UNIVERSIDAD DE COSTA RICA
SISTEMA DE ESTUDIOS DE POSGRADO

EVALUACION Y PROPUESTA DE LAS POLITICAS DE SEGURIDAD DE TECNOLOGIAS DE INFORMACION BASADO EN EL MODELO DE NEGOCIOS PARA LA SEGURIDAD DE LA INFORMACION (BMIS)

Trabajo Final de Graduación sometido a la consideración de la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas para optar al grado y título de Maestría Profesional en Auditoría de Tecnologías de Información

RODOLFO CARRIÓN CORONAS

Ciudad Universitaria Rodrigo Facio, Costa Rica
2013

DEDICATORIA

A Dios, por permitirme obtener este logro en mi vida profesional, Él sabe lo he pasado y la razón de la toma de esta decisión, a mi padre Álvaro (q.e.d) que sé que este logro lo hubiera llenado de felicidad y orgullo, a mi madre Olga que me ha apoyado durante todo este recorrido, a mi hermana Sylvia, que también me apoyado incondicionalmente y a mi hermano Gustavo, que sé que está ahí.

AGRADECIMIENTOS

A Xiomar Delgado Rojas, precursor y director de esta maestría, quien con su empeño y dedicación ha logrado que un campo tan especializado como el de la Auditoría de Tecnologías de Información tenga una maestría que nos permita seguir creciendo como profesionales.

A todos los profesores que nos dieron lecciones siempre les agradeceré la dedicación por enseñarnos.

"Este trabajo final de investigación aplicada fue aceptado por la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas de la Universidad de Costa Rica, como requisito parcial para optar por el grado y Título de Maestría Profesional en Auditoría en Tecnologías de Información."

_____

Dr. Sergio Guido Espinoza
Profesor Guía

_____

MBA. Álvaro Gerardo Jaikel Chacón
Lector (Profesor de Posgrado)

_____

MBA Ginette González Espinoza
Lectora de Empresa

_____

Dr. Aníbal Barquero Chacón
Director Programa de Posgrado en Administración y Dirección de Empresas

_____

Rodolfo Carrión Coronas
Sustentante

Tabla de contenido

“RESUMEN”

Esta práctica profesional se fundamentada en el análisis a una entidad financiera de la Seguridad de la Información, basado en el Modelo de Negocios para la Seguridad de la Información (BMIS) propuesto por ISACA.

El modelo propone el análisis de la Seguridad de la Información desde cuatro elementos (Organización, Procesos, Tecnología y Personas) y seis Interconexiones dinámicas (Gobierno, Arquitectura, Habilitación y Soporte, Factores Humanos, Emergentes y Cultura) con la finalidad de permitir un análisis holístico de la Seguridad de la Información que identifique riesgos y oportunidades de mejora que de otra forma no se conseguirían observar y poder proveer de soluciones eficientes y efectivas que abarquen de forma integral la gestión de la Seguridad de la Información de la entidad.

La finalidad de la práctica profesional es la propuesta de las políticas de Seguridad de la Información de alto nivel que permita direccionar a la entidad financiera en la puesta en práctica de las medidas de Seguridad necesarias basados en sus requerimientos, tanto a nivel normativo como a nivel organizacional, sin embargo, los análisis realizados muestran la gran cantidad de beneficios que se obtienen a partir de los mismos y que apoyarán a la entidad en un examen exhaustivo se la seguridad de la información.

Para lograr la propuesta se siguió la metodología del BMIS consistente básicamente en la identificación de los requerimientos, las soluciones existentes y un análisis de la brecha que implica lo que tenemos hoy y lo que se necesita para lograr el cumplimiento de los requerimientos. Como se mostrará en las tablas del trabajo el análisis permite el estudio de los elementos y sus relaciones de forma aislada pero a la vez integral de sus relaciones permitiendo un análisis más profundo de las diversas situaciones de la Seguridad de la Información.

El lector encontrará una serie de “mapeos” que apoyan y facilitan la identificación y el análisis de los elementos con las interrelaciones de las conexiones dinámicas del BMIS los cuales se constituyen en la base para un análisis holístico.

Lista de Tablas

Lista de Figuras

Lista de Abreviaturas

- BMIS – El modelo de negocio para la Seguridad de la Información
- COBIT 4.1 - Control Objectives for Information and Related Technology (Objetivos de control para la información y Tecnologías relacionadas), Versión 4.1
- DI – DIs – Interconexiones Dinámicas
- ISACA - *Information Systems Audit and Control Association* (Asociación de Auditoría y Control de Sistemas de Información),
- SUGEF - Superintendencia General de Entidades Financieras
- TI – Tecnologías de Información
- TIC – Tecnologías de Información y Comunicación

Introducción

La presente práctica profesional se realizó en una entidad financiera que por razones de confidencialidad no se puede mencionar su nombre.

La necesidad de una adecuada seguridad de la Información ha venido incrementándose paulatinamente a niveles exponenciales debido al crecimiento de la tecnología de la Información y Comunicación (TIC) por lo que se ha hecho imprescindible contar con directrices que generan una adecuada gestión de la Seguridad de la Información.

Las entidades financieras se encuentran actualmente en un proceso en donde las transacciones se realizan en línea y los volúmenes de información son significativos, hoy en día se observa como cada vez más se hace necesario tener presencia en la nube y en un futuro no muy lejano prácticamente será ubicuo el tener en los teléfonos inteligentes (smarthphones) las aplicaciones necesarias para realizar prácticamente cualquier transacción.

La cantidad de dispositivos de almacenamiento de la información que se adquieren por bajos precios y/o almacenamiento en la nube, permiten la transferencia de grandes volúmenes de datos que pueden ser, y de hecho lo son, una amenaza constante a la seguridad de la información por lo que la regulación en este sentido se vuelve un requisito necesario en las institución, mucho más cuando se trata de una institución financiera que mantiene información sensitiva de muchas organizaciones.

La creciente regulación en Costa Rica en materia de Tecnología de Información y Comunicación (TIC) y específicamente en seguridad de información es una realidad que ha tomado por sorpresa a muchas entidades bancarias las cuales no han respondido a tiempo a los requerimientos regulatorios, entre otros, debido a la falta de personal capacitado sobre todo en las entidades financieras medianas y pequeñas.

En el presente trabajo se realizó una evaluación de las políticas sobre seguridad de TIC basado en el Modelo de Negocios para la Seguridad de la Información (BMIS), este modelo constituye una forma de incorporar la seguridad de la información en las empresas de manera integral y está constituido por cuatro elementos (Organización, Procesos, Personas y Tecnología) y 6 Interconexiones Dinámicas (DIs) (Gobierno, Cultura, Arquitectura, Recurso Humano, Emergentes y Habilitación y Soporte). Cada uno de los elementos y DIs se correlacionan entre si y, el estudio de cada una de ellas proporciona una modelo de análisis de la problemática de la seguridad de la información.

El uso de este modelo pretende ofrecer un marco de acción que permite realizar un análisis integral de los elementos que forman la seguridad de la información, buscando encontrar un equilibrio entre la protección de los activos de la información y el negocio.

EL BMIS, al ser un modelo, presenta características que deben ser tomadas en cuenta en el momento en que se definen los requerimientos del negocio en cuanto a la necesidad de la seguridad de la información y que son, o deberían ser, dirigidas por las políticas de la empresa en esta materia.

En la actualidad no se conoce ningún estudio aplicado a una empresa que tome en consideración este modelo debido a que el mismo es muy reciente por lo cual aportará un primer acercamiento a un desarrollo de políticas de seguridad de la información que pretende incorporar en la empresa un enfoque integral de los diversos componentes que lo conforman y como lo propone el BMIS.

La finalidad del trabajo consiste en realizar una evaluación de las políticas actuales sobre seguridad de la información en la entidad financiera, basado en las características que propone el modelo BMIS con la finalidad de proponer mejoras para el gobierno de la seguridad de la información y que dichas mejoras serán presentadas ante las autoridades de la entidad financiera con el fin de su aprobación y de su implementación.

Desde el punto de vista de intereses profesionales esta práctica profesional proporcionará un conjunto de políticas generales que permitirán dirigir un buen gobierno de la seguridad de la información actualizado con las últimas tendencias en materia de Seguridad de la Información las cuales podrán servir, una vez terminado el trabajo, como un conjunto de directrices que pueden ser implementadas mediante marcos de control y estándares de seguridad de la información.

El principal beneficio como interés profesional pretende realizar un análisis del modelo BMIS aplicado a una empresa que permitirá aumentar las destrezas en la definición de políticas de seguridad de la información, así como, ofrecer un primer acercamiento a la implementación de un modelo muy nuevo que a la fecha no hay un estudio publicado en ese sentido.

Capítulo I – El Modelo de Negocios para la Seguridad de la Información (BMIS)

1.1.- Objetivo Principal

Proponer un conjunto de políticas para la seguridad de la información de las tecnologías de información y comunicación utilizando el modelo de negocios para la seguridad de la información con la finalidad de proveer una guía a la entidad financiera que sirvan como un conjunto de directrices para un adecuado gobierno de la seguridad de la información para la gestión de la información.

1.2.- Objetivos específicos

- Realizar una revisión de las políticas de seguridad de la información actuales en la entidad financiera que permita obtener un adecuado entendimiento de la situación actual.
- Elaborar un análisis del modelo del BMIS que permita relacionar cada uno de las características de los elementos y las conexiones dinámicas a las diferentes políticas de seguridad de información que satisfagan los requerimientos de la entidad financiera.
- Proponer un conjunto de políticas que permitan dirigir la gestión de la seguridad de la información de TI en la institución financiera para su adopción e implementación.

1.3.- Alcance

EL modelo BMIS será el marco de acción en el cual se fundamentará el análisis y propuesta.

1.4.- Limitaciones

Se tomará como cierta y definitiva la información que proporcione la entidad financiera una vez validada.

1.5.- Funcionamiento del Modelo BMIS

1.5.1.- Operacionalidad de las Variables.

El modelo de Negocios para la Seguridad de la Información (BMIS) representa un conjunto de variables que deben ser analizadas e implementadas en una empresa, por los cual el primer paso es entender cómo funciona y que pretende lograr con su implementación.

El BMIS propone una solución integral para el diseño, implementación y gestión de seguridad de la información basada en sus 4 elementos y 6 interconexiones dinámicas que representan a toda la empresa en su contexto y que permite realizar un análisis de sus componentes con el fin de lograr una mejora significativa en la resolución de los problemas que se presentan día a día en la empresa, así como, el maximizar dichos componentes para beneficio de las empresa.
La siguiente figura 1 proporciona una perspectiva del modelo el cual representa los elementos en color amarillo y las interconexiones dinámicas en color verde.

Figura 1 : El Modelo de Negocios para la Seguridad de la Información

EL BMIS parte de los siguientes supuestos:

- EL BMIS es ante todo un modelo en tres dimensiones.
- Se compone de cuatro elementos y seis interconexiones dinámicas (DIs).
- Como regla general, todas las partes del BMIS interactúan unos con otros.
- Los elementos están conectados entre sí a través de la DIs.
- Si alguna parte del modelo se cambia, otras partes también se cambiarán
- En un universo de información de seguridad integral y bien administrada, el modelo se considera que esta en equilibrio. Si las partes del modelo se cambian, o si persisten las debilidades de seguridad, el equilibrio del modelo se distorsiona.
- Las Interdependencias entre las partes de BMIS son el resultado del enfoque sistémico global.
- Las DIs pueden verse afectadas directa o indirectamente por los cambios en cualquiera de los componentes dentro del modelo, no sólo a los elementos en cada extremo.

1.5.2.- Elementos

1.5.2.1.- Organización

El elemento Organización se considera como una red de personas que interactúan entre sí por medio de procesos.

Todas estas relaciones, ya sean internas y externas, en su conjunto ponen los fundamentos para la eficacia operativa, el éxito y la sostenibilidad de la empresa.

Se enfoca en los conductores del negocio y en la dirección de la organización hacia el cumplimiento de sus objetivos, es un punto focal para la responsabilidad y la rendición de cuentas y un sólido punto de partida para llevar el diseño de seguridad en todas las unidades de negocio de la empresa. También tiene el potencial de influir sustancialmente en la cultura de la empresa.

Con conexiones en el proceso, las personas y los elementos de la tecnología, el elemento de la Organización actuará como piloto para demostrar el valor del programa de seguridad para la empresa y tendrá una enorme influencia en el éxito del programa de seguridad de la información.

1.5.2.2.- Procesos

El elemento procesos son creados para ayudar a las organizaciones a lograr su estrategia, en el BMIS el elemento del proceso es único y ofrece un enlace vital para todas las conexiones dinámicas del modelo ya que representan las actividades estructuradas que se crean para lograr un resultado en particular a través de las persona o de una serie de tareas aplicadas consistentemente.

El elemento del proceso explica las prácticas y procedimientos de las personas y organizaciones qué quieren lograr y como consecuencia representa los requisitos de una empresa para desarrollar, difundir, educar y hacer cumplir las prácticas y procedimientos de seguridad en forma continua.

Las interrelaciones del elemento proceso con las DIs son las siguientes:

- Proceso – Gobierno: El proceso se define como un resultado de la estrategia de la organización para lograr ciertos patrones de comportamiento mientras que la habilitación y el soporte es apoyado por la de la tecnología.

- Proceso – Emergentes: Un proceso necesita flexibilidad para ajustarse y adaptarse a nuevas e inesperadas situaciones y tener en cuenta la entrada de las personas, así como el comportamiento, con base en la experiencia y asesoramiento. La gestión de estos ajustes es soportado y apoyado por las personas.

- Proceso - Habilitación y Soporte: Un proceso necesita estar alineado con la tecnología para que la organización pueda recibir el beneficio completo de soluciones técnicas en forma permanente. Esto funciona en ambos sentidos: la tecnología automatiza los procesos, pero también los procesos permiten a la tecnología, como por ejemplo una mesa de ayuda (help desk) de apoyo soporta las aplicaciones de software.

1.5.2.3.- Personas

El elemento Personas representa los recursos humanos en una organización, los empleados, contratistas, vendedores y proveedores de servicios. El BMIS define el personal primario y el secundario, el primario representa a empleados o asociados con la organización y el secundario, se da en eventuales subcontrataciones como en el caso de los proveedores de servicios administrados o soluciones tecnológicas.

"Las personas" no son sólo unidades de uno y no pueden ser estudiados de manera independiente. Para entender cómo afecta la seguridad de la información, y cómo se ve afectada por la gente, un enfoque sistémico es necesario, el estudio de la interacción de las personas con el resto de los elementos del modelo a través de las DIs como se muestra a continuación.

- Personas – Cultura: Las personas tienen sus propias creencias, valores y comportamientos y a su vez, el conjunto de dichos atributos definen sus propias creencias, valores y comportamientos en la empresa así como el grado en que las personas se espera que cumplan con la seguridad, esto se refleja en la el elemento DI Cultura.

- Personas – Factores Humanos: Toda persona tiene reacciones que dependen de su propia naturaleza dando como resultado los factores humanos, como por ejemplo, un problema de aceptación de una tecnología puede hacer invalidar la tecnología. Esta relación es representa el vínculo entre ambos.

- Personas – Emergentes: Las personas son las que deben actuar en el caso en que se presenten situaciones emergentes de algunos de los procesos, tecnología y organización, y son las que primariamente son afectadas.

1.5.2.4.- Tecnología

El elemento tecnología ofrece las herramientas necesarias para llevar a cabo la misión y la estrategia de la empresa como un todo, incluyendo los parámetros generales de seguridad de la confidencialidad, integridad y disponibilidad.

La tecnología representa todas las aplicaciones técnicas del conocimiento utilizado en la organización cuyo propósito es el de apoyar y lograr las metas organizacionales por lo que dentro de una organización, la tecnología abarca más que las tradicionales de TI.

La tecnología, para efectos del BMIS, tiene 2 componentes, los objetos que representan cualquier tipo de tecnología y la capacidad de aplicación dentro de la empresa lo que implica que las empresas podrían tener mucha o poca dependencia de la tecnología.

Para el BMIS, el elemento de la tecnología se refiere a cada puesta en práctica de habilidades técnicas y conocimientos que podría tener un impacto en la seguridad general de la información.

Las interconexiones dinámicas del elemento tecnología son las siguientes:

- Tecnología – Arquitectura: Hay muchas opciones dentro de las herramientas, el riesgo de la empresa y el riesgo de procesos de negocio son las fuerzas impulsoras detrás del programa de seguridad para ello la arquitectura empresarial es un enlace en el cual apoya q la organización en el establecimiento de la tecnología a necesitar.

- Tecnología – Factores Humanos: La selección de la tecnología siempre direcciona a la utilidad, la eficiencia y la productividad de la empresa por medio de los factores humanos. Una vez que la tecnología es seleccionada e implementada, la formación debe ser dada a aquellos que necesitan utilizar las herramientas y el monitoreo será necesario para comprobar que la tecnología funciona adecuadamente.

- Tecnología – Habilitación y Soporte: la tecnología es fundamental en la empresa, sin embargo, si no se aplica y/o se ignora, ya sea por desconocimiento o ignorancia, se puede dar a la empresa una falsa sensación de seguridad. Habilitación y soporte permite mitigar este riesgo.

1.5.3.- Interconexiones Dinámicas (DIs)

1.5.3.1.- Gobierno

El DI gobierno representa los límites de lo que la empresa desea en materia de seguridad de la información, es decir, traduce los conceptos de gobierno y las medidas que se deben seguir para cumplir con la misión y objetivos, y establecer límites y controles a nivel de procesos.

1.5.3.2.- Cultura

El DI Cultura provee la más completa imagen de la empresa. El impacto de la Cultura en las personas es un tema clave en la Seguridad de la Información desde que las personas

sean capaces de contribuir a la seguridad de la información o, por el contrario, se comprometan con esto.

1.5.3.3.- Arquitectura

El DI Arquitectura comienza como un concepto, un conjunto de objetivos de diseño que se deben cumplir, luego avanza hacia un modelo, o sea, una visión a partir de los servicios. Esto es seguido por la preparación de planos detallados, herramientas que se utilizan para transformar la visión/modelo en un producto real y el acabado que permite conocer la empresa como un todo de la tecnología de información, dando paso a un modelo de Seguridad de la Información.

1.5.2.4.- Habilitación y Soporte

Habilitación y Soporte, en términos de BMIS, es el DI a través del cual la tecnología permite un proceso, y el proceso a su vez, soporta la entrega y la operación de la tecnología.

1.5.2.5.- Factores Humanos

Los Factores Humanos se refiere a la interacción persona-computador, la interfaz - hombre-máquina- y la ergonomía por lo que gran parte del trabajo en la facilidad de uso.

Los tres objetivos principales se relacionan con el operador humano (cuerpo y mente) y los sistemas circundantes que interactúan con el usuario humano. Para entender y manejar la tensión en este DI, el primer paso es diagnosticar o identificar los problemas y deficiencias en la interacción hombre-sistema de un sistema de seguridad existente.

1.5.2.6.- Emergentes

Los Emergentes para el BMIS, es visto como el surgimiento de nuevas oportunidades de negocio, nuevos comportamientos, nuevos procesos y otros elementos relevantes para la seguridad.

1.6.- Metodología de Investigación

La definición de los elementos de la investigación que se utilizaron son los siguientes:

1.6.1.- Recopilación de la información

Se solicitó la información actual que tenga la entidad financiera referente a lo relacionado con gobierno corporativo y políticas de la organización en general así como las políticas específicas de TI y las de seguridad de la información.

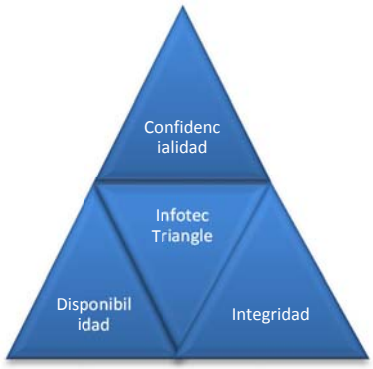
1.6.2.- Consulta de las fuentes

Se realizaron entrevistas con la finalidad de obtener información sobre los elementos y conexiones dinámicas que permitan establecer un conocimiento detallado sobre el elemento organización y las conexiones dinámicas de factores humanos y cultura básicamente, las cuales permitirán evaluar las características presentadas en el BMIS. Estas entrevistas estarán dirigidas a los diferentes niveles de la entidad financiera con la finalidad de poder obtener una visión sobre las políticas, específicamente el comité de TI, el comité de Riesgos, el comité de vigilancia así como la alta dirección.

Se tomó como referencia fundamental teórica el modelo de negocios para la seguridad de la información (BMIS) expuesto en el punto 1.6 anterior el cual se analizó y se detallaron los componentes a ser evaluados en la entidad financiera.

Se analizaron otros modelos de seguridad de la información con la finalidad de tener una perspectiva más amplia sobre la seguridad de la información el cual es el modelo de acceso basado en roles de control (RBAC) el cual se enfoca en la las violaciones de la privacidad y reducción del riesgo y el modelo “Infosec triangle” (Triangulo de la información de la seguridad) que presenta tres componentes básicos denominados CAI (Confidencialidad, Integridad y Disponibilidad) que es un modelo comúnmente aceptado como el modelo de prescripción para el análisis, la gestión y seguridad de la información de auditoría el cual define el triángulo de la seguridad de la información como se muestra en la siguiente figura 2:

Figura 2: Triángulo de la Información de la Seguridad



1.6.3.-Tratamiento de la información

Cada una de las fuentes de información proporcionó las diferentes características que deben encontrarse en los elementos y conexiones dinámicas del BMIS las cuales proveyeron de la información base que sirvió para la determinación de las políticas propuestas a la entidad financiera.

Con las características obtenidas de la aplicación del BMIS se realizó una comparación y/o mapeo entre las características que propone este modelo y las características que se encontraron en la entidad financiera y que sirvió de base para determinar la brecha existente entre ambas.

Una vez establecidas las diferencias se realizó un análisis de las mismas con la finalidad de obtener los elementos faltantes de las mismas en las políticas que actualmente tiene la entidad financiera y se propuso un conjunto de políticas que fueron el resultado de la aplicación del BMIS.

EL análisis del BMIS y sus componentes fue esencial para obtener las características necesarias para un adecuado gobierno de la seguridad de la información el cual sirvió para:

1.6.3.1.- Determinar los criterios aplicados en la evaluación de la seguridad de la información

1.6.3.2.- Comparar las características del BMIS con las políticas actuales de la entidad financiera

1.6.3.3.- Determinar la brecha entre la propuesta del BMIS y las políticas actuales de la organización.

1.6.3.4.- Fundamentar las conclusiones del análisis

Una vez analizadas las políticas se desarrollaron y/o modificaran de acuerdo con las necesidades de la entidad financiera las conclusiones que permitieron dar fundamento a la propuesta de las políticas de seguridad de la información.

Dentro de estas conclusiones se realizó un análisis comparativo y se determinó la brecha existente.

1.6.3.5.- Propuesta de las políticas de seguridad de la información

Se propuso un conjunto de políticas de seguridad de la información que permita cerrar la brecha existente con su adecuada valoración y selección, así como, el diseño y elaboración de la propuesta para que la entidad financiera posibilite su aprobación e implementación.

Capítulo II – Revisión de las políticas de Seguridad de la Información actuales en la entidad financiera.

2.1.- Análisis de las políticas de Seguridad de la Información actuales.

Como parte del BMIS, explicado en el capítulo anterior, es importante resaltar el enfoque holístico que representa el valor agregado del modelo, esto conlleva a que las políticas de Seguridad de la Información deben enfocarse en la entidad como todo y no únicamente como un conjunto de políticas que involucren al departamento de tecnologías de información, sino a todo el personal de la entidad.

Por tal motivo se realizará un resumen de las políticas de seguridad actuales que permita tener un conocimiento general de las políticas actuales de la entidad.

2.1.1.- Resumen de las políticas actuales

Para efecto de realizar el resumen de las políticas de la entidad se procedió a extraer la idea principal de cada grupo de política tomando en consideración la misma redacción que se utilizó por parte de la entidad.

La entidad financiera cuenta actualmente con un conjunto de políticas distribuidas en 10 capítulos que contienen 100 artículos, que están enfocadas a establecer las políticas generales de TI con el propósito de orientar y facilitar la toma de decisiones en los diferentes niveles de la organización y que permitan gestionar adecuadamente el departamento de TI, logrando agilidad y oportunidad en el desarrollo de sistemas de información y la automatización de procesos.

El alcance de las mismas se define como políticas generales para el desarrollo de las tecnologías de información y aplican a todo el personal de la entidad financiera, tanto en las oficinas centrales como en las sucursales, así mismo manifiestan que son de aplicación obligatoria y fueron aprobadas por la Junta Directiva de la entidad.

El objetivo general de las políticas está enfocado en el crecimiento y desarrollo del área de TI que permita prestar servicios de calidad y ser oportunos para los usuarios, tanto externos como internos.

A continuación se describe un breve resumen de los 10 capítulos con sus principales directrices.

- Capítulo 1; Definiciones, se refiere a todas las definiciones de los términos que se utilizaran en el documento de políticas.

- Capítulo 2; Administración del área de TI, básicamente expone los elementos de gestión del departamento de TI y emite directrices necesarias en cuanto a plan estratégico, manual de puestos, capacitaciones, contrataciones, adquisición de recursos, contratos con terceros, comunicaciones, solicitudes y modificaciones de sistemas y la administración de proyectos.

- Capítulo 3; Gestión de seguridad física, se refiere a cómo se debe gestionar la seguridad física en las instalaciones como: ubicación y acceso al cuarto de servidores, accesos a la unidad de TI, plan de evacuación y control de plagas.

- Capítulo 4; Seguridad lógica y acceso a datos, se refiere al control de acceso a los sistemas, bases de datos y servidores en cuanto a creación de usuarios, responsabilidad del uso de palabras de paso, gestión de los usuarios en general.

- Capítulo 5; Evaluación de sistemas de información, básicamente se refiere a las fases en el desarrollo de la evaluación, y su función principal es gestionar todo lo referente al desarrollo de sistemas tomando como parámetro para el desarrollo de sistemas, la metodología del ciclo de vida para el desarrollo de los mismos.

- Capítulo 6: Software y base de datos, se refiere a toda la parte de gestión de implementación y control de software de base de datos, de sistemas operativos, de redes, correo electrónico y de licencias en general.

- Capítulo 7; Hardware y Redes, se refiere a la gestión y control de hardware incluyendo su contenido de información, así como de redes en lo referente a conexiones y comunicaciones, monitoreo del desempeño.

- Capítulo 8; Continuidad de operaciones, se refiere a la política de respaldos de información, continuidad antes fallas en la red pública y cobertura de seguros.

- Capítulo 9; Condiciones de uso, servicios financieros por internet, se refiere al uso de los sistemas de información web donde define la utilización de claves de acceso, reglas del servicio, confidencialidad y responsabilidad, condiciones del servicio entre otras.
- Capítulo 10: Administración del servicio, se define el horario del servicio, situaciones del mantenimiento, acceso de los sistemas en línea y monitoreo en general.

Otro aspecto importante es que algunas, pero no todas las políticas, están relacionadas con su respectivo reglamento, procedimiento y/o a una política más detallada.

2.1.2.- Filosofía Empresarial sobre las políticas de Seguridad de la Información

La filosofía empresarial representa la visión de la entidad respecto a la forma en que la Seguridad de la Información permea en la organización, desde los niveles gerenciales que son los responsables hasta los niveles más bajos que son los responsables de velar por el cumplimiento de las políticas a nivel netamente operativo.

La entidad no tiene un proceso formal de elaboración y gestión de las políticas de seguridad de la información que permita establecer un adecuado sistema que identifique los puntos necesarios para una adecuada protección de la seguridad.

Las políticas de seguridad están formalizadas. Para la puesta en marcha de controles cada uno de los coordinadores implementa de acuerdo a su mejor criterio los se consideren necesarios, algunas veces controles básicos de seguridad.

La organización de la seguridad de la información recae en el personal de Tecnologías de Información (TI) los cuales son los encargados de tomar las acciones necesarias de acuerdo a su mejor entender y conocimiento de sus coordinadores. Estas acciones involucran tres grandes áreas que son: Sistemas de información, Redes y comunicaciones y Seguridad física.

Por ejemplo, en materia de seguridad física se han realizado esfuerzos significativos que permiten un mejor manejo del departamento de TI con nuevas instalaciones, consiguiendo el resguardo de la seguridad física adecuado, asimismo cuentan con un oficial de seguridad que es el encargado de la gestión de la seguridad física.

En materia de seguridad de redes se cuenta con tecnología que apoya la gestión de la información, sin embargo, no está definido un sistema formal que permita gestionar por ejemplo, los incidentes de seguridad, que en materia de seguridad es muy relevante.

El conocimiento en de seguridad de la información es difuso en el resto de la organización, por lo que existen oportunidades de mejora importantes en la implementación de campañas que eduquen al personal en esta área y que conlleven a una gestión basada en el conocimiento y no en las percepciones de cada persona en lo que a seguridad se refiere, el conductor de valor se puede fortalecer en la conciencia de las personas para el resguardo de la información dirigida por el compromiso de la gerencia.

Existe dentro de la entidad un marco de políticas generales que involucra aspectos de seguridad que no permiten definir claramente las oportunidades de mejoras por lo que las políticas actuales no cubren las necesidades de la seguridad de la información.

La estructura, alcance y contenido están desactualizadas, de hecho se realizaron hace más de 8 años y no se han revisado encontrándose puntos que son claramente identificables en las políticas generales que no corresponden a las necesidades actuales por lo que la entidad,

en el reconocimiento de su importancia, ha decido implementar un estándar en materia de seguridad de la información como el BMIS.

Desde el punto de vista gerencial se realizaron entrevistas en donde se manifiesta que están satisfechos con los avances hechos a la fecha , sin embargo, y por cumplimiento de los requerimientos de la Súper Intendencia General de Entidades Financieras (SUGEF), se debe mejorar en la implementación, aunque se reconoce que es un costo que supera el beneficio.

En términos de conciencia referente a la seguridad de la información, la gerencia considera que no es necesario tanta seguridad puesto que la información es prácticamente pública, ya que se han dado cuenta que la información de clientes esta diseminada entre las operadoras crediticias y cualquier persona, con el hecho de contratar los servicios de este tipo de entidades ya tiene la información que desee.

En general existen oportunidades de mejora en la aplicación, evaluación, mejora continua de la seguridad de la información y reconocen que la actualización de las políticas de seguridad de la información viene a satisfacer sus requerimientos en esta materia.

2.1.3.- Análisis de requerimientos de la entidad

Una vez realizada la descripción de las políticas vigentes en la entidad es importante definir los requerimientos, es decir, los requerimientos son los objetivos que proporcionaran una meta hacia a donde debe enfocar los esfuerzos la entidad con la finalidad de cumplir con las necesidades de la Seguridad de la Información.

Uno de los retos más importantes para las organizaciones de hoy y específicamente en Costa Rica en el campo de TI, es la regulación de la directriz SUGEF 14-09 es la implementación de dicha directriz.

El impacto de esta regulación muchas veces implica la implementación de marcos y estándares que no están de acuerdo con las características específicas de las entidades, en cuanto a cultura organizacional principalmente. Tampoco permiten una adaptación “a la

medida" a las entidades debido a que en algunos casos, los requerimientos sobrepasan la disponibilidad y capacidad de la organización.

Debido a lo prácticamente los requerimientos para la seguridad de información de la entidad, se determinan por las necesidades de los entes regulatorios y se considera, para efectos de este trabajo, que los estándares proporcionarán el objetivo que la entidad debe de lograr. Para ello es importante primeramente definir una línea base para la seguridad de la información, que constituirá el punto de partida a alcanzar para luego entrar en un proceso de madurez que permita obtener el objetivo propuesto por los estándares.

Dicho lo anterior, el requerimiento básico de la entidad financiera es el logro de la implementación de las siguientes normativas.

2.1.3.1.- Cumplimiento de la normativa SUGEF 14-09

La Implementación de los marcos y estándares de Seguridad de la Información establecidos en la directriz emitida por la SUGEF denominada SUGEF 14-09 que es el reglamento sobre la gestión de la tecnología de información cuyo objetivo es "… *la definición de los criterios y metodología para la evaluación y calificación de la gestión de la tecnología de información (TI)" (Acuerdo SUGEF 14-09, p.1).*

Este reglamento dirige a las organizaciones bajo su supervisión a la implementación de los procesos en el marco de objetivos de control conocido como COBIT 4.1 (IT Governace Institute, 2007) el cual consta de 34 procesos y de los cuales son obligatorios 17 de los 34 en una primera etapa. Además el nivel de madurez 3 es necesario para lograr cumplir los requerimientos para cada uno de los procesos establecidos en la primera etapa de implementación del marco normativo.

Adicionalmente, es importante mencionar que el artículo 6 de dicho reglamento expone la necesidad de contar con un marco general para la gestión de TI que involucra el diseño, implementación y mantenimiento de dicho marco.

Para efectos del trabajo y específicamente en materia de seguridad de la información, se debe considerar inevitablemente aquellos de los 17 procesos obligatorios de la normativa,

que satisfagan los requerimientos se seguridad que universalmente están definidos por 3 criterios aplicados a la información, que son: Integridad, Confidencialidad y Disponibilidad.

Basados en el marco COBIT 4.1 se establecen los procesos que inciden en la seguridad de la información, como los siguientes:

- PO 09 Riesgos de TI
- AI 06 Administración de Cambios
- DS 04 Garantizar la continuidad del Negocio
- DS 05 Seguridad de los sistemas de Información
- DS 11 Administración de Datos
- DS 12 Administración del ambiente Físico

Adicionalmente es importante incorporar las mediciones adecuadas de la seguridad de la información en procesos que no necesariamente tienen como principal requerimiento los criterios de la seguridad de la información para ellos también se toma como requerimiento el proceso ME-2 Monitorear y evaluar el control interno con la finalidad de que las mediciones en general sobre la seguridad de la información se logren integrar al proceso de gestión de la entidad.

2.1.3.2.- Estándar de seguridad

Como un requerimiento de la seguridad de la información, basado en los procesos de COBIT 4.1, apoyado por la visión y reconocimiento de la administración de la entidad financiera, se decidió adoptar un estándar de seguridad de la información el cual es el estándar ISO/IEC 27001-2008 (Inteco, 2008).

Hay que tomar en cuenta que para una óptima implementación de este estándar es importante apoyarse en la guía de prácticas de control que ofrece la misma norma anterior y que direcciona a la norma ISO/IEC 27002:2005 (Inteco, 2005), aunque el objetivo no es el implementar todos los controles definidos en dicha norma sirven de un buen punto de comparación.

Tomando en consideración los puntos anteriores se define la siguiente tabla como un resumen general de los requerimientos externos e internos de la entidad financiera.

Tabla 2 1: Requerimientos de la entidad financiera en Seguridad de la Información

ISO/IEC 27001-2008	ISO/IEC 27002:2005
4.- Sistema de Gestión 5.- Responsabilidad de la Dirección 6.- Auditorías Internas 7.- Revisión del SGSI por parte de la Dirección 8.- Mejora del SGSI Objetivo: Proporciona un modelo para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora del Sistema de Gestión para la Seguridad de la Información (SGSI)	4.- Gestión de Riesgos 5.- Políticas de Seguridad de la Información 6.- Organización Interna 7.- Gestión de Activos 8.- Seguridad de RRHH 9.- Seguridad Física 10.- Gestión de comunicación y Operaciones 11.- Control de Acceso 12.- Desarrollo de Software 13.- Gestión de Incidencias 14.- Continuidad de Negocio 15.- Cumplimiento Objetivo: Proporcionar un marco de referencia para la implementación de los controles de seguridad del SGSI
COBIT 4.1	Entidad Financiera - <u>Políticas Generales que incluyen seguridad</u>
PO 09 Riesgos de TI AI 06 Administración de Cambios DS 04 Garantizar la continuidad del Negocio DS 05 Seguridad de los sistemas de Información DS 11 Administración de Datos DS 12 Administración del ambiente Físico Criterios para definir esos procesos Integridad, Confidencialidad y Disponibilidad Objetivo: Procesos a implementar de la directriz SUFEG 14-09	1.- Definiciones 2.- Administración de TI 3.- Seguridad Física 4.- Seguridad Lógica – Acceso a Datos 5.- Desarrollo de Sistemas 6.- Software y Base de Datos 7.- Hardware y Redes 8. Continuidad de Operaciones 9.- Condiciones de uso Servicios financieros. Por Internet 10.- Administración del Servicio Objetivo: Establecer políticas para el crecimiento y desarrollo del área de TI con el propósito de prestar los servicios a los usuarios internos y externos con mayor oportunidad y calidad

Fuente: Elaboración Propia

Como se desprende de la tabla 2.1 el objetivo para el cumplimiento de los requerimientos es lograr la integración de diferentes aspectos de seguridad de la información en un marco más general como lo es el marco de gestión de TI, que permita direccionar las políticas de seguridad de la información dentro de los mismos procesos de gestión de TI en general.

Para efectos del trabajo el requisito de la entidad financiera involucra, la implementación de las políticas de seguridad de la información en la implementación de los procesos COBIT 4.1 como marco de gestión general y a la vez incorporar el estándar ISO/IEC 27001-2008 que es guiado y/o que hay que considerar la familia de normas ISO 27000, específicamente la norma ISO/IEC 27002:2005 para asegurar que la implementación de la norma ISO/IEC 27001-2008.

2.2.- Comparación de las políticas de seguridad analizadas en el contexto del BMIS.

Una vez identificado los requerimientos de la entidad en Seguridad de la Información es importante realizar una comparación que permita tener un visión de las diferencias entre lo que nos solicitan los requerimientos que se debe cumplir y lo que realmente se tiene en la práctica en la entidad con la finalidad poder identificar claramente los esfuerzos necesarios que se necesitan para dar cumplimiento a dichos requerimientos.

Para lograr una adecuada comparación de las políticas de seguridad en relación al BMIS es necesario el conocer también las soluciones en toda su amplitud de las medidas de seguridad que tiene la entidad financiera, razón por la cual se realizó un mapeo entre dichas medidas que incluyen las políticas como parte de las soluciones de seguridad con el BMIS.

El propósito del mapeo de las políticas actuales a COBIT 4.0 (Requerimientos SUGEF 14-09), COBIT 4.1, ISO/IEC 27001-2008 y por último al BMIS, es correlacionar éstos a cada uno de los elementos del BMIS generando el valor de asociarlos a los requerimientos de la entidad.

2.2.1.- Elementos

Para el BMIS existen 4 elementos que son, Organización, Procesos, Personas y Tecnología, por lo que es importante analizar cada uno de ellos en su contexto como se definieron en el capítulo 1, ya que nos permite puntualizar aspectos de la Seguridad de la Información que de otra forma se podría pasar por alto, siendo esto uno de los beneficios principales del BMIS que es la atomización de cada elemento de las entidades con la finalidad de identificar riesgos y medidas que mitiguen esos riesgos. Cuando se analiza y se compara con la realidad de la entidad es que nos permite empezar a tener una visión holística que apoyará a la entidad en la implementación de mejoras de la Seguridad de la Información.

2.2.1.1 Elemento Organización

Este elemento identifica la forma en que se ha estructurado en la entidad para la gestión, la cual está sustentada en departamentos los cuales tienen su correspondiente función y no se logra diferenciar una estructura que corresponda a la seguridad de la información como tal, sino que son un conjunto de posiciones funcionales excepto por un oficial de seguridad que se encarga básicamente de la seguridad física, actualmente la entidad está en proceso de contratación de un oficial de seguridad que permita apoyar la gestión de seguridad desde el punto de vista de tecnologías de información y comunicación.

La forma de gestionar la seguridad de la información parte del comité de TI quien brinda las directrices a la administración para la implementación de los procesos Desde el punto de vista formal el oficial de seguridad reporta a uno de los coordinadores de TI.

La forma en que se implementan los procesos es por medio de un plan general que afecta directamente a todo el departamento de TI e involucra como tal la seguridad de la información como un aspecto más a considerar.

Los coordinadores de TI son los encargados de aplicar la seguridad de la información a las aplicaciones y en general en su gestión diaria, aunque se pudo corroborar que las acciones de la organización en seguridad de la información son reactivas, así mismo, las acciones no son sustentadas en los riesgos debido a que se encuentran desactualizados.

La persona a cargo del puesto de dirección sustenta sus decisiones en los criterios de los coordinadores de TI los cuales la retroalimentan de las necesidades específicas en materia de seguridad de la información por lo que no cuentan con un plan específico de seguridad de la información.

La entidad se encuentra en proceso de implementación de las regulaciones exigidas en materia de tecnologías de información por los entes supervisores para lo cual se nombró a tres personas que están a cargo de realizar las actividades necesarias y dentro de lo cual exigen la adopción de un estándar en materia de seguridad de la información y se adoptó el estándar ISO/IEC 27001-2008. Este estándar básicamente provee de un Sistema de Gestión de la Seguridad de la Información el cual debe ser implementado por la entidad y se encuentra actualmente en planificación para su puesta en marcha.

Con la finalidad de poder hacer una comparación adecuada con fundamento en el BMIS es importante realizar un mapeo del elemento organización y analizarlo de acuerdo con las relaciones identificadas en el modelo. Estas relaciones se pueden observar en el punto 1.5.2.1 del capítulo anterior.

Para lograrlo se identificaron las políticas y/o documentos que la entidad tiene que afectan a la Seguridad de la Información y que se asignan al elemento organización y se mapearon, primeramente al elemento organización y luego se realizó un análisis de su relación de acuerdo con cada una de las DI que lo afectan.

Las principales relaciones que interactúan el modelo del BMIS del elemento organización con las diferentes interconexiones dinámicas se muestran en la tabla 2.2.

Tabla 2 2: Mapeo del elemento Organización a las Conexiones dinámicas del BMIS

Nombre	Gobierno (G)	Arquitectura (A)	Cultura (C)	Habilitación y Soporte (HS)	Factores Humanos (FH)	Emergentes (E)
Mejoramiento del SGSI	G		C			E
Este apartado corresponde a la implementación de la norma ISO/IEC 27001-2008 que la entidad ha adoptado, sin embargo, se está iniciando el proceso de implementación, es importante tomar en cuenta que la mejora continua es un requerimiento de la norma y por ende afecta directamente a la cultura empresarial debido al cambio de mentalidad que implica por sí mismo el cambio, así mismo afecta directamente al DI emergente ya que desde el punto de vista del requerimiento de la norma implica un proceso que involucra el ciclo de mejora continua.						
Políticas de contratación de Proveedores para servicios TI	G			HS		
La entidad no cuenta con los acuerdos de nivel de servicio (SLA´s) necesarios para la implementación de las política de contratación de proveedores, por lo que es importante que se defina a nivel táctico y operativo la implementación de dichos acuerdos estableciendo los requerimientos mínimos necesarios con el fin de proporcionarle la habilitación y soporte necesarios para su adecuada gestión.						
Políticas de Tecnología de Información	G		C	HS		
La entidad cuenta con una conjunto de políticas generales que no diferencian adecuadamente las necesidades específicas de la seguridad de la información aunque si las contempla, dichas políticas no cuentan con una adecuada gestión y mantenimiento lo que implica que el gobierno es el encargado de girar las respectivas instrucciones con la finalidad de crear una adecuada cultura así como una definición clara de las acciones que debe emprender habilitación y soporte para el logro de una gestión eficaz de acuerdo con las directrices proporcionadas por el gobierno.						
Requisitos Generales ISO/IEC 27001-2008	G		C			
La entidad debe de proporcionar por medio del Gobierno los requisitos para la implementación de la norma ISO/IEC 27001-2008 principalmente tomando en consideración la cultura empresarial.						
Compromiso de la gerencia	G		C			
El compromiso de la gerencia es un factor crítico del éxito para una buena implementación de la norma ISO/IEC 27001-2008 la cual impacta directamente en la forma de gestión proporcionada por el gobierno y la cultura de la organización, la cultura es el elemento clave para una adecuada implementación.						
Revisión Gerencial del SGSI	G					E
Este punto es un requerimiento de la norma la cual implica el establecimiento de los mecanismos necesarios de medición por medio del gobierno para que la gerencia pueda tener la información necesaria para controlar y gestionar los elementos relacionados con las acciones de oportunidades de mejora y tomar las acciones pertinentes.						
Política Seguridad Física	G	A		HS		

Dentro de las políticas generales de la entidad se encuentra un capítulo dirigido a la seguridad física el cual es adecuado.						
Política Seguridad Lógica – Acceso a Datos	G	A		HS		
La entidad cuenta con las políticas de acceso a datos y es impactada por la forma de dirección por medio del gobierno, la arquitectura lógica de la entidad así como su correspondiente aplicación por medio de habilitación y soporte. Es importante el poder tener un esquema lógico de la seguridad de los datos ya que esto apoyará necesariamente la actividad de habilitación y soporte.						
Política Desarrollo de Sistemas	G			HS	FH	
La entidad cuenta con una política de desarrollo de sistemas que impacta directamente en la habilitación y soporte de los sistemas y que se ve afectada por los factores humanos que deben contar con las facilidades necesarias en cuanto a la gestión de los sistemas de información.						
Política Software y Base de Datos	G	A		HS		
Esta política permite direccionar adecuadamente los requerimientos en función de la seguridad de la información en materia de adquisición, respaldos, instalación de sistemas operativos, monitoreo, y otros relacionados la cual se ve afectada por la arquitectura en materia de seguridad y por la habilitación y soporte. La entidad cuenta con los respectivos manuales con que se debe implementar esta política.						
Política Hardware y Redes	G	A		HS		
Esta política es implementada por medio del gobierno para lo cual está la correspondiente política y procedimiento.						
Política Continuidad de operaciones	G	A	C	HS	FH	
Existe una política de continuidad de operaciones por escrito, aunque no está implementada. Como se muestra en el mapeo de las DI, para el cumplimiento de esta política necesariamente se debe tomar en cuenta prácticamente todas las DIs ya que depende de todos elementos.						
Política Condiciones de Uso, Servicios financieros por internet	G		C	HS		
Por aspectos de tiempo del personal de la entidad no se puedo evaluar este requerimiento en su totalidad, de acuerdo a los criterios externados esta política es adoptada adecuadamente por medio de las soluciones de la entidad, es importante hacer notar la influencia que tiene esta directriz en materia de cultura y habilitación y soporte debido a que es una entidad financiera la cual proporciona los medios de transacciones por internet						
Procedimientos de Recepción y Manejo de Claves Compartidas	G			HS		
Este procedimiento se cumple a cabalidad y es soportado y habilitado de forma confidencial.						

Procedimiento para el cambio de clave base datos	G			HS	FH	
Este procedimiento se cumple a cabalidad y es soportado y habilitado de forma confidencial y debe tener especial cuidado en factores humanos debido a su confidencialidad.						
Procedimiento para la creación eliminación y revisión de usuario	G			HS	FH	
El procedimiento está aplicado adecuadamente.						
Sistema de Gestión ISO/IEC 27001-2008	G	A	C		FH	E
Se está en proceso de implementación, evidentemente el sistema de gestión involucra todos los aspectos de las DI, principalmente la arquitectura, cultura, factores humanos y emergentes						
Responsabilidad de la Gerencia	G		C			
Se puede afirmar que la responsabilidad de la gerencia se ve impactada por la capacidad que tenga la gerencia en la cultura empresarial, la cual no es adecuada.						

Fuente: Elaboración Propia

2.2.1.2 Elemento Procesos

Los procesos representan la forma en que la organización gestiona la Seguridad de la Información los cuales deben ser implementados por el DI Gobierno, y es sustentada principalmente por el DI Habilitación y Soporte y el DI Emergentes como se explicó en el punto 1.5.2.2 del capítulo anterior.

Al igual que el elemento organización, se procedió a mapear las políticas y/o documentos que se asignaron al elemento procesos y se analiza en el entorno de las DI que se relacionan con este elemento y se realiza la comparación.

El elemento Procesos corresponde a los procesos de TI que han sido implementados y cómo éstos se relacionan con las diferentes interconexiones dinámicas como se muestra en la tabla 2.3

Tabla 2 3: Mapeo del elemento Procesos a las Conexiones dinámicas del BMIS

Nombre	Gobierno (G)	Arquitectura (A)	Cultura (C)	Habilitación y Soporte (HS)	Factores Humanos (FH)	Emergentes (E)
Normas y procedimientos relacionados con el uso de mensajería interna y externa	G		C		FH	
Se encuentra implementado por medio de firewalls de diferentes tipos a los cuales se les monitorea						
Respaldos Automáticos	G	A		HS		
La entidad cuenta con respaldos automáticos de la información, aunque no existe una arquitectura de información debidamente definida lo que no garantiza que los respaldos sean de acuerdo a la criticidad de la información. EL factor humano es importante en la definición de la criticidad de los datos sensibles						
Procedimiento para Monitoreo de Red (Manual)		A	C	HS		
La Entidad cuenta con técnicas de seguridad y procedimientos para la administración de la seguridad de redes formalmente documentados. Asimismo, se identificó la existencia de IPS, FIREWALLS y segmentación de redes. Asimismo, se cuenta con certificados para garantizar que la información desde dentro hacia fuera y afuera hacia dentro.						
Procedimientos para Monitoreo de Riesgos (Informe)	G		C			E

La entidad no cuenta con informe de riesgos de la redes que identifique los principales puntos a evaluar e informar, la cultura de la entidad influye directamente en la gestión de gestión de los riesgos y no se identifican los riesgos de seguridad para ser mitigados por medio de la identificación de eventos de violación a la seguridad de situaciones que se puedan presentar						
Procedimiento para Caso de Negocio (Manual)	G		C			
Se tiene un procedimiento de gestión de procesos en donde se identifica el caso de negocios como punto de partida para la toma de decisiones. La cultura es un aspecto importante para poder generar valor a las inversiones de TI						
Procedimientos para la Seguridad TI (Manual)	G		C	HS		
La Entidad cuenta con prácticas de administración de la seguridad de TI documentadas, aunque no cuenta con un plan de seguridad de TI, el cual indique la frecuencia de ejecución y otros aspectos que brindarán una garantiza de la información y configuración de los equipos. Esto para minimizar el riesgo de pérdida de información. La cultura de la entidad no es adecuada en este sentido. El factor humano es determinante en este apartado para la implementación adecuada de los procedimientos de seguridad.						
Procedimientos para la Administración Integral de Riesgos	G	A	C			
La entidad cuenta con un sistema formal de gestión de riesgos en donde se identifican los principales riesgos a mitigar, una definición de la arquitectura empresarial podría mejorar la definición de riesgos identificando riesgos que no sean detectados, esto se ve directamente relacionado con la cultura empresarial.						
Procedimientos de la Unidad de Riesgos, políticas, límites y funciones	G	A	C			
Al igual que el punto anterior, la entidad cuenta con un sistema formal de gestión de riesgos en donde se identifican los principales riesgos a mitigar, una definición de la arquitectura empresarial podría mejorar la definición de riesgos identificando riesgos que no sean detectados, esto se ve directamente relacionado con la cultura empresarial. De hecho las relaciones con el gobierno, arquitectura y cultura son los mismos.						
Control de proveedores de servicios de TI	G			HS	FH	
La entidad debe proporcionar el procedimiento de administración de contratos para que contenga lineamientos y actividades que aseguren que se incluyan cláusulas sobre desempeño, niveles de servicios, seguridad, procedimientos de arbitraje. La administración debe ejecutar los lineamientos para que TI puede habilitar y soportar estos contratos de una forma eficiente, los factores humanos en cuanto a conocimiento contractual debe ser dirigido por el departamento legal						
Establecer y manejar el SGSI	G	A	C	HS		
Este es el foco principal del Sistema de Gestión de la Seguridad de la Información que está en proceso de implementación, este SGSI debe fundamentarse sobre una cultura fuerte dirigida a la seguridad de la información, sin menospreciar una adecuado proceso de identificación de riesgos por medio de la arquitectura y con el apoyo de la administración, de forma tal, que permita a TI habilitarlo y sobre todo soportarlo a través del tiempo						

Requisitos de documentación	G			HS		
La entidad está en proceso de documentación de la Gestión del Sistema de Seguridad de la información el cual se implementa como una directriz adoptada por administración que debe ser realizada por habilitación y soporte						
Gestión de Recursos	G	A	C	HS		
La entidad debe proveer los recursos necesarios para la adecuada gestión de la seguridad de la información que se relaciona con la arquitectura, mejora en la cultura, y el personal que habilita y soporta la implementación						
Auditorías Internas	G					E
Se deben establecer como parte del sistema de gobierno para evaluar las oportunidades de mejora y tener un adecuada retroalimentación						
Procedimientos para claves para servicios y equipos de comunicación		A		HS		
Se cuenta con los procedimientos para la gestión de claves en la entidad						
PO 09 Riesgos de TI	G	A		HS		
La entidad no cuenta con una evaluación de riesgos específicamente en seguridad de la información lo que impacta en la arquitectura que brinda la base para dicha evaluación y que debe ser soportada por habilitación y soporte.						
AI 06 Administración de Cambios		A		HS		
La Entidad cuenta con un procedimiento para la ejecución de los cambios, en el cual se ejecuta un proceso de evaluación del impacto de acuerdo al tipo de cambios, asimismo, estos son priorizados de acuerdo al grado de impacto y con llevan una autorización de la coordinación de TI, o del Jefe de Operaciones con el fin de realizar la mejora respectiva.						
DS 04 Garantizar la continuidad del Negocio	G	A	C	HS	FH	E
La Entidad cuenta con un plan de continuidad de TI, sin embargo, este se encuentra enfocado únicamente sobre el ambiente principal y no establece medidas de contingencias. Por lo que no se identifican los siguientes aspectos: los requerimientos de resistencia, el procesamiento alternativo, la capacidad de recuperación, los lineamientos de uso, las funciones y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de las pruebas.						
DS 05 Seguridad de los sistemas de Información	G	A	C	HS		
La Entidad cuenta con una política y procedimiento para la administración de la seguridad de TI, en el cual se puede identificar que existen proceso para alinear la seguridad de TI acorde a los requerimientos del negocio. Así como garantizar la vigilancia y el monitoreo de la seguridad en el ambiente de TI.						
DS 11 Administración de Datos		A		HS		
La Entidad no ha definido una política y/o procedimiento para la administración de las librerías de medios de datos, por lo cual no se puede garantizar la existencia de un inventario de medios y garantizar su uso (mediante revisiones oportunas y seguimiento a cualquier discrepancia).						
DS 12 Administración del ambiente Físico	G		C	HS		

La Entidad implemento medidas de seguridad alineadas al negocio con el fin de mantener un ambiente seguro para la gestión de la información en un ambiente disponible, íntegro y con un grado de confidencialidad. Por lo que se identificaron diferentes medidas de seguridad en el proceso de revisión, tales como: perímetros de seguridad de acceso, ubicación del equipo crítico y áreas de envío y recepción de la información. Asimismo, se cuenta con procedimiento de seguimiento y monitoreo de los incidentes de seguridad sobre los aspectos mencionados y en el cual se realizan revisiones mensuales.						
ME 2 Monitorear y evaluar el control interno	G				FH	E
La Entidad no ha diseñado un procedimiento de control interno el cual establezca la administración de las excepciones al control, así como: análisis de la causa subyacente como la acción correctiva, individuo responsable de la función y cuáles excepciones deberían ser escaladas y partes afectadas.						

Fuente: Elaboración Propia

2.2.1.3 Elemento Tecnología

El elemento Tecnología corresponde a las soluciones con que cuenta la entidad financiera para enfrentar los riesgos asociados a la Seguridad de la Información.

En el punto 1.5.2.4 del capítulo anterior se observan las diferentes relaciones de este elemento con las distintas DI.

Para la comparación se identificaron las soluciones de Tecnología de la entidad y se realizó un análisis de su interrelación con las DI como se muestra en la tabla 2.4.

Tabla 2 4: Mapeo del elemento Tecnología a las Conexiones dinámicas del BMIS

Nombre	Gobierno (G)	Arquitectura (A)	Cultura (C)	Habilitación y Soporte (HS)	Factores Humanos (FH)	Emergentes (E)
Bitácora cambio de claves de servidores y equipos de comunicación	G		C	HS		
Data Lost Prevention		A	C	HS		
Host Intrusion Prevention		A		HS		
Antivirus Mcafee VirusScan		A	C	HS		
Antispyware Mcafee		A	C	HS		
Secure CRT		A		HS		
AC Aire acondicionado		A		HS		
Arreglo de Discos para Servidores de virtualización		A		HS		
Enrutador Secundario		A		HS		
Servidor de Monitoreo		A		HS		
Servidor BD Pruebas		A		HS		
NAS Respaldos servidores		A		HS		
Ups principal servidores		A		HS		
Ups área operativa		A		HS		
Arreglo discos		A		HS		
Planta energía eléctrica		A		HS		
Servidor Active Directory Secundario		A		HS		
Módulos de seguridad de los sistemas		A	C	HS		

Cámara CC	G	A		HS		
Detector Humo	G	A		HS	FH	
Sensor temperatura	G	A		HS		
Firewall Pag Trans		A		HS		
Firewall Principal		A		HS		
La entidad cuenta con recursos importante y significativos para un adecuada gestión de la seguridad de la información, la relación con la arquitectura es básica para proveer de una adecuada gestión así como los recursos para la habilitación y soporte						

Fuente: Elaboración Propia

2.2.1.4 Elemento Personas

El elemento Personas corresponde a los recursos humanos, no solo al personal interno, sino a cualquier persona que tenga relación de alguna forma con la entidad, en el punto 1.5.2.3 del capítulo anterior se describe claramente este elemento.

Para la comparación se identificaron las políticas y/o documento que corresponden a este elemento y se analizó en lo conducente con las diferentes DI que se relaciona.

El análisis se muestra a continuación en la tabla 2.5

Tabla 2 5: Mapeo del elemento Personas a las Conexiones dinámicas del BMIS

Nombre	Gobierno (G)	Arquitectura (A)	Cultura (C)	Habilitación y Soporte (HS)	Factores Humanos (FH)	Emergentes (E)
Plan de capacitación TI			C		FH	
Manual descriptivo Clases de Puestos			C		FH	
Oficial de Seguridad física			C		FH	
La relación entre la cultura y los factores humanos con el elemento persona es básico para la adecuada gestión de los recursos de TI, es importante que el plan de capacitación de Involucre a todo el personal de la entidad, no solamente al personal de TI.						

Fuente: Elaboración Propia

2.2.2.- Interconexiones Dinámicas (DIs)

Las conexiones dinámicas representan la forma en que se relacionan los elementos, para efectos de la comparación se mapearon con los diferentes elementos y se les identifico las respectivas políticas y/o documentos que pertenecen de acuerdo con la visión holística del BMIS.

Es importante en este punto repasar la lectura de lo descrito en el capítulo anterior en el punto 1.5.3 en donde se explica cada una de estas DIs con la finalidad de obtener un mejor entendimiento de cada una

Para efectos de este trabajo el nivel de profundidad no es significativo ya que se trata del establecimiento de políticas únicamente, no se pretende hacer un análisis exhaustivo de cada interconexión ya que esto requeriría de mucho tiempo y ampliación del trabajo, sin embargo, si es importante acotar que el estudio de estas DIs proporcionará a la entidad una base que le permitirá el poder implementar de manera eficiente la Seguridad de la Información en la entidad.

A continuación se detallan las políticas y/o documentos asociados a cada una de las DIs con su correspondiente relación con los elementos y otras DIs.

2.2.2.1 Interconexión Dinámica Gobierno

Este DI se relaciona directamente con el elemento procesos y el elemento organización su mapeo es como se puede ver en la tabla 2.6

Tabla 2 6: Mapeo de DI Gobierno a los Elementos y Conexiones dinámicas del BMIS

Nombre	Elemento	Arquitectura (A)	Cultura (C)	Habilitación y Soporte (HS)	Factores Humanos (FH)	Emergentes (E)
8. Mejoramiento del SGSI	ORG		C			E
Políticas para la contratación de Proveedores para servicios TI	ORG			HS		
Políticas de Tecnología de Información	ORG		C	HS		
4.1 Requisitos Generales ISO/IEC 27001-2008	ORG		C			
5.1 Compromiso de la gerencia	ORG		C			
7. Revisión Gerencial del SGSI	ORG					E
Política Seguridad Física	ORG	A		HS		
Política Seguridad Lógica – Acceso a Datos	ORG	A		HS		
Política Desarrollo de Sistemas	ORG			HS	FH	
Política Software y Base de Datos	ORG	A		HS		
Política Hardware y Redes	ORG	A		HS		
Política Continuidad de operaciones	ORG	A	C	HS	FH	
Política Condiciones de Uso, Servicios financieros por internet	ORG		C	HS		
Procedimientos de Recepción y Manejo de Claves Compartidas	ORG			HS		
Procedimiento para el cambio de clave base datos	ORG			HS	FH	
Procedimiento para la creación eliminación y revisión de usuario	ORG			HS	FH	

Procedimiento de Asistencia de Eventos Tecnológico (Reporte)	ORG	A		HS	FH	
Sistema de Gestión ISO/IEC 27001-2008	ORG	A	C		FH	E
5 Responsabilidad de la Gerencia	ORG		C			
Normas y procedimientos relacionados con el uso de mensajería interna y externa	PRO		C		FH	
Respaldos Automáticos	PRO	A		HS		
Procedimientos para Monitoreo de Riesgos (Informe)	PRO		C			E
Procedimiento para Caso de Negocio (Manual)	PRO		C			
Procedimientos para la Seguridad TI (Manual)	PRO		C	HS		
Procedimientos para la Administración Integral de Riesgos (Manual)	PRO	A	C			
Procedimientos de la Unidad de Riesgos, políticas, límites y funciones (Manual)	PRO	A	C			
Control de proveedores de servicios de TI	PRO			HS	FH	
4.2 Establecer y manejar el SGSI	PRO	A	C	HS		
4.3 Requisitos de documentación	PRO			HS		
6. Auditorías Internas	PRO					E
PO 09 Riesgos de TI	PRO	A		HS		
DS 04 Garantizar la continuidad del Negocio	PRO	A	C	HS	FH	E
DS 05 Seguridad de los sistemas de Información	PRO	A	C	HS		
DS 12 Administración del ambiente Físico	PRO		C	HS		
ME 2 Monitorear y evaluar el control interno	PRO				FH	E

Bitácora cambio de claves de servidores y equipos de comunicación	TEC		C	HS		

Fuente: Elaboración Propia

La entidad adoptó el estándar ISO/IEC 27001-2008 el cual se encuentra en su fase de planificación el cual impacta directamente en los procesos que se debe de realizar para poder tener una adecuada implementación.

2.2.2.2. Interconexión dinámica Arquitectura

El DI Arquitectura se relaciona directamente con el elemento organización y tecnología su mapeo es como se puede ver en la tabla 2.7

Tabla 2 7: Mapeo de DI Arquitectura a los Elementos y Conexiones dinámicas del BMIS

Nombre	Elemento	Gobierno (G)	Cultura (C)	Habilitación y Soporte (HS)	Factores Humanos (FH)	Emergentes (E)
Política Seguridad Física	ORG	G		HS		
Política Seguridad Lógica – Acceso a Datos	ORG	G		HS		
Política Software y Base de Datos	ORG	G		HS		
Política Hardware y Redes	ORG	G		HS		
Política Continuidad de operaciones	ORG	G	C	HS	FH	
Procedimiento de Asistencia de Eventos Tecnológico (Reporte)	ORG	G		HS	FH	
Sistema de Gestión ISO/IEC 27001-2008	ORG	G	C		FH	E
Respaldos Automáticos	PRO	G		HS		
Procedimiento para Monitoreo de Red (Manual)	PRO		C	HS		
Procedimientos para la Administración Integral de Riesgos (Manual)	PRO	G	C			
Procedimientos de la Unidad de Riesgos, políticas, límites y funciones (Manual)	PRO	G	C			
4.2 Establecer y manejar el SGSI	PRO	G	C	HS		
5.2 Gestión de Recursos	PRO		C	HS		
Procedimientos para claves para servicios y equipos de comunicación	PRO			HS		
PO 09 Riesgos de TI	PRO	G		HS		

AI 06 Administración de Cambios	PRO			HS		
DS 04 Garantizar la continuidad del Negocio	PRO	G	C	HS	FH	E
DS 05 Seguridad de los sistemas de Información	PRO	G	C	HS		
DS 11 Administración de Datos	PRO			HS		
AC Aire acondicionado	TEC			HS		
Arreglo de Discos para Servidores de virtualización	TEC			HS		
Enrutador Secundario	TEC			HS		
Servidor de Monitoreo	TEC			HS		
Servidor BD Pruebas	TEC			HS		
NAS Respaldos servidores	TEC			HS		
Ups principal servidores	TEC			HS		
Ups área operativa	TEC			HS		
Arreglo discos	TEC			HS		
Planta energía eléctrica	TEC			HS		
Servidor Active Directory Secundario	TEC			HS		
Data Lost Prevention	TEC		C	HS		
Host Intrusion Prevention	TEC			HS		
Antivirus Mcafee VirusScan	TEC		C	HS		
Antispyware Mcafee	TEC		C	HS		
Secure CRT	TEC			HS		
Módulos de seguridad de los sistemas	TEC		C	HS		
Firewall Pag Trans	TEC			HS		
Firewall Principal	TEC			HS		

Fuente: Elaboración Propia

La entidad no tiene una arquitectura de seguridad definida adecuadamente.

2.2.2.3 Interconexión dinámica Cultura

El DI Cultura se relaciona directamente con el elemento organización y Personas su mapeo es como se puede ver en la tabla 2.8

Tabla 2 8: Mapeo de DI Cultura a los Elementos y Conexiones dinámicas del BMIS

Nombre	Elemento	Gobierno (G)	Arquitectura (A)	Habilitación y Soporte (HS)	Factores Humanos (FH)	Emergentes (E)
8. Mejoramiento del SGSI	ORG	G				E
Políticas de Tecnología de Información	ORG	G		HS		
4.1 Requisitos Generales ISO/IEC 27001-2008	ORG	G				
5.1 Compromiso de la gerencia	ORG	G				
Política Continuidad de operaciones	ORG	G	A	HS	FH	
Política Condiciones de Uso, Servicios financieros por internet	ORG	G		HS		
Sistema de Gestión ISO/IEC 27001-2008	ORG	G	A		FH	E
5 Responsabilidad de la Gerencia	ORG	G				
Plan de capacitación TI	PER				FH	
Manual descriptivo Clases de Puestos	PER				FH	
Oficial de Seguridad física	PER				FH	
Normas y procedimientos relacionados con el uso de mensajería interna y externa	PRO	G			FH	
Procedimiento para Monitoreo de Red (Manual)	PRO		A	HS		

Procedimientos para Monitoreo de Riesgos (Informe)	PRO	G				E
Procedimiento para Caso de Negocio (Manual)	PRO	G				
Procedimientos para la Seguridad TI (Manual)	PRO	G		HS		
Procedimientos para la Administración Integral de Riesgos (Manual)	PRO	G	A			
Procedimientos de la Unidad de Riesgos, políticas, límites y funciones (Manual)	PRO	G	A			
4.2 Establecer y manejar el SGSI	PRO	G	A	HS		
5.2 Gestión de Recursos	PRO		A	HS		
DS 04 Garantizar la continuidad del Negocio	PRO	G	A	HS	FH	E
DS 05 Seguridad de los sistemas de Información	PRO	G	A	HS		
DS 12 Administración del ambiente Físico	PRO	G		HS		
Bitácora cambio de claves de servidores y equipos de comunicación	TEC	G		HS		
Data Lost Prevention	TEC		A	HS		
Antivirus Mcafee VirusScan	TEC		A	HS		
Antispyware Mcafee	TEC		A	HS		
Módulos de seguridad de los sistemas	TEC		A	HS		

Fuente: Elaboración Propia

Con base en las entrevistas realizadas la entidad considera que la seguridad de información es adecuada y que muchas exigencias generan costos que no tienen un valor agregado real para la entidad, asimismo, existen muchos perspectivas diferentes en los entrevistados, la cultura de seguridad de la información no es fuerte.

2.2.2.4 Interconexión dinámica Habilitación y Soporte

El Di Habilitación y Soporte se relaciona directamente con el elemento Procesos y Tecnología su mapeo es como se puede ver en la tabla 2.9

Tabla 2 9: Mapeo de DI Habilitación y Soporte a los Elementos y Conexiones dinámicas del BMIS

Nombre	Elemento	Gobierno (G)	Arquitectura (A)	Cultura (C)	Factores Humanos (FH)	Emergentes (E)
Políticas para la contratación de Proveedores para servicios TI	ORG	G				
Políticas de Tecnología de Información	ORG	G		C		
Política Seguridad Física	ORG	G	A			
Política Seguridad Lógica – Acceso a Datos	ORG	G	A			
Política Desarrollo de Sistemas	ORG	G			FH	
Política Software y Base de Datos	ORG	G	A			
Política Hardware y Redes	ORG	G	A			
Política Continuidad de operaciones	ORG	G	A	C	FH	
Política Condiciones de Uso, Servicios financieros por internet	ORG	G		C		
Procedimientos de Recepción y Manejo de Claves Compartidas	ORG	G				
Procedimiento para el cambio de clave base datos	ORG	G			FH	
Procedimiento para la creación eliminación y revisión de usuario	ORG	G			FH	
Procedimiento de Asistencia de Eventos Tecnológico (Reporte)	ORG	G	A		FH	
Respaldos Automáticos	PRO	G	A			
Procedimiento para Monitoreo de Red (Manual)	PRO		A	C		

Procedimientos para la Seguridad TI (Manual)	PRO	G		C		
Control de proveedores de servicios de TI	PRO	G			FH	
4.2 Establecer y manejar el SGSI	PRO	G	A	C		
4.3 Requisitos de documentación	PRO	G				
5.2 Gestión de Recursos	PRO		A	C		
Procedimientos para claves para servicios y equipos de comunicación	PRO		A			
PO 09 Riesgos de TI	PRO	G	A			
AI 06 Administración de Cambios	PRO		A			
DS 04 Garantizar la continuidad del Negocio	PRO	G	A	C	FH	E
DS 05 Seguridad de los sistemas de Información	PRO	G	A	C		
DS 11 Administración de Datos	PRO		A			
DS 12 Administración del ambiente Físico	PRO	G		C		
Bitácora cambio de claves de servidores y equipos de comunicación	TEC	G		C		
AC Aire acondicionado	TEC		A			
Arreglo de Discos para Servidores de virtualización	TEC		A			
Enrutador Secundario	TEC		A			
Servidor de Monitoreo	TEC		A			
Servidor BD Pruebas	TEC		A			
NAS Respaldos servidores	TEC		A			
Ups principal servidores	TEC		A			
Ups área operativa	TEC		A			
Arreglo discos	TEC		A			
Planta energía eléctrica	TEC		A			
Servidor Active Directory Secundario	TEC		A			
Data Lost Prevention	TEC		A	C		
Host Intrusion Prevention	TEC		A			
Antivirus Mcafee VirusScan	TEC		A	C		

Antispyware Mcafee	TEC		A	C		
Secure CRT	TEC		A			
Módulos de seguridad de los sistemas	TEC		A	C		
Cámara CC	TEC	G				
Detector Humo	TEC	G			FH	
Sensor temperatura	TEC	G				
Firewall Pag Trans	TEC		A			
Firewall Principal	TEC		A			

Fuente: Elaboración Propia

El departamento de Tecnologías de Información se encuentra con actividades que se sobreponen a la prioridad de la seguridad de la información, existe una definición de los principales riesgos que deben ser soportados y habilitados por el departamento, estos riesgos se definieron en conjunto con el comité de auditoría. Eso son las aplicaciones que tienen prioridad empresarial para cumplir con disponibilidad, sin embargo, no se consideran aspectos como la integridad de los datos.

2.2.2.5 Interconexión dinámica Factores Humanos

El DI Factores Humanos se relaciona directamente con el elemento Personas y Tecnología su mapeo es como se puede ver en la tabla 2.10

Tabla 2 10: Mapeo de DI Factores Humanos a los Elementos y Conexiones dinámicas del BMIS

Nombre	Elemento	Gobierno (G)	Arquitectura (A)	Cultura (C)	Habilitación y Soporte (HS)	Emergentes (E)
Política Desarrollo de Sistemas	ORG	G			HS	
Política Continuidad de operaciones	ORG	G	A	C	HS	
Procedimiento para el cambio de clave base datos	ORG	G			HS	
Procedimiento para la creación eliminación y revisión de usuario	ORG	G			HS	
Procedimiento de Asistencia de Eventos Tecnológico (Reporte)	ORG	G	A		HS	
Sistema de Gestión ISO/IEC 27001-2008	ORG	G	A	C		E
Plan de capacitación TI	PER			C		
Manual descriptivo Clases de Puestos	PER			C		
Oficial de Seguridad física	PER			C		
Normas y procedimientos relacionados con el uso de mensajería interna y externa	PRO	G		C		
Control de proveedores de servicios de TI	PRO	G			HS	
DS 04 Garantizar la continuidad del Negocio	PRO	G	A	C	HS	E
ME 2 Monitorear y evaluar el control interno	PRO	G				E
Detector Humo	TEC	G			HS	

Fuente: Elaboración Propia

Existen muchos criterios en formas de pensar de cómo implementar las actividades de tecnologías de información por lo que cada persona lo realiza de la forma que desea sin

tener claro una visión de conjunto, esto genera diferencias de criterios que impactan en la relaciones como equipo de la entidad.

2.2.2.6 Interconexión dinámica Emergentes

El DI Emergentes se relaciona directamente con el elemento Personas y Procesos su mapeo es como se puede ver en la tabla 2.11

Tabla 2 11: Mapeo de DI Emergentes a los Elementos y Conexiones dinámicas del BMIS

Nombre	Elemento	Gobierno (G)	Arquitectura (A)	Cultura (C)	Habilitación y Soporte (HS)	Factores Humanos (FH)
8. Mejoramiento del SGSI	ORG	G		C		
7. Revisión Gerencial del SGSI	ORG	G				
Sistema de Gestión ISO/IEC 27001-2008	ORG	G	A	C		FH
Procedimientos para Monitoreo de Riesgos (Informe)	PRO	G		C		
6. Auditorías Internas	PRO	G				
DS 04 Garantizar la continuidad del Negocio	PRO	G	A	C	HS	FH
ME 2 Monitorear y evaluar el control interno	PRO	G				FH

Fuente: Elaboración Propia

Se encuentra en proceso de diseño el estándar ISO/IEC 27001-2008 con la finalidad de establecer un sistema de gestión que permita aprovechar las oportunidades de mejora en la entidad, actualmente se trabaja de modo reactivo. En la actualidad no hay un programa formal de seguimiento de oportunidades de mejora.

2.3.- Determinación de la Brecha actual.

EL determinar la brecha implica el poder definir claramente lo que se tienen versus lo que falta por hacer con la finalidad de poder cumplir con los requerimientos que se definieron en punto 2.1.3 anterior.

Para efectos de lograrlo adecuadamente se tomó en cuenta el plan remedial que tiene la entidad en proceso de implementación como resultado de una auditoría realizada al proceso de implementación de los procesos COBIT 4.1 que se realiza actualmente, también se tomó la norma ISO/IEC 27001-2008 que se mapeo con COBIT 4.1 y por último se mapearon con el elementos y DIs del BMIS, por lo que a continuación se muestran estos mapeos en la tabla 2.12.

2.3.1.- Mapeo del Plan Remedial con el BMIS

Con la finalidad de valorar el programa actual y establecer la brecha existente se mapeo el plan remedial de la entidad con los elementos y conexiones dinámicas del BMIS como se muestra a continuación en la tabla 2.12.

Tabla 2 12: Mapeo del Plan remedial de la entidad con el BMIS

Detalle de la acción / actividad	COBIT 4.1	BMIS									
		Elementos				Conexiones Dinámicas					
		ORG	PRO	TEC	PER	GOB	ARQ	HYS	CUL	EME	FAC
b. Asegurar que la adquisición de equipos para la prestación de servicios críticos se basa en criterios donde la configuración de los	DS 4.1 Marco de continuidad de TI	X	X			X		X			

equipos contempla componentes de alta disponibilidad.											
b. Adopción de un estándar de seguridad de la información y definición de una estrategia que posibilite en un plazo adecuado consolidar la función de seguridad de la información dentro de la cooperativa.	DS 5.1 Administración de la seguridad de TI DS 5.2 Plan de seguridad de TI	X				X		X			
d. Definición de procedimientos operativos a ejecutar por el oficial de seguridad de TI que permitan el monitoreo de las herramientas de seguridad implementadas y la detección de incidentes.	DS 5.5. Pruebas, vigilancia y monitoreo de la seguridad	X				X		X			
a. Emitir una directriz para que la ejecución de procesos de gestión de riesgos de TI (identificación, evaluación, respuesta) se ejecute una vez al año como actividad previa a la formulación de planes tácticos de manera que las respuestas al riesgo que lo ameriten se incluyan como metas o actividades en los planes anuales y se disponga de recursos para su implementación.	PO 9.1 Alineación de la administración de riesgos de TI y del negocio	X									

d. Definición de lineamientos institucionales para el manejo de información sensitiva en equipos portátiles, tabletas, celulares y medios de almacenamiento externo como llaves USBB o memorias. Estos lineamientos deben considerar tanto el almacenamiento que está autorizado como los métodos sugeridos para el borrado de datos de dichos dispositivos.	DS 11.4 Eliminación	X									
b. Negociación con entidades financieras afines y de características de tamaño y estructura de servicios de TI similares para formalizar acuerdos para comparar el grado de implementación del marco de gestión de TI que se tenga y poder implementar un modelo de benchmarking.	ME 2.1 Monitorear el marco de trabajo de control interno	X									
a. Aprovechar el inventario de recursos críticos para definir un esquema de procesamiento alternativo basado en una estrategia de respaldos y recuperación que permita una restauración del servicio en un plazo razonable.	DS 4.1 Marco de continuidad de TI		X					X	X		

c. Fortalecimiento de los procesos de respaldo para incorporar dentro de estos el envío a un sitio alterno con una periodicidad apropiada los respaldos de bases de datos, de programas fuentes, del repositorio de la configuración, de archivos de usuario final.	DS 4.8 Recuperación y reanudación de los servicios de TI		X					X		X	
c. Integración de procedimientos operativos de gestión de cuentas de usuario con los procesos operativos de recursos humanos definidos para la gestión de ingresos y salidas de funcionarios, gestión de incapacidades, permisos y suspensiones para fortalecer la administración de cuentas de usuario y el mantenimiento de los roles asignados a cada funcionario según el puesto que desempeña.	DS 5.4 Administración de cuentas de usuario		X					X		X	
a. Implementación de los procedimientos operativos para gestión de cambios de procedimientos, procesos, parámetros de sistemas, parámetros de servicios y plataforma base.	AI 6.1 Estándares y procedimientos para cambios		X					X			
b. Implementación de los mecanismos para la atención y documentación de cambios de	AI 6.3 Cambios de emergencia		X					X			

emergencia.											
b. Efectuar las pruebas de conectividad en el nuevo edificio.	DS 12.1 Selección y diseño del centro de datos DS 12.2 Medidas de seguridad física		X					X			
a. Mantener un inventario de los proveedores de servicios de TI para los cuales la entidad logró establecer acuerdos contractuales para recibir en forma periódica informes de control interno.	ME 2.5 Control interno para terceros		X					X			
a. Adaptación de los procedimientos como derivación de las mejoras realizadas a los roles de usuario a nivel de bases de datos, dominio y aplicaciones.	DS 5.4 Administración de cuentas de usuario		X							X	
b. Adaptación de formularios para facilitar el mantenimiento de perfiles por parte de los usuarios designados como administradores de sistemas.	DS 5.4 Administración de cuentas de usuario		X							X	
d. Mejoramiento de los procesos de respaldo de fuentes para garantizar que existan respaldos externos periódicos que permitan la recuperación ante una contingencia.	DS 11 5 Respaldo y recuperación		X							X	

a. Revisión integral de todos los procedimientos operativos de TI para asegurar que cada uno de ellos define actividades expresas de monitoreo y supervisión enfocadas a garantizar el cumplimiento cabal de las acciones definidas y el reporte de las desviaciones detectadas.	ME 2.1 Monitorear el marco de trabajo de control interno		X							X	
a. Formalizar un procedimiento operativo de ejecución de autoevaluaciones de control interno que se ejecute al menos una vez al año, antes de iniciar la formulación de planes operativos de manera que las mejoras de control interno que ameriten metas o recursos puedan ser contempladas en el plan anual y se les dote de los recursos correspondientes.	ME 2.4 Autoevaluaciones de control interno		X							X	
d. Ejecutar un proceso de gestión de riesgo de TI durante el 2012 aplicando el marco ajustado.	PO 9.1 Alineación de la administración de riesgos de TI y del negocio		X								
a. Elaboración y formalización de procedimientos operativos para la gestión de cambios en procedimientos, procesos, parámetros del sistema,	AI 6.1 Estándares y procedimientos para cambios		X								

parámetros de servicios y plataforma base (vincular con gestión de la configuración)											
b. Aplicación de un proceso de afinamiento de roles y derechos por tipo de puesto que permita estandarizar los privilegios asignados a los usuarios en los sistemas de misión crítica según las responsabilidades que tenga en la cooperativa. .	DS 5.3 Administración de identidad		X								
b. Definición de métodos de archivo de medios alternos seguros que garanticen su conservación y seguridad.	DS 11.3 Sistemas de administración de librerías de medios		X								
a. Implementación de un procedimiento operativo para la catalogación de los medios que conservan respaldos de bases de datos, programas fuentes, datos de configuración, software, archivos sensibles de usuarios relevantes de la entidad que permita conocer cuántos medios de respaldo existen, qué contenido tiene, donde está almacenado, su identificación externa(etiqueta), fecha inicial en que fue utilizado, fecha en que procede su reemplazo)	DS 11.3 Sistemas de administración de librerías de medios		X								

c. Definición del procedimiento operativo que utilizara el método de borrado de datos establecidos y del tipo de documentación (acta de borrado) que se conservara de las acciones ejecutadas.	DS 11.4 Eliminación		X								
a. Definición de procedimientos operativos para la ejecución periódica (al menos una vez por semana) de respaldos de los programas fuentes asociados a los ejecutables que están instalados en el ambiente en producción.	DS 11.5 Respaldo y recuperación		X								
b. Definición de procedimientos operativos para la ejecución de pruebas de restauración de fuentes. .	DS 11.5 Respaldo y recuperación		X								
c. Definición de procedimientos operativos para la ejecución periódica de respaldos del repositorio de configuración.	DS 11.5 Respaldo y recuperación		X								
d. Definición de procedimientos operativos para la ejecución de pruebas de restauración de elementos del repositorio de configuración.	DS 11.5 Respaldo y recuperación		X								

e. Documentación y reporte de los tiempos requeridos para la restauración de bases de datos, fuentes y archivos de configuración que se obtuvieron en las pruebas que se aplican en forma periódica.	DS 11.5 Respaldo y recuperación		X								
c. Establecimiento de la documentación que deberá mantenerse de los cambios de emergencia atendidos.	AI 6.3 Cambios de emergencia				X			X			
b. Identificar el personal de la cooperativa que debe participar en el proceso de gestión de riesgos de TI y brindarle una capacitación sobre el marco de gestión vigente.	PO 9.1 Alineación de la administración de riesgos de TI y del negocio				X						X
b. Definición de criterios para clasificar y dar tratamiento a cambios de emergencia.	AI 6.3 Cambios de emergencia					X		X			
e. Definición de contenido mínimo de reportes sobre la gestión de cambios de: aplicaciones, procedimientos, procesos, parámetros del sistema y de servicios, plataforma base, que se deberán estar generando en forma semestral.	AI 6.4 Seguimiento y reporte del estado del cambio					X		X			

a. Revisión y ajuste de alcances definidos para la función de seguridad de TI y del perfil requerido para ejecutar labores de oficial de seguridad de TI (no oficial de seguridad de la información).	DS 5.1 Administración de la seguridad de TI					X		X			
e. Definición de lineamientos para tipificar lo que se considerará dentro de la cooperativa un incidente de seguridad (ejemplo: intento de acceso con la cuenta de un funcionario que ceso labores), de mecanismos para registrar en bitácoras los eventos que se hayan tipificado como tal y de acciones a ejecutar según el nivel de impacto que pueda llegar a tener.	DS 5.6 Definición de incidentes de seguridad					X		X			
a. Alinear el marco de gestión de riesgos de TI para que los criterios de calificación de la probabilidad e impacto de los eventos, los mapas de riesgo (aceptación de riesgo) y las actividades de identificación, evaluación y administración de riesgo tengan uniformidad con lo que a nivel institucional se establezca para la medición del riesgo operativo.	PO 9.1 Alineación de la administración de riesgos de TI y del negocio					X					

b. Incorporar en el marco de gestión de riesgos de TI criterios para efectuar valoraciones cuantitativas de eventos.	PO 9.1 Alineación de la administración de riesgos de TI y del negocio PO 9.4 Evaluación de riesgos de TI					X					
c. Incorporar en el marco de gestión de riesgos de TI lineamientos para que la elaboración de respuestas al riesgo contemplen el análisis y documentación de los costos y beneficios estimados de los controles propuestos para mitigar riesgo.	PO 9.1.Alineación de la administración de riesgos de TI y del negocio PO 9.5 Respuesta a los riesgos					X					
e. Ajustar la normativa del comité de TI y la del comité de riesgos para que los informes de riesgo de TI sean conocidos en el seno del comité de riesgos y se propicie mayor alineamiento entre el marco de riesgo institucional y el de TI.	PO 9.1 Alineación de la administración de riesgos de TI y del negocio					X					
a. Planificación de cursos de administración de información.	DS 11.1 Requerimientos del negocio para la administración de datos					X					
b. Definir el contenido y periodicidad del informe de control interno que la cooperativa considera apropiado (entiéndase cuáles	ME 2.5 Control interno para terceros					X					

procesos de COBIT 4.1, con qué frecuencia se reciben los informes)											
c. Negociar con los proveedores que la SUGEF ha identificado a partir del perfil tecnológico como proveedores relevantes la remisión anual de informes de auditoría y de planes correctivos cuyo alcance no debe ser menor al marco de gestión que la superintendencia definió. Negociar a su vez, informes semestrales de cumplimiento de los planes correctivos que fueron suministrados.	ME 2.5 Control interno para terceros					X					
b. Catalogado de todos los medios de respaldo en uso según los lineamientos definidos en el procedimiento.	DS 11.3 Sistemas de administración de librerías de medios						X	X			
a. Inventariado de equipos de la institución (servidores, estaciones de trabajo, portátiles, tabletas, celulares) en los que maneja información sensitiva.	DS 11.4 Eliminación						X	X			
f. Generar informes semestrales de la ejecución de planes de mitigación para conocimiento y aprobación en el comité de riesgos.	PO 9.6 Mantenimiento y monitoreo de un plan de acción de riesgos							X	X		

c. Generación semestral de informes de la gestión de cambios según el contenido mínimo establecido.	AI 6.4 Seguimiento y reporte del estado del cambio							X	X		
a. Configurar a partir de las revisiones de la ejecutoria de los procedimientos operativos un registro unificado de excepciones de control detectadas que permita darle un seguimiento estandarizado a las causas de las desviaciones y generar acciones correctivas.	ME 2.3 Excepciones de control							X		X	
d. Crear un repositorio de eventos de riesgo que se hayan materializado donde se registre datos básicos sobre el incidente (ejemplo, fecha, descripción del incidente, detalle del impacto estimado para la entidad desde las perspectivas de incremento de costo, imagen, afectación de la disponibilidad del servicio, retraso en el cumplimiento de objetivos, reducción de ingresos, etc.). Este repositorio es de especial importancia para fortalecer los criterios futuros de calificación de eventos, su probabilidad y	PO 9.3 Identificación de eventos PO 9.6 Mantenimiento y monitoreo de un plan de acción de riesgos							X			

consecuencia sobre bases más objetivas.											
d. Formalización de mecanismo de seguimiento de cambios a procedimientos, procesos, parámetros del sistema y de servicios, plataforma base que permita conocer el estado de cada solicitud de cambio que está siendo atendida.	AI 6.4 Seguimiento y reporte del estado del cambio							X			
d. Mantener enlaces redundantes para las oficinas sucursales de mayor volumen transaccional.	DS 4.8 Recuperación y reanudación de los servicios de TI							X			
a. Generación de un inventario de las cuentas de usuario activas definidas a nivel de sistema operativo, bases de datos y sistemas de misión crítica.	DS 5.3 Administración de identidad							X			
c. Generación de un inventario de los derechos y privilegios asignados a cada usuario a nivel de sistema operativo (grupos a los que está asociado y derechos que tenga ese grupo dentro del dominio) y bases de datos (roles y derechos asignados).	DS 5.3 Administración de identidad							X			
d. Consolidación de un repositorio con las	DS 5.3 Administración							X			

identidades asignadas a cada usuario y los derechos asignados a cada uno a nivel de aplicaciones, bases de datos y sistema operativo.	de identidad										
a. Definición de criterios institucionales sobre la vida útil de los datos transaccionales que permita consolidar una estrategia para conservar en las bases de datos los datos que son utilizables y para extraer hacia medios alternos aquellos que cumplieron con su ciclo transaccional.	DS 11.2 Acuerdos de almacenamiento y conservación							X			
e. Inventariado de los métodos aplicados para cifrado de datos (palabras de paso, datos sensitivos, etc.) y definición de un método para limitar el acceso ha dicho material.	DS 11.6 Requerimientos de seguridad para la administración de datos							X			
f. Mantenimiento en bóvedas de sobres marchamados con las claves de usuario privilegiado a nivel de sistema operativo, bases de datos y aplicaciones para atender posibles contingencias.	DS 11.6 Requerimientos de seguridad para la administración de datos							X			
b. Definición de un método para borrado de datos de estos equipos cuando dicho dispositivo cumple su vida útil, se asigna a otro funcionario o es devuelto a una	DS 11.4 Eliminación							X			

empresa que lo había entregado por un contrato de arrendamiento)											
a. Completar la instalación de enlaces, aires acondicionados, muebles para habilitar el nuevo edificio.	DS 12.1 Selección y diseño del centro de datos DS 12.2 Medidas de seguridad física							X			
c. Trasladar las oficinas de los funcionarios de TI hacia la nueva edificación construida	DS 12.1 Selección y diseño del centro de datos DS 12.2 Medidas de seguridad física							X			
d. Trasladar el "data center" a la nueva edificación.	DS 12.1 Selección y diseño del centro de datos DS 12.2 Medidas de seguridad física							X			
c. Mejoramiento de los métodos de conservación de documentos (garantías, pagarés, formularios de beneficiarios, etc.) que son complemento fundamental de datos sensitivos registrados en las bases de datos de la institución para garantizar que no están expuestos a deterioro, robo o destrucción	DS 11.2 Acuerdos de almacenamiento y conservación									X	

c. Coordinar con el área de recursos humanos para que mantenga un programa de inducción periódico en la temática de riesgos de TI que se brinde cada vez que ingresen nuevos funcionarios que deban ejecutar dicha labor o cuando se ejecuten cambios sustantivos en el marco de gestión de riesgos de TI.	PO 9.1 Alineación de la administración de riesgos de TI y del negocio										X

Fuente: Elaboración Propia

2.3.2.- Mapeo de la norma ISO/IEC 27001-2008 con COBIT 4.1.

EL mapeo de la norma ISO/IEC 27001-2008 con COBIT 4.1 se realzó con la finalidad de establecer la correspondencia de los requerimientos. En la tabla 2.13 se muestra la relación.

Tabla 2 13: Mapeo de la Norma ISO/IEC 27001-2008 con COBIT 4.1

Capítulo ISO/IEC 27001-2008	Sub-Ítem Capítulo	MAPEO COBIT 4.1	Áreas Clave /Requerimiento
4	4.1	PO 1.4	Requisitos Generales
4	4.2	PO1.1.	Establecer y manejar el SGSI
4	4.2.1	PO1.4	Creación del SGSI
4	4.2.1.a	PO 1.2.	a) Definir el alcance y los límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología e incluyendo los detalles de y la justificación de cualquier exclusión del alcance (ver 1.2).
4	4.2.1.b.	PO 1.2.	b) Definir una política SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología que:
4	4.2.1.b.1	PO 1.2.	1. incluya un marco referencial para establecer sus objetivos y establezca un sentido de dirección general y principios para la acción con relación a la seguridad de la información
4	4.2.1.b.2	PO 1.2.	2. tome en cuenta los requerimientos comerciales y legales o reguladores, y las obligaciones de la seguridad contractual
4	4.2.1.b.3	PO 1.2.	3. esté alineada con el contexto de la gestión riesgo estratégico de la organización en el cual se dará el establecimiento y mantenimiento del SGSI
4	4.2.1.b.4	PO 1.2.	4. establezca el criterio con el que se evaluará el riesgo (ver 4.2.1c);
4	4.2.1.b.5	PO 1.2.	5. haya sido aprobada por la gerencia.
4	4.2.1.c	PO 9.1 - PO 9.2	c) Definir el enfoque de valuación del riesgo de la organización

4	4.2.1.c,1	PO 9.1 - PO 9.2	1. Identificar una metodología de cálculo del riesgo adecuado para el SGSI y los requerimientos identificados de seguridad, legales y reguladores de la información comercial
4	4.2.1.c,2	PO 9.3	2. Desarrollar los criterios para aceptar los riesgos e identificar los niveles de riesgo aceptables (ver 5.1f).
4	4.2.1.d	PO 9.3	d) Identificar los riesgos
4	4.2.1.d.1	PO 9.3	1) Identificar los activos dentro del alcance del SGSI y los propietarios de estos activos.
4	4.2.1.d.2	PO 9.3	2) Identificar las amenazas para aquellos activos.
4	4.2.1.d.3	PO 9.3	3) Identificar las vulnerabilidades que podrían ser explotadas por las amenazas
4	4.2.1.d.4	PO 9.3	4) Identificar los impactos que pueden tener las pérdidas de confiabilidad, integridad y disponibilidad sobre los activos
4	4.2.1.e	PO 9.4	e) Analizar y evaluar el riesgo
4	4.2.1.e.1	PO 9.4	1) Calcular el impacto comercial sobre la organización que podría resultar de una falla en la seguridad, tomando en cuenta las consecuencias de una pérdida de confidencialidad, integridad o disponibilidad de los activos
4	4.2.1.e.2	PO 9.4	2) Calcular la probabilidad realista de que ocurra dicha falla a la luz de las amenazas y vulnerabilidades prevalecientes, y los impactos asociados con estos activos, y los controles implementados actualmente.
4	4.2.1.e.3	PO 9.4	3) Calcular los niveles de riesgo.
4	4.2.1.e.4	PO 9.4	4. Determinar si el riesgo es aceptable o requiere tratamiento utilizando el criterio de aceptación del riesgo establecido en 4.2.1 (c) (2).
4	4.2.1.f.	PO 9.5	f) Identificar y evaluar las opciones para el tratamiento de los riesgos
4	4.2.1.g	PO 9.5	g) Seleccionar objetivos de control y controles para el tratamiento de riesgos
4	4.2.1.h	PO 9.6	h) Obtener la aprobación de la gerencia para los riesgos residuales propuestos.
4	4.2.1.i	PO 9.6	i) Obtener la autorización de la gerencia para implementar y operar el SGSI.
4	4.2.1.j	PO 9.5	j) Preparar un Enunciado de Aplicabilidad, que incluya

4	4.2.1.j.1	PO 9.5	1) los objetivos de control y los controles seleccionados en 4.2.1 (g) y las razones para su selección
4	4.2.1.j.2	PO 9.5	2) los objetivos de control y controles implementados actualmente (ver 4.2.1 (e) 2); y
4	4.2.1.j.3	PO 9.5	3) la exclusión de cualquier objetivo de control y control en el Anexo A (ISO/IEC 27002:2005) y la justificación para su exclusión
4	4.2.2	PO 1.5	Implementación y Operación del SGSI
4	4.2.2.a	PO 1.5	a) Formular un plan de tratamiento de riesgo que identifique la acción gerencial apropiada, los recursos, las responsabilidades y prioridades para manejar los riesgos de la seguridad de información (ver 5).
4	4.2.2.b	PO 9.5	b) Implementar el plan de tratamiento de riesgo para poder lograr los objetivos de control identificados, los cuales incluyen tener en consideración el financiamiento y asignación de roles y responsabilidades.
4	4.2.2.c	DS5-AI06-Ds11-DS12-DS4 y ME02	c) Implementar los controles seleccionados en 4.2.1 (g) para satisfacer los objetivos de control.
4	4.2.2.d	PO 1.5	d) Definir cómo medir la efectividad de los controles o grupos de controles seleccionados y especificar cómo se van a utilizar estas mediciones para evaluar la efectividad del control para producir resultados comparables y reproducibles (ver 4.2.3 c)).
4	4.2.2.e	DS 7	e) Implementar los programas de capacitación y conocimiento (ver 5.2.2).
4	4.2.2.f	D S 5	f) Manejar las operaciones del SGSI.
4	4.2.2.g	D S 5	g) Manejar recursos para el SGSI (ver 5.2).
4	4.2.2.h	DS 5.6	h) Implementar los procedimientos y otros controles capaces de permitir una pronta detección de y respuesta a incidentes de seguridad (véase el apartado 4.2.3.a)
4	4.2.3	DS 5.6	Supervisión y Revisión
4	4.2.3.a	DS 5.6	a) Ejecutar procedimientos de monitoreo y revisión, y otros controles para:
4	4.2.3.a.1	DS 5.6	1) detectar prontamente los errores en los resultados de procesamiento;

4	4.2.3.a.2	DS 5.6	2) identificar prontamente los incidentes y violaciones de seguridad fallidos y exitosos
4	4.2.3.a.3	DS 5.6	3) permitir a la gerencia determinar si las actividades de seguridad delegadas a las personas o implementadas mediante la tecnología de información se están realizando como se esperaba
4	4.2.3.a.4	DS 5.6	4) ayudar a detectar los eventos de seguridad, evitando así los incidentes de seguridad mediante el uso de indicadores; y
4	4.2.3.a.5	DS 5.6	5) determinar si son efectivas las acciones tomadas para resolver una violación de seguridad.
4	4.2.3.b	ME 2	b) Realizar revisiones regulares de la efectividad del SGSI (incluyendo satisfacer la política y objetivos de seguridad del SGSI, y revisar los controles de seguridad) tomando en cuenta los resultados de auditorías de seguridad, incidentes, mediciones de seguridad, sugerencias y retroalimentación de todas las partes interesadas
4	4.2.3.c	ME 2	c) Medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.
4	4.2.3.d	ME 2	d) Revisar las evaluaciones del riesgo a intervalos planeados y revisar el nivel de riesgo residual y riesgo aceptable identificado, tomando en cuenta los cambios en:
4	4.2.3.d.1	ME 2	1) la organización;
4	4.2.3.d.2	ME 2	2) tecnología;
4	4.2.3.d.3	ME 2	3) objetivos y procesos comerciales;
4	4.2.3.d.4	ME 2	4) amenazas identificadas;
4	4.2.3.d.5	ME 2	5) efectividad de los controles implementados; y
4	4.2.3.d.6	ME 2	6) eventos externos, como cambios en el ambiente legal o regulador, cambios en obligaciones contractuales y cambios en el clima social.
4	4.2.3.e	ME 2	e) Realizar auditorías SGSI internas a intervalos planeados (ver 6).
4	4.2.3.f	ME 2	f) Realizar una revisión gerencial del SGSI sobre una base regular para asegurar que el alcance permanezca adecuado y se identifiquen las mejoras en el proceso SGSI (ver 7.1).

4	4.2.3.g	ME 2	g) Actualizar los planes de seguridad para tomar en cuenta los descubrimientos de las actividades de monitoreo y revisión
4	4.2.3.h	ME 2	h) Registrar las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño del SGSI (ver 4.3.3).
4	4.2.4	ME 4	Mantenimiento y Mejora del SGSI
4	4.2.4.a	ME 4	a) Implementar las mejoras identificadas en el SGSI.
4	4.2.4.b	ME 4	b) Tomar las acciones correctivas y preventivas apropiadas en concordancia con 8.2 y 8.3. Aplicar las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y aquellas de la organización misma
4	4.2.4.c	ME 4	c) Comunicar los resultados y acciones a todas las partes interesadas con un nivel de detalle apropiado de acuerdo a las circunstancias y, cuando sea relevante, acordar cómo proceder.
4	4.2.4.d	ME 4	d) Asegurar que las mejoras logren sus objetivos señalados
4	4.3	PO 1.5	Requisitos de la documentación
4	4.3.1	PO 1.5	Generalidades
4	4.3.1	PO 1.5	La documentación debe incluir los registros de las decisiones gerenciales, asegurar que las acciones puedan ser monitoreadas a las decisiones y políticas gerenciales, y los resultados registrados deben ser reproducibles. Es importante ser capaces de demostrar la relación desde los controles seleccionados y de regreso a los resultados del proceso de evaluación del riesgo y tratamiento del riesgo, y subsecuentemente, de regreso a la política y objetivos del SGSI
4	4.3.1.a	PO 1.2	a. enunciados documentados de la política SGSI (ver 4.2.1b)) y los objetivos;
4	4.3.1.b	PO 1.2	b. el alcance del SGSI (ver 4.2.1a));
4	4.3.1.c	PO 1.5	c. procedimientos y controles de soporte del SGSI;
4	4.3.1.d	PO 9.1	d. una descripción de la metodología de evaluación del riesgo (ver 4.2.1c));
4	4.3.1.e	PO 9.4	e. reporte de evaluación del riesgo (ver 4.2.1c) a 4.2.1g));
4	4.3.1.f	PO 9.5	f. plan de tratamiento del riesgo (ver 4.2.2b));

4	4.3.1.g	PO 1.5	g. Los procedimientos documentados necesarios por la organización para asegurar la planeación, operación y control de sus procesos de seguridad de la información y describir cómo medir la efectividad de los controles (ver 4.2.3c));
4	4.3.1.h	PO 1.5	h. registros requeridos por este Estándar Internacional (ver 4.3.3); y
4	4.3.1.i	PO 9.5	i. Enunciado de Aplicabilidad.
4	4.3.2	PO 1.5	Control de Documentos
4	4.3.2.a	PO 1.5	a. aprobar la idoneidad de los documentos antes de su emisión;
4	4.3.2.b	ME 2	b. revisar y actualizar los documentos conforme sea necesario y re-aprobar los documentos
4	4.3.2.c	ME 2	c. asegurar que se identifiquen los cambios y el status de la revisión actual de los documentos
4	4.3.2.d	ME 2	d. asegurar que las versiones más recientes de los documentos relevantes estén disponibles en los puntos de uso;
4	4.3.2.e	ME 2	e. asegurar que los documentos se mantengan legibles y fácilmente identificables;
4	4.3.2.f	ME 2	f. asegurar que los documentos estén disponibles para aquellos que los necesitan; y sean transferidos, almacenados y finalmente eliminados en concordancia con los procedimientos aplicables para su clasificación;
4	4.3.2.g	ME 2	g. asegurar que se identifiquen los documentos de origen externo
4	4.3.2.h	ME 2	h. asegurar que se controle la distribución de documentos;
4	4.3.2.i	ME 2	i. evitar el uso indebido de documentos obsoletos; y
4	4.3.2.j	ME 2	j. aplicarles una identificación adecuada si se van a retener por algún propósito
4	4.3.3	PO 1.5	Control de Registros
4	4.3.3	PO 1.5	Se deben establecer y mantener registros para proporcionar evidencia de conformidad con los requerimientos y la operación efectiva del SGSI. Deben ser protegidos y controlados.

4	4.3.3	PO 1.5	El SGSI debe tomar en cuenta cualquier requerimiento legal o regulador relevante
4	4.3.3	PO 1.5	Los registros deben mantenerse legibles, fácilmente identificables y recuperables.
4	4.3.3	PO 1.5	Se deben documentar e implementar los controles necesarios para la identificación, almacenaje, protección, recuperación, tiempo de retención y disposición de los registros.
4	4.3.3	ME 2	Se deben mantener registros del desempeño del proceso tal como se delinea en 4.2 y de todas las ocurrencias de incidentes de seguridad significativos relacionados con el SGSI.
5		PO 1.1	Responsabilidad de la gerencia
5	5.1	PO 1.1	Compromiso de la gerencia
5	5.1.a	PO 1.1	a) establecer una política SGSI;
5	5.1.b	PO 1.4	b) asegurar que se establezcan objetivos y planes SGSI;
5	5.1.c	PO 1.5	c) establecer roles y responsabilidades para la seguridad de información;
5	5.1.d	PO 1.2	d) comunicar a la organización la importancia de lograr los objetivos de seguridad de la información y cumplir la política de seguridad de la información, sus responsabilidades bajo la ley y la necesidad de un mejoramiento continuo
5	5.1.e	PO 1.1	e) proporcionar los recursos suficientes para desarrollar, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI (ver 5.2.1);
5	5.1.g	PO 9.5	f) decidir el criterio para la aceptación del riesgo y los niveles de riesgo aceptables;
5	5.1.f	ME 2	g) asegurar que se realicen las auditorías internas SGSI (ver 6);
5	5.1.h	ME 2	h) realizar revisiones gerenciales del SGSI (ver 7).
5	5.2	PO 1.1	Gestión de recursos
5	5.2.1	PO 1.1.	Provisión de recursos
5	5.2.1.a	PO 1.1	a) establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI;

5	5.2.1.b	PO 1.2	b) asegurar que los procedimientos de seguridad de la información respalden los requerimientos comerciales;
5	5.2.1.c	PO 1.2	c) identificar y tratar los requerimientos legales y reguladores y las obligaciones de seguridad contractuales;
5	5.2.1.d	ME 2	d) mantener una seguridad adecuada mediante la correcta aplicación de todos los controles implementados;
5	5.2.1.e	ME 2	e) llevar a cabo revisiones cuando sean necesarias, y reaccionar apropiadamente ante los resultados de estas revisiones;
5	5.2.1.f	ME 2	f) donde se requiera, mejorar la efectividad del SGSI.
5	5.2.2	PO 7	Capacitación, conocimiento y capacidad
5	5.2.2	PO 7	La organización debe asegurar que todo el personal a quien se asignó las responsabilidades definidas en el SGSI sea competente para realizar las tareas requeridas para
5	5.2.2.a	PO 7	a) determinar las capacidades necesarias para el personal que realiza trabajo que afecta el SGSI;
5	5.2.2.b	PO 7	b) proporcionar la capacitación o realizar otras acciones (por ejemplo; emplear el personal competente) para satisfacer estas necesidades
5	5.2.2.c	ME 2	c) evaluar la efectividad de las acciones tomadas
5	5.2.2.d		d) mantener registros de educación, capacitación, capacidades, experiencia y calificaciones (ver 4.3.3).
6	6	PO 1.5	Auditorías Internas del SGSI
6	6	PO 1.5	La organización debe realizar auditorías internas SGSI a intervalos planeados para determinar si los objetivos de control, controles, procesos y procedimientos del SGSI:
6	6.a	PO 1.5	a) cumplen con los requerimientos de este Estándar Internacional y la legislación y regulaciones relevantes
6	6.b	PO 1.5	b) cumplen con los requerimientos de seguridad de la información identificados;
6	6.c	ME 2	c) se implementan y mantienen de manera efectiva; y
6	6.d	ME 2	d) se realizan conforme lo esperado

6	6	PO 1.5	Se debe planear un programa de auditoría tomando en consideración el status e importancia de los procesos y áreas a ser auditados, así como los resultados de auditorías previas.
6	6	PO 1.5	Se debe definir el criterio, alcance, frecuencia y métodos de auditoría.
6	6	PO 1.5	Las responsabilidades y requerimientos para la planeación y realización de las auditorías, y para el reporte de resultados y mantenimiento de registros (ver 4.3.3) se deben definir en un procedimiento documentado
6	6	ME 2	La gerencia responsable para el área siendo auditada debe asegurar que se den sin demora las acciones para eliminar las no-conformidades detectadas y sus causas.
6	6	ME 2	Las actividades de seguimiento deben incluir la verificación de las acciones tomadas y el reporte de los resultados de verificación (ver 8).
7	7	PO 5.1	Revisión Gerencial del SGSI
7	7.1	PO 5.1	Generalidades
7	7.1	PO 5.1	La gerencia debe revisar el SGSI de la organización a intervalos planeados (por lo menos una vez al año) para asegurarse de su continua idoneidad, conveniencia y efectividad.
7	7.1	PO 5.1	Esta revisión debe incluir oportunidades de evaluación para el mejoramiento y la necesidad de cambios en el SGSI, incluyendo la política de seguridad y los objetivos de seguridad de la información
7	7.1	ME 2	Los resultados de las revisiones deben documentarse claramente y se deben mantener registros (ver 4.3.3).
7	7.2	PO 1.5	Insumo de la revisión debe incluir;
7	7.2.a	PO 1.5	a) resultados de auditorías y revisiones del SGSI;
7	7.2.b	PO 1.5	b) retroalimentación de las partes interesadas
7	7.2.c	PO 1.5	c) técnicas, productos o procedimientos, que se podrían utilizar en la organización para mejorar el desempeño y efectividad del SGSI;
7	7.2.d	PO 1.5	d) status de acciones preventivas y correctivas;
7	7.2.e	PO 1.5	e) vulnerabilidades o amenazas no tratadas adecuadamente en la evaluación de riesgo previa;

7	7.2.f	PO 1.5	f) resultados de mediciones de efectividad
7	7.2.g	PO 1.5	g) acciones de seguimiento de las revisiones gerenciales previas;
7	7.2.h	PO 1.5	h) cualquier cambio que pudiera afectar el SGSI; y
7	7.2.i	PO 1.5	i) recomendaciones para el mejoramiento
7	7.3	PO 1.5	Resultados de la Revisión
7	7.3	PO 1.5	El resultado de la revisión gerencial debe incluir cualquier decisión y acción relacionada con lo siguiente
7	7.3.a	PO 1.5	a) mejoramiento de la efectividad del SGSI;
7	7.3.b	PO 1.5	b) actualización de la evaluación del riesgo y el plan de tratamiento del riesgo;
7	7.3.c	PO 1.5	c) modificación de procedimientos y controles que afectan la seguridad de la información, si fuese necesario, para responder a eventos internos o externos que pudieran tener impacto sobre el SGSI, incluyendo cambios en
7	7.3.c.1	PO 1.5	1) requerimientos comerciales;
7	7.3.c.2	PO 1.5	2) requerimientos de seguridad;
7	7.3.c.3	PO 1.5	3) procesos comerciales que afectan los requerimientos comerciales existentes
7	7.3.c.4	PO 1.5	4) requerimientos reguladores o legales;
7	7.3.c.5	PO 1.5	5) obligaciones contractuales; y
7	7.3.c.6	PO 1.5	6) niveles de riesgo y/o criterio de aceptación del riesgo
7	7.3.d	PO 1.5	d) necesidades de recursos;
7	7.3.e	PO 1.5	e) mejoramiento de cómo se mide la efectividad de los controles
8	8	PO 1.4	Mejoramiento del SGSI
8	8.1	ME 2	Mejoramiento continuo
8	8.1	ME 2	La organización debe mejorar continuamente la efectividad del SGSI a través del uso de la política de seguridad de la información, objetivos de seguridad de la información, resultados de auditoria, análisis de los eventos monitoreados, acciones correctivas y preventivas, y la revisión gerencial

8	8.2	PO 1.5	Acción correctiva
8	8.2	PO 1.5	El procedimiento documentado para la acción correctiva debe definir los requerimientos para:
8	8.2.a	PO 1.5	a) identificar las no-conformidades;
8	8.2.b	PO 1.5	b) determinar las causas de las no-conformidades
8	8.2.c	PO 1.5	c) evaluar la necesidad de acciones para asegurar que las no- conformidades no vuelvan a ocurrir;
8	8.2.d	PO 1.5	d) determinar e implementar la acción correctiva necesaria;
8	8.2.e	PO 1.5	e) registrar los resultados de la acción tomada (ver 4.3.3); y
8	8.2.f	ME 2	f) revisar la acción correctiva tomada
8	8.3	PO 1.5	Acción preventiva
8	8.3.a	PO 1.5	a(identificar las no-conformidades potenciales y sus causas;
8	8.3.b	PO 1.5	b) evaluar la necesidad para la acción para evitar la ocurrencia de no-conformidades;
8	8.3.c	PO 1.5	c) determinar e implementar la acción preventiva necesaria;
8	8.3.d	PO 1.5	d) registrar los resultados de la acción tomada (ver 4.3.3); y
8	8.3.e	ME 2	e) revisar la acción preventiva tomada.
8	8.3	PO 1.1	La organización debe identificar los riesgos cambiados e identificar los requerimientos de acción preventiva enfocando la atención sobre los riesgos cambiados significativamente.
8	8.3.	PO 1.1.	La prioridad de las acciones preventivas se debe determinar en base a los resultados de la evaluación del riesgo

Fuente: Elaboración Propia

2.3.3.- Mapeo del BMIS con la Brecha de la Entidad

La brecha de la entidad es determinada por los la situación actual las cuales se compararon el respectivo requerimiento de la norma ISO/IEC 27001-2008 el resultado se muestra en la siguiente tabla 2.14.

Tabla 2 14: Determinación de la Brecha de la Entidad

Fuente	Requerimiento	Elemento / DI	Brecha
ISO/IEC 27001-2008	8. Mejoramiento del SGSI	EME	En proceso de implementación
ISO/IEC 27002:2005	Seguridad del Recurso Humano	FAC	En proceso de implementación
ISO/IEC 27001-2008	4.1 Requisitos Generales	GOB	En proceso de implementación
ISO/IEC 27001-2008	5.1 Compromiso de la gerencia	GOB	Por cumplimiento regulatorio se debe tomar el acuerdo de adopción del compromiso
ISO/IEC 27001-2008	7. Revisión Gerencial del SGSI	GOB	En proceso de implementación
ISO/IEC 27002:2005	Políticas de seguridad de la información	GOB	En proceso de implementación
ISO/IEC 27002:2005	Organización interna	GOB	En proceso de implementación
ISO/IEC 27002:2005	Seguridad Física	GOB	Se cuenta con una adecuada protección física
ISO/IEC 27002:2005	Continuidad de Negocio	GOB	No se ha implementado un plan de continuidad de negocio
ISO/IEC 27002:2005	Gestión de Activos	HYS	En proceso de implementación
ISO/IEC 27002:2005	Gestión de Comunicación y Operaciones	HYS	Se cuenta con herramientas que proveen una seguridad razonable
ISO/IEC 27002:2005	Control de Accesos	HYS	Se cuenta con herramientas que proveen una seguridad razonable
ISO/IEC 27002:2005	Desarrollo de Software	HYS	Se sigue un estándar de desarrollo de software
ISO/IEC 27002:2005	Gestión de Incidencias	HYS	No se cuenta con una gestión de incidencias de seguridad de la información

COBIT 4.1	PO 09 Riesgos de TI	ORG	Existe procedimientos de riesgos junto con documentos de informes
ISO/IEC 27001-2008	Sistema de Gestión	ORG	En proceso de implementación
ISO/IEC 27001-2008	5 Responsabilidad de la Gerencia	ORG	La Gerencia los conoce y está en proceso de implementación
ISO/IEC 27002:2005	Cumplimiento	ORG	Se tienen identificados los requerimientos de la seguridad
ISO/IEC 27001-2008	4.2 Establecer y manejar el SGSI	PRO	En proceso de implementación
ISO/IEC 27001-2008	4.3 Requisitos de documentación	PRO	En proceso de implementación
ISO/IEC 27001-2008	5.2 Gestión de Recursos	PRO	En proceso de implementación
ISO/IEC 27001-2008	6. Auditorías Internas	PRO	En proceso de implementación
ISO/IEC 27002:2005	Evaluando riesgos de seguridad	PRO	Básicamente se cumple con el PO 09
COBIT 4.1	P09.1 Evaluar y Administrar los Riesgos de TI.	PRO	Los riesgos significativos de TI son de conocimiento de la alta gerencia y están acordados en el comité de TI y comité de Riesgos de la Institución.
COBIT 4.1	PO9.2 Establecimiento del Contexto del Riesgo	PRO	La Entidad cuenta con un reglamento de la unidad de riesgos para la gestión de los procesos de riesgos, este incluyo la gestión de riesgos de TI.
COBIT 4.1	PO9.3 Identificación de Eventos	PRO	Existe una evaluación de los riesgos de TI con base a 10 riesgos críticos para la organización y TI, los cuales ayudan a realizar la gestión de TI de manera adecuada y con orientación hacia los restantes riesgos de TI.
COBIT 4.1	PO9.4 Evaluación de Riesgos de TI	PRO	La Entidad cuenta con una unidad de riesgos y un marco orientador de la gestión de riesgos de TI en la cual realizo un proceso de definición de los principales riesgos para el área de TI.
COBIT 4.1	PO9.5 Respuesta a los Riesgos	PRO	La Entidad cuenta con un procedimiento en el que cuando el riesgo es determinado se le asigna un propietario y se identifica el dueño del proceso afectado.
COBIT 4.1	PO9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos	PRO	La Entidad no ha realizado un avance de ninguno de los principales riesgos y no existe un cronograma para realizar los avances de los proyectos.
COBIT 4.1	AI 06 Administración de Cambios	PRO	

COBIT 4.1	AI6.1 Estándares y Procedimientos para Cambios	PRO	La Entidad cuenta con unas políticas y procedimientos para la gestión de los cambios, sin embargo, no se identificó que la política indique los cambios en los procedimientos, procesos y plataforma base.
COBIT 4.1	AI6.2 Evaluación de Impacto, Priorización y Autorización	PRO	La Entidad cuenta con un procedimiento para la ejecución de los cambios, en el cual se ejecuta un proceso de evaluación del impacto de acuerdo al tipo de cambios, asimismo, estos son priorizados de acuerdo al grado de impacto y con llevan una autorización de la coordinación de TI, o del Jefe de Operaciones con el fin de realizar la mejora respectiva.
COBIT 4.1	AI6.3 Cambios de Emergencia	PRO	La Entidad no cuenta con un procedimiento para la administración de cambio de emergencia para toda la infraestructura de TI, con el fin de contar con un proceso efectivo para definir, sensibilizar, evaluar y autorizar la administración de cambios de la Infraestructura de TI (software, hardware y servicios).
COBIT 4.1	AI6.4 Seguimiento y Reporte del Estatus de Cambio	PRO	La Entidad cuenta con un procedimiento para la ejecución de los cambios y estos son registrados en la aplicación automática diseñada para la administración de solicitudes
COBIT 4.1	AI6.5 Cierre y Documentación del Cambio	PRO	La Entidad cuenta con un procedimiento para la ejecución de los cambios en los parámetros de servicios y estos son registrados en la aplicación automática diseñada para la administración de solicitudes, por lo que cada cambio cuenta con una documentación asociada para su ejecución, asimismo, los clientes internos son notificados para que estos verifiquen que lo solicitado este acorde a lo solicitado por estos.
COBIT 4.1	DS 04 Garantizar la continuidad del Negocio	PRO	No existe un plan específico de seguridad de la información
COBIT 4.1	DS4.1 Marco de Trabajo de Continuidad de TI	PRO	El departamento de TI cuenta con un marco para la continuidad de TI, sin embargo, la Entidad no cuenta con un marco de continuidad para el negocio por lo cual el marco de continuidad de TI no se encuentra alineado al negocio.
COBIT 4.1	DS4.2 Planes de Continuidad de TI	PRO	La Entidad cuenta con un plan de continuidad de TI, sin embargo, este se encuentra enfocado únicamente sobre el ambiente principal y no establece medidas de contingencias. Por lo que no se identifican los siguientes aspectos: los requerimientos de resistencia, el procesamiento alternativo, la capacidad de recuperación, los lineamientos de uso, las funciones y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de las pruebas.

COBIT 4.1	DS4.3 Recursos Críticos de TI	PRO	La Entidad cuenta con un plan de continuidad de TI, sin embargo, este se encuentra enfocado únicamente sobre el ambiente principal y no contempla los recursos críticos de TI que serán utilizados en el sitio alterno. Por lo que no se podría construir resistencia y establecer prioridades en situaciones de recuperación y con el cual se evitaría enfocarse en aspectos menos importantes.
COBIT 4.1	DS4.4 Mantenimiento del Plan de Continuidad de TI	PRO	La Entidad no cuenta con un plan para el mantenimiento del plan de continuidad de TI en cuanto a políticas y procedimientos con el fin de mantener el plan de continuidad actualizado.
COBIT 4.1	DS4.5 Pruebas del Plan de Continuidad de TI	PRO	La Entidad no cuenta con un plan de pruebas para el plan de continuidad de TI, con el cual se pueda establecer escenarios, requerimientos y recursos de TI, con el fin de garantizar que las deficiencias identificadas sean atendidas y que el plan sigue siendo aplicable.
COBIT 4.1	DS4.6 Entrenamiento del Plan de Continuidad de TI	PRO	La Entidad cuenta con un plan de continuidad de TI documentado, sin embargo, este se encuentra enfocado a la infraestructura actual y no incluye el sitio alterno, por lo que No se han realizado sesiones para el entrenamiento sobre el plan de continuidad de TI.
COBIT 4.1	DS4.7 Distribución del Plan de Continuidad de TI	PRO	La Entidad cuenta con un plan de continuidad de TI documentado, sin embargo, este se encuentra enfocado a la infraestructura actual y no incluye el sitio alterno, por lo cual no ha sido distribuido a la Entidad por medio del sitio de distribución de documentos.
COBIT 4.1	DS4.8 Recuperación y Reanudación de los Servicios de TI	PRO	La Entidad cuenta con un plan de continuidad de TI documentado, sin embargo, este se encuentra enfocado a la infraestructura actual y no incluye el sitio alterno, por lo cual no han sido diseñados los planes de recuperación y reanudación de los servicios de TI con base a la infraestructura actual y de sitio alterno. Además, este documento debe incluir aspectos asociados a: activación de sitio de respaldos, procesamiento alternativo, comunicación a clientes e interesados y procesos de reanudación.
COBIT 4.1	DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones	PRO	La Entidad cuenta con un proceso de traslado de medios de respaldo fuera de la institución, sin embargo, estos respaldos están asociados a respaldos de la base de datos y no incluyen aspectos como configuraciones, documentaciones y otros. Asimismo, no se cuenta con una clasificación de la información por lo que no se ha determinado por parte del negocio y TI la información crítica. Adicionalmente, al no existir un sitio alterno no se ha realizado una evaluación de la compatibilidad del hardware y software para restaurar los sistemas.

COBIT 4.1	DS4.10 Revisión Post Reanudación	PRO	La Entidad cuenta con un plan de continuidad de TI, sin embargo, no se logró identificar cuáles son los procesos a ejecutar post-reanudación.
COBIT 4.1	DS 05 Seguridad de los sistemas de Información	PRO	
COBIT 4.1	DS5.1 Administración de la Seguridad de TI	PRO	No existe un sistema de Gestión de la Seguridad de información
COBIT 4.1	DS5.2 Plan de Seguridad de TI	PRO	No se cuenta con un plan de seguridad de TI
COBIT 4.1	DS5.3 Administración de Identidad	PRO	La Entidad cuenta con un procedimiento para la administración de la Identidad, sin embargo, se observó que existen debilidades que reportar con respecto a la implementación del mismo
COBIT 4.1	DS5.4 Administración de Cuentas del Usuario	PRO	La Entidad cuenta un proceso de gestión de cuentas de usuario en el cual se pudo evaluar el proceso ejecutado por el departamento de TI, y el cual es utilizado por el departamento de Recursos Humanos para la creación del usuario.
COBIT 4.1	DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad	PRO	La Entidad no realiza pruebas para mantener la seguridad de TI de manera proactiva. Por tal razón, la Entidad no puede garantizar o acreditar que la seguridad de TI es un nivel aprobado y monitoreado por el Departamento de TI.
COBIT 4.1	DS5.6 Definición de Incidente de Seguridad	PRO	La Entidad no cuenta con una definición sobre incidentes de seguridad de la información por lo cual la no hay un clara definición sobre posibles incidentes, impactos, roles y funciones de personal interno o externo para tratar los incidentes.
COBIT 4.1	DS5.7 Protección de la Tecnología de Seguridad	PRO	La Entidad debe realizar un proceso de evaluación a profundidad (hardening) para garantizar que todos los recursos de TI no estén expuestos al sabotaje.
COBIT 4.1	DS5.8 Administración de Llaves Criptográficas	PRO	El proceso es ejecutado por un proveedor externo de la Entidad.
COBIT 4.1	DS5.9 Prevención, Detección y Corrección de Software Malicioso	PRO	La Entidad cuenta con la aplicación para monitorear el software malicioso en las estaciones de trabajo y servidores de la Entidad, esto son actualizados diariamente
COBIT 4.1	DS5.10 Seguridad de la Red	PRO	La Entidad cuenta con técnicas de seguridad y procedimientos para la administración de la seguridad formalmente documentados. Asimismo, se identificó la existencia de IPS, FIREWALLS y segmentación de redes. Asimismo, se cuenta con certificados para garantizar que la información desde dentro hacia fuera y afuera

			hacia dentro.
COBIT 4.1	DS5.11 Intercambio de Datos Sensitivos	PRO	La Entidad no cuenta con una definición de rutas de intercambio de información sensitiva
COBIT 4.1	DS 11 Administración de Datos	PRO	
COBIT 4.1	DS11.1 Requerimientos del Negocio para Administración de Datos	PRO	La Entidad cuenta con un procedimiento para la administración de datos, asimismo, se establecen mecanismos para garantizar que la información sea procesada correctamente por los sistemas de la Entidad.
COBIT 4.1	DS11.2 Acuerdos de Almacenamiento y Conservación	PRO	La Entidad no cuenta con un procedimiento para el archivo y almacenamiento de los datos, y que estos sean accesibles y utilizables por parte de los interesados.
COBIT 4.1	DS11.3 Sistema de Administración de Librerías de Medios	PRO	La Entidad no ha definido una política y/o procedimiento para la administración de las librerías de medios de datos, por lo cual no se puede garantizar la existencia de un inventario de medios y garantizar su uso (mediante revisiones oportunas y seguimiento a cualquier discrepancia).
COBIT 4.1	DS11.4 Eliminación	PRO	La Entidad no ha definido la política y/o procedimiento para la eliminación de los datos, esto con el fin de garantizar que no se pueda recuperar la información almacenada en todos los medios de almacenamiento de la infraestructura.
COBIT 4.1	DS11.5 Respaldo y Restauración	PRO	La Entidad no ha definido procedimientos para los respaldos y restauraciones de los sistemas y configuraciones de los sistemas de información de la Entidad, así como la infraestructura.
COBIT 4.1	DS11.6 Requerimientos de Seguridad para la Administración de Datos	PRO	La Entidad no ha establecido mecanismos de identificar y aplicar mecanismos de seguridad con respecto a la recepción y entrega de información y mensajes sensitivos.
COBIT 4.1	DS 12 Administración del ambiente Físico	PRO	
COBIT 4.1	DS12.1 Selección y Diseño del Centro de Datos	PRO	La Entidad implemento medidas de seguridad alineadas al negocio con el fin de mantener un ambiente seguro para la gestión de la información en un ambiente disponible, íntegro y con un grado de confidencialidad. Por lo que se identificaron diferentes medidas de seguridad en el proceso de revisión, tales como: perímetros de seguridad de acceso, ubicación del equipo crítico y áreas de envío y recepción de la información.

COBIT 4.1	DS12.2 Medidas de Seguridad Física	PRO	La Entidad cuenta con procedimiento para otorgar, limitar y revocar el acceso al centro de datos y a las áreas de telecomunicaciones de la Entidad, asimismo, se identificaron medios para monitorear el acceso al centro físico como lo son bitácoras de acceso al centro de datos que deben ser completadas por el visitante, usuario interno y proveedores.
COBIT 4.1	DS12.3 Acceso Físico	PRO	Existe un monitoreo de manera automática por la herramienta web con la que cuenta la Entidad por lo que se observó que en caso de existir un diferencia o discrepancia en el control, este notifica al jefe de operaciones para que este tome medidas.
COBIT 4.1	DS12.4 Protección Contra Factores Ambientales	PRO	Existe un monitoreo de manera automática por la herramienta web con la que cuenta la Entidad por lo que se observó que en caso de existir un diferencia o discrepancia en el control, este notifica al jefe de operaciones para que este tome medidas.
COBIT 4.1	DS12.5 Administración de Instalaciones Físicas	PRO	La Entidad no ha definido una administración de los equipos eléctricos y comunicaciones de las instalaciones físicas en cuanto a las leyes y regulaciones.
COBIT 4.1	ME 2 Monitorear y evaluar el control interno	PRO	
COBIT 4.1	ME2.1 Monitoreo del Marco de Trabajo de Control Interno	PRO	La Entidad no ha diseñado una política y procedimiento para la administración del marco de control de interno de TI y del marco de control. No obstante, la Entidad en sus revisiones del plan estratégico y actas de comité de TI realizan una revisión del avance de los controles de TI.
COBIT 4.1	ME2.2 Revisiones de Auditoría	PRO	La Entidad ha realizado un proceso para la evaluación de las mejores prácticas de la industria de acuerdo a la evaluación de la auditoría externa e interna de Sistemas de TI.
COBIT 4.1	ME2.3 Excepciones de Control	PRO	La Entidad no ha diseñado un procedimiento de control interno el cual establezca la administración de las excepciones al control, así como: análisis de la causa subyacente como la acción correctiva, individuo responsable de la función y cuáles excepciones deberían ser escaladas y partes afectadas.
COBIT 4.1	ME2.4 Control de Auto Evaluación	PRO	La Entidad ha realizado auto-evaluación para el cumplimiento regulatorio de la SUGEF, sin embargo, al no contar con una política y/o procedimiento de control interno no se ha definido un plan de autoevaluaciones de control, el cual indique cuales son los criterios de evaluación, la frecuencia de ejecución, los roles y responsabilidades y los resultados e informes.

COBIT 4.1	ME2.5 Aseguramiento del Control Interno	PRO	La Entidad ha realizado proceso para la evaluación de las mejores prácticas de la industria de acuerdo a la evaluación de la auditoría externa e interna de Sistemas de TI.
COBIT 4.1	ME2.6 Control Interno para Terceros	PRO	La Entidad no ha definido una política y/o procedimiento para evaluar el control interno para los proveedores de servicios "Terceros", sin embargo, se nos indicó que los proveedores de servicios críticos están realizando una evaluación del control interno
COBIT 4.1	ME2.7 Acciones Correctivas	PRO	La Entidad realiza un proceso intuitivo para la respuesta hacia las acciones correctivas, sin embargo, no se identificó que haya una política y/o procedimiento que establezca cuales van a ser las acciones correctivas a desarrollar por parte de TI, en el cual se pueda identificar los siguientes

Fuente: Elaboración Propia

Capítulo III – Conclusiones sobre las políticas de Seguridad Actuales

Una vez realizado el análisis de los mapeos del capítulo 2 anterior, se procede con las conclusiones, cabe destacar las relaciones de los diferentes elementos y las DIs que nos proveen la base sobre la cual dirigir el análisis.

Por la naturaleza del trabajo las conclusiones son generales, sin embargo, es importante tomar en consideración que cada una de las relaciones nos van a proporcionar un aspecto relevante de la Seguridad de la Información que nos permitirán tienen un análisis holístico.

3.1.- Elementos

3.1.1.- Elemento Organización

En el punto 2.2.1.1 se realizó el análisis de este elemento del cual se concluye lo siguiente:
La estructura organizacional de la entidad tiene definido requerimientos específicos en seguridad de la información y básicamente corresponde a la implementación de los procesos de COBIT 4.1 exigidos por la SUGEF y el estándar ISO/IEC 27001-2008 que se encuentra en proceso de adopción.

Actualmente la entidad se encuentra en proceso de implementación de la norma ISO/IEC 27001-2008 y con un plan remedial en la parte de los procesos COBIT 4.1 para cumplimiento de normativa.

La estructura organizacional no proporciona un entendimiento de las necesidades de la seguridad de la información ya que está delegado en el departamento de TI y en las personas que están implementando la normativa de SUGEF.

El compromiso de la gerencia no está de acuerdo con la necesidad de la organización ya que no existen programas efectivos que logren permear en la conciencia de los empleados, la necesidad de la seguridad de la información como un punto focal es de importancia para la organización.

La entidad tiene claramente identificado los requerimientos para la seguridad de la información lo que permite tener un objetivo claro, el reto consiste en lograr cumplirlo Específicamente en lo que a políticas de Seguridad se refiere la entidad cuenta con un conjunto de políticas que están desactualizadas.

3.1.2.- Elemento Procesos

El punto anterior 2.2.1.2 nos muestra el mapeo del elemento procesos, a continuación las conclusiones de este elemento.

Los procesos de la seguridad de la información forman parte de un conjunto de procesos de TI que se deben implementar de acuerdo a los procesos COBIT 4.1, si bien existen procesos en los que se toma en cuenta la seguridad de la información, estos no son priorizados ni se le da la importancia requerida.

Cada encargado de departamento toma sus decisiones de acuerdo con su mejore criterio. Así mismo, se observó que la entidad tiene sus propios procesos y los procesos COBIT 4.1 se ven como una forma más rígida de realizar el trabajo diario, por lo que alguno de los requerimientos se realizan por cumplimiento pero no por convencimiento de la necesidad de poder mejorar con procesos más eficientes.

Existe un proceso básico para la seguridad de la información que forma parte de un proceso general de incidencias, sin embargo, los requerimientos de los marcos regulatorios establece un proceso aparte para la gestión de incidencias de seguridad de la información. Tampoco existe un proceso que involucre la elaboración y seguimiento de un plan de seguridad de TI que permita dar cumplimiento a las medidas de seguridad de la entidad.

En general no se cuenta con procesos definidos específicos de seguridad de la información, así mismo, el seguimiento de los procesos es manual, únicamente se cuenta con un sistema de gestión de solicitudes.

3.1.3.- Elemento Tecnología

En el punto 2.2.1.3 anterior se muestra el mapeo del elemento Tecnología, a continuación las conclusiones.

La entidad cuenta con las medidas necesarias en materia de tecnología que permiten una gestión para enfrentar situaciones de vulnerabilidades como lo son: aplicaciones anti-malware, control de claves, medidas de respaldos, enrutamientos segundarios de red, módulos de seguridad de los sistemas, sistemas de protección de fuga de datos y otros.

Todas las medidas anteriores son adecuadas, sin embargo, es importante mencionar que no se cuenta con un software que permita administrar o gestionar dicha tecnología de acuerdo con los requerimientos de gestión por procesos, por ejemplo un software que apoye a la entidad como un todo en los procesos y que permita un manejo automatizado de muchos de los procesos que se realizan y que pueda permitir una mejor gestión.

La entidad no cuenta con una arquitectura de la seguridad de la información debidamente identificada.

3.1.4.- Elemento personas

El punto 2.2.1.4 anterior nos muestra el mapeo de este elemento, a continuación las conclusiones

La entidad no cuenta con una persona encargada de la seguridad de la información que tenga las capacidades necesarias para implementar adecuadamente la seguridad de la información, tampoco cuenta con un plan de capacitación para el personal de la entidad en esta materia.

3.2.- Interconexiones Dinámicas

3.2.1.- DI Gobierno

EL punto 2.2.2.1 anterior mapea esta DI con los diferentes elementos, a continuación las conclusiones.

La entidad cuenta con un grupo de personas que se encuentran en proceso de implementación de la normativa y el estándar ISO/IEC 27001-2008, algunas al 100% del tiempo otras con un porcentaje definido de su tiempo total, por lo que es un hecho que se está trabajando y avanzando.

La gerencia considera que el aporte del estándar sobre pasa las necesidades de la entidad y no representa un valor agregado ya que el costo-beneficio es muy alto

La forma de implementación se basa en un plan correctivo fundamentado en una revisión de auditoría, sin que se logre un plan que integre la seguridad de la información como un aspecto relevante a considerar.

3.2.2.- DI Arquitectura

En el punto 2.2.2.2. Se encuentra el mapeo de esta DI con los elementos, a continuación las conclusiones:

La entidad no cuenta con una arquitectura de la seguridad de la información definida.

3.2.3.- DI Cultura

En el punto 2.2.2.3 se encuentra el mapeo de eta DI con los elementos, a continuación

La cultura en la entidad no beneficia una adecuada implementación de la seguridad de la información, así mismo, impera una seguridad satisfactoria en las personas del departamento de TI y la gerencia, por el contrario, las personas que están implementando al 100% la normativa sí le ven la importancia, pero sus esfuerzos no son del todo tomados en cuenta.

3.2.4.- DI Habilitación y Soporte

En el punto 2.2.2.4 se encuentra el mapeo de este DI con los elementos, a continuación las conclusiones.

El departamento de Tecnologías de Información se encuentra con actividades que se sobreponen a la prioridad de la seguridad de la información.

No existen los procesos que permitan identificar adecuadamente la forma en que habilitación y soporte deba apoyar la seguridad de la información de acuerdo con los requerimientos definidos por el elemento organización.

De acuerdo con las regulaciones la entidad debe tener un oficial de seguridad que sea el responsable de la seguridad de la información, sin embargo, no se cuenta con el personal idóneo para esta función.

3.2.5.- DI Factores Humanos

En el punto 2.2.2.5 se encuentra el mapeo de esta DI con los elementos, a continuación las conclusiones

Existe un elemento primordial para una adecuada comunicación en las organizaciones y es tener los objetivos claros y el cómo se debe llegar a ellos, el objetivo se tiene claro y es el cumplimiento de la normativa, sin embargo, el cómo llevarlo a cabo y las prioridades no se considera que se encuentren alineadas.

3.2.6.- DI Emergentes

La entidad trabaja en un modo reactivo a las necesidades de la seguridad de la información por lo que es difícil el observar oportunidades de mejora que permitan beneficiar a la misma.

Capítulo IV - Propuesta de Políticas de la Seguridad de la Información.

4.- Propuesta de las Políticas de Seguridad de la información

4.1.- Introducción

Activo es una palabra que normalmente se asocia a un producto que se puede ver y palpar fácilmente, pensamos en que un automóvil, en un escritorio, en una casa, etc. Cuando se habla de seguridad para la protección de los activos se piensa en las alarmas de los automóviles, puertas seguras y guardas de seguridad para evitar que intrusos puedan tener acceso a las oficinas, rejas en nuestras casas con la finalidad de dificultar el acceso a la misma, y otros métodos de seguridad.

Cuando se habla de Seguridad de la información a veces es difícil comprender el término ya que no es tan palpable como se quisiera, de hecho, lo que se observa es básicamente que de una computadora salen algún tipo de información en diferentes formas, como por ejemplo, un reporte impreso, ya sea un estado de cuenta, una consulta de personas autorizadas, el monto de inversión de una persona en una entidad financiera, estados financieros y en general se puede hacer una análisis exhaustivo que permita darnos cuenta de la cantidad de información que nos proporcionan las computadoras.

Cuando se habla de seguridad de la información básicamente se refiere a aspectos que nos conciernen a todas las personas, más aún en el ámbito empresarial. El punto es cómo se protege dicha información? A esa protección es a la que se conoce como “Seguridad de la información”.

Para toda organización o entidad, más en el ámbito financiero, debido a que se debe resguardar la información de los clientes, se deben establecer la forma en que se debe manejar la información, por lo que un manual de políticas en un entidad no es otra cosa más que un conjunto de normas y/o formas de actuar que se deben poner en funcionamiento

en todas las empresas. A estas formas de actuar la llamaremos “Políticas de Seguridad de la Información” y se detallan en este documento para la entidad financiera.

4.2.- Definiciones y Términos

De acuerdo a COBIT 4.1 y la norma ISO/IEC 27001-2008, en Seguridad de la información se establecen los siguientes términos de referencia que defino a continuación:

- Disponibilidad: Se refiere a que cada usuario de la entidad tenga acceso autorizado a la información que debe tener de acuerdo a su cargo y cuando se requiera.
- Integridad: Se refiere a que la información de la entidad sea exacta y completa y que los procesos (Entrada-Procesamiento-Salida) garantice a los clientes interno y externos su adecuada gestión.
- Confidencialidad: Se refiere a que cada funcionario de la entidad tiene acceso solo a la información necesaria autorizada para su cargo y que cada cliente puede ver solo la información que le incumbe a él.

4.3.- Principios fundamentales de la entidad

La seguridad no es un producto: es un proceso. Un proceso continuo que debe ser controlado, gestionado y monitorizado por lo que se adoptan los 12 principios básicos definidos en COBIT 5 y en concordancia con la norma ISO/IEC 27001-2008 como base para la implementación de cualquier política, norma o procedimiento de seguridad de la información que se desarrolle en la entidad

Estos principios se encuentran catalogados en 3 grandes áreas, y cuentan cada uno con un objetivo y una descripción, por lo que la Seguridad de la Información debe cumplir con lo siguiente:

4.3.1.- Área 1: Apoyo a la entidad

- Enfocada en la entidad: Debe asegurar que es integrada en las actividades esenciales de la entidad.
- Debe entregar calidad y valor a la entidad: Si una solución no genera valor no se debe implementar y/o se deben buscar soluciones alternativas.
- Cumplir con las leyes y requisitos reglamentarios: no debe ir en contra de los requerimientos legales
- Debe proporcionar información oportuna y precisa, sobre rendimiento de la seguridad: Para la toma de decisiones en seguridad de información
- Evaluar las actuales y futuras amenazas a la información: No es estática, se debe de estar actualizando.
- Promover la mejora continua sobre la seguridad de la información: Se debe crear el mecanismo necesario que permita mejorar.

4.3.2.- Área 2: Defensa de la Entidad

- Adoptar un enfoque basado en riesgos: Evaluar de acuerdo a los riesgos de la entidad.
- Proteger la información clasificada: Establecer mecanismos para la identificación y clasificación de los datos sensitivos.
- Concentrarse en las aplicaciones críticas del negocio: Identificar las operaciones críticas de la entidad.
- Desarrollar sistemas de seguridad: Desarrollar un Sistema de Gestión de la Seguridad de la Información, basado en la norma ISO/IEC 27001-2008.

4.3.3.- Área 3: Promover un comportamiento responsable de seguridad

- Actuar de una manera profesional y ética: Las actividades son realizadas de una manera fiable, responsable y eficaz

- Fomentar una cultura de seguridad positiva: que permita desarrollar un adecuado comportamiento de los usuarios finales, reduzca la probabilidad de incidentes de seguridad y limite el impacto de la entidad.

4.4.- Políticas de Seguridad de la Información

4.4.1.- Objetivos

a) Proteger la información de la entidad y la tecnología utilizada para su procesamiento de a amenazas, internas o externas, deliberadas o accidentales, para el asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información.
b) Asegurar la implementación de las medidas eficaces de seguridad, identificando los recursos adecuados y fundamentados en el costo-beneficio para la entidad.
c) Mantener la Política de Seguridad de la entidad actualizada.

4.4.2.- Sanciones por Incumplimiento

EL incumplimiento de las Políticas de Seguridad de la Información tendrá como resultado la aplicación de sanciones, que deberán ser definidas y establecidas por el régimen sancionatorio de la entidad y hacerlas efectivas por la gerencia general.

4.5.- Marcos y estándares adoptados por la entidad

4.5.1.- Marco de Control COBIT 4.1

La entidad establece y es consciente de implementar por normativa de la SUGEF los siguientes procesos del marco de control COBIT 4.1.

- PO 09 Riesgos de TI
- AI 06 Administración de Cambios
- DS 04 Garantizar la continuidad del Negocio
- DS 05 Seguridad de los sistemas de Información

- DS 11 Administración de Datos
- DS 12 Administración del ambiente Físico

4.5.2.- Estándar de Seguridad ISO/IEC 27001-2008

La entidad adopta el Estándar ISO/IEC 27001-2008 para la gestión de la Seguridad de Información para lo cual se debe desarrollar un Sistema de Gestión de la Seguridad de la Información (SGSI) con el cual se deberá implementar y gestionar la seguridad de la información.

4.6.- Organización de la Seguridad de la Información

4.6.1.- El comité de Tecnologías de Información deberá crear un Sub-comité de Seguridad de la Información el cual será en encargado de velar por el cumplimiento de la seguridad de información dentro de la entidad. Para efectos prácticos podrá estar constituido por las mismas personas, sin embargo, debe contar con al menos una persona, ya sea externa o interna a la entidad, que cuente con suficientes conocimientos en materia de seguridad de la información y se debe incorporar al reglamento de funciones y responsabilidades del sub-comité.

4.6.2.-La gerencia deberá asignar la responsabilidad de la seguridad de la información al oficial de seguridad de la información de la entidad, el cual será el encargado de velar por la adecuada implementación en la entidad de las funciones relativas a la seguridad de los sistemas de información y rendirá cuentas al mismo subcomité sobre las políticas establecidas en este documento. El Sub-comité de Seguridad de la información asesorará al oficial de Seguridad de la Información.

4.6.3.- Cada encargado de departamento será responsable de la aplicación de las políticas de seguridad de la información, así mismo, cada encargado de las sucursales de la entidad deberá velar por la aplicabilidad de las políticas en su ámbito de acción específico.

4.6.4.- Es responsabilidad individual de todos los funcionarios de la entidad el velar por el cumplimiento de la seguridad de información.

4.6.5.- El oficial de seguridad de la información no dependerá ¿técnicamente? del departamento de tecnologías de información, sino directamente del subcomité de seguridad, sin embargo, deberá proponer al subcomité las funciones específicas que deben cumplir el departamento de TI en materia de seguridad dela información.

4.7.- Áreas de cobertura de la Seguridad de la información

De acuerdo con el estándar adoptado por la entidad los siguientes corresponden a los controles de seguridad que se deben seleccionar, evaluar y establecer.

4.7.1.- Gestión de Activos

4.7.1.1.- Alcance

Esta Política se aplica a todo el personal de la entidad y representa los activos de la información de la entidad, en cualquier medio de soporte en que se encuentre y son la base del sistema de gestión de la seguridad de la información.

4.7.1.2.- Política

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

El Oficial de Seguridad de la información es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplido de acuerdo a lo establecido en la presente Política.

Los requerimientos mínimos de seguridad son los siguientes:

- Responsabilidad sobre los activos (inventario, propiedad y uso aceptable de los activos)
- Clasificación de la información (Directrices de clasificación, etiquetado y manipulado de los activos)

4.7.2.- Seguridad de los recursos humanos

4.7.2.1.- Alcance

Esta Política se aplica a todo el personal de la entidad y al personal externo que sea contratado con cualquier finalidad y tiene la finalidad de educar y capacitar al personal de la entidad sobre lo que se espera de ellos en materia de seguridad de la información y aspectos de confidencialidad para lo cual del departamento de recursos humanos debe realizar las capacitaciones con asistencia del departamento de TI cuando se requiera asesoría para asuntos específicos

4.7.2.2.- Política

El Responsable del Área de Recursos Humanos incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, así mismo deberá informar al personal nuevo sus obligaciones de cumplimiento de esta política.

El Oficial de Seguridad de la información es el responsable del seguimiento de los incidentes de seguridad con apoyo del departamento de tecnologías de información en coordinación con los propietarios de la información.

El subcomité de Seguridad de la Información será responsable velar el cumplimientos de las medidas correctivas necesarias para la mitigación de los incidentes se seguridad.

EL subcomité de Seguridad de la información tendrá la responsabilidad de definir los reportes necesarios para el adecuado seguimiento de la seguridad de la información.
Todo el personal de la entidad es responsable de reportar al oficial de seguridad cualquier incidente de seguridad que detecten.

Los requerimientos mínimos de seguridad son los siguientes:

- Seguridad Antes del Empleo (Funciones y responsabilidades, Investigación de antecedentes, términos de la contratación)
- Seguridad durante el empleo (Inducción, responsabilidades, concientización, formación, capacitación y proceso disciplinario)
- Seguridad de cese del empleo o cambio de puesto (Responsabilidades, devolución de activos, revocación de derechos de acceso y/o establecimiento de nuevos derechos si se trata de un cambio de puesto)

4.7.3.- Seguridad física y del entorno

4.7.3.1.- Alcance

Esta Política se aplica a todo el personal y abarca los recursos físicos relativos a los sistemas de información de la entidad: instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, etc.

4.7.3.2.- Política

El Oficial de Seguridad de la información definirá junto con el jefe del departamento de tecnologías de información y en conjunto con los encargados de departamento las medidas de seguridad física y del entorno para el resguardo de los activos críticos, los cuales se deberán sustentar en un análisis de riesgo.

EL responsable del cumplimiento de esta política será el encargado de departamento, para efecto de las sucursales, este será la persona encargada de la sucursal

Los requerimientos mínimos de seguridad son los siguientes:

Áreas seguras

- Perímetro de seguridad física.
- Controles físicos de entrada.
- Seguridad de oficinas y sucursales.
- Protección contra las amenazas externas y de origen ambiental.
- Áreas de acceso público.

Seguridad de los equipos

- Ubicación de equipos
- Protección ante fallos
- Seguridad de cableado
- Mantenimiento de equipos
- Seguridad fuera de las instalaciones
- Información que se maneja en los equipos

El Oficial de seguridad es el responsable del cumplimiento de esta política de acuerdo con las distintas necesidades de la entidad ya sea de cada sucursal, oficina central y equipo móvil.

4.7.4.- Gestión de comunicaciones y operaciones

4.7.4.1.- Alcance

Esta política aplica al departamento de tecnologías de la información, al oficial de seguridad y a los jefes de departamento.

4.7.4.2.- Política

Los jefes de departamento, el jefe del departamento de tecnologías de información y el oficial de seguridad de la información deberán en conjunto determinar los requerimientos de la información a resguardar de acuerdo con los niveles de criticidad definidos en el análisis de riesgo el cual deberá quedar plasmado en un documento formal.

Los requerimientos mínimos de seguridad son los siguientes:

Responsabilidades y procedimientos de operación, involucra los siguientes aspectos:

- Documentación de los procedimientos de operación
- Gestión de cambios
- Segregación de tareas
- Separación de los recursos de desarrollo, prueba y operación

Gestión de la provisión de servicios por terceros, involucra los siguientes aspectos

- Provisión de servicios.
- Supervisión y revisión de los servicios prestados por terceros.
- Gestión del cambio en los servicios prestados por terceros

Planificación y aceptación del sistema, involucra los siguientes aspectos

- Gestión de capacidades
- Protección contra código malicioso y descargable
- Controles contra el código malicioso
- Controles contra el código descargado en el cliente

Copias de seguridad, involucra básicamente la gestión de las copias de seguridad de la información de los diferentes departamentos

Gestión de la seguridad de las redes, involucra los siguientes aspectos

- Controles de red.
- Seguridad de los servicios de red.

Manipulación de los soportes, involucra los siguientes aspectos

- Gestión de soportes extraíbles.
- Procedimientos de manipulación de la información.

- Seguridad de la documentación del sistema

Intercambio de información, involucra los siguientes aspectos

- Políticas y procedimientos de intercambio de información
- Acuerdos de intercambio.
- Soportes físicos en tránsito
- Mensajería electrónica
- Sistemas de información de la entidad

Servicios de comercio electrónico, involucra los siguientes aspectos

- Comercio electrónico
- Transacciones en línea

Monitoreo, involucra los siguientes aspectos.

- Registro de auditorías.
- Supervisión del uso del sistema
- Protección de la información de los registros
- Registros de administración y operación
- Registro de fallos

4.7.5- Control de Acceso

4.7.5.1.- Alcance

Está política aplica al departamento de tecnologías de información, al oficial de seguridad de la información y a los jefes de departamento de la entidad y representa las medidas definidas por la entidad para controlar y monitorear el acceso a la red institucional

4.7.5.2.- Política

El jefe de departamento es el responsable de definir los accesos a la información en su ámbito de acción y definir los perfiles de accesos a la información.

Una vez definidos los perfiles deberán ser aprobados por el subcomité de seguridad de la información y en consulta con el departamento de tecnologías de información con la finalidad de que éste último valide la posibilidad de los sistemas de contar con la seguridad necesaria.

Los requerimientos mínimos de seguridad son los siguientes:

Se deben definir los requerimientos de la entidad por medio de una política de control de accesos que contenga los siguientes aspectos de seguridad.

- Gestión de acceso de usuario, que involucra, el registro de usuarios, privilegios y contraseñas
- Definición de responsabilidades del usuario
- Definición del uso de contraseñas
- Política de estaciones de trabajo como pantalla limpia
- Controles de acceso a la red que provea de una política de uso de los servicios de red, autenticación de conexiones externas, identificación de los equipos en las redes, diagnostico remoto y protección de puertos de configuración, control de conexión de redes, segregación de redes, control de encaminamientos de la red
- Control de acceso al sistema operativo que provea procedimientos seguros de inicio de sesión, identificación y autenticación, sistemas de gestión de contraseñas, uso de los recursos.
- Controles de acceso a las aplicaciones de la entidad y a la información, que posean restricciones de acceso a la información y aislamiento de sistemas sensibles.
- Definición de políticas para computadores portátiles y eventualmente teletrabajo.

4.7.6.- Adquisición, desarrollo y mantenimiento de los sistemas de información.

4.7.6.1.- Alcance

Esta política aplica al departamento de tecnologías de información, al oficial de seguridad y a la auditoría interna.

4.7.6.2.- Política

Esta Política se aplica a todos los sistemas informáticos de la entidad, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes de la entidad.

El oficial de seguridad de la información en conjunto con el junto con el jefe de departamento interesado y el departamento de Auditoría Interna, definirán los controles a ser implementados en los sistemas desarrollados en la entidad o por terceros, para lo cual deberán desarrollar una evaluación de riesgos específica de los sistemas en desarrollo.

El oficial de seguridad de la información, junto con el jefe del departamento interesado, serán los responsable de definir la criticidad de la información. Los sistemas críticos de la entidad deberán tener protección criptográfica.

Los requerimientos mínimos de seguridad son los siguientes:

- Análisis y especificación de los requisitos de seguridad
- Validación de los datos de entrada
- Control del procesamiento interno
- Validación de los datos de salida
- Política de uso de los controles criptográficos
- Gestión de claves
- Seguridad de los archivos de sistema
- Protección de los datos de prueba del sistema.
- Control de acceso al código fuente de los programas
- Procedimientos de control de cambios
- Gestión de las vulnerabilidades técnicas

4.7.7.- Gestión de incidentes de seguridad de la información

4.7.7.1.- Alcance

Esta política involucra al departamento de tecnologías de información y al oficial de seguridad.

4.7.7.2.- Política

Se debe crear un proceso de gestión de las incidencias en la entidad de acuerdo con la criticidad de las operaciones definidas

Los requerimientos mínimos de seguridad son los siguientes:

- Notificación de los eventos de seguridad de la información.
- Notificación de los puntos débiles de la seguridad
- Gestión de incidentes de seguridad de la información y oportunidades de mejoras que involucre las responsabilidades y procedimientos, el aprendizaje de los incidentes

4.7.8.- Gestión de la continuidad del negocio

4.7.8.1.- Alcance

Esta política abarca a todo el personal de la entidad

4.7.8.2.- Política

El Oficial de Seguridad de la información deberá promover y definir la documentación, prueba y actualización de los planes de contingencia.

Los jefes de departamento, con apoyo del oficial de seguridad deberán realizar las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos de la entidad y definir planes de acción para remediarlas.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones por medio de un análisis de impacto.
- Identificar los controles preventivos que mitiguen el riesgo de materialización de los eventos.
- Desarrollar un plan estratégico, táctico y operativo que se pondrá en práctica ante una eventualidad.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades de la entidad.

4.7.9.- Cumplimiento

4.7.9.1.- Alcance

Esta política aplica al Oficial de seguridad de la información, al departamento legal y a la auditoría interna de la entidad

4.7.9.2.- Política

Se debe de cumplir con los requerimientos del estándar adoptado por la entidad en todos sus extremos.

Se deberán documentar claramente todos los requisitos regulatorios en materia de seguridad de la información normativos y contractuales para cada sistema de información de la entidad.

El oficial de seguridad de la información con apoyo del departamento legal deberá definir los aspectos de derecho de propiedad intelectual del software

Capítulo V - Conclusiones y Recomendaciones.

5.- Conclusiones y Recomendaciones

La entidad responde a las regulaciones del entorno costarricense referente a la Súper Intendencia General de Entidades Financieras (SUGEF), el trabajo realizado propone un marco de políticas de Seguridad de la Información que pretende servir como guía para toda la gestión de la Seguridad, sin embargo, el análisis basado en el BMIS permitió observar y analizar situaciones que se encuentran fuera del alcance de este trabajo con la finalidad de proporcionarle a la entidad un fundamento de análisis que permita establecer oportunidades de mejora, la cuales por la naturaleza e impacto de confidencialidad no queda plasmadas en este documento pero fueron entregadas directamente a la Gerencia de la Entidad.

A continuación se detallan las principales conclusiones y recomendaciones, así como una conclusión personal del beneficio que tuvo para mi persona este trabajo.

5.1.- A la Entidad

5.1.1.- Conclusiones

5.1.1.1- Formalización de una estructura de Seguridad de la Información

Las medidas de seguridad se traslapan dentro de toda la estructura de la entidad, por lo que su reconocimiento, comprensión y si realmente están siendo efectivas, no es fácil de analizar y de verificar si los controles establecidos realmente están cumpliendo con su objetivo.

5.1.2.- Análisis de riesgos de la Seguridad de la Información

La identificación de los riesgos de la Seguridad de la Información no se tiene definido y debe ser el punto de partida para una adecuada mitigación de los riesgos asociados.

5.1.3.- Gestión de la Seguridad de la Información

La entidad cuenta con una línea base definida de Seguridad de la Información que puede mejorar con el apoyo de un adecuado sistema de Gestión.

5.1.4.- Cultura de la Seguridad de la Información

La necesidad de un cambio cultural de la Seguridad de la Información es palpable en la entidad, se debe reconocer que la implementación de normativas internacionales como lo son la norma ISO/IEC 27001-2008 y COBIT 4.1. son difíciles de implementar ya que la cultura empresarial no es la adecuada.

5.1.2.- Recomendaciones

5.1.2.1.- Formalización de una estructura de Seguridad de la Información

Es importante la identificación a nivel conceptual y lógico de la estructura de la entidad para la Seguridad de la Información que permita un análisis holístico del cual se desprenda el esquema de Seguridad que la entidad requiera.

5.1.2.2.- Análisis de riesgos de la Seguridad de la Información

Los riesgos son la base para cualquier análisis que se requiera en la Seguridad de la Información, es muy recomendable que la entidad realice un análisis exhaustivo de los riesgos con la finalidad de obtener una protección adecuada de la Seguridad.

5.1.2.3.- Gestión de la Seguridad de la Información

La adopción de la norma ISO/IEC 27001-2008 que se está implementando apoyará significativamente en este aspecto por lo que se recomienda seguir en ese sentido.

5.1.2.4.- Cultura de la Seguridad de la Información

Con la implementación de la norma adoptada por la entidad se establecen oportunidades de mejora en la cultura de las empresas, siendo esta la recomendación más acertada.

5.2.- Personales del uso del BMIS

Cuando me decidí por el tema de este trabajo la idea primordial era realizar un trabajo que fuera distinto a todos lo que se habían realizado anteriormente y considero que el objetivo se logró.

El tema se Seguridad de la Información es muy amplio y afecta todos los aspectos de una organización, basta busca en internet y se encuentra una infinidad de material en donde nos explican qué se debe hacer, cómo se debe implementar, aspectos generales, aspectos específicos, mejores prácticas, estándares, guías, políticas que se deben tomar, etc. Sin embargo, todos nos dicen qué hacer pero casi ninguno nos dice el cómo hacerlo.

El reto de "pensar en función del BMIS" para realizar un análisis integral de la entidad que me ha permitido ver mucho más allá de las medidas básicas que se implementan en una organización, la Seguridad de la Información es mucho más de tener un Firewall bien configurado, afecta los aspectos desde la forma de pensar de las personas hasta las medidas más básicas que se deben tener para una adecuada gestión de la Seguridad de la Información y que esta gestión sea efectiva.

El análisis de las interrelaciones entre los elementos nos brinda la oportunidad de establecer relaciones que de otro modo no se podrían ver, situaciones específicas que pueden atentar contra adecuada implementación de la Seguridad de la Información.

Si bien es cierto tuve algunas limitaciones debido a que fui un analista externo, el hecho de que el encargado de la seguridad de la información en una organización aplique este modelo para su función definitivamente será de mucho apoyo para su gestión, ya que el estar día a día en la entidad podrá conocer con más detalle las características de su organización y le mostrará el cómo podría establecer oportunidades de mejora.

El aspecto más relevante es la cultura organizacional hacia la Seguridad de la Información, sobre todo en el caso de entidades que tienen regulaciones que deben implementar, es que el cambio cultural es fuerte debido a que la cultura en general del costarricense es de ser muy confiado y poco estructurado y nos enfrenta a una aplicación de marcos y estándares de culturas diferentes por lo que uno de los retos más importantes es lograr este cambio.

Actualmente me encuentro dando una consultoría en Seguridad de la Información y el apoyo de ya haber hecho este trabajo me ha sido muy significativo para identificar los riesgos y los problemas en esta materia. La forma de pensar y ver la empresa holísticamente me ha permitido un mucho mejor entendimiento de los problemas relacionados y las diferentes alternativas de solución para los mismos.

6.- Bibliografía

- II Governance Institute (2007), COBIT 4.1.
  Rolling Meadows, E.E.UU.
- II Governance Institute (2008), Alineando COBIT 4.1, ITIL V3 e ISO/IEC 27002 en beneficio de la empresa.
  Rolling Meadows, E.E.UU.
- Instituto de Normas Técnicas de Costa Rica (INTECO), Norma ISO/IEC 27001-2008, Tecnología de Información, Técnicas de Seguridad, Sistemas de gestión de la seguridad de la información, Requisitos.
- Instituto de Normas Técnicas de Costa Rica (INTECO), Norma ISO/IEC 27002-2009, Tecnología de Información, Código de prácticas para la gestión de la seguridad dela información.
- ISACA (Information Systems Audit and Control Association). The Business Model for Information Security, 2010