguridad en el acceso a la información es muy importante que toda los datos de la empresa sean sumamente protegidos por tipos de riesgos que constantemente se interceptan en la Organización, poniendo en peligro la información precisa que sea divulgada causando graves problemas en todo tipo de trabajo, por eso se ve factible colocar o implementar herramientas o estándares como una forma de protección para dichos problemas, esas herramientas estarán jugando el papel protector de la empresa y así no ser divulgado por personas que no pertenecen a la organización.

2.1.8.5. Seguridad en las estaciones de trabajo.

En este tipo de seguridad no se deben de confundir que una estación de trabajo es una PC por ende toda la información que se produce en la empresa es importante, para ello se restringen varios tipos de entretenimientos, páginas web que no intervienen en el uso general de la empresa, para un buen funcionamiento en su trabajo viéndose de tal manera se verificara algunos restricciones importantes que se realiza en este tipo de seguridad para no tener problemas en posteriores informaciones acerca del trabajo que se emplean en la organización.

- Las computadoras de trabajo no deben tener instalado ningún otro software como juegos o cualquier otro software de entretenimiento que no sea el licenciado y requerido para que el usuario desarrolle su trabajo.
- Todos los equipos deben contar con software antivirus instalado y activo, así como la última actualización del mismo y la definición de virus.
- Queda estrictamente prohibido emplear cualquiera configuración manual como dirección IP, DNS17, puerta de enlace o default Gateway, rutas estáticas, etc.; en las estaciones de trabajo de los usuarios, deben ser configuradas para obtener una dirección IP automáticamente.
- Siempre se deben de escanear los discos flexibles y cualquier archivo o medio electrónico de transmisión antes del acceso a la información contenida en ellos.
- Respaldar periódicamente los datos de aplicaciones y configuraciones, y almacenarlos en un lugar seguro.
- Solo el personal autorizado del área de informática puede efectuar cambios en la configuración siempre y cuando se justifique.
- Queda estrictamente prohibido que los usuarios remuevan o agreguen componentes tanto de software como de hardware a los equipos.
- Queda estrictamente prohibido que los usuarios cambien el equipo del lugar al que han sido asignados.
- Los equipos deben configurarse para que empleen el protocolo TCP/IP y debe removerse cualquier otro protocolo innecesario."

2.1.9. Integridad de la información.

La integridad de la información se basa en que ninguna persona no autorizada puede hacer uso de cambios o modificaciones en el sistema ya sea con fin propio para beneficiar o perjudicar a la organización, es

por eso que se tiene una herramienta para este tipo de problemas haciendo que cada personal de la empresa posea una firma digital en donde el que ingresa sea procesado y sea la persona que al ingresar la única culpable en el desarrollo del sistema hablando de la parte informática específicamente.

2.1.10. Copias de seguridad.

Se le denomina copias de seguridad a todo tipo de respaldo que se realiza con el fin de desempeñar una breve recuperación de los datos y restaurar el original después de que se prevenga las pérdidas totales de la información importante en cualquier organización o archivos importantes para su bien común.

Según (Mejías, 2016) Son llamadas también backup, son respaldos de información con el fin de que puedan utilizare para restaurar información modificada accidentalmente o después de una pérdida de datos, según datos estadísticos el 66% de usuarios de internet han sufrido una pérdida grave de la información.

Fundamentalmente son útiles para 2 cosas:

- Recuperación de información ante una catástrofe informática
- Recuperación una pequeña cantidad de información que se pudieron haber eliminado accidentalmente o corrompido.

Cuando una computadora esta en uso, se ejecuta la copia de seguridad, incluyendo la posibilidad de que haya ficheros abiertos o trabajando sobre ellos. Si un fichero está abierto, el contenido posiblemente no se refleje en lo que el usuario ve.

2.1.11. Soporte de almacenamiento.

Se establece que el dueño de un archivo informático no pueda modificar los permisos que está bajo un control de accesos obligatorio, para lo cual, a cada usuario, dato, etc. se le asigna una etiqueta o un nivel de seguridad jerárquico y una categoría Cada usuario puede tener

acceso a un solo tipo de información. También se verifica que la información esté debidamente etiquetada con un nombre informativo.

Se verifica que la información se guarde en formatos establecidos por políticas y como debe estar encriptado dicha información, dependiendo de la importancia de cada uno de ellas. Cada cambio que se realice debe estar registrado en un historial de cambios tales como fecha, hora, cambios realizados y por quien; para que así poder registrar malos entendidos en algún cambio realizado.

2.1.12. Gestión de seguridad de la red

(ISO/IEC 27002, 2013) Asegurar la protección de la información en redes y la protección de la infraestructura de soporte. La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de data, implicancias legales, monitoreo y protección. También se pueden requerir controles adicionales para proteger la información confidencial que pasa a través de redes públicas.

2.1.13. Restauración de datos.

Se verifica si se es posible recuperar información perdida en un sistema de información, y si se gestiona estas pérdidas y cuál fue el motivo por el que dicha información se eliminó. Mediante el respaldo de información se asegura de haber guardado la información de manera correcta sin modificaciones.

2.1.14. Repositorio de datos.

(Carvajal, 2015) Es el conjunto de datos que se compone de registros de incidentes de seguridad informática, documentos y archivos digitales de la organización y activos de información con las que el personal hace uso constante.

2.1.15. Servidor.

Un servidor es una computadora que da servicio a otros ordenadores llamados clientes. También se suele denominar a un servidor como una aplicación informática que realiza ciertas tareas en beneficio de otras aplicaciones cliente. Ofrece servicio de acceso a archivos o información, permite almacenar y acceder a archivos de una computadora y servicios de aplicaciones que los realiza el usuario final.

2.1.16. Piratas informáticos.

Su actividad consiste en la apropiación de copia ilegal de programas rompiendo sus sistemas de protección y licencias. Después realizan la distribución con fines lucrativos u otros la promueven como la libertad en la distribución.

Hackers.

Hacker es un vocablo utilizado por los informáticos para referirse a un experto en varias o alguna rama técnica relacionada con la informática tales como: programación, redes de computadora, sistemas operativos, etc.

Algunos de ellos, sin embargo, son verdaderos piratas informáticos, o debo decir expertos informáticos que se sienten cómodos profundizando en el área gris de la ley y más allá (Willson, 2016).

Cracker.

Es una persona con grandes conocimientos informáticos y con un propósito de luchar en contra de lo que está prohibido, empieza a investigar la forma de bloquear o traspasar protecciones hasta lograr su objetivo. Los crackers usan programas propios o bajados del internet gratuitamente, con esos programas se intenta desbloquear claves de acceso con generadores automáticos de claves. Se distinguen varios tipos de crackers:

Lammer: Es una persona con poco conocimiento informático, que consiguen herramientas ya creadas para atacar ordenadores. Ejecutan aplicaciones sin saber que están causando grandes daños.

Trasher: Son personas que buscan en la basura y en papeleras números de tarjetas de crédito, claves de acceso, cuentas bancarias, etc.; para cometer estafas y actividades fraudulentas a través de internet.

Insiders: Crackers corporativos, empleados de las empresas que las atacan desde dentro, movidos usualmente con motivos de venganza.

2.1.17. Virus informático.

Los virus informáticos son programas de software que se ejecutan y se propagan localmente, realizando copias de sí mismo en otro programa o documento, infectando otros ordenadores.

La principal característica es el consumo de recursos que ocasionan problemas tales como la pérdida de productividad, que la PC no este 100% funcionando, pérdida de información, etc. Otra característica es tienen la posibilidad de replicarse por todo el ordenador ya sea localmente o por medio de redes que no tienen seguridades adecuadas.

Malware.

Se explicará todo el tipo de malware (troyanos, backdoors, rootkits, adware, virus, worms, botnet, ransomware, spyware, crypter.) incluyendo un apartado propio de la criptografía llamado estenografía. Se creará un malware a medida y se infectará un sistema entre otras cosas (Jimenez, 2016).

Métodos de protección y tipos.

Existen métodos para disminuir o reducir el riesgo de infección o reproducción de los virus como:

Antivirus: Son programas que tratan de descubrir huellas dejadas por software malicioso para así detectarlo, eliminarlo o contenerlo en

cuarentena para evitar su reproducción Intenta tener controlado el sistema de intrusos como medida de seguridad.

Tipos de vacunas: Pueden existir varios tipos de vacunas, entre ellos:

- Solo detección: Solo actualizan archivos infectados, pero no pueden eliminarlos o desinfectarlos.
- Detección y desinfección: Detectan archivos infectados y pueden desinfectarlos.
- Detección y aborto de la acción: Detectan archivos infectados y detiene las acciones del mismo.
- Comparación de firmas: Comparan las firmas de los archivos infectados para conocer si estos están infectados.
- Comparación de firmas de archivo: Compara las firmas de los atributos guardados en la computadora.
- Métodos heurísticos: Se usa métodos heurísticos para comparar archivos, puede como no ser la mejor alternativa.
- Invocado por el usuario: Se activan por petición del usuario.

2.1.18. Procesos organizacionales.

Este proceso es un conjunto de pasos parcialmente ordenados donde una empresa desarrolla y ejecuta organizadamente sus actividades y operaciones con recursos humanos, tecnológicos, estructuras organizacionales y limitaciones. Obligando al cumplimiento de actividades y secuencias dadas dentro de la organización que son propuestas y mejoradas para aspirar a un posicionamiento en el mercado a nivel internacional.

2.1.19. Gestión de continuidad de negocio.

Está focalizada en garantizar a la organización la continuidad del negocio frente a contingencias, gracias al desarrollo de mecanismos y planes de continuidad para restaurar los procesos, y de esa manera asegurar el servicio al cliente y a la vez la reputación de la empresa.

2.2. Marco Conceptual.

- **Apetito de riesgo:** El nivel de riesgo que la empresa está dispuesta a asumir en su búsqueda de rentabilidad y valor.
- **Base de datos:** Un conjunto de datos almacenados sistemáticamente.
- **Core Bancario**: Sistema financiero que realiza el intercambio en tiempo real centralizado.
- **Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO):** Enfoque para la mejora del control interno de organizaciones que consta de 5 componentes relacionadas entre sí.
- **Comité de Auditoría Interna:** Grupo conformado por el directorio, gerencia general y Auditoría para tratar debilidades y controles de la organización.
- **Consultoría:** Es un servicio profesional prestado por empresas o individual conocidos como Consultores.
- **Control Interno:** Diseñado para proveer un aseguramiento razonable en el logro de objetivos referidos a la eficacia y eficiencia de las operaciones, confiabilidad de la información financiera, y cumplimiento de las leyes aplicables y regulaciones.
- **Directorio:** Grupo formado por los inversionistas o dueños.
- **Gerencia:** Conjunto de personas encargadas de dirigir y gestionar un Área de una organización.
- **Organización Internacional de Normalización (ISO):** Es una organización para la creación de estándares internacionales compuesta por diversas organizaciones nacionales de estandarización.
- **Observación:** Acción observada de la Auditoría que explica o para establecer de qué manera se realizan ciertas operaciones, procedimientos y/o procesos.
- **Papeles de trabajo:** Documentos que son evidencia o sustento de la auditoría realizada.
- **Programa de Auditoría:** Documento preparado por el auditor donde se señala las tareas específicas que deben ser cumplidas por el equipo de auditoría para llevar a cabo el examen o evaluación.

- **Plan de pruebas:** Actividades planteadas a realizar por cada control o proceso a probar, pueden ser revisar, recalcular, verificar, testear, confrontar, etc.
- **Plan de acción:** Medidas determinadas o respuestas planteadas a las observaciones encontradas en la Auditoría.
- **Riesgo:** Es la probabilidad de que las vulnerabilidad y debilidades se convierta en un desastre acción que conlleva a perdida.
- **Recomendaciones:** Acción realizada por el auditor, que permitan promover mejoras en la conducción de las actividades u operaciones del área o áreas examinadas según las observaciones.
- **Seguimiento:** Supervisión del progreso de los planes de acción de las observaciones presentadas en los informes emitidos, así como a las observaciones identificadas por los auditores externos, y SBS.
- **Superintendencia de Banca y Seguros (SBS):** Organismo encargado de la regulación y supervisión del Sistema Financiero de Seguros y del Sistema Privado de Pensiones en el Perú.

2.3. Hipótesis de la investigación.

Al implantar el proceso de auditoría de seguridad de información bajo la norma ISO/IEC 27002, se logrará reducir el costo de la Auditoría de Seguridad de Información realizado por la Gerencia de Auditoría Interna, Caja Los Andes, Puno-2016.

2.4. Limitaciones.

- En la presente investigación se limita a implantar un proceso según la Circular G-140 Gestión de la seguridad de la información, SBS-2009.
- La investigación analiza el beneficio de tener un proceso establecido, pero acepta modificaciones para el mejoramiento de dicho proceso y no discute otras prácticas no establecidas en la norma ISO/IEC 27002.
- El proceso se limita a una auditoría de seguridad de información y no discute otras Auditorías como desarrollo de proyectos, Gobierno de TI, etc.

CAPITULO III

3. MATERIALES Y METODOS.

3.1. Diseño y tipo de investigación

La investigación tiene un enfoque o metodología **cuantitativa** para dicha existencia requerimos elementos del problema de investigación exista una relación en este caso el nivel es simple es decir:

$$Y = f(X) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(Ec. 01)}$$

El tipo de **investigación es descriptiva** ya que el propósito es describir el proceso y eventos que serán sometidos a análisis y se mide cada una de ellas independientemente y describir lo que se investiga.

3.2. Sistema de variables.

Para un mejor entendimiento de las variables lo presentaremos en la tabla 1 identificando la variable independiente, dependiente, dimensiones, indicadores, técnicas e instrumentos.

Variables	Dimensiones	Indicadores	Técnicas	Instrumentos
Independiente: Proceso de auditoría de seguridad de información basada en la norma ISO/IEC 27002	Estructura del proceso en base a la norma ISO/IEC 27002.	Coherencia del esquema del proceso con la realidad.	Observación	Guía de observación del proceso.
	Control y operatividad del proceso	N° de procesos afectados por la implantación.	Observación	Ficha estructurada.
Dependiente: Auditoría de seguridad de información	Concientización y capacitación de auditorías internas de SI.	N° de observaciones por errores humanos N° de empleados capacitados en seguridad.	Entrevistas Entrevistas	Guía de entrevistas al personal involucrado. Guía de entrevistas al personal involucrado.
	Aplicabilidad de resultados en la organización	Nivel de cumplimiento de normas y estándares de Auditoría interna. Nivel de cumplimiento de estándares de seguridad de información.	Análisis Análisis	Evaluación de verificación del proceso. Evaluación de cumplimiento de ISO 27002.

Tabla 1: Operatividad de Variables.

Elaboración: Propia

3.3. Población y muestra.

3.3.1. Población.

Para determinar la muestra, se toma como universo los procesos de auditoría de seguridad de información realizada durante los últimos años en la Caja Los Andes, Puno-2016. La Gerencia de Auditoría Interna es la encargada de ejecutar dicha Auditoría denominada "Evaluación de la Administración de la Seguridad de Información e Infraestructura". Fundamentada en la Normal Internacional NIA-530, muestreo de auditoría. En la tabla 2 se muestra la población con los costos de las dos últimas auditorías como referencia de lo que se quiere reducir.

N°	Año	Sociedades	Precio	Días	N° Observaciones	Calidad Informe
01	2015	Barrientos Rodríguez & Asociados	S/. 8,600.00	30	06	Aceptable
02	2014	Alfonzo Muñoz & Asociados	S/. 7,956.00	30	09	Bueno

Tabla 2: Costo de Auditorías Pasadas.

Fuente: Obtenida de las cotizaciones de Caja los Andes.

3.3.2. Muestra.

Para ello se toma la muestra indiscriminado lo cual el auditor selecciona la muestra sin emplear una técnica estructurada, sin embargo, el análisis de la muestra no debe extrapolarse para forma una opinión de otros procesos. Fundamentada en el A12 de la (NIA-350, 2013). Seleccionamos como muestra uno de los factores que interviene en el costo de la auditoría de seguridad de información como se puede observar en la tabla 3, el tiempo en horas que tomó ejecutar las actividades del proceso.

Proceso	Actividades	Tiempo (H)
I01	Reunión de inicio	1
I02	Requerimiento de información	16
P01	Organigrama del área	3
P02	Las responsabilidades asignadas.	3
P03	Relaciones Jerárquicas.	3
P04	Modelos de gestión y mecanismos.	2
P05	Nivel académico, Experiencia	3
P06	Proveedores de Servicio	4
P07	Plan de seguridad del Oficial.	5
P08	Operación de la seguridad.	5
P09	Categorización de incidentes.	3
P10	Seguridad física y del entorno	16
P11	Seguridad de equipos.	5
P12	Clasificación, control de activos.	3
P13	Control de seguridad del Host - series	4
P14	Control de seguridad, Bases de Datos	6
P15	Control de seguridad, Redes Comunicaciones	10
P16	Control de seguridad, Plataforma de Usuarios	6
P17	Control de seguridad en el Directorio Activo	6
P18	Canales de información y reportes	8
P19	Uso de información, sistemas de información	9
P20	Identificación de evaluación, cambios.	8
P21	Monitoreo del rendimiento del Oficial	10
F01	Redacción del informe	12
F02	Exposición de observaciones	1
F03	Armado de papeles de trabajo	4

Tabla 3: Tiempo de Ejecución por Actividad

Elaboración: Propia.

3.4. Ubicación y descripción de la población.

Realizado en Jr. Santiago Giraldo N° 262 de la ciudad de Puno 2016, Caja Los Andes. El proceso implantado es realizado por la Gerencia de Auditoría Interna de dicha entidad responsable de ejecutar la evaluación y presentación de resultados al Comité de Auditoría.

3.5. Métodos de recolección de datos.

Para la demostración de la hipótesis se emplearon las técnicas de recolección de datos como análisis documental, encuestas y entrevistas:

- **Análisis Documental:** De las auditorias pasadas se analizó e identifico la información de los papeles de trabajo de las auditorías realizadas en años pasados encontrando un registro completo de todos los documentos y herramientas utilizadas por los consultores.
- **Entrevistas:** Se hizo entrevistas con la finalidad de recabar información sobre la situación del proceso de la auditoría de seguridad de información, con el fin de obtener diferentes percepciones, de si es comprensibles y beneficioso para la Gerencia de Auditoría Interna.
- **Observación:** Realizada para observar o mirar con mucha atención y detenimiento para adquirir conocimiento sobre sus características del proceso de auditoría de seguridad de información.

3.6. Métodos de procesamiento y análisis de datos

3.6.1. Tratamiento y procesamiento de datos.

Para el tratamiento de datos se utiliza operaciones y procedimientos técnicos, que permitan las siguientes tareas:

- Recopilación y tabulación de la información recabada.
- Interpretación de los datos
- Validación de la hipótesis

Para el procesamiento de datos y la prueba de hipótesis se utilizará el Software Estadístico R.

3.6.2. Análisis de datos.

Para dicho análisis sobre los beneficios del proceso se usarán técnicas estadísticas para evaluar y aprobar la amigabilidad del proceso de auditoría de seguridad de información a partir de la información recolectada y de su aprobación por el usuario que interactúa con el proceso, así mismo, evaluar aspectos que ayudarán a ver claramente los beneficios:

- Observar si el proceso genero reducción de costo de la Auditoría de seguridad de información.
- Evaluar el porcentaje de número de observaciones.
- Evaluar el porcentaje de reducción de tiempo de ejecución.
- Evaluar la calidad del informe de auditoría.
- Evaluar el porcentaje de reducción del uso del material físico.

3.6.3. Pruebas de hipótesis.

Para determinar la existencia de las evidencias en la muestra, platearemos dos hipótesis para lo cual se realizará mediante un procedimiento de cinco pasos. Para saber si la hora promedio del trabajo realizado en el nuevo proceso implementado que cuenta con 26 actividades es menor de 6.78 horas = μ(media poblacional); sabiendo que una auditoria se realiza en 30 días hábiles (176 horas), y tenemos 26 actividades.

$$\mu = \frac{\sum X}{N} = \frac{176}{26} = 6.78 \ldots\ldots\ldots\ldots\ldots\ldots \text{(Ec. 02)}$$

Paso 1: Como las consultoras realizan la auditoría en 30 días hábiles (un mes), con el nuevo proceso se realiza en menos de los 30 días hábiles del mes, entonces deseamos una H_1. Siendo:

H_0 = La implantación de un proceso de auditoría de seguridad de información **incrementa o mantiene el costo** de ejecución luego de implementar el proceso donde se aplica las recomendaciones y buenas prácticas indicadas en la norma ISO/IEC 27002 en la entidad financiera de Puno.

$$H_0 \geq 6.78 \ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(Ec. 03)}$$

H_1 = La implantación de un proceso de auditoría de seguridad de información **reduce el costo** de ejecución luego de implementar el proceso donde se aplica las recomendaciones y buenas prácticas indicadas en la norma ISO/IEC 27002 en una entidad financiera de Puno.

$H_1 < 6.78$…… (Ec. 04)

Paso 2: El nivel de significancia para la prueba es de: $\alpha = 0.05$

Paso 3: Se calcula el valor estadístico de la prueba a partir de los datos de la muestra para este caso usaremos el estadístico t.

$$t = \frac{\bar{X} - \mu}{\sqrt{\frac{S}{n}}} \text{…… (Ec. 05)}$$

Para obtener la desviación estándar S la ecuación siguiente:

$$S = \sqrt{\frac{\sum(X - \bar{X})^2}{(n-1)}} \text{…… (Ec. 06)}$$

Los cálculos son procesados por el software estadístico R y dichos resultados son presentados en la tabla 4, y en la figura 2 se muestra la región crítica de color rojo y el valor estadístico de prueba t.

N°	Tiempo (H)	$X - \bar{X}$	$(X - \bar{X})^2$
1	1	-5	25
2	16	10	100
3	3	-3	9
4	3	-3	9
5	3	-3	9
6	2	-4	16
7	3	-3	9
8	4	-2	4
9	5	-1	1
10	5	-1	1
11	3	-3	9
12	16	10	100
13	5	-1	1
14	3	-3	9
15	4	-2	4
16	6	0	0
17	10	4	16
18	6	0	0
19	6	0	0
20	8	2	4
21	9	3	9
22	8	2	4
23	10	4	16
24	12	6	36
25	1	-5	25
26	4	-2	4
∑	156		420

Valores Calculados	
$\bar{X}$	6.00
S	4.09
t	-0.96
GL	25.00

GL: Grados de Libertad
S: Desviación Estándar
t: Valor, tabla T-Student

Tabla 4: Cuadro de Cálculo Usando la Tabla t-student.

Elaboración: Propia.

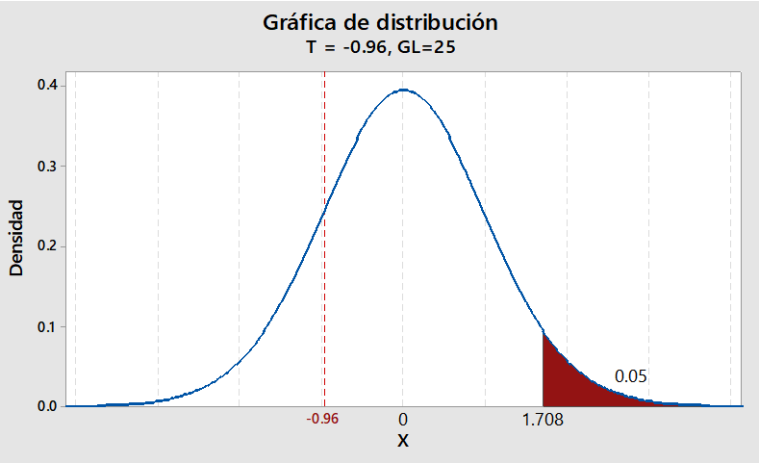

Figura 2: Grafica de la Región Crítica y Valor de Prueba.

Fuente: Generada por el Software Estadístico R.

Paso 4: Teniendo en cuenta el área de rechazo para la hipótesis nula (H_0) lado izquierdo de 1.708. El valor crítico para 0.05 da un valor de t = -0.96. Por tanto, la regla de decisión: es rechazar la hipótesis nula y aceptar la hipótesis alternativa. Vea figura 2.

Paso 5: Como dio t = -0.96 entonces, el estadístico cae en la parte izquierda del valor critico de 1.708, se rechaza H_0. Por tanto, se confirma el supuesto de hipótesis alternativa H_1.

Interpretación

El costo respecto al tiempo de ejecución de la Auditoría disminuye después de implementar el proceso de auditoría de seguridad de información, Además existe otras diferencias significativas como en el precio y la calidad del informe como se puede observar en la tabla 5.

Año	Ejecutor	Precio	%	Horas	%	N° Observaciones	Calidad Informe
2015	Consultora	S/. 8,600.00	100%	176	100%	6	Aceptable
2016	Gerencia de Auditoría Interna	S/. 2,500.00	29%	156	89%	6	Bueno
Diferencia		S/. 6,100.00	71%	20	11%	0	

Tabla 5: Cuadro Resumen de Interpretación.

Elaboración: Propia.

CAPITULO IV

4. RESULTADOS Y DISCUSIÓN

4.1. Implantación del Proceso de Auditoría de Seguridad de Información

El proceso propuesto se realizó a falta de auditores de TI y de procesos que cubran las auditorias de seguridad de información y continuidad del negocio, asimismo, se pudo observar que la Gerencia de Auditoría interna no realiza las evaluaciones referentes a tecnologías de información y seguridad estos lo realizan las consultoras que contratan.

Entonces se propuso el procedimiento de Auditoría de seguridad de información que fue expuesto en el comité de auditoría sobre los beneficios y la importancia de implantar el proceso, una vez aprobada se inició con la elaboración de la estructura de las fases: Planificación del Programa, Ejecución de Actividades y Presentación de Resultados, en cada una de las fases existe sub procesos:

Planificación del programa: Entendimiento de la actividad a realizar, de los controles que tienen los procedimientos, riesgos, funciones del personal, software que usan, políticas, directrices, etc.

Ejecución de actividades: Aplicar las pruebas de control que se implementaron en la matriz de evaluación que tiene un enfoque COSO distribuyendo las actividades en sus 5 componentes según correspondan y todas estas actividades y plan de pruebas están basada en norma ISO/IEC 27002. Y termina con realizar el seguimiento de las observaciones que hayan tenido en anteriores auditorias. En esta fase el auditor puede aplicar las herramientas necesarias para cumplir con las pruebas como entrevistas, testeo, recalculo, etc.

Presentación de Resultados: Elaboración del informe final con los planes de acción presentada por el auditado, luego se realiza el armado de los papeles de trabajo y exposición de las observaciones encontradas.

Como parte de la documentación se presenta el manual para entendimiento del presente proceso mediante el diagrama de flujo que se tiene que seguir por parte de los personajes que son participes del proceso.

Dicho proceso fue explicado y expuesto en la gerencia de auditoría interna para la aprobación por el gerente y luego ser propuesto en el comité de auditoría que dieron el visto bueno para ejecutar e implantar el proceso que hacía mucha falta.

Cumpliendo con el objetivo de Implantar el proceso de auditoría de seguridad de la información basada en la norma ISO/IEC 27002 que redujo los costos de la auditoría de seguridad de información realizada por la Gerencia de Auditoría Interna, Caja Los Andes, Puno-2016.

4.2. Análisis Situacional sobre Auditoría de Seguridad de Información

4.2.1. Gerencia de Auditoria Interna

La gerencia de Auditoría interna cada año realizan un plan anual donde se describe todas las actividades a desarrollarse entre ellas se tiene la denominada Evaluación de la administración de la seguridad de información e infraestructura. Esta actividad tiene que desarrollarse mínimamente dos veces al año.

Para el cumplimiento de las actividades programadas sobre seguridad de información la gerencia de Auditoría interna propuso se realice mediante trabajo tercerizado, esto debido a que a la fecha el personal no se encontraba plenamente capacitado para realizar la evaluación. En el último año realizaron un gasto de S/. 7,956.00 en la evaluación, para una mejor interpretación en la tabla 6 se muestra los costos y la lista de consultores que se dedican a este rubro, los cuales fueron obtenidas de las cotizaciones realizadas por la Gerencia de Auditoria Interna del cual se presenta un resumen para una mejor presentación.

N°	Consultoría	Costos Aprox.	Personal	Experiencia en Auditorías
01	Gamero Juárez & Asociados S.C.	S/. 7,200.00	Analista de sistema. Br. Ing. Sistemas José Pardo	1. Caja Rural Inkasur. (2011 - 2012) 2. Cooperativa Prestasur. (2010-2013) 3. Cooperativa Selva Alegre. (2011-2012)
02	Barrientos Rodríguez & Asociados SOC. civil	S/. 9,900.00	Auditor de Sistemas. Ing. Alejandro Camarena Ames	1. CRAC Cajamarca S.A.A. (2013) 2. EDPYME S.A.C. (2007-2013) 3. Cooperativa Coronel Bolognesi (2012-2013)
03	Ramírez y Enríquez & Asociados	S/. 8,460.00	Ingeniero de Sistemas. Alfredo Ramos Muñoz	1. CRAC Señor de Luren. 2. Banco Agropecuario. 3. Caja Municipal de Ahorro y Crédito de Sullana
04	Alfonzo Muñoz & Asociados	S/. 7,956.00	Auditor Senior. Ing. Mónica Córdova Puré	1. Caja Rural de Ahorro y Crédito de Luren (2015) 2. Caja Rural de Ahorro y Crédito Centro (2014) 3. CRAC - LASA (2014)
05	Portal Vega & Asociados	S/. 16,200.00	Sistemas. Ing. Héctor Henríquez Hernández	1.- EDPYME Solidaridad y Desarrollo Empresarial S.A.C. (2009 - 2013)
06	Panez Chacaliaza & Asociados S.C.R. Ltda.	S/. 20,600.00	Socio de TI. Ing. Econ. José Córdova Sunico	1.- Banco Falabella. 2.- Banco Azteca. 3.- Mi banco 4.- Prisma - Microempresa.

Tabla 6: Cotización de Precios a Consultoras.

Fuente: Cotización realizada por la Caja Los Andes.

Se observó que cuando la consultora termina su trabajo presenta sus papeles de trabajo, el informe final impreso y digital que es expuesta a los involucrados en la evaluación, posteriormente, a la gerencia de Auditoría interna que toma posesión del informe, en ella están las observaciones y oportunidades de mejora que son expuesta en el comité de auditoría interna y luego registradas en la base de datos de observaciones de la entidad financiera.

Asimismo, en el informe SBS. (2014). 08-VI-2014-DSM “B. en las visitas de inspección por la SBS, que recibe la entidad financiera fue observada la Gerencia de Auditoría Interna de las cuales se toma las que aportan a la investigación como es:

- Deficiencias en los informes y papeles de trabajo. “Cuatro (04) informes en cuyos papeles de trabajo no se evidencian: (i) el programa de trabajo utilizado; (ii) los hallazgos, debilidades, observaciones y/o recomendaciones determinados en el trabajo de campo; ni (iii) las comunicaciones remitidas a las unidades orgánicas evaluadas informando el resultado de los exámenes, con el fin de que formulen sus descargos.”
- Debilidades en el Programa de Aseguramiento y Mejora de la Calidad. “La incorrecta orientación de la evaluación interna de la labor efectuada por la GAI; así como, la no evidencia de que la evaluación externa de dicha labor sea realizada en lo que resta del año 2015, impide tener una idea clara de la calidad y eficacia de la función de la auditoría interna en la Caja, y si la misma agrega valor a los procesos de la empresa y, en consecuencia, contribuye al cumplimiento de los objetivos institucionales.”

Indica que no se cuenta con un procedimiento establecido para realizar la evaluación de seguridad de información ya que la consultora contratada realiza el 95 % del trabajo. Además, se tiene muchas situaciones que mejorar en la gestión y calidad de la gerencia de Auditoría interna.

Organigrama de la Gerencia de Auditoria Interna que muestra la jerarquía y jefes inmediatos del auditor de TI ver Figura 03.

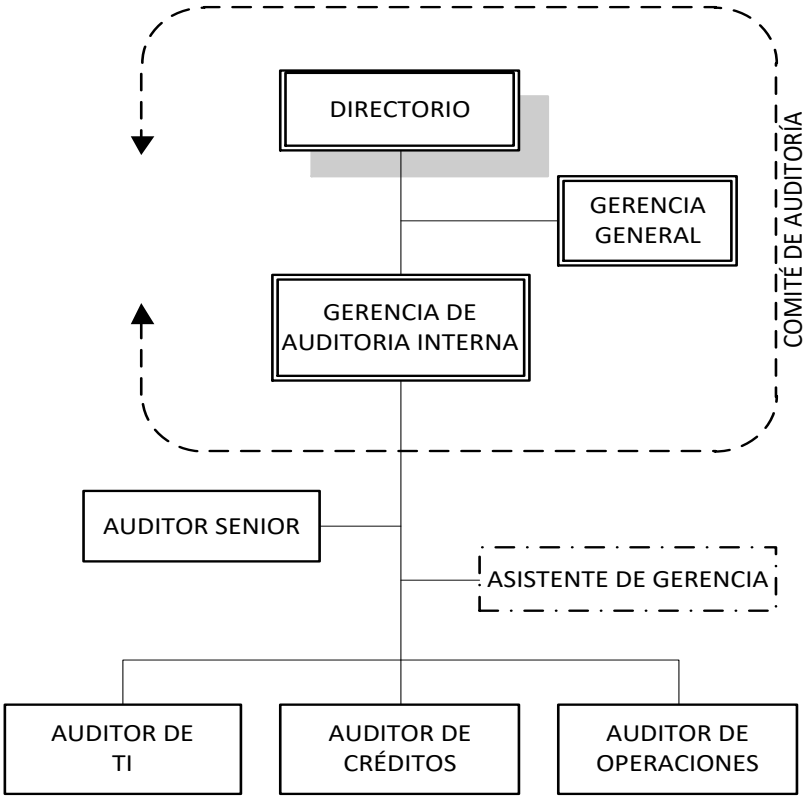

Figura 3: Organigrama de Auditoría.

Fuente: Obtenida del Organigrama de Caja Los Andes.

4.2.2. Valorización Dada a las Observaciones.

Luego de revisar el manual de la Gerencia de Auditoría Interna se ve que en base al apetito de riesgo aceptado por la Alta Dirección al nivel de los riesgos y a los resultados de las pruebas realizadas sobre la efectividad de los controles, las observaciones se clasifican conforme a la metodología expuesta. Sin embargo, la Gerencia de Auditoria Interna considera también aspectos cualitativos fundamentales al momento de la evaluación, primando en el juicio profesional y la experiencia del equipo de auditoria en su conjunto. Las observaciones pueden catalogarse cualitativamente de la siguiente forma:

Riesgo Nivel Extremo:

- Estos tienen el potencial de generar graves pérdidas financieras y por tanto poner en riesgo significativo la fortaleza financiera de la organización.
- Representan graves casos de incumplimiento de leyes y regulaciones.
- Tiene el potencial de poner en grave riesgo la reputación de la Entidad.
- Tiene el potencial de poner en grave riesgo la autorización de funcionamiento de la caja u originar una intervención.
- Tienen el potencial de poner a la entidad en régimen de vigilancia.

Riesgo Nivel Alto:

- Tiene el potencial de general significativas pérdidas financieras, y poner en riesgo alto la seguridad y fortaleza de la organización.
- Representan significativos casos de incumplimiento de leyes y regulaciones.
- Tienen el potencial de poner en significativo riesgo la reputación de la entidad.
- Tiene el potencial riesgo de suspensión de Directores o Empleados de la entidad por parte de los entes reguladores.
- Tienen el potencial de generar importante pérdidas financieras.
- Representan incumplimientos de normas internas de la entidad.
- Tienen el potencial de poner en moderado riesgo la reputación de la entidad.
- Tienen el potencial de generar multas por parte de la SBS u otras autoridades.
- Representan incumplimientos de cláusulas contractuales que deriven en demandas y daños a la entidad.

Riesgo Nivel Medio:

- Tienen el potencial de generar moderadas pérdidas financieras.
- No aseguran un cumplimiento integral de normativas internas
- Tienen el potencial de poner en bajo riesgo la reputación de la Caja.
- Tienen el potencial de exponer a la organización a amonestaciones de los entes reguladores.
- Representan incumplimiento de cláusulas contractuales que podrían derivar a pérdidas menores a la entidad.

Riesgo Nivel Bajo:

- Tienen el potencial de generar pérdidas menores para la Caja.
- Son considerados necesarios para impedir que en el mediano plazo la actuación a administración de las operaciones de la organización pierda su eficiencia.

4.2.3. Calificativo como Resultado del Informe.

Los resultados de los exámenes realizados por la Gerencia de Auditoria estarán comprendidos dentro de los siguientes niveles:

Satisfactorio: Cuando los controles existentes son satisfactorios y sugieren mejoras prácticas en la gestión de riesgo. No son observadas necesidades de mejora significativa. Las operaciones / procesos son ejecutadas sobre una base sólida en todos sus aspectos. Requiere monitoreo y supervisión normal por parte de la Gerencia General.

Aceptable: Los controles existentes son adecuados y atienden de manera general sus objetivos. En los controles o en las prácticas adoptadas fueron observadas debilidades que no comprometen el ambiente de control del proceso. Las operaciones / procesos son ejecutados sobre una base normal en todos sus aspectos; sin embargo,

existen debilidades modestas que pueden ser corregidas por la Gerencia en el curso normal de las operaciones.

Regular: En los controles o en las prácticas adoptadas, fueron observadas debilidades que, aisladamente o en conjunto exponen el proceso a riesgos que exigen atención y urgente aplicación de acciones correctivas. Las operaciones / procesos se encuentran con debilidades en cuanto a administración del riesgo, controles operacionales y cumplimiento. Requiere atención inmediata por parte de la Gerencia General.

Deficiente: Altísima exposición a riesgo. Cuando los controles son insuficientes, ineficaces o inexistentes y determinan fragilidades significativas a las principales rutinas o actividades del proceso. Exigen inmediata intervención estructural en el ambiente de control. Requieren urgente atención por parte de la Gerencia General.

4.2.4. Plan Anual de Trabajo basado en riesgos.

La Gerencia de Auditoria Interna desarrolla el Plan Anual de Auditoría basada en riesgos, focalizándose en la revisión de los aspectos más riesgosos de sus procesos en base a los objetivos y alcances definidos por el Directorio, la evaluación de riesgos existentes, los procesos establecidos en la cadena de Valor, los sistemas de Información, requerimientos regulatorios y expectativas de la alta Gerencia (Directorio, Comité de auditoría, Gerencia General), priorizando así los riesgos y orientando los recursos hacia las áreas de mayor exposición de Riesgo de la entidad.

4.2.5. Estructura del Sistema de Gestión de Seguridad de Información.

En la entidad financiera implementaron su SGSI, en la Figura 4 (Sanchez, 2015), veremos la estructura de dicho sistema que fue adaptada de acuerdo a las necesidades de la entidad.

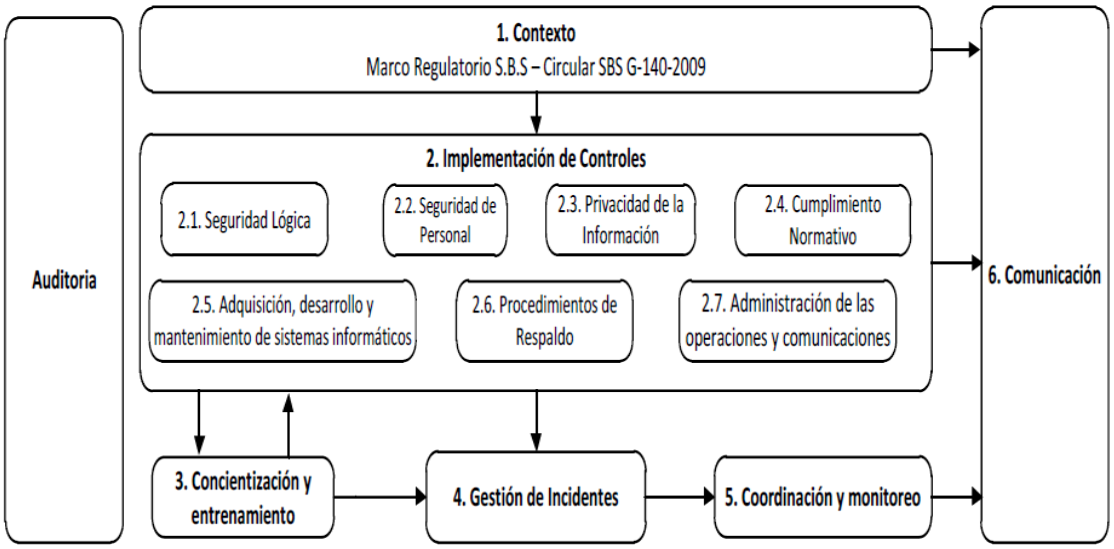

Figura 4: Estructura del SGSI de la Entidad.

Fuente: Documento de la Caja Los Andes (Sanchez, 2015)

Y en la Figura 5 descrita por (Sanchez, 2015) se ve la estructura organizacional donde se contempla a todas las Gerencias de Línea como patrocinadores de la implementación y monitoreo del SGSI. Y a los Jefes como Coordinadores de Seguridad de la Información.

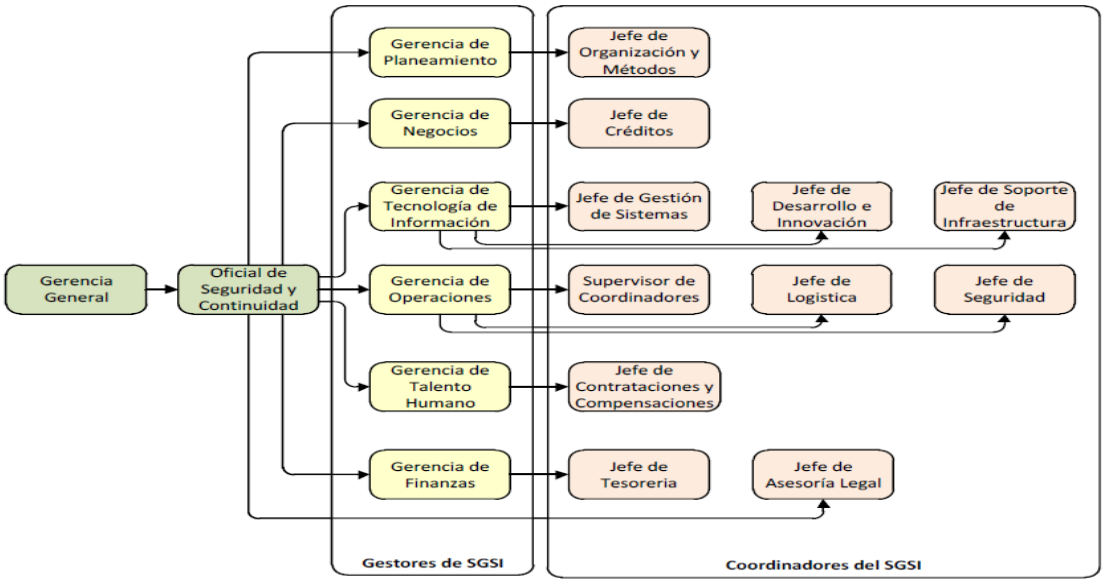

Figura 5: Estructura Organizacional del SGSI

Fuente: Documento de la Caja Los Andes (Sanchez, 2015)

4.3. Diseño y esquema del proceso de auditoría implantado.

Se desarrolló el proceso de Auditoría que comprende de tres (03) fases definidas que describen el proceso implementado que son supervisados en cada una de las fases parte el Gerente o Auditor sénior. Vea Figura 6.

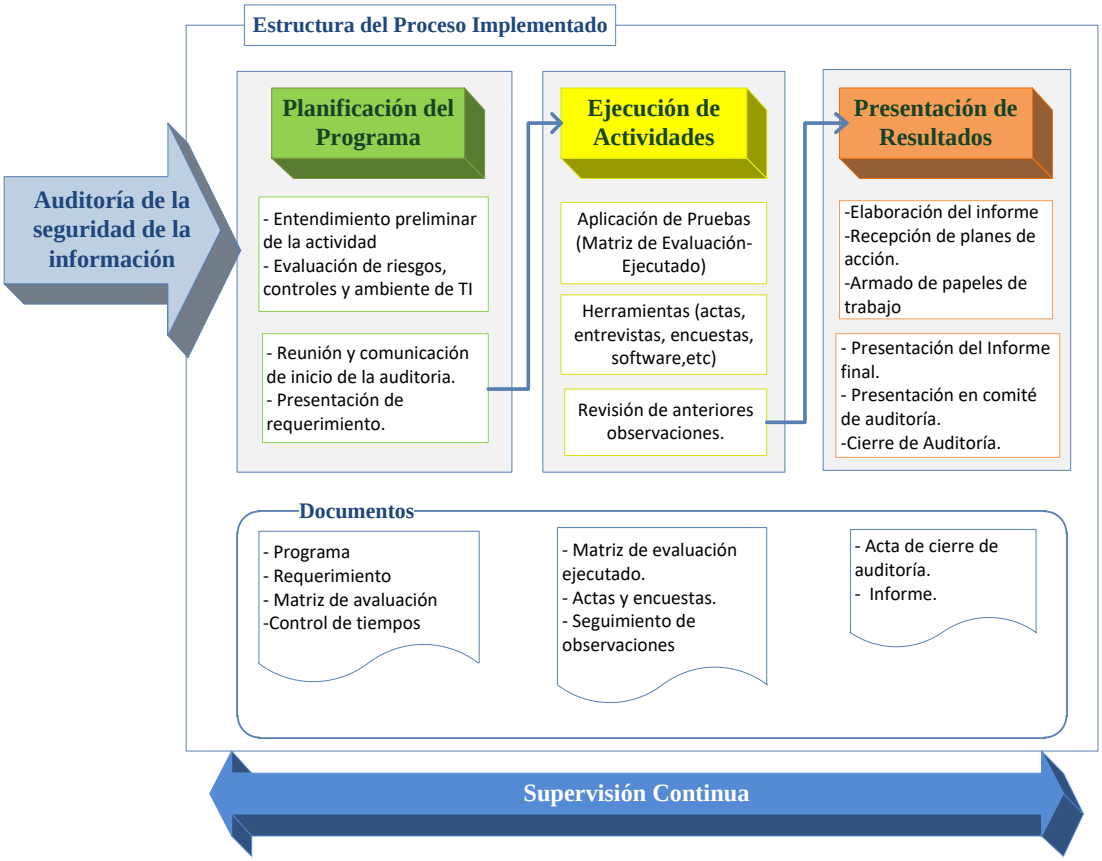

Figura 6: Fases del Proceso Implementado.

Elaboración: Propia

4.3.1. Planificación del Programa.

Como en toda actividad de Auditoría se inicia elaborando el programa, en ella se determina las prioridades de la evaluación como; objetivo, alcance y recursos, para la elaboración se considera las recomendaciones y observaciones en anteriores informes, También se debe considerar los incidentes, identificación, evaluación de riesgos y controles respecto al tema. A veces el objetivo de la auditoria también puede ser dispuesto por el Directorio, teniendo en cuenta los objetivos

estratégicos de la entidad financiera. Cabe indicar que los objetivos no siempre se mantendrán en las próximas evaluaciones estos cambian según las consideraciones antes mencionadas.

Identificación de Riesgos: Para identificar riesgos de las actividades a auditar se requiere el entendimiento del proceso/subproceso (inputs, outputs, sistemas, personas, etc.) en ellas identificar los riesgos que podrían causar que los objetivos del proceso/subproceso no se alcancen. Para ello, se plantean, entre otras, las siguientes preguntas:

- ¿Qué es lo que puede impedir la consecución de los objetivos del proceso/subproceso?
- ¿Qué es lo que puede salir mal en el proceso/subproceso?
- ¿Qué impacto podrían tener algunos eventos externos en el proceso/subproceso?
- ¿Existen demoras en el proceso/subproceso para alcanzar sus objetivos en la forma más eficaz y económica posible?

Evaluación de Riesgos: Cada uno de los riesgos identificados, deberá ser evaluado según los criterios de calificación establecidos por la entidad financiera, considerando su estado natural, a lo cual se le denomina riesgo bruto o inherente**.**

Identificación y Evaluación de Controles: El control es toda medida tomada para mitigar o gestionar el riesgo, y que incrementa la probabilidad que el proceso logre sus metas y objetivos. Son incorporados en los procesos para garantizar que se cumplan los requerimientos del flujo de trabajo y los objetivos generales de la entidad y de los procesos.

Programa: En la tabla 7 se ve el respectivo programa de Auditoría para la evaluación de seguridad de información, en el Anexo 1 presentamos programa completo de la auditoría realizada.

Objetivo del Programa	**Evaluación de la administración de la seguridad de información e infraestructura.** • Efectuar la evaluación de seguridad de información basada en la norma emitida por la SBS, la Circular G 140-2009 "Gestión de la Seguridad de Información", identificando las brechas y generar recomendaciones. • Verifique, evalúe y evidencie los controles implementados y operativos aplicados. • Verifique las actividades desarrolladas para la implementación del Sistema de Gestión de Seguridad de Información (SGSI). • Verifique, evalúe y evidencie los mecanismos de seguridad establecidos en la subcontratación de los servicios externos de Tecnología de Información. • Verifique las responsabilidades asignadas al oficial de seguridad de información y comité de riesgos • Evaluar la identificación de eventos de pérdida y gestión de riesgos operacionales asociados a la seguridad de la Información. • Verifique que los contratos suscritos con terceros asociados a tecnologías de información contemplen las cláusulas necesarias asociadas a la seguridad de información.
Alcance del Programa	**Cumplimiento:** Verificar la adherencia de la entidad financiera a las normas, políticas, reglamentarias y de autorregulación que le son aplicables. **Estratégico:** Evaluar y monitorear del desempeño del sistema de gestión de seguridad de información. **Gestión y Resultados:** Verificar las actividades relativas a la gestión del SGSI, con el fin de determinar el grado de eficiencia y eficacia en el manejo de los recursos, incidentes, riesgos y controles.
Recursos	**Tecnológicos:** Equipos de cómputo, sistemas de información, sistemas de redes, correo electrónico de la empresa, entre otros.

Tabla 7: Programa de Auditoría

Elaboración: Propia

Matriz de avaluación: Los procesos descritos en la matriz esta en basa al enfoque COSO que concuerda con las normas de Auditoría Internacionales y las normas de auditoría vigentes en Perú y que es usada por la gerencia de Auditoría interna a continuación destallamos sus componentes:

- **Ambiente de control**. Evaluar el comportamiento y estructura en la organización, las directivas de la organización que ejerzan

supervisión, capacitación y mantenga personal con un alto conocimiento y experiencia.

- **Evaluación de riesgos**. Evaluar sus actividades, procesos y mecanismos para identificar y evaluar riesgos de la organización, incluyendo los riesgos particulares asociados con el cambio.
- **Actividades de control**. Revisar las acciones, normas y procedimientos que tiende a asegurar que se cumplan las directrices y políticas del directorio y alta gerencia para afrontar los riesgos identificados.
- **Información y comunicación**. Ver sistemas que permiten que el personal de la entidad capte e intercambie la información requerida para desarrollar, gestionar y controlar sus operaciones.
- **Supervisión**. Evaluar la calidad del control interno en el tiempo. Es importante para determinar si éste está operando en la forma esperada y si es necesario hacer modificaciones o actualizaciones.

Tomando en cuenta el enfoque, la matriz tiene 21 procesos de prueba descritas según consideraciones de la norma ISO 27002, además se considera las buenas practicas mencionadas en la norma, listada las acciones a realizar por el auditor, esto lo podemos observar con mayor detalle en el Anexo 2.

Requerimiento de Información: Se enlista toda la información necesaria para poder realizar la evaluación normalmente se solicita antes de iniciar la Auditoría, pero existen requerimientos adicionales que surgen durante la ejecución a consecuencia del análisis exhaustivo en puntos de posibles observaciones en el Anexo 4 se puede ver el control de los documentos solicitados.

Control de Tiempos: En muchas de las organizaciones buscan el mejor rendimiento de sus empleados en este caso se tiene un cuadro del control de tiempo en ella se registra el tiempo estimado por el auditor y el tiempo real que llevo realizar cada proceso. Esto con el fin de poder sacar un nuevo tiempo para la siguiente actividad y ver cuán eficiente

fue el auditor en su labor. Para mejor detalle en el Anexo 3 donde se muestra con los tiempos ya ejecutados.

4.3.2. Ejecución de Actividades

La fase de ejecución comienza con la aplicación del plan de pruebas establecido en el la matriz de evaluación obteniendo evidencias y formulando de ser el caso los hallazgos o desviaciones de control con sus respectivas recomendaciones, cuidando los tiempos y recursos planteados para el mismo, cumpliendo con su ejecución de acuerdo con las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna.

Matriz de Evaluación Ejecutado: Cuando ya se tenga la información necesaria el auditor inicia con la actividad que mejor le parezca, siempre en cuando lleven el control de las actividades realizadas, para ello las acciones realizadas se van registrando en la matriz de evaluación adicionando columnas, en la tabla 8 mostramos dichos campos y en el anexo 5 la matriz completa con las acciones realizadas. Definimos los campos como:

- **Descripción de pruebas**, registrar si se realizó una entrevista, Check List, cuestionarios.
- **Descripción de riesgo**, después de realizado las pruebas se redacta los hallazgos e identificando el posible riesgo.
- **Código de riesgo**, se obtiene de la base de datos de **matriz de riesgos** según al riesgo identificado en caso no figure el riesgo se considera como nuevo.
- **Nivel de riesgo**, esta se encuentra en la matriz de riesgo según el código de riesgo encontrado.
- **Observación**, se define la observación encontrada vinculada al riesgo identificada ya sea si existe o no en la matriz de riesgos.
- **Referencia**, Se redacta el documento que hace hincapié a la observación como evidencia del hallazgo.

Evaluación del Auditor						
Código de Proceso	Descripción de pruebas	Descripción de Riesgo	Código de riesgo	Nivel de Riesgo	Observación	Referencia
P01						
P02						

Tabla 8: Evaluación del Auditor.

Elaboración: Propia

Herramientas: En la presente evaluación se han empleado los procedimientos y técnicas de Auditoría siguientes:

- Elaboración de Actas de entrevistas (vea Anexo 8) cuyo cuestionario ha estado basado en objetivos de norma ISO 27002, normativa SBS, alineándolos a los objetivos de la presente evaluación, los mismos que se aplicaron a los siguientes:
  - Gerente de Riesgos
  - Oficial de Seguridad de Información y Continuidad del Negocio
  - Analista de Riesgo Operacional.
  - Administrador de Base de Datos
  - Jefe de Unidad de Soporte, Infraestructura y Comunicaciones
  - Jefe de Unidad de Gestión de Sistemas y Aplicaciones
  - Jefe de Unidad de Desarrollo e Innovación
  - Jefe de Unidad de Organización y Métodos
- Elaboración de la encuesta (vea Anexo 9) a aplicar a los usuarios de las siguientes agencias:
  - Oficina de Puno
  - Oficina de Pedro Vilcapaza
  - Oficina de Ayaviri
  - Oficina de Juliaca
  - Oficina de Ilave
  - Oficina de Azangaro

- Oficina de Ayacucho
- Visita de inspección al Centro de Datos, Puno.
- Visitas de verificación a la Oficina Especial Puno, Santiago Giraldo.
- Recopilación, revisión y lectura de la información requerida en forma física y electrónica.

Seguimiento de observaciones: Todas las observaciones y recomendaciones realizadas por la gerencia de auditoría interna son almacenados en una base de datos. El seguimiento es obtener de la base de datos observaciones referidas al tema de avaluación y ver el avance, los sustentos y los planes de acción tomadas para luego darle un estado de: Implementado, en proceso o pendiente. Las observaciones lo extraemos en una tabla como se muestra en la tabla 9, para un mayor detalle con los campos completos vea Anexo 6.

Seguimiento de Observaciones								
Informe	Tipo Obs.	N° OBS.	Observación	Gerencia Responsable	Plan de acción	Estado	Fecha	Comentarios del Auditor
INFORME Nº 08-VI-2014-DSMB								

Tabla 9: Seguimiento de Observaciones.

Elaboración: Propia

4.3.3. Presentación de resultados

El informe es el documento mediante el cual la Gerencia de Auditoria Interna expone el resultado final de su trabajo a través de juicios fundamentados en las evidencias obtenidas durante la fase de ejecución, con la finalidad de brindar suficiente información a los funcionarios del área auditada, presentando sobre las deficiencias o desviaciones más significativas, e incluir las recomendaciones que permitan promover mejoras en la conducción de las actividades u operaciones del área o áreas examinadas.

Elaboración del informe: El documento se redacta después de la evaluación realizada dando a conocer el hallazgo de las observaciones con sus respectivas recomendaciones. Luego es presentado y enviado a la alta gerencia, al comité de auditoría y al directorio. Dicho informe se muestra en el Anexo 7.

Papeles de trabajo: En la Auditoría es vital tener los sustentos como pueden ser físicos o digitales como informes, procedimiento, manuales, directivas, normas, políticas, reportes, audios, videos, etc. También están los materiales y herramientas usadas por el auditor que dan solvencia a las observaciones y son parte de la evidencia.

Para custodiar los papeles de trabajo se creó un repositorio y una estructura para guardar los documentos como se muestra en las siguientes figuras 7, 8, 9 y 10.

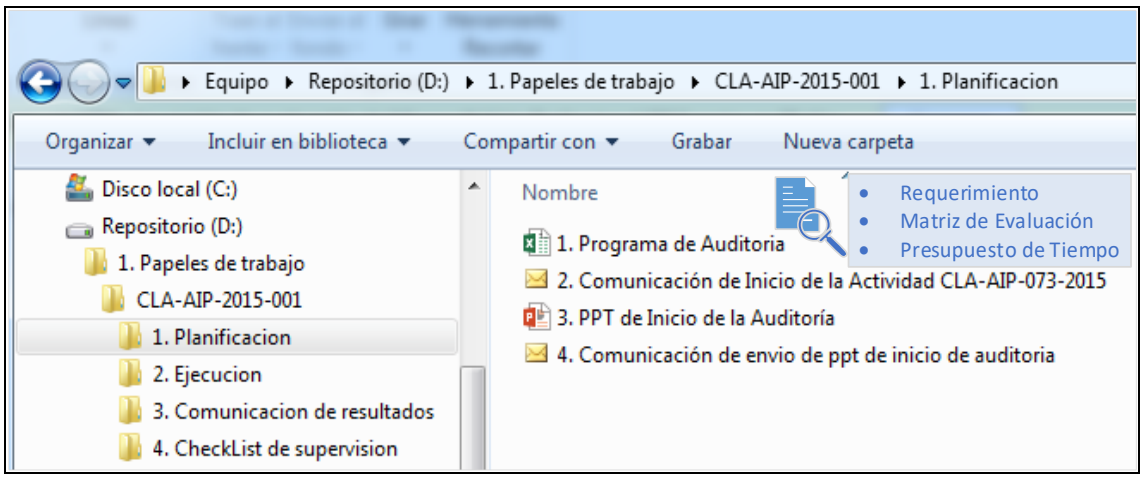

Figura 7: Papales de la Parte de Planificación

Elaboración: Propia

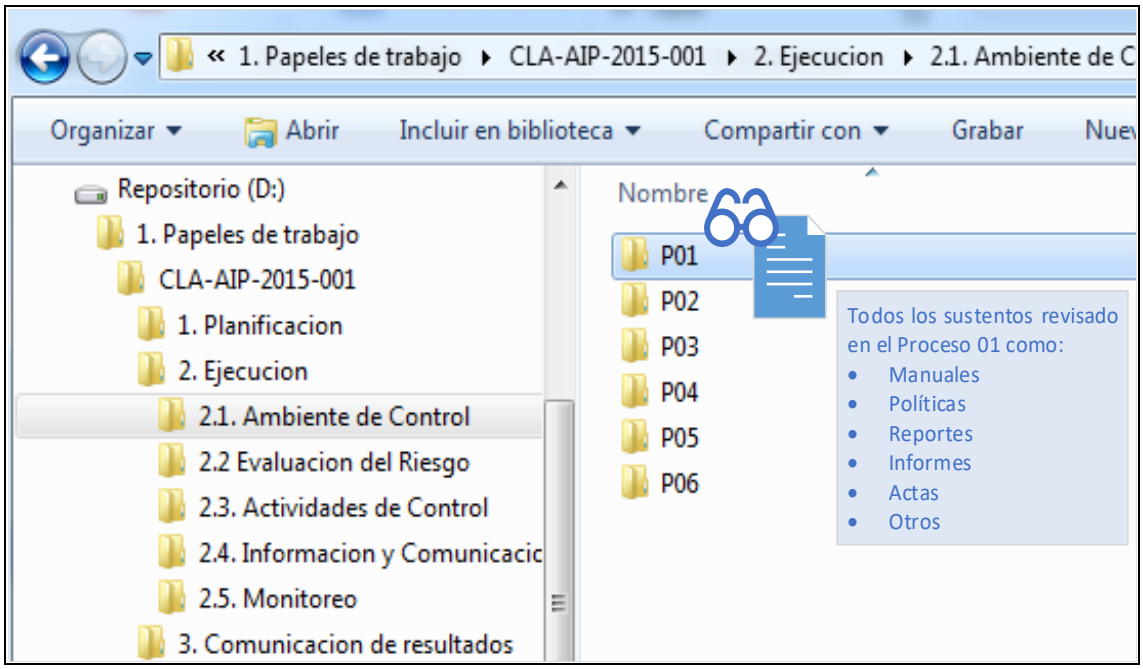

Figura 8: Papales de la Parte de Ejecución.

Elaboración: Propia

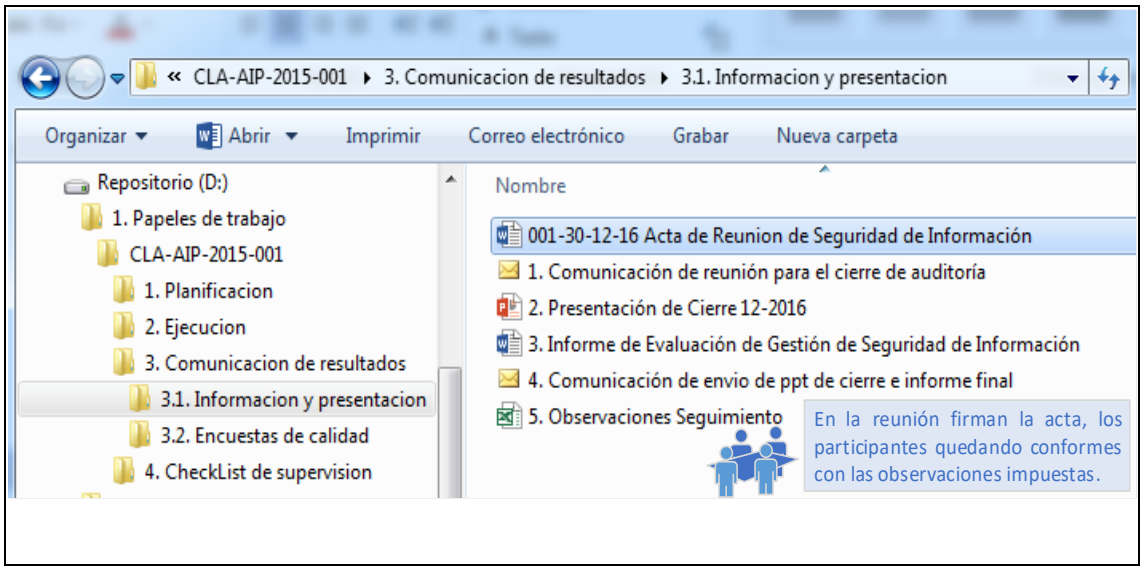

Figura 9: Papeles de la Parte de Resultados.

Elaboración: Propia

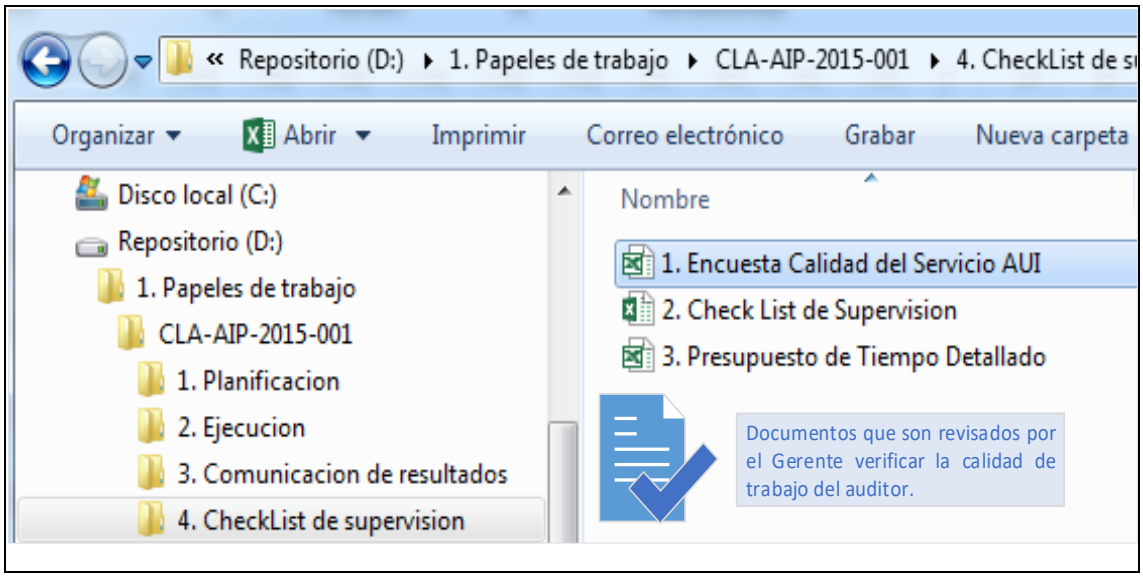

Figura 10: Papeles de la Parte de Supervisión.

Elaboración: Propia

4.3.4. Manual y procedimiento de Auditoría de seguridad de información.

Para el entendimiento se crea el manual que como objetivo es ser instrumento de gestión, de apoyo para identificar quién y cómo se realiza la evaluación de seguridad de información dentro y fuera de la gerencia de auditoría interna y contiene los siguientes apartados:

a) **Simbología**, indica nombre y significado de los símbolos utilizados en los diagramas de flujo de cada procedimiento. Ver tabla 10.

Símbolo	Descripción
	Indica el inicio y término del procedimiento
	Decisión y/o alternativa: Indica el punto dentro del flujo en el que son posibles varios caminos o alternativas.
	Operación: Representa la ejecución de una actividad o acciones a realizar con excepción de decisiones o alternativas.
	Documento: Representa cualquier tipo de documento que se utilice, reciba, se genere o salga del procedimiento.
	Base de Datos: Representa una base de datos con información abultada y custodia de información restringida.
	Dirección de flujo o líneas de unión: Conecta los símbolos señalando el orden en que deben realizarse las distintas operaciones.

Tabla 10: Descripción de la Simbología.

Fuente: Definición del Software Microsoft Visio

b) **Descripción del procedimiento,** Para un mejor entendimiento del proceso se incluye la figura 11 en ella mostramos el diagrama de flujo de actividades y la interacción del auditor y los participantes en todo el proceso de Auditoría de Seguridad de Información.

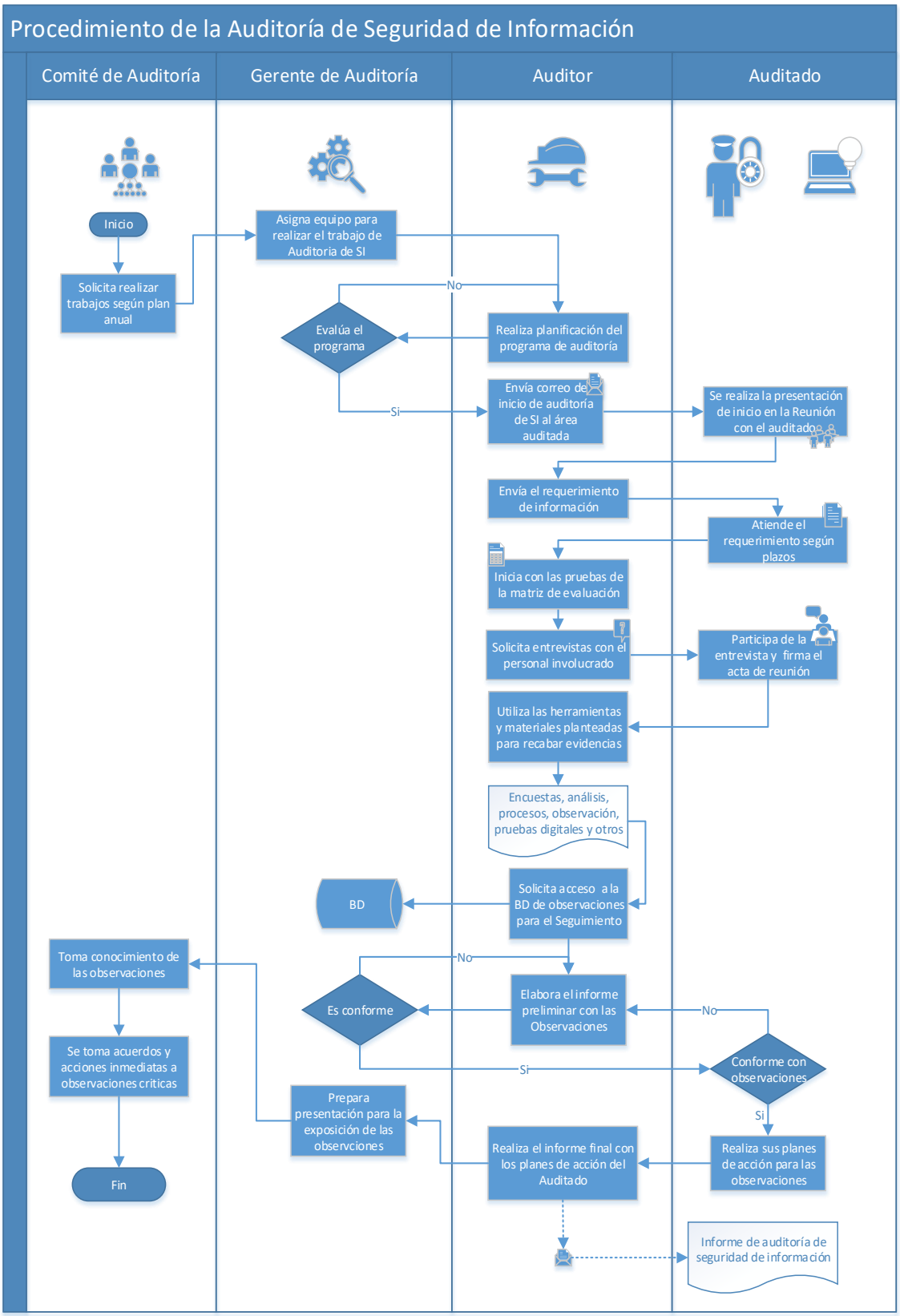

Figura 11: Diagrama de Flujo del Procedimiento.

Elaboración: Propia.

4.4. Evaluación del costo de auditoria luego de implementar el proceso.

Después de la implementación del proceso se pudo reducir el tiempo que tomaba realizarlo, durante la recopilación de tiempos, se tenía los tiempos estimados que debería tomar ejecutar cada actividad pero una vez ejecutado el proceso, en algunas actividades aumento el tiempo pero aun así se logró reducir el tiempo. Este acontecimiento es porque el personal del área auditada no dispone al 100% de su tiempo para participar de la auditoria.

Con la implantación del proceso se tuvo que asignar a una persona de la gerencia de auditoría interna para realizar el trabajo, al igual que las consultoras disponía de un personal, pero en cuanto a gastos se reduce en gran porcentaje siendo más económico realizar la auditoria con el proceso implantado.

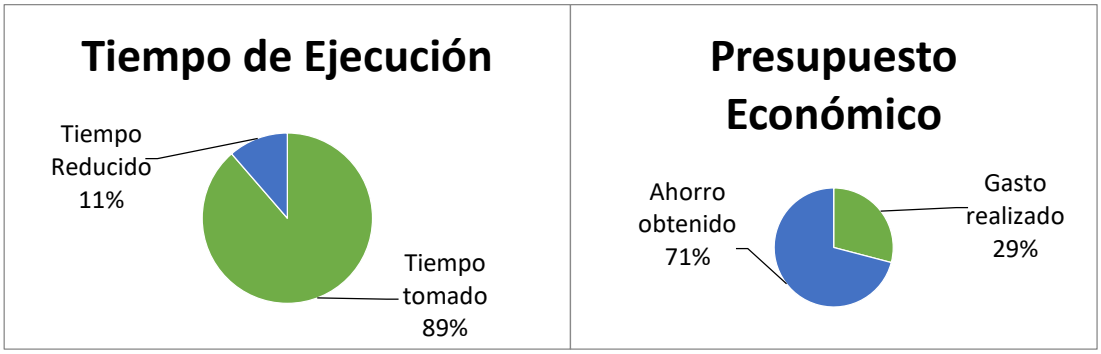

Figura 12: Resultados en Porcentajes.

Elaboración: Propia.

En la Figura 12 mostramos gráficamente el resultado obtenido; en el Tiempo de Ejecución se redujo el tiempo en las actividades en un 11%, porque con el proceso implantado se hiso en 156 horas que viene a ser el 89% dado que el 100% son las 176 horas (mes, días hábiles). Y en el Presupuesto Económico podemos observar que se ahorró un 71%, gracias a que con el proceso implementado se hiso uso de S/. 2500.00 que es el 29%. Siendo el S/. 8600.00 el 100%. Para la aceptación del proceso había que demostrar que el costo se reduciría de la última auditoría realizada por la Consultora que se realizó en un mes (176 horas) a un precio de S/. 8600.00

Como los resultados de la implementación del proceso se generó varios beneficios como la inclusión de la norma ISO/IEC 27002, el orden en general, control de tiempo, supervisión, actividades programas, comunicación constante, mejoramiento de manejo de evidencias y papeles de trabajo. Según los resultados los problemas en la gerencia de auditoria interna es a falta de no tener definido sus procedimientos, estos se deben formalizar y documentar como se hizo con la auditoria de seguridad de información. Ver tabla 11 para ver el comparativo.

Proceso	**Consultoría**
• Gasto realizado durante el mes s/.2500.00. • Tiempo trabajado 156 horas. • Informe Bueno y genero 6 observaciones • Manual del proceso. • Repositorio de Papeles de trabajo. • Supervisión constante. • Control de tiempo. • Matriz de evaluación.	• Gasto realizado durante el mes s/. 8600.00 • Tiempo trabajado 176 horas. • Informe Bueno y genero 6 observaciones

Tabla 11: Cuadro Comparativo.

Elaboración: Propia

CONCLUSIONES

PRIMERO: De los resultados obtenidos se concluye que la implantación del proceso de Auditoría de Seguridad de Información basada en la norma ISO/IEC 27002, fue un éxito logrando reducir el costo de la auditoría de seguridad de información realizada en la Caja Los Andes, Puno-2016, gracias a que el proceso facilita al auditor interno tener herramientas, pautas técnicas, plan de pruebas, una estructura de custodia de papeles de trabajo, una ficha de control de tiempos, un informe y una estructura sistematizada para realizar la auditoria de seguridad de información.

SEGUNDO: Del diagnóstico obtenido sobre el análisis situacional se puede concluir que al establecer un proceso hay que conocer cómo se venía trabajando y tomar en cuenta ese expertis que tienen los empleados para afianzar las actividades del proceso implantado.

TERCERO: Del diseño y esquema del proceso de auditoría de seguridad de información presentado en tres fases: planificación del programa, ejecución de actividades y presentación de resultados, y una matriz de evaluación con plan de pruebas basada en la norma ISO/IEC 27002, se concluye, que dicho proceso debe ser ejecutado continuamente y el número de actividades de la matriz de evaluación puede variar de acuerdo a las necesidades de la organización.

CUARTO: Luego de ejecutar el proceso propuesto de auditoría de seguridad de información, se obtuvo que si existe una reducción del costo, de cuando este era realizado por terceros antes de la implantación, con el proceso implantado se logra reducir un 11% en tiempo de ejecución y un 71% en gastos económicos.

RECOMENDACIONES

PRIMERO: Creo necesario darle importancia a este tipo de auditorías porque confiamos nuestros datos personales y financieros a entidades financieras que puede que no estén cumpliendo con su deber de garantizar una adecuada seguridad de la información.

SEGUNDO: Para la siguiente implementación de un proceso de seguridad de información se recomienda tomar en cuenta los acuerdos tomados en el comité de gestión de riesgos.

TERCERO: Respecto a los tiempos de ejecución de la Auditoría es necesario tener un tiempo de holgura ya que pueden existir muchas demoras, en alguno de ellos se doblaron el tiempo estimado esto porque el personal auditado nunca dispondrá del 100% de su tiempo. Ahora la idea es que sean ejecutadas por un auditor interno ya que se recomienda que la entidad financiera de Puno cuente con un auditor de TI certificado.

CUARTO: También comentar que en la gerencia de auditoría interna hace falta un proceso de evaluación de gestión de riesgos del gobierno de TI, gestión de proyectos de sistemas de información son necesidades que pueden ser tomadas como trabajos futuros. A consecuencia del crecimiento de la entidad existirá la necesidad de la automatización de la gestión de observaciones generadas por Auditoría interna, Auditoría externa y SBS.

REFERENCIAS

Benavides, M. del C., Enriquez, E. R., & Solarte, F. N. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica - ESPOL*, *28*(5), 492–507. Obtenido de http://learningobjects2006.espol.edu.ec/index.php/tecnologica/article/view/456

Blanco, J. (2009). *Implementación de un sistema de gestión de seguridad de la información basada en las recomendaciones de la norma técnica peruana NTP/ISO 17799 en la empresa de generación eléctrica San Gabán S.A.* Universidad Nacional del Altiplano, Puno, Perú.

Carvajal, C. J. (2015). Extracción de reglas de clasificación sobre repositorio de incidentes de seguridad informática mediante programación genética. *Tecnura*, *19*(44), 109–119. Obtenido de https://doi.org/10.14483/udistrital.jour.tecnura.2015.2.a08

Gestión de la seguridad de la información, S. (2009). CIRCULAR Nº G- 140 -2009. *Superintendencia de Banca Y Seguros*. Obtenido de http://www.esan.edu.pe/programa/gestion-seguridad-iso-27001/2012/03/05/G-140-2009C.pdf

Gómez, R., & Noreña, R. (2016, April). La lucha contra el soborno y la corrupción , prioridad mundial para empresas y gobiernos. *Centro de Estudios EY*, *14ª Encues*, 4. Obtenido de http://www.ey.com/Publication/vwLUAssets/EY-encuesta-global-sobre-fraude-2016-resumen-ejecutivo/$FILE/EY-encuesta-global-sobre-fraude-2016-resumen-ejecutivo.pdf

ISO/IEC 27002. (2013). Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información. *Control*.

Jimenez, C. (2016). *Seguridad en Redes y Sistemas: Técnicas y conceptos sobre Hacking y pentesting*. *Repositorio Institucional UOC*. Universidad Oberta de Catalunya. Obtenido de http://hdl.handle.net/10609/52944

Mejías, J. (2016). *Metodología para Auditorías de Ciberseguridad*. *Repositorio Documental UVA*. Universidad De Valladolid. E.T.S. Obtenido de http://uvadoc.uva.es/handle/10324/15240

Muñoz, M., & Rivas, L. (2015). Estado actual de equipos de respuesta a incidentes de seguridad informática. *RISTI - Revista Ibérica de Sistemas E Tecnologias de Información*, *2015*(E3), 1–15. Obtenido de https://doi.org/10.17013/risti.e3.1-15

NIA-350. (2013). Norma internacional de auditoría 530 muestreo de auditoría (NIA-530). Obtenido de http://www.icac.meh.es/NIAS/NIA 530 p def.pdf

Pérez, M. M. (2013). Seguridad de la Información. ISO 27001.[Figura]. Obtenido de https://www.auditool.org/blog/control-interno/1935-seguridad-de-la-informacion-iso-27001

Sanchez, W. (2015). SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN-CAJA LOS ANDES.

Willson, D. (2016). Who Are the Hackers? *Cyber Security Awareness for CEOs and Management*, 25–29. Obtenido de https://doi.org/10.1016/B978-0-12-804754-5.00003-9

Zurita, P. H. (2009). *Implementación de Auditoría Informática en Instituciones Públicas de la Ciudad de Puno*. Universidad Nacional del Altiplano, Puno, Peru.

ANEXOS

ANEXO 1: PROGRAMA DE AUDITORIA

PROGRAMA DE AUDITORIA	
Nombre de la Evaluación o Auditoría	Subprocesos Identificados
Evaluación de la administración de la seguridad de información e infraestructura.	Continuidad del negocio, Riesgos de TI
Cargo del Responsable	Nombre del Responsable
Gerente de Auditoría Interna	

Ultimo año realizado	Duración Estimada	Calificación de última auditoría
2015	1 mes	Regular

Objetivo del Programa	Evaluación de la administración de la seguridad de información e infraestructura.	
	· Efectuar la evaluación de seguridad de información basada en la norma emitida por la SBS, la Circular G 140-2009 “Gestión de la Seguridad de Información”, identificando las brechas y generar recomendaciones.	
	· Verifique, evalúe y evidencie los controles implementados y operativos aplicados.	
	· Verifique las actividades desarrolladas para la implementación del Sistema de Gestión de Seguridad de Información (SGSI).	
	· Verifique, evalúe y evidencie los mecanismos de seguridad establecidos en la subcontratación de los servicios externos de Tecnología de Información.	
	· Verifique las responsabilidades asignadas al oficial de seguridad de información y comité de riesgos	
	· Evaluar la identificación de eventos de pérdida y gestión de riesgos operacionales asociados a la seguridad de la Información.	
	· Verifique que los contratos suscritos con terceros asociados a tecnologías de información contemplen las cláusulas necesarias asociadas a la seguridad de información.	
Alcance del Programa	Proyectado:	Se realizará en 1 mes
	Cumplimiento:	Verificar la adherencia de la entidad financiera a las normas, políticas, reglamentarias y de autorregulación que le son aplicables.
	Estratégico:	Evaluar y monitorear del desempeño del sistema de gestión de seguridad de información.
	Gestión y Resultados:	Verificar las actividades relativas a la gestión del SGSI, con el fin de determinar el grado de eficiencia y eficacia en el manejo de los recursos, incidentes, riesgos y controles.
Recursos	Tecnológicos:	Equipos de cómputo, sistemas de información, sistemas de redes, correo electrónico de la empresa, entre otros.

Nombre del Auditor	Fecha de elaboración
Max Y. Puma Arosquipa	31/11/2016

Nombre del Supervisor /Jefe	Fecha de Revisión
Gerente de Auditoría Interna	01/12/2016

ANEXO 2: MATRIZ DE EVALUACIÓN

PROGRAMA - MATRIZ DE EVALUACIÓN			
Auditor	Max Y. Puma Arosquipa		
Actividad	Evaluación de la administración de la seguridad de información e infraestructura.		
Información del trabajo de Auditoría			
Áreas Auditadas	Áreas	Responsables	
	Oficial de Seguridad de Información		
	Gerencia de Riesgos		
	Gerencia de TI		
Antecedentes	En años pasados se realizaron Auditorías aplicando distintas formas de ejecución		
Normativas o Criterio	ISO 17799, ISO 27001, COBIT, Expansión, Control Interno, Auditoría y Seguridad Informática: un enfoque práctico		
1. Ambiente de Control			
Cód. de Proceso	Proceso	Descripción	Actividades a Realizar
P01	Organigrama del área	Deberemos verificar que el control y la gestión de la tecnología se encuentran segregados conforme al modelo de ciberseguridad.	1. Verificar que tenga las tres líneas de defensa según el modelo de seguridad de información
P02	Las responsabilidades asignadas al Directorio, a la Gerencia referidas y al oficial de seguridad.	Verificar dentro de las funciones y responsabilidades del Oficial de seguridad de información esté el desarrollar, elaborar y proponer a aplicar las normas y metodologías de seguridad de TI, pruebas de seguridad, Analizar las fuentes de exposición de Riesgo Tecnológico y demás funciones correspondientes según normativas.	1. Verificar que las funciones del personal estén contempladas en el MOF. 2. Verificar la Segregación de funciones e identificar posibles conflictos de interés. 3. Verificar que el personal cumpla razonablemente con el perfil y haya suscrito los acuerdos de confidencialidad de la información que maneja. 4. Analizar la suficiencia de recursos y jerarquía respecto a la seguridad de información.

Continúa…

P03	Relaciones Jerárquicas	Analizaremos las responsabilidades de las áreas que recaen responsabilidades y la jerarquía en las que se trata los importantes riegos de la seguridad de la información.	1. Ver de la existencia de la jerarquía y niveles de aprobación de accesos a información e ingreso de ambientes restringidos. 2. Verificar de las áreas involucradas sus registros de actividades respecto a la seguridad. 3. Comprobar que se han implementado comités.
P04	Modelos de gestión y mecanismos para control de Seguridad de Información	La Gestión de seguridad de la información ha de estar alineado con los estándares definidos en esta materia (NIST, COBIT e ISO) y las directrices de los reguladores, tanto internacionales como nacionales y se debe analizar la existencia de herramientas y/o mecanismos para la supervisión de la actividad de la 1ª línea de defensa y que cubren todos los dominios del riesgo tecnológico (Seguridad de la información, Producción, Desarrollo y Gestión de la tecnología).	1. Analizar y verificar la implantación de un modelo de gestión de seguridad de información (como Identificar, Proteger, Detectar, Recuperar e informar) el en plan anual del oficial. 2. Ver el disponer de herramientas y procedimientos a incidentes de phishing (fraude mediante webs o emails falsos que imitan los sitios oficiales), vishing (fraude telefónico realizando pagos u operaciones a nombre de la víctima) y smishing (similar al phishing con origen a través de mensajes de texto telefónicos).
P05	Nivel académico, Experiencia y Capacitación	Es necesario identificar el personal y que éste tenga un correcto perfil académico, también verificar que todos y cada uno de los empleados pertenecientes al área (oficialía de seguridad de información), tengan capacitaciones periódicas.	1. Ver la existencia de un plan de Capacitación Anual, presupuesto y beneficiados. 2. Ejecución de la Capacitación. Facturas y Certificados.
P06	Proveedores de Servicio	Se debe Identificar los proveedores que tienen las áreas, quien nos proporcionará contratos y SLAS vigentes en la fecha de la auditoría. En especial debemos recabar información de aquellos proveedores que se encarguen de temas de ciberseguridad (antivirus, SOC, etc.).	1. Analizar la definición de Proveedores Críticos 2. Revisar los Contratos con apoyo Legal. 3. Revisar los registros de Gestión de SLAs 4. Ver si revisan la Gestión de Riesgos de Proveedores. 5. Analizar y revisar los Informes de Riesgos y Auditoría
2. Evaluación de Riesgos			
P07	Plan de seguridad del Oficial de seguridad de información	Deberemos verificar que se haya establecido un proceso de administración de la seguridad, que garantice la integridad de la información y la protección de los activos de la Caja.	1. Verificar que esté aprobado dicho plan de seguridad. 2. Ver que esté cumpliendo con su plan de seguridad. 3. Analizar su Gestión del Alcance, Tiempo, Costo y Calidad de los Requerimientos para el plan de seguridad. 4. Ver en el plan actividades como informan a los empleados de posibles riesgos que podrían afectarles.

Continúa…

P08	Operación de la seguridad.	Se debe verificar en aquellos procedimientos que permiten comprobar que la actividad de los operadores (Oficial de seguridad) se encuentra regulada recogiéndose las principales tareas: Gestión de usuarios y claves (alta, baja, modificación y desbloqueo), Utilización de usuarios de emergencia, Gestión de claves criptográficas, Gestión de accesos desde el exterior, Configuración de sistemas y dispositivos de seguridad.	1. Analizar sus procedimientos de: - Políticas y normas de utilización del correo electrónico, internet. (Instrucciones generales, aviso legal a incluir en los correos electrónicos). - Control y gestión de accesos a los sistemas informáticos. (Nomenclatura, USERID, Control y administración de acceso a sistemas, Empresas externas) - Normas de seguridad de información. (para el oficial, la utilización del material informático, gestión de incidentes, terceros, gestión y clasificación de activos, Adquisición y mantenimiento de software y control de accesos) - Control y gestión de incidentes de seguridad. (procedimientos de comunicación entre áreas implicadas en la gestión de incidentes, matriz de incidentes de seguridad) - Respuestas a incidentes de Phishing, Vishing e SMiShing. (procedimiento de respuestas a los incidentes) - Políticas de escritorios limpio. (Clean Desk)

Continúa…

P09	Categorización de incidentes de seguridad de información	Se deberá contar con un procedimiento correctamente definido dónde se detalle la categorización de los mismos.	1. Revisar que tenga categorías como: - Acceso externo no autorizado. (Ataques externos no autorizados que permitan acceder, modificar datos o interrumpir un servicio utilizando técnicas de hacking como SQL Inyección, Cross-Site, ataques de ingeniería social, etc.) - Acceso interno no autorizado. (Acceso interno no autorizado a los sistemas que comprometan la integridad, confidencialidad y accesibilidad o disponibilidad de los negocios críticos utilizando técnicas como hacking o ingeniería social) - Robos (Robos de dispositivos no cifrados que contengan información confidencial como PC, laptops, tablets, smartphones, pendrives, etc.) - Incumplimientos. (Incumplimientos de funciones y normas relacionados con la seguridad de la información causadas por un acto deliberado y que tengan consecuencias directas en las operaciones de negocio.) - Malware. (Indisponibilidad de funciones críticas de negocio debido a programas virus, troyanos con posibilidad de afectar a otras entidades del grupo) - DoS. (Ataques de denegación de servicio que causen indisponibilidad de servicios críticos o que puedan repercutir en la imagen de la compañía) - Otros. (Cualquier otro tipo de incidente)

P10	Seguridad física y del entorno	Los recursos para el tratamiento de información crítica o sensible para la organización deberían ubicarse en áreas seguras protegidas por un perímetro de seguridad definido, con barreras de seguridad y controles de entrada apropiados. Se debería dar protección física contra accesos no autorizados, daños e interferencias.	1. Debe estar con perímetro de paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción, alarmas, rejas, etc. 2. Debe tener sistemas de detección de intrusos (cámaras de seguridad, sensores de movimiento y golpes). 3. Ver que las visitas a las áreas seguras hayan sido supervisadas a no ser que hayan sido aprobadas. 4. Ver que se usen controles de autenticación (DNI, tarjetas, registros, huellas, firmas, etc.). 5. Los materiales peligrosos y combustibles deben ser distantes a las seguras.
P11	Seguridad de equipos.	Evitar pérdidas, daños o comprometer los activos, así como la interrupción de las actividades de la organización. También se debería considerar su instalación (incluyendo su uso fuera del local) y disponibilidad. Pueden requerirse medidas o controles especiales contra riesgos de accesos no autorizados y para proteger los sistemas de apoyo, como la alimentación interrumpida o la infraestructura de cableado.	1. Los controles deben ser adoptados p… riesgos de posibles amenazas como explosivos, humo, agua, polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, radiaciones electromagnéticas. 2. Ver que deben incluir en su política cuestiones sobre fumar, beber y comer cerca de los equipos.
		3. Actividad de Control	
P12	Clasificación, respaldo y control de activos	Deberían identificarse los propietarios para todos los activos importantes, y se debería asignar la responsabilidad del mantenimiento de los controles apropiados. La responsabilidad de la implantación de controles debería delegarse. Pero la responsabilidad debería mantenerse en el propietario designado del activo. La información debería clasificarse para indicar la necesidad, prioridades y grado de protección.	1. La existencia de un inventario de información. 2. Responsables de los activos, revisión periódica de accesos, clasificación y actualización de políticas 3. Existencia de guías de clasificación de información, iniciales y a través del tiempo. 4. Procedimientos para marcado de activos físicos y digitales. 5. Tener copias de seguridad y ensayando su oportuna recuperación. 6. Los respaldos se deben probar con regularidad, está en una locación remota y protegidos por medios de encriptación.

Continúa…

P13	Control de seguridad del Host - series	El objetivo de una Auditoría de seguridad host para servidores series comprobar que tengan procedimientos relativos a la configuración de la seguridad de la plataforma zSeries/series y que estas han sido construidas teniendo en cuenta los estándares de seguridad (NIST, FIPS, ANSI, IEEE, ISO, IEC, ISACA, etc.)	1. Comprobar que los sistemas cuenten con un nivel de actualización (parches de seguridad). 2. Verificar el número de licencias instaladas se adecua a los contratos de software. 3. Verificar que existe mecanismos que regulan y limitan el acceso de los usuarios a los sistemas. 4. Verificar y analizar que exista un inventario de los usuarios con privilegios especiales (técnicos /administradores). 5. Comprobar que los logs son almacenados y custodiados de manera segura. 6. Ver si se efectúan pruebas de seguridad de forma periódica sobre los sistemas series.
P14	Control de seguridad de Bases de Datos	El objetivo es proteger la Base de Datos contra accesos no autorizados. Se llama también privacidad. Incluye aspectos como legales, sociales y éticos, Políticas de la empresa, niveles de información pública y privada, Controles de tipo físico, acceso a las instalaciones, Identificación de usuarios: voz, retina del ojo, etc. En relación al SGBD, debe mantener información de los usuarios, su tipo y los accesos y operaciones permitidas a éstos.	1. Comprobar en nivel de parch 2. El número de licencias instaladas. 3. Los parches se realizan en entornos de prueba y herramientas automáticas de gestión de parches. 4. Comprobar que los accesos son mediante usuarios, longitud y composición de clave acorde a las definiciones en las políticas. 5. Control y vigencias de contraseñas de los usuarios. 6. Ver el inventario de los usuarios con privilegios especiales (técnicos/administradores). 7. Ver si las administraciones de la base de datos se realizan mediante protocolos seguros a través de redes e interfaces. 8. Verificar los logs, si son almacenadas y custodiados de manera segura en SIEM/SIM o un servidor Syslog) y ser modificadas. 9. Analizar si los SGBD se encuentran bajo el perímetro de revisión de herramientas específicas de monitorización de la actividad (DAM) como guardián de IBM o Imperva.

Continúa…

Continúa…

P15	Control de seguridad en Redes y Comunicaciones.	Debemos Identificar y obtener las políticas y procedimientos relativos a la configuración de la seguridad de los dispositivos de red (Firewalls, IDS/IPS, enrutadores y switches y accesorios de seguridad en red como proxies, email o VPN).	1. Revisar y analizar el mapa de red global y verificar la existencia de mecanismos de seguridad. (Firewalls, switches, sistemas de análisis de correo, antivirus, proxies, conexión VPN, etc.) 2. Contrastar la configuración de los dispositivos de red son aprobadas por el oficial y que estén alineadas con los procedimientos establecidos por el área. 3. Verificar las versiones firmware instalado, nivel de parcheado, número de licencias se adecuan a los contratos de software. 4. Verificar los accesos se efectúan siempre utilizando un usuario y una contraseña que identifique de forma inequívoca al usuario administrador que está accediendo. 5. Ver que la longitud y composición de la clave debe ser acorde a las definidas en las políticas de seguridad. 6. Ver si los accesos de administrador a los dispositivos de red se realizan mediante el uso de protocolos seguros (evitando servicios como FTP, telnet, snmp v2, http). 7. Asegurar la existencia de redes diferenciadas para empleados e invitados, así como el control de acceso a los medios. 8. Ver si existen procedimientos y herramientas para detectar software no autorizado en la red. 9. Analizar que el administrador y personal de seguridad no tenga acceso a modificación o eliminación. 10. Evidenciar que se efectúan las pruebas de seguridad de forma periódica.

Continúa…

P16	Control de seguridad en Plataforma de Usuarios	Debemos identificar y obtener las políticas y procedimientos relativos a la configuración de la seguridad de los dispositivos de plataforma de usuario, como por ejemplo Workstation, notebooks, tablets o teléfonos inteligentes.	1. Ver si para la gestión de parcheo se utiliza plataformas de prueba y herramientas automáticas de gestión de parches, por ejemplo: System Center Configure Manager o Windows Server Update services para plataformas windows. 2. Controles como bloquear después de varios intentos, vigencia de contraseñas, almacenamiento cifrado. 3. En situaciones de acceso a los datos de dispositivos móviles o externas, firmar acuerdos de confidencialidad, políticas de uso razonable de los dispositivos y de la información almacenada en ella y procedimientos de retorno. 4. Protección en caso de pérdida o robo de dispositivos, backup de dispositivos, protección contra malware. 5. Inventario de usuarios con privilegios especiales ellas MDM. 6. Verificar que el personal de soporte se conecte mediante protocolos seguros. 7. Verificar que se estén almacenado los logs que son revisados por el oficial de seguridad y ver que exista revisiones periódicas
P17	Control de seguridad en el Directorio Activo	En el Directorio activo es un servicio establecido en uno o varios servidores donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red.	1. Ver las políticas y procedimientos relativos a la configuración de la seguridad de los servicios de directorio tales como Microsoft Active Directory u otros compatibles con LDAP. 2. Ver que se tenga la descripción lógica del servicio de directorio, objetos, bosques, árboles y dominios. 3. Los accesos se efectúan siempre mediante usuarios y contraseñas, longitud mínima, vigencia, numero de intentos, duración del bloqueo de cuenta. 4. Inventario de usuarios privilegiados en los servicios de directorio. 5. Ver que los accesos sean mediante protocolos seguros (FTP, TELNET, SNMP, HTTP).

4. Información y comunicación			
P18	Canales de información y reportes	Verificar el tratamiento de reportes e informes respecto a la seguridad de información, el oficial debe tener formatos para poder captar los incidentes de seguridad de información que los usuarios pueden brindar a la vez exponerlos a alta gerencia sobre los eventos sucedidos.	1. Verificar los formatos y medios de recolección de incidentes relacionados con la seguridad 2. Verificar que estas sean expuestas a la alta gerencia. 3. Ver el análisis de los reportes mensuales y anuales si son elaboradas con objetividad.
P19	Uso de información y de sistemas de información	Identifique el grado de conocimiento de los usuarios del sistema de la Caja sobre la seguridad de información. Además, ver que el oficial haya realizado capacitaciones y divulgación de la importación de la seguridad de la información a los usuarios.	1. Realizar una encuesta sobre el grado de conocimiento de los usuarios sobre seguridad de información. 2. Revisar las capacitaciones realizadas respecto al tema
5. Supervisión			
P20	Identificación y evaluación de cambios relevantes.	Verifique si el oficial de seguridad de información es participe en los proyectos asociados a cambios significativos en los distintos proyectos de sistemas de información y de la infraestructura tecnológica. Asimismo, ver que este pendiente y actualizado sobre cambios en los procesos que existan riesgo de pérdida de información, además revisar las acciones y planes que realiza el oficial cuando se presente este tipo de eventos.	1. Revisar los informes emitidos durante el año respecto a proyectos realizados. 2. Ver si dentro de funciones este incluido la de participar en Proyectos de gran envergadura. 3. Verificar las acciones tomadas en los proyectos. 4. Verificar dentro de sus actividades sobre cambios en procesos que afecten la seguridad de la Caja.
P21	Monitoreo del rendimiento del Oficial	Revisar la realización de las pruebas de plan de continuidad del negocio, plan de recuperación de servicios de TI y verificar la calidad y la eficiencia de la labor realizada en la mejora de la gestión de seguridad de información, detección de incidentes y el nivel de protección de la Caja.	1. Revisar las actas de ejecución del plan de continuidad del negocio y de recuperación de servicios de TI. 2. Analizar y ver los formatos de control si son adecuados para dichos planes mencionados. 3. Ver la evaluación de desempeño del oficial de seguridad.

Continúa…

ANEXO 3: CONTROL DE TIEMPOS

CONTROL DE TIEMPO DETALLADO	
Nombre de la evaluación:	Evaluación de la administración de la seguridad de información e infraestructura.
Auditor a cargo:	Max Yonel Puma Arosquipa
Fecha:	30/12/2016

Proceso	Actividades	Tiempo(H)		Auditor 1		Auditor 2		Comentarios
		Estimado	Real	Estimado	Real	Estimado	Real	
		9	17					
I01	Reunión de inicio	1	1	1	1			
I02	Requerimiento de información	8	16	8	16			El personal auditado no presento a tiempo
Ambiente de control		17	18					
P01	Organigrama del área	2	3	2	3			
P02	Las responsabilidades asignadas.	2	3	2	3			
P03	Relaciones Jerárquicas.	2	3	2	3			
P04	Modelos de gestión y mecanismos.	4	2	4	2			
P05	Nivel académico, Experiencia	4	3	4	3			
P06	Proveedores de Servicio	3	4	3	4			
Evaluación de riesgos		22	34					
P07	Plan de seguridad del Oficial.	4	5	4	5			
P08	Operación de la seguridad.	4	5	4	5			
P09	Categorización de incidentes.	2	3	2	3			
P10	Seguridad física y del entorno	8	16	8	16			
P11	Seguridad de equipos.	4	5	4	5			
Actividad de control		27	35					
P12	Clasificación, control de activos.	2	3	2	3			
P13	Control de seguridad del Host - series	4	4	4	4			

Continúa…

P14	Control de seguridad, Bases de Datos	5	6	5	6			
P15	Control de seguridad, Redes Comunicaciones	8	10	8	10			
P16	Control de seguridad, Plataforma de Usuarios	4	6	4	6			
P17	Control de seguridad en el Directorio Activo	4	6	4	6			
Información y comunicación		12	17					
P18	Canales de información y reportes	6	8	6	8			
P19	Uso de información, sistemas de información	6	9	6	9			
Supervisión o monitoreo		14	18					
P20	Identificación de evaluación, cambios.	6	8	6	8			
P21	Monitoreo del rendimiento del Oficial	8	10	8	10			
Otros		9	17					
F01	Redacción del informe	6	12	6	12			
F02	Exposición de observaciones	1	1	1	1			
F03	Armado de papeles de trabajo	2	4	2	4			
Tiempo total por actividad		110	156					
Tiempo total en Días		13.75	19.5					

Tiempo perdido	46
Tiempo óptimo de perdida	23
Nuevo tiempo estimado	133

ANEXO 4: REQUERIMIENTO DE INFORMACIÓN

REQUERIMIENTO DE INFORMACIÓN							
N°	Requerimientos	Estado	Entregado por	Referencia	Aprobado por	Comentario Caja	Comentario Auditoría
A	Documentación General						
1	Manual de Organización y Funciones - MOF	Atendido	Oficial	Manual de organización y funciones.v4.2	SD N° 213-2014 27/03/2014		
2	Política de Seguridad de la Información.	No se tiene	Oficial	Política general de seguridad de la información v2.1		Se tiene definido políticas por cada proceso	Las políticas están definidas respectivos las normativas.
3	Reglamento Interno de Trabajo	Atendido	Oficial	Reglamento interno de trabajo 2014	SD N° 219-2014 28/07/2014		
4	Plan de trabajo del oficial de seguridad - 2016	Atendido	Oficial	SGSI			
5	Sistema de gestión de seguridad de la información		Oficial				
6	Código de conducta de la institución						
7	Relación de Personal involucrado en la seguridad de información, estudios y certificaciones (currículo vitae).	Atendido	Recursos Humanos	Relación de Personal TI y Oficial de seguridad.			
B	Documentación de Gestión de Seguridad de Información.						
8	Plan Estratégico del oficial de seguridad, vigente durante el periodo auditado	Atendido	Asistente del Oficial	Plan Estratégico			Se solicitó el PEI pero no fue entregado
9	Plan de trabajo anual del oficial de seguridad, vigentes durante el periodo auditado, incluye informes pericos de avance.	Atención Parcial	Asistente del Oficial	POA			Falta POA. Sólo existen avances
10	Procedimientos de Operación de cada uno de los Sistemas.	Atendido	Gerencia de TI	Política de Seguridad, Gestión, operación y	SD N° 204-2013 19/06/2013		

Continúa…

				Funcionamiento			
11	Directiva y Procedimiento de evaluación y control de usuarios y perfiles de Core financiero	Atendido	Gerencia de TI	Directiva para la Administración de Derechos y Perfiles del Sistema Core			
12	Procedimiento de seguridad sobre redes, medios de almacenamientos y de equipos de comunicación	Atendido	Gerencia de TI	Repositorio de Procedimientos			
13	Procedimiento sobre verificación de antecedentes del personal	Atendido	Recursos Humanos	Repositorio de Procedimientos			
14	Procedimientos de Administración de Bibliotecas de Software.	Atendido	Gerencia de TI	Política de Seguridad, Gestión, Operación y Funcionamiento	SD N° 204-2013 19/06/2013		
15	Procedimiento de monitoreo de servicios terceros		Asistente del Oficial				
16	Metodología de gestión y clasificación de activos de información	Atendido	Gerencia de TI	Política de Seguridad, Gestión, Operación y Funcionamiento	SD N° 204-2013 19/06/2013		
17	Procedimientos de Gestión y atención de solicitudes e incidencias, incluye relación de incidencias durante el periodo auditado, conteniendo como mínimo: descripción detallada, reportado por, responsable, fecha de ingreso, fecha de atención, planes de acción y situación actual.	Atendido parcial	Asistente del Oficial, Gerencia de TI	011-3100-1.2.0 - Directiva de Uso del Sistema de Mesa de Ayuda			Directiva en Borrador. No tiene aún formato de Normas de la caja
18	Inventario de Equipos existentes.	Atendido	Gerencia de TI	inventario hw y sw procesado			No se tiene un repo
19	Inventario general y clasificación de activos.	Atendido	Asistente del Oficial	Inventario de Activos de Información			

Continúa…

20	Inventario de Software instalado en cada equipo.	Atendido	Gerencia de TI	WinAudit.			
21	Informe emitido de seguridad física, lógica y personal	Atendido	Asistente del Oficial	Evaluación de Accesos y Perfiles			
22	Reportes y monitoreo realizados de seguridad en año	Atendido	Asistente del Oficial	Capacitaciones 2do trimestre			
23	Registros de Mantenimientos de equipos tecnológicos realizados.	Atendido	Asistente del Oficial			EN FISICO. 2 veces al año.	
24	Reportes de ethical hacking						No se hizo
25	Niveles de Servicio establecidos con los servicios de TI tercerizados, incluye informes de SLA durante el periodo	Atendido parcial	Gerencia de TI	SLA-claro			Solicitar la relación de servicios
26	Niveles de Servicio de Operación establecidos por TI, incluye informes.	Atendido parcial	Asistente del Oficial	Directiva de Uso del Sistema Mesa de Ayuda			
27	Base de datos de Riesgos identificados y eventos de perdida	Atendido	Gerencia de Riesgos	Matriz de riegos IT, SI, CN, EP		Actualizado Al octubre 2015	
28	Directiva para el uso del servicio de internet	No se tiene	Asistente del Oficial			No se realizó capacitación	No capacitación
29	Procedimiento de backups de sistemas	No se tiene	Gerencia de TI				Se consideró como Hallazgo
30	Políticas y procedimientos de configuración del sistema de gestor de base de datos		Gerencia de TI				
31	Lista de usuarios, administradores y privilegios de Base de datos		Gerencia de TI				
32	Directiva del diccionario de tablas de la base de datos		Gerencia de TI				

ANEXO 5: MATRIZ DE EVALUACIÓN EJECUTADO

MATRIZ DE EVALUACIÓN - EJECUTADO							
1. Ambiente de Control		Evaluación del Auditor					
Cód. de Proceso	Proceso	Descripción de pruebas	Descripción de Riesgo	Código de riesgo	Nivel de Riesgo	Observación	Referencia
P01	Estructura Organizacional	Ver la existencia de 3 líneas: 1. Controles gerenciales, medidas de control interno. 2. controles financieros, seguridad, gestión de riesgos, calidad y cumplimiento. 3. Auditoría Interna.	Pérdidas financieras debido al conflicto de intereses en la revisión de perfiles y accesos.	12-TI	Nivel Medio	-	
P02	Responsabilidades asignadas al Directorio, Gerencia y oficial Seguridad.	Lectura del manual de funciones de la organización, evaluaciones de Auditoría externa, SBS y cuestionario	Exposición a pérdidas económicas por ausencia de procedimientos y responsabilidades formales	12-EE	Nivel Medio	-	
P03	Relaciones Jerárquicas	Análisis de organigrama, comité de riesgos y seguridad	Posibilidad de fraudes al contratar personal de bajos valores éticos al no existir controles formales de verificación de antecedentes de personal.	30-EE	Nivel Medio	-	
P04	Modelos de gestión y mecanismos para control de Seguridad de Información	Encuesta al Oficial de seguridad y análisis de documentos.	Ausencia de controles de seguridad física y lógica sobre los servidores y bases de datos de los sistemas críticos durante el tránsito a la nueva ubicación.	21-EE	Nivel Alto	-	
P05	Nivel académico, Experiencia y Capacitación	Revisión de currículo vitae	Posibilidad de incurrir en gastos extras por ausencia de participación y disponibilidad de personal especializado.	37-EE	Nivel Medio	-	

Continúa…

P06	Proveedores de Servicio	Observar los contratos	Posibles inversiones significativas en la adquisición de servidores que no soportan servicios críticos o que requieren de características técnicas superiores.	13-EE	Nivel Alto	-	
2. Evaluación de Riesgos							
P07	Plan de seguridad del Oficial de seguridad de información	Observación de correos, lista de usuarios, lectura de los reportes de incidentes.	Debilidades en la identificación de los escenarios adversos de y planificación ante contingencias que prolongarían la operatividad de los sistemas y servicios.	20-EE	Nivel Extremo	-	
P08	Operación de la seguridad.	Observación de correos, lista de usuarios, lectura de los reportes de incidentes.	Exposición a pérdida de información por debilidades en el servicio de correo electrónico.	15-TI	Nivel Medio	De la revisión a la Directiva para Uso del Servicio de Internet a, se identifica que el propósito es gestionar de manera adecuada el acceso al servicio del Internet; sin embargo, no señala las reglas específicas de acceso basado en Niveles de acuerdo a perfiles (prioridad y necesidad del usuario) con fines de alinearse a las mismas.	D:\1. Papeles de trabajo\CLA-AIP-2015-001\2. Ejecución\2.2 Evaluación del Riesgo\P08
P09	Categorización de incidentes de seguridad de información	Encuestas a usuarios, revisión de incidentes, pequeñas pruebas de ataques	Debilidades en la identificación de los escenarios adversos de y planificación ante contingencias que prolongarían la operatividad de los sistemas y servicios	20-EE	Nivel Extremo	De la revisión a la Directiva para Uso del Servicio del Correo Electrónico aprobado en Sesión de Directorio Nº 200-2013 de fecha 28 de febrero del 2013, se identifica que una de las finalidades es “Regular el uso”; sin embargo, no señala los niveles y Reglas (permite otros dominios, peso de correo, peso de adjunto, cantidad de adjuntos, etc.) de los recursos que puede disponer el usuario.	

P10	Seguridad física y del entorno	Visitas de inspección, ver los controles de seguridad	Ausencia de controles de seguridad física y lógica sobre los servidores y bases de datos de los sistemas críticos durante el tránsito a la nueva ubicación.	21-EE	Nivel Alto	-	
P11	Seguridad de equipos.	señales de seguridad, cuestionarios, etc.	Posible pérdida de operatividad de la oficina producto de inundación por lluvias excesivas ocasionarían corte de circuito eléctrico generado por enchufes y equipos de cómputo (UPS) en el suelo del ambiente de TI, y pasadizos sin techo.	2-OC	Nivel Alto	No se tiene controles para proteger la información que contienen estos equipos, frente al riesgo de robo o pérdida de los mismos.	D:\1. Papeles de trabajo\CLA-AIP-2015-001\2. Ejecución\2.2 Evaluación del Riesgo\P11
3. Actividad de Control							
P12	Clasificación, respaldo y control de activos	Análisis del inventario de activos, procedimientos, preguntas, etc.	Ausencia de copias de seguridad a activos de información que son de alto interés para CRAC Los Andes	28-EE	Nivel Alto	La Gerencia de Tecnologías de Información, éstos no son los dueños del proceso que genera dichas incidencias, por lo tanto, No es propietario del Producto. Así como el presente contexto, es necesario analizar otros activos, de acuerdo a su tipo y aplicación en la Caja.	D:\1. Papeles de trabajo\CLA-AIP-2015-001\2. Ejecución\2.3. Actividades de Control\P12
P13	Control de seguridad del Host - series	Entrevista con el jefe de desarrollo e innovación, observación de los logs, lista de administradores, lectura de contratos de software y políticas de accesos a los sistemas.	Pérdidas financieras debido al conflicto de intereses en la revisión de perfiles y accesos.	12-TI	Nivel Medio	-	
P14	Control de seguridad de Bases de Datos	Revisión de diccionario de Base a datos, lista de administradores, reportes que general con el SGBD, entrevistas con el personal.	Incertidumbre sobre la implicancia en montos, número y tipo de operaciones con inconvenientes de voucher's en blanco, así como los ajustes realizados por el personal de TI a la base de datos SIfcNet	34-EE	Nivel Extremo	-	

Continúa…

P15	Control de seguridad en Redes y Comunicaciones.	Análisis de mapa de red, vlan, vpn, aplicar wireshark	Pérdidas financieras debido a posibles modificaciones para la instalación del cableado estructurado de redes en la apertura de oficinas especiales	16-TI	Nivel Alto	-	
P16	Control de seguridad en Plataforma de Usuarios	Encuestas a usuarios, revisión de incidentes, pequeñas pruebas de ataques	Posibilidad de ejecución de operaciones no autorizadas en razón a la vigencia de usuarios no existentes en la base de datos de trabajadores.	24-EE	Nivel Alto	-	
P17	Control de seguridad en el Directorio Activo	Análisis de redes vlan, vpn, aplicar wireshark y ver la seguridad.	Ausencia de copias de seguridad a activos de información que son de alto interés para CRAC Los Andes	28-EE	Nivel Alto	-	
4. Información y comunicación							
P18	Canales de información y reportes	Analizar los reportes, formatos, informes del mes, etc.	Posibles pérdidas de información confidencial producto de robo de información generado por puertos USB y lectora de CD/DVD habilitados	2-OS	Nivel Alto	De la revisión a los servicios que presta la Mesa de Ayuda, según Directiva de uso de Mesa de Ayuda, se evidencia dos niveles de servicio adecuadamente identificados.	D:\1. Papeles de trabajo\CLA-AIP-2015-001\2. Ejecución\2.4. Información y Comunicación\P18
P19	Uso de información y de sistemas de información	Ver las políticas respecto al uso de la información	Ausencia de copias de seguridad a activos de información que son de alto interés para CRAC Los Andes.	28-EE	Nivel Alto	-	
5. Supervisión							
P20	Identificación y evaluación de cambios relevantes.	Encuestas a usuarios, revisión de incidentes, escenarios, etc.	Se tiene el riesgo de tener cambios inusuales que provoque errores del sistema ocasionando una pérdida de tiempo, financiera y conflictos en el trabajo cotidiano.	1-TI	Nivel Alto	No se han desarrollado procedimientos de revisión de estos Logs (registro de acceso de sistemas), que permitan identificar eventos inusuales o accesos no autorizados	D:\1. Papeles de trabajo\CLA-AIP-2015-001\2. Ejecución\2.5. Monitoreo\P20
P21	Monitoreo del rendimiento del Oficial	Entrevistas con el oficial y gerentes responsables	Posibilidad de fraudes al contratar personal de bajos valores éticos al no existir controles formales de verificación de antecedentes.	30-EE	Nivel Medio		

Continúa…

ANEXO 6: SEGUIMIENTO DE OBSERVACIONES

N	Nro. Informe	Nombre de Informe	Título de la Observación	Detalle de la Observación	Observación	Comentarios		Responsable
						AUI	Área Auditada	
1	INFORME N° 046-2014	N° 046-2014 / INFORME GESTION DE RIESGOS DE TI	No se ha realizado la capacitación que se planificó y presupuestó para el personal de TI.	De la revisión realizada al PETI y al programa de capacitación anual, se evidenció que no se ha realizado la ejecución de la capacitación programada y presupuestada para el personal de la Gerencia de TI.	(A/E/I) Atrasada	Se mantendrá la observación en atrasado hasta que evidencien las capacitaciones.	Se ha cumplido en Remitir los programas de Capacitación propuestos por la Gerencia de TI, sin embargo, no se ha dado su Aprobación ni ejecución. Por otro lado, para la elaboración de Plan de Capacitaciones se tendrá en consideración la Implementación del Core Financiero debido a que se dará el uso de nuevas tecnologías, por lo que se considerarán como tema de capacitaciones los aspectos que se consideren necesarios para poder tener un desempeño adecuado para la Implementación del Core Financiero	Gerencia de tecnología de información
2	INFORME N° 046-2014	N° 046-2014 / INFORME GESTION DE RIESGOS DE TI	Falta la conciliación del inventario de TI con el inventario contable de Logística	De la revisión realizada al Inventario de Hardware y la entrevista con el Jefe de la Unidad de Soporte, Infraestructura y Comunicaciones, se pudo evidenciar que durante el 2014 se realizó el inventario físico de los equipos de cómputo desplegados en la Oficina Principal y la Red de Agencias de la Caja Los Andes. Sin embargo, aún no se ha realizado la respectiva conciliación con los registros contables, para efectos, de determinar la valorización de estos inventarios.	(A/E/I) En proceso	Debido a la información revisada aceptamos la ampliación de plazo a octubre del 2015	En coordinación con la Unidad de Logística se realizará una conciliación con el Inventario de TI para tal fin se adjunta el Cronograma del Plan del Conciliación, adicionalmente el control del Monitoreo del Inventario actualizado se ejecutará con las Visitas a las Oficinas y PACs programadas, con la Actividad de "Verificación de Inventario de las Oficinas de la CRAC LASA" en el Cronograma, en donde se realizará la verificación del Inventario de Tecnologías de Información, cumpliendo con el tema de actualización del Inventario de Activos de T.I,	Gerencia de tecnología de información
3	INFORME N° 50-2014	N° 050-2014 / EVALUACION DE LOS	No se tiene implementado la transferencia	De la revisión al Centro de Computo Alterno – CCA, y a la configuración de replicación de datos, se identificó que se	(A/E/I) En proceso	Actividades en proceso	En relación a la observación, es correcto lo vertido por el Jefe de Gestión de Sistemas, ya que nuestros gestores de base de datos (Pervasive SQL) presenta limitaciones como	Gerencia de tecnología de información

N	Nro. Informe	Nombre de Informe	Título de la Observación	Detalle de la Observación	Observación	Comentarios		Responsable
						AUI	Área Auditada	
		SISTEMAS DE GESTION DE SEGURIDAD DE LA INFORMACIÓN Y GESTION DE CONTINUIDAD DEL NEGOCIO	automática de la información registrada en el CCA en Contingencia, cuando luego de un siniestro, se reactiva el CCP.	tiene activada la replicación de ida, del CPP al CCA con intervalos de 10 minutos, sin embargo, no se tiene implementado la replicación de regreso. Es decir, si el CCA es activado en contingencia, la información ingresada durante ese periodo, no puede ser replicada de manera automática al CCP.			la réplica automática de datos en dos vías, es por ello que contemplando estas limitaciones se viene desarrollando el proyecto de implementación del proyecto CORE.	
4	INFORME N° 50-2014	N° 050-2014 / EVALUACION DE LOS SISTEMAS DE GESTION DE SEGURIDAD DE LA INFORMACIÓN Y GESTION DE CONTINUIDAD DEL NEGOCIO	Existen diferentes sistemas que manejan de manera independiente la seguridad de acceso. Con diferentes criterios básicos de complejidad al definir las claves	De lo revisado a la documentación de los Sistemas de Información y la entrevista con el Jefe de Desarrollo, se determinó que cada sistema tiene su propio catálogo de usuarios, es decir, cuando ingresa una persona a laborar a la Caja, se crea su usuario en cada sistema. Asimismo, no se tiene una política de claves que establezca un estándar de robustez de las claves, referente tanto en la longitud (número de caracteres) como de complejidad (sólo dígitos, combinación de dígitos con caracteres, uso de caracteres especiales, etc.), frecuencia de cambio, repetición de claves históricas y número de intentos permitidos.	(A/E/I) En proceso	La Gerencia de Riesgos procedió a actualizar la Política General de Seguridad de Información en la cual contempla en su Art. 6 Políticas de Seguridad Lógica inciso "e. Los sistemas y aplicaciones deberán contar en la medida posible con mecanismos que exijan al usuario a utilizar contraseñas cuya composición sea compleja usando una combinación de letras números y caracteres alfanuméricos, así como de exigir su regular actualización." Se adjunta la política vigente como Anexo N°2.1 Así mismo para otorgar viabilidad a esta disposición la Gerencia de TI informo	La Gerencia de Riesgos procedió a actualizar la Política General de Seguridad de Información en la cual contempla en su Art. 6 Políticas de Seguridad Lógica inciso "e. Los sistemas y aplicaciones deberán contar en la medida posible con mecanismos que exijan al usuario a utilizar contraseñas cuya composición sea compleja usando una combinación de letras números y caracteres alfanuméricos, así como de exigir su regular actualización." Se adjunta la política vigente como Anexo N°2.1 Así mismo para otorgar viabilidad a esta disposición la Gerencia de TI informo mediante Informe N°004-2015-CRACLASA/GTI/HICA, indico que es viable mediante la implementación del Directorio Activo más únicamente para con los sistemas internos de CRAC Los Andes. Así mismo la implementación del Directorio Activo se encuentra programada dentro del plan de actividades del proyecto CORE en fecha 30/06/2015, tanto el informe como la planificación se encuentran adjuntos al presente como Anexo N°2.2. Considérese que la implementación de este Directorio	Gerencia de Riesgos

Continúa…

N	Nro. Informe	Nombre de Informe	Título de la Observación	Detalle de la Observación	Observación	Comentarios		Responsable
						AUI	Área Auditada	
						mediante Informe N°004-2015-CRACLASA/GTI/HICA, indico que es viable la implementación del Directorio Activo para con los sistemas internos de Los Andes.	Activo estará en función a la planificación y ejecución del proyecto Core y estando bajo responsabilidad de la Gerencia de TI se encuentra pendiente en proceso.	
11	CONTROL INTERNO 2014 REA-2DA VISITA	CONTROL INTERNO 2014 REA-2DA VISITA	Vulnerabilidad de la aplicación SIFCNET del Core financiero por su naturaleza y dependencia funcional de un solo proveedor.	Vulnerabilidad de la aplicación SIFCNET del Core financiero por su naturaleza y dependencia funcional de un solo proveedor.	(A/E/I) En proceso	Se ha iniciado con el proyecto Core financiero	Actualmente Caja los Andes se encuentra en un proceso de migración de Core financiero, cuya planificación estratégica se encuentra en el Plan Estratégico de Tecnólogas de Información 2013-2015 como "Implantación del Nuevo Core Financiero COREBANK", el objetivo principal es ser la Herramienta estratégica que permitirá automatizar gran parte de las operaciones que en la actualidad se realizan manualmente, ahorrando tiempo y su vez brindando información más oportuna, así como mejorar los controles y las comunicaciones para una atención eficiente y efectiva a los clientes. Cabe mencionar que la duración de este proyecto es de un año, habiéndose iniciado en el mes de febrero 2015.	Gerencia de tecnología de información

ANEXO 7: INFORME DE AUDITORÍA

INFORME	EVALUACIÓN DE LA ADMINISTRACIÓN DE LA SEGURIDAD DE INFORMACIÓN E INFRAESTRUCTURA.

Fecha Informe	30/12/2016

Dirigido a: **Comité de Auditoría**
Presidente del Comité de Auditoría

Distribución: **Gerencia General**
Gerente de Riesgos
Gerencia de Tecnología de Información

PAA: CLA-AIP-62-2016	**FECHA DE INICIO:**	13/12/2016	**FECHA DE TÉRMINO:**	30/12/2016

I. ANTECEDENTES

El origen de la presente actividad se realiza en cumplimiento del Plan Anual de Trabajo del Año 2016 de la Gerencia de Auditoría Interna.

La última evaluación efectuada por el área de Auditoría Interna, sobre Evaluación de: la Gestión de Seguridad de Información, fue en el informe CLA-AIP-073-2015 evaluación de los sistemas de gestión de seguridad de la información y gestión de continuidad del negocio.

Periodo	Diciembre 2015
Calificación	Sin calificación

II. OBJETIVOS, PERIODO Y ALCANCE

OBJETIVOS:

Efectuar la revisión de auditoría basada en el cumplimiento de las normas emitidas por la Superintendencia de Banca, Seguros y AFP, la norma G 140-2009 “Gestión de la Seguridad de Información”, así como la identificación de brechas y generación de recomendaciones.

PERIODO:
Información al cierre de octubre 2016.

ALCANCE

La evaluación se realizó sobre la base de la estructura de Control Interno de COSO, que incluye los cinco componentes básicos de control interno: ambiente de control, evaluación del riesgo, actividades de control, información y comunicación y monitoreo.

A. Ambiente de control
   1. Estructura Organizacional
   2. Las responsabilidades asignadas al Directorio, a la Gerencia referidas y al oficial de seguridad.
   3. Relaciones Jerárquicas
   4. Modelos de gestión y mecanismos para control de Seguridad de Información
   5. Nivel académico, Experiencia y Capacitación
   6. Proveedores de Servicio

B. Evaluación de riesgos
   1. Plan de seguridad del Oficial de seguridad de información
   2. Operación de la seguridad.
   3. Categorización de incidentes de seguridad de información
   4. Seguridad física y del entorno
   5. Seguridad de equipos.

C. Actividades de control
   1. Clasificación, respaldo y control de activos
   2. Control de seguridad del Host - series
   3. Control de seguridad de Bases de Datos
   4. Control de seguridad en Redes y Comunicaciones.
   5. Control de seguridad en Plataforma de Usuarios
   6. Control de seguridad en el Directorio Activo

D. Información y comunicación
   1. Canales de información y reportes
   2. Uso de información y de sistemas de información.

E. Monitoreo
   1. Identificación y evaluación de cambios relevantes.
   2. Monitoreo del rendimiento del Oficial.

En cumplimiento del Plan Anual de Auditoría, el personal de la Gerencia de Auditoría Interna realizó la presente evaluación basada en la Normas Internacionales ISO 27002 de la seguridad de información para el Ejercicio profesional de auditor de tecnología de información y oficial de seguridad de información.

III. DESCRIPCION DE LAS ACTIVIDADES DE AUDITORÍA

Durante la auditoría se desarrollaron las siguientes actividades:

- ✓ Reuniones de apertura y entendimiento del proceso.
- ✓ Revisión y lectura de políticas, normas y procedimientos externos e internos.
- ✓ Análisis de la información.
- ✓ Pruebas técnicas y confirmación de los procedimientos aplicados.

IV. EQUIPO QUE REALIZÓ LA AUDITORÍA	Max Puma – Auditor Junior de TI

V. CONCLUSIÓN	ACEPTABLE

De la revisión al cumplimiento de las normas SBS G 140-2009 “Gestión de la Seguridad de Información” se ha identificado que la documentación asociada al Sistema de Gestión de Seguridad de Información se encuentra razonablemente elaborada; sin embargo, la metodología de Gestión de Riesgos de Seguridad de la Información no se aplica en la práctica.

La estructura organizacional identificada en el Sistema de Gestión de la Seguridad de la Información de la Caja Los Andes se encuentra adecuadamente identificada; sin embargo, la Gerencia de Riesgos a través del Oficial de Seguridad de Información y Continuidad del Negocio no ha logrado impulsar la implementación del SGSI, toda vez que no se ha identificado los controles al respecto en la matriz de riesgos asociada.

VI. RESULTADO DE LA REVISIÓN

OBSERVACIÓN N° 01	R	RECOMENDACIONES	PLAN DE ACCIÓN
Título: Se carece de políticas para la gestión de las contraseñas del súper usuario del mismo modo con respecto a la identificación de sus roles de administradores de servicios incidiendo en la seguridad del despliegue de los mismos		La Oficial de Seguridad deberá disponer se revisen, elaboren, implementen y monitoreen las Políticas de Seguridad de Información de la Caja asociadas a las responsabilidades, tenencia, modificación y conocimiento de las contraseñas del supe usuario (usuarios especiales que proveen los servicios de Tecnologías de Información). Asimismo, se deberá identificar los roles de dichos súper usuarios y sus accesos a los servicios que proveerá con la implementación del proyecto Data Center.	Proponer a la Gerencia General y posterior aprobación de Directorio la función de otorgamiento de acceso a los sistemas de información.
De la revisión a la Política General de Seguridad de la Información aprobado por Sesión de Directorio Nº 240- 2015, de fecha 27-08-2015, se identifica que el numeral 6. Políticas de Seguridad Lógica señala una relación de políticas las cuales básicamente están asociadas al usuario, obviando aquellas referidas al súper usuario (usuarios especiales que proveen los servicios de tecnologías de información), como identificación de sus roles (administradores de servicios), y la gestión de las contraseñas asociadas a dichos roles (resguardo, tenencia, cambios, etc.). Se ha evidenciado dos sobres cerrados, cada uno con la denominación del equipo servidor crítico de la Caja, los mismos que según señala el Gerente de Tecnologías de Información tienen la contraseña del servidor asociado; asimismo, se ha evidenciado que los sobres se conservan en un mueble de la oficina de la Gerencia de TI, siendo vulnerables a perdidas. No se ha identificado alguna referencia si dichos sobres resguardan la contraseña del Administrador de la Base de Datos. Por lo demás, es necesario recalcar que los roles de súper usuarios, basado en la próxima implementación del Proyecto Data Center, no deben ser reactivos pues se dispondrá de servicios TI adicionales.			**Responsable:** Oficial de Seguridad Gerencia de TI **Fecha Compromiso:** **20/05/2017**
Riesgo Asociado: Se corre el riesgo potencial de que los servicios de Tecnología de la Información de la Caja queden bloqueados en todas sus operaciones debido a situaciones involuntarias o voluntarias de los poseedores de las contraseñas de estos servicios, toda vez que no podrían acceder al sistema institucional, al no haberse enfocado en forma eficiente las responsabilidades, tenencia, modificación y conocimiento de las contraseñas de los súper usuarios.			

OBSERVACIÓN N° 02	R	RECOMENDACIONES	PLAN DE ACCIÓN
Título: El servicio de Mesa de Ayuda se encuentra ceñido a las incidencias y/o requerimientos que se reportan actualmente, pudiendo ser proactivo con respecto a facilitar en línea dichas incidencias a Riesgos; así como, identificando desde ya el nivel de servicio.		La Gerencia General deberá disponer que las gerencias competentes actualicen e implementen las políticas y procedimientos de la Directiva de Mesa de Ayuda, alineados a fortalecer dicho servicio aportando ágilmente en la gestión de riesgos.	Elaboración de Procedimientos donde se contempla sobre el manejo de incidencias del servicio de mesa de ayuda.
De la revisión a los servicios que presta la Mesa de Ayuda, según Directiva de Uso del Sistema de Mesa de Ayuda aprobado por Sesión de Directorio Nº 204-2013 de fecha 19 de junio del 2013, se evidencia dos niveles de servicio adecuadamente identificados, los mismos que no necesariamente aplican debido a la herramienta software actualmente en producción. Asimismo, se evidencia que la Base de Datos de Mesa de Ayuda actual registra requerimientos, entre otro tipo de atenciones, por lo que el alcance de la misma se ha flexibilizado, teniendo que determinar otros canales de atención, actualizando dicho servicio. Por otro lado, los registros que contiene la base de datos de mesa de ayuda, pudieran servir de insumo para la gestión de riesgos, la que de hecho es emitida a la Unidad de Riesgos, pero no en línea. Cabe señalar que de cara a las pruebas integrales se debe establecer un oportuno y adecuado seguimiento y solución de las incidencias que se van a producir, por lo que, además, por temas de concientización, se deben aplicar efectivamente las políticas de uso a actualizar de dicha Mesa de Ayuda.			**Responsable:** Gerencia General Gerencia de TI Oficial de Seguridad **Fecha Compromiso:** 20/05/2017
Riesgo Asociado: El riesgo de que las incidencias maduren y lleguen a ser amenazas siempre en cuando no lo tomen en consideración.			

OBSERVACIÓN N° 03	R	RECOMENDACIONES	PLAN DE ACCIÓN
Título: Los recursos de tecnologías de información que se dispone tanto para acceso al internet como del servicio de correo, no se encuentran identificados de acuerdo a niveles según prioridad y/o necesidades del usuario.		La Gerencia de Tecnologías de Información en coordinación con el Comité de Continuidad y Seguridad de la Información deberán establecer los lineamientos a fin se determine acertadamente los niveles de acceso y uso de los recursos disponibles en los servicios de Internet y Correo Electrónico, redundando en la fluidez de la red de la Caja Los Andes.	Proponer los lineamientos y los niveles de acceso en las políticas de seguridad respecto al uso del correo electrónico e internet.
De la revisión a la Directiva para Uso del Servicio de Internet aprobado en Sesión de Directorio Nº 195-2012 de fecha 28 de Setiembre del 2012 Acuerdo Nº 1929, se identifica que el propósito del mismo es "gestionar de manera adecuada el acceso al servicio del Internet"; sin embargo, no señala las reglas específicas de acceso basado en Niveles de acuerdo a perfiles (prioridad y/o necesidad del usuario) con fines de alinearse a las mismas. De la revisión a la Directiva para Uso del Servicio del Correo Electrónico aprobado en Sesión de Directorio Nº 200-2013 de fecha 28 de febrero del 2013, se identifica que una de las finalidades es "Regular el uso"; sin embargo, no señala los niveles y Reglas (permite otros dominios, peso de correo, peso de adjunto, cantidad de adjuntos, etc.) de los recursos que puede disponer el usuario. Ambos servicios están asociados al adecuado uso de los recursos de tecnologías de información			**Responsable:** Gerencia de TI Oficial de Seguridad **Fecha Compromiso:** 20/05/2017
Riesgo Asociado: La implementación de dichos niveles se desarrolla en la práctica, pero el que lo aplica se encuentra insubordinado a reglas. Saturación en la red por inadecuada aplicación de los recursos de Internet y/o Correo.			

OBSERVACIÓN N° 04	R	RECOMENDACIONES	PLAN DE ACCIÓN
Título: El Inventario de Activos de información no integra adecuadamente los activos críticos de la Caja Los Andes		La Gerencia General deberá disponer que las Gerencia competentes en coordinación con el Oficial de Seguridad de Información establezcan una revisión integral del Inventario de Activos de Información, basada en una identificación certera del tipo de activo, actualizando la metodología de la gestión de activos de información.	Reorganizar el inventario de activos de información de la caja y clasificarlos según criticadas.
Entre los activos de información críticos de la Caja están: • Los sistemas en producción ANDES Bank • Los documentos digitales y físicos asociados a la Continuidad del Negocio (Plan de Crisis, Plan de Contingencias, entre otros.) El sistema de producción ANDES Bank en el inventario de Activos de información están identificados entre otros como software, cuyo propietario es la Gerencia de Tecnologías de Información. Si bien es cierto que el Producto por presentar reiteradas incidencias, su base de datos es sometida a revisiones y soluciones por parte de la Unidad de Gestión de Sistemas y Aplicaciones que pertenece a la Gerencia de Tecnologías de Información, éstos no son los dueños del proceso que genera dichas incidencias, por lo tanto, No es propietario del Producto. Así como el presente contexto, es necesario analizar otros activos, de acuerdo a su tipo y aplicación en la Caja. Los documentos digitales y físicos asociados a la Continuidad del Negocio no se encuentran identificados en el Inventario de activos de información.			**Responsable:** Gerencia de TI Oficial de Seguridad **Fecha Compromiso:** 20/04/2017
Riesgo Asociado: Ausencia de copias de seguridad a activos de información que son de alto interés para CRAC Los Andes de acuerdo a la clasificación de activos.			

OBSERVACIÓN N° 05	R	RECOMENDACIONES	PLAN DE ACCIÓN
Título: Existen gerentes y asesores que utilizan Laptops de la Caja o personales con información confidencial y restringida, sin embargo, no poseen controles frente a robos o pérdida		Una alternativa podría ser el encriptado del disco duro o la información Confidencial y Restringida no sea copiada en las Laptops.	Las informaciones serán evaluados acorde al nivel de riesgo al que se exponen y se aplicarán los controles pertinentes
No se tiene controles para proteger la información que contienen estos equipos, frente al riesgo de robo o pérdida de los mismos.			**Responsable:** Gerencia de TI Oficial de Seguridad **Fecha Compromiso:** 20/06/2017
Riesgo Asociado: Riesgo de perder información crítica de los clientes y actividades de la organización.			

OBSERVACIÓN N° 06	R	RECOMENDACIONES	PLAN DE ACCIÓN
Título: Falta realizar revisiones sobre accesos no autorizados a la red y a los sistemas y al firewall. Esta actividad debe ser realizada por SI tampoco se ha realizado el Monitoreo de algunos controles de seguridad de información.		Que la Gerencia de Riegos, establezca e implemente un procedimiento de monitoreo que debe ser realizado por el Oficial de SI	- Desarrollar el procedimiento de monitoreo. - Desarrollar el procedimiento para el otorgamiento de accesos remotos. - Evaluar la asignación de usuarios y perfiles a los sistemas.
No se han desarrollado procedimientos de revisión de estos Logs (registro de acceso de sistemas), que permitan identificar eventos inusuales o accesos no autorizados La finalidad es asegurar la eficacia y eficiencia de estos controles y detectar vulnerabilidades o actividades no autorizadas.			**Responsable:** Gerencia de TI Oficial de Seguridad **Fecha Compromiso:** 20/06/2017
Riesgo Asociado: Se tiene el riesgo de tener cambios inusuales que provoque errores del sistema ocasionando una pérdida de tiempo, financiera y conflictos en el trabajo cotidiano de la organización.			

ANEXO 8: ACTAS DE ENTREVISTAS

A. ACTA DE ENTREVISTA 01

Declara lo siguiente:

Riesgo Operacional

- Con respecto a la gestión de eventos de perdida de parte del usuario se cuenta con un sistema de incentivos monetarios y no monetarios "Metodología de aplicación de Incentivos por contribuir a la Gestión de Riesgo Operacional" y "Procedimiento para la aplicación de incentivos monetarios y no monetarios".
- Se cuenta con Manual de gestión de incidentes y eventos de perdida.
- Desde el 19 de Setiembre del presente año se ha determinado un conjunto de cuentas contables con la participación de Riesgos y Contabilidad, con fines de asociarlo al tipo de evento.
- Todavía no se ha determinado el tiempo que lleva desde la confirmación del evento de pérdida, hasta su conciliación contable.
- Existe 2 comités exclusivos para riesgo Operacional (comité Táctico y Comité Gerencial), ambos comités cuentas con su respectivo reglamento.
- Los controles identificados no cuentan con código, los mismos están asociados directamente al riesgo definido.
- Los talleres de identificación de riesgos por procesos se encuentran en proceso de maduración.
- El SOGRO se encuentra inoperativo. Se han hecho las coordinaciones para su puesta en producción, pero a la fecha aún no aplica.
- Las matrices (señalar cuales) que se aplican a la fecha se encuentran en proceso de maduración.

Seguridad de la Información

- Con respecto a la integridad de la Base de datos del CORE en producción a la fecha no se han revelado incidencias de integridad, sino más bien de conectividad y funcionales (ej.: Voucher en blanco).
- Todavía no se ha considerado la evaluación de riesgos asociadas al pre lanzamiento y lanzamiento del nuevo CORE. Los riesgos identificados, al respecto básicamente están referidos a las "evaluaciones a los acuerdos contractuales establecidos entre la entidad", "evaluación a los principales requerimientos de los macro procesos" y "evaluación de nivel de cumplimiento de la etapa de Requerimientos".
- Todavía no se ha aplicado una revisión del inventario de Activos de información,

Continuidad del Negocio

- Con respecto a la información asociada a continuidad, la misma se encuentra toda en forma electrónica; a excepción del Plan de Recuperación de Desastres de Tecnología de Información ubicado en el Centro de Datos Alterno.
- Se cuenta con procedimientos de continuidad para la atención a clientes mediante recibos provisionales; sin embargo no se encuentra vigente y falta actualizar.

B. ACTA DE ENTREVISTA 02

Declara lo siguiente:

Con fines de gestionar adecuadamente la mesa de ayuda, se aplica el Software libre ITOP. Se aplica desde hace 3 meses, la anterior no se acondicionaba a nuestras necesidades. (PT.- print screen)

Actualmente el Usuario registra su requerimiento. En caso de carecer de corriente eléctrica en ese momento, llaman por teléfono y se registra por mesa de ayuda. Dicho ITOP permite registrar incidentes, mide tiempos de atención, entre otros.

Si, ha habido casos que se ha atendido requerimiento de Gerencias, de información correspondiente a otros procesos del negocio, pero estos requerimientos son escalados al nivel superior y autorizados vía correo electrónico.

Con fines de prevenir fuga de información, control de dispositivos; así como, de infecciones se ha renovado la licencia de Sophos por dos años más, pues contempla dichos mecanismo. (PT)
A la fecha no se aplicado ethical hacking (pruebas de vulnerabilidades), debido a que se está por implementar nuevo firewall. Si se han aplicado pruebas básicas de verificación de intrusiones. (PT)
Con respecto a los niveles de acceso al Internet definido por la Caja, considero que se van implementar las mismas políticas en la nueva infraestructura; sin embargo, las mismas falta formalizarlas.
La red de la entidad en la sede principal se encuentra organizada y estructurada, debido a que las instalaciones son nuevas y se contó con las previsiones de caso. En la sede de Juliaca la estructura de la red se encuentra interconectada a través de una VPN y una proxy con una salida a internet (señalar como se encuentra la distribución de la red de Juliaca).
No se cuenta con servicio de active directory. Las altas y bajas de usuarios actualmente se basan en 2 procedimientos. Se encuentra encaminada la adquisición de dicho servicio. (PT del proyecto Sala de Datos).

Con respecto a las contraseñas de los servidores que administro, aplico normalmente el de mi usuario personal, por mis actividades del día a día. La contraseña del usuario administrador se conserva en sobre cerrado, es de uso esporádico, la última vez que lo utilice fue el 25 de noviembre para paramétricas y configurar los servicios.

El monitoreo que se aplica actualmente a la operatividad de los sistemas va por la revisión de espacio en disco, utilización de CPU, etc. Es un proceso manual y de verificación regular.

Se cuenta con 2 UPS conectado a generador de contingencia manual.

ANEXO 9: ENCUESTA REALIZADA

Pregunta	Texto de la pregunta	Texto de la respuesta	Porcentaje	Numero
Pregunta 01	¿Está de acuerdo con los derechos de acceso a la Red institucional que se le ha asignado para el cumplimiento de sus labores?	SI	92%	118
		NO	8%	118
Pregunta 02	En su presente cargo, ¿cuántas veces ha identificado cambios en alguno de los procedimientos que aplica?	0	25%	118
		1	18%	118
		2	19%	118
		3	8%	118
		Muchas	31%	118
Pregunta 03	De ser “0” la respuesta anterior, ¿considera que debe haber alguna mejora en dichos procedimientos?	SI	61%	118
		NO	21%	118
Pregunta 04	Enumere alguno de los riesgos a los que está expuesto en su puesto de trabajo:	Procesos internos (de captaciones o colocaciones) inconsistentes	23%	118
		Sistema con errores	54%	118
		Paralizaciones del sistema	58%	118
		Compañeros que no conocen su trabajo	19%	118
		Compañeros que incurren en comportamientos inadecuados	15%	118
Pregunta 05	Que incidencia es más usual en su puesto de trabajo:	Interrupción en la comunicación	65%	118
		Corte de energía eléctrica (Apagón)	47%	118
Pregunta 06	Indique el tiempo máximo perdido en minutos. En caso de interrupción en la comunicación o Apagón	15 min	25%	118
		30 min	36%	118
		60 min	14%	118
		90 min	6%	118
		120 min	3%	118
		Más de 120 min	10%	118
		Menos de 15 min	5%	118
Pregunta 07	En caso de interrupción de sus funciones mayor a 30 min. Debido a causas externas ¿cómo procede?	Espera	20%	118
		Aplica procedimientos contingentes	31%	118
		Reporta la incidencia.	40%	118
		Otros	25%	118

Pregunta	Texto de la pregunta	Texto de la respuesta	Porcentaje	Numero
Pregunta 08	¿Ha sido capacitado en Temas de Continuidad de Negocio?	SI	81%	118
		NO	16%	118
Pregunta 09	¿Ha sido capacitado en Temas de Seguridad de Información?	SI	89%	118
		NO	9%	118
Pregunta 10	¿Ha sido capacitado en Temas de Gestión de Riesgos Operacionales?	SI	93%	118
		NO	5%	118
Pregunta 11	¿Se le ha evaluado en el desempeño de sus funciones?	SI	81%	118
		NO	16%	118
Pregunta 12	¿Ha participado en pruebas de continuidad del negocio?	SI	62%	118
		NO	36%	118
		Ninguno	7%	118
Pregunta 13	Considera que la atención del servicio de TI solicitado es:	Muy bueno	2%	118
		Bueno	42%	118
		Regular	52%	118
		Malo	4%	118
		Muy malo	0%	118