FACULTAD DE POSGRADOS

PROPUESTA DE UN MODELO DE GESTIÓN PARA MEJORAR LA CAPACIDAD DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE UNA INSTITUCIÓN FINANCIERA DEL SECTOR PÚBLICO.

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Magister en Gerencia de Sistemas y Tecnologías de la Información

Profesora Guía

MSc. Katalina del Rocío Coronel Hoyos

Autora

Cecilia del Pilar Puga Hermosa

Año

2017

DECLARACIÓN DEL PROFESOR GUÍA

Declaro haber dirigido este trabajo a través de reuniones periódicas con la maestrante Cecilia del Pilar Puga Hermosa, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.

_____

Katalina del Rocío Coronel Hoyos
Máster en Gerencia de Tecnologías de la Información
CC.: 1711000016

DECLARACIÓN DEL PROFESOR CORRECTOR

Declaro haber revisado este trabajo, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.

_____

Marco Vinicio Vásquez Chávez
Maestro en Administración
CC.: 1707997746

DECLARACIÓN AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes".

_____

Cecilia del Pilar Puga Hermosa
Ingeniero en Informática
CC.: 1709151268

AGRADECIMIENTOS

Agradezco a Dios por permitirme llegar a cumplir esta meta en la vida y por darme la oportunidad de compartir con mi madre y hermanos cada instante de esfuerzo y sacrificio que ha significado el alcanzar este título.

A los profesores y compañeros por los conocimientos y experiencias compartidas.

A mi tutora que con su sabiduría y paciencia supo guiar el éxito de este trabajo.

DEDICATORIA

Dedico este trabajo a mi madre querida, a mis hermanos por su apoyo incondicional y sus palabras de ánimo para seguir adelante y a mis dos angelitos que desde el cielo me cuidan.

RESUMEN

Al ser la información un recurso clave para las empresas y por el papel que juega la tecnología desde el momento en que la información se crea hasta que se destruye, la necesidad de proteger la información y los activos de TI de continuas amenazas a través de la mitigación de riesgos se vuelve imprescindible.

Para garantizar que la seguridad de la información sea gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI (Sistema de Gestión de la Seguridad de la Información).

La presente investigación se centra en proponer un modelo de gestión para mejorar la capacidad de gestión de la seguridad de la información de una Institución Financiera del Sector Público, que contribuya al cumplimiento de los objetivos estratégicos de la Institución, a través de la adopción de tres prácticas y estándares específicos (COBIT 5, ITIL v3,ISO 27001:2013), los que están siendo ampliamente adoptados a nivel global y que deben ser implementadas en base al Esquema Gubernamental de Seguridad de la Información (EGSI) desarrollado en septiembre de 2013 mediante Acuerdo Ministerial 166.

En el capítulo 1, “Introducción y Marco Teórico”, se expone los objetivos que se alcanzarán con la investigación basados en los antecedentes y en los posibles problemas detectados en la Gestión de la Seguridad de la Información de la Institución Financiera, así como una breve descripción de los conceptos que a lo largo del desarrollo serán de mucha utilidad.

En el capítulo 2, “Análisis de la Situación Actual”, se analiza el contexto de la Institución Financiera a través de su misión, visión, principios y valores, objetivos estratégicos y estructura organizacional que pueden afectar la

capacidad de lograr los resultados esperados de su Sistema de Gestión de la Seguridad de la Información. Se realiza un primer diagnóstico en base a los resultados de las auditorías realizadas entre los años 2010 y 2014 y de los problemas recurrentes categorizándolos en base al nivel de impacto.

En el capítulo 3, “Análisis de causa raíz e identificación de la brecha con las mejores prácticas”, se realiza un diagnóstico de la situación actual de la Institución con relación a la seguridad de la información que servirá como línea base para la implementación del modelo propuesto.

En el capítulo 4, “Modelo de Implementación del Sistema de Gestión de la Seguridad de la Información”, se propone un modelo que logra la excelencia a través de la mejora continua, fundamentado en la norma ISO27001:2013 que tiene embebido el ciclo PDCA o ciclo de Deming.

En el capítulo 5, “Conclusiones y Recomendaciones”, se emite finalmente una serie de conclusiones y recomendaciones de este trabajo de investigación.

ABSTRACT

Information as a key resource for companies and by the role played by technology from the moment the information is created until it is destroyed; the need to protect information and its assets from threats through risk mitigation becomes indispensable.

To ensure the security of the information be managed correctly, you must make use of a systematic, documented and known process throughout the Organization, from a business risk approach, that is an ISMS (Information Security Management System).

The present research focuses on proposing a management model to improve the management capacity of the information security of a public financial institution, that contributes to the implementation of its strategic objectives, through the adoption of specific standards and three practices (COBIT 5, ITIL v3, ISO 27001:2013), which are being widely adopted at a global level and should be implemented on the basis of the Government Information Security Plan (EGSI) developed in September 2013 through the Agreement Ministerial 166.

The Chapter 1, "Introduction and theoretical framework", outlines the objectives to be achieved with research based on the background and the potential problems identified in the management of the information security of the financial institution, as well as a brief description of the concepts that will be useful throughout the document.

The Chapter 2, "Analysis of the current situation", discusses the context of the financial institution through its mission, principles and values, strategic objectives and organizational structure that can affect the ability to achieve the results expected of its information security management system; this is an initial diagnosis on the basis of the results of the audits carried out between the years

2010 and 2014 and the recurring problems of categorizing them based on the level of impact.

The Chapter 3, "Analysis of causes root and the gap identification with the best practices ", is a diagnosis of the current situation of the institution in relation to the information security that will serve as a baseline for the implementation of the proposed model.

The Chapter 4,"Model of implementation of the information security management system" proposes a model that achieves excellence through continuous improvement, based on the standard ISO27001:2013 that has embedded the PDCA cycle, or Deming’s cycle.

The Chapter 5, "Conclusions and recommendations", finally issues a series of conclusions and recommendations of this study.

INDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. CAPÍTULO I. INTRODUCCIÓN Y MARCO TEÓRICO

1.1 Objetivos

1.1.1 Objetivo General

Proponer un modelo para mejorar la capacidad de gestión de la seguridad de la información de una Institución Financiera del Sector Público.

1.1.2 Objetivos Específicos

- Identificar los problemas asociados al proceso de Gestión de la Seguridad de Información y que son observados por los organismos de control.
- Hacer un estudio para establecer de manera precisa las causas de dichos problemas.
- Utilizar procesos basados en estándares y buenas prácticas que permitirán mejorar la Gestión de la Seguridad de la Información.
- Proponer un modelo que mejore la capacidad de gestión de seguridad de la información.

Para cumplir con los objetivos específicos, a lo largo de la presente investigación se utilizará información obtenida de documentos confidenciales de la Institución Financiera del Sector Público.

1.2 Antecedentes

Uno de los procesos de asesoría al Directorio de la Institución Financiera del Sector Público, es la Dirección Nacional de Auditoría Interna, cuya misión es la de evaluar el funcionamiento del sistema de control interno y la utilización de los recursos públicos; asesorar en el ámbito de control para la mejora de los procesos; y, verificar el cumplimiento de las leyes aplicables y la normativa legal vigente, a fin de proveer una garantía razonable acerca de la eficiencia y

eficacia de las operaciones, salvaguardia de los activos y de la información y adecuada presentación de los estados financieros.

Una de las responsabilidades y atribuciones de la Subgerencia General de la Institución Financiera en base al estatuto orgánico, es la de supervisar el cumplimiento de las recomendaciones de Auditoría Interna y otros órganos de control.

Como producto de las acciones de control, efectuadas por los organismos de control y/o la Dirección Nacional de Auditoría Interna de la Institución Financiera, se tiene regularmente una serie de recomendaciones que son de cumplimiento obligatorio para la Coordinación General de Tecnologías de la Información y Comunicación, las mismas que tienden a mejorar o lograr un adecuado control interno con el fin de obtener mayor eficiencia operacional y administrativa en el proceso de Gestión de la Seguridad de la Información de la Institución Financiera.

En base a las estadísticas que se muestran en las Figuras 16, 17 y 18, se evidencia tanto para la auditoría interna como externa, que el porcentaje de cumplimiento de las recomendaciones cada vez disminuye dentro del período comprendido entre el 2010 al 2014.

1.3 Justificación

Del análisis de las causas para que el número de recomendaciones en lugar de disminuir aumenten de período en período y haciendo un recuento en cada una de las actividades y procesos que se ha realizado en el área durante 23 años, y contrastando la información con los criterios e ideas expuestas por compañeros de trabajo en el área, se presumen varias circunstancias de origen por las cuales se generan los problemas o irregularidades de la implementación de acciones que prevean incurrir en situaciones de riesgo o acciones que lejos de lograr eficacia dentro de sus funciones, muchas veces son la causa de que los

procesos y las actividades tengan un sin número de circunstancias que las vuelven tortuosas y de baja eficacia. Es entonces importante realizar esta investigación para comprobar el origen de dichas causas que las generan.

En base a los problemas detectados y por la importancia que tiene el cumplimiento de las recomendaciones emitidas por los organismos de control internos y externos de la Institución Financiera, el presente tema de tesis se centrará en proponer un modelo de gestión para mejorar la capacidad de gestión de la seguridad de la información de una Institución Financiera del Sector Público, que contribuya al cumplimiento de los objetivos estratégicos de la Institución para alcanzar el Buen Vivir. De igual forma, en caso de que el modelo llegue a ser implementado, su uso mejorará la gestión de la calidad y la fiabilidad de la información, mediante la adopción de estándares y buenas prácticas.

1.4 Identificación del Problema

Se ha realizado un análisis de las posibles causas para que el número de recomendaciones relacionadas a seguridad de la información, en lugar de disminuir aumenten de período en período.

A continuación parte de los problemas identificados dentro de la Coordinación General de Tecnologías de Información y Comunicación, que lejos de puntualizar en cada una de las causas o posibles fuentes, intenta inducir causas genéricas o sistémicas que puedan ser resueltas con la gestión o implementación de rutinas, controles o metodologías que hagan del sistema amigable, eficiente, sostenible.

Causas o problemas:

- Ausencia de procedimientos o procedimientos desactualizados en lo que tiene que ver con la seguridad de la información.

- No existen métricas ni una evaluación periódica del desempeño y eficacia del Sistema de Gestión de Seguridad de la Información que establezcan acciones de mejora continua.
- Falta de concienciación y conocimiento en temas de seguridad de la información por parte de todos los funcionarios de la Institución.
- No se aíslan los datos sensibles en los ambientes de desarrollo y pruebas (son los mismos de producción).
- No se cuenta con un proceso de gestión de incidentes de seguridad de la información
- No se tiene claramente definido los roles y responsabilidades de la seguridad de la información.
- Los niveles de seguridad de los usuarios no están de acuerdo con la norma establecida para la creación de usuarios.
- Alta rotación de personal, personal nuevo no tiene una inducción apropiada sobre los procedimientos establecidos.
- No existe un registro de los cambios de la configuración.
- Falta de seguimiento a los incidentes de seguridad.

A nivel institucional, por la importancia que tiene la gestión y procesos implementados y monitoreados por la Institución Financiera, es ineludible generar de manera constante e indefinida modificaciones, variaciones, que ayuden en este empeño. En tanto en cuanto los procesos generen sinergia en los diferentes niveles, se harán evidentes acciones para la mitigación y/o eliminación de riesgos que conlleva el cambio continuo en la manera particular de hacer las cosas, en todos los ámbitos de gestión de la Institución.

Es por esto que los procesos que auditan las acciones implementadas y normadas serán un norte que posibilita indagar en los posibles problemas e inconvenientes que suscitan los actuales protocolos y prácticas con sus anomalías sistemáticamente producidas.

Es así que la mitigación y/o eliminación de los riesgos, propenderá en un camino constante de la eficacia y la adopción de mejores prácticas ayudará a minimizar los aspectos de cumplimiento y la preocupación de los auditores:

- Logrando el cumplimiento y la aplicación de controles internos.
- Demostrando adherirse a buenas prácticas aceptadas y probadas de la industria.
- Mejorando la confianza y la seguridad de la dirección y los usuarios.
- Generando respeto de los reguladores y otros supervisores externos. (Urbina Ríos y Valle, 2011, p.14)

Los estándares y las mejores prácticas no son una panacea; su efectividad depende de cómo se implementan y mantienen. (ISACA, 2008, p. 6.). La implementación de las mejores prácticas debería ser consistente con el marco de control y la gestión de riesgos de la Institución.

1.5 Seguridad de la Información

Existen muchas definiciones del término y la mayoría cubre los conceptos globalmente aceptados de confidencialidad, integridad y disponibilidad. ISACA define a la seguridad de la información como algo que:

“Asegura que, dentro de la empresa, la información está protegida contra su divulgación a usuarios no autorizados (confidencialidad), modificación inadecuada (integridad) y su falta de acceso cuando se la necesita (disponibilidad)”. (ISACA, 2012, p.19).

- La confidencialidad significa preservar las restricciones autorizadas sobre el acceso o divulgación, incluyendo los medios para proteger la privacidad y la información propietaria.

- La integridad significa proteger contra la destrucción o modificación inadecuada de la información e incluye asegurar el no repudio y autenticidad de la información.
- La disponibilidad significa asegurar que se puede acceder y usar la información de manera confiable y en el momento adecuado.

Al ser la información un recurso clave para las empresas y por el papel que juega la tecnología desde el momento en que la información se crea hasta que se destruye, la necesidad de proteger la información y los activos de TI de continuas amenazas a través de la mitigación de riesgos se vuelve imprescindible.

La seguridad de la información es un catalizador de negocio que está intrínsecamente unido a la confianza de las partes interesadas, ya sea tratando los riesgos de negocio o creando valor para la empresa como una ventaja competitiva.

Para garantizar que la seguridad de la información sea gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI (Sistema de Gestión de la Seguridad de la Información). (ISO27001, 2013, p.3). (ver figura 1).

Figura 1. *Análisis y Gestión de Riesgos*
Tomado de: ISO27000, 2012

1.6 Estándares, buenas prácticas y marcos de referencia para la gestión de la seguridad de la información.

1.6.1 COBIT 5

COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas (ISACA, 2012, p. 13), es decir les ayuda a crear el valor óptimo desde la tecnología de la información, manteniendo un equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

COBIT 5 para la Seguridad de la Información se basa en los mismos cinco principios que el marco de COBIT 5 (ver figura 2)

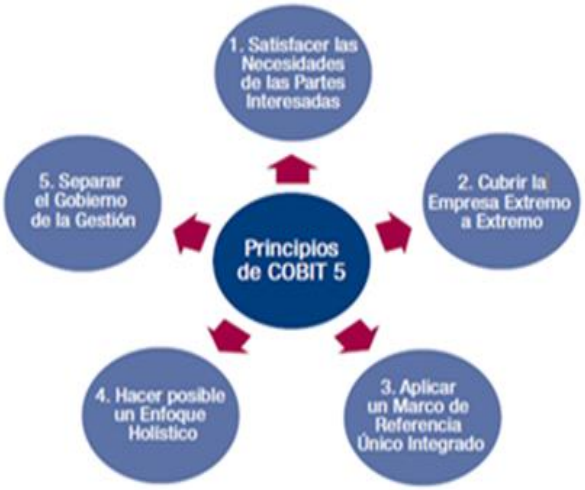

Figura 2. Principios de COBIT 5
Tomado de: ISACA, 2012

Principio1. Satisfacer las Necesidades de las Partes Interesadas.- La seguridad de la información es una necesidad importante para las partes interesadas, y esto se traduce en metas relacionadas con seguridad de la información para la empresa, para TI y finalmente para los catalizadores que los soportan.

Como cada empresa tiene objetivos diferentes, se debe utilizar la cascada de metas para personalizar COBIT 5 al contexto propio de cada institución (ver figura 3).

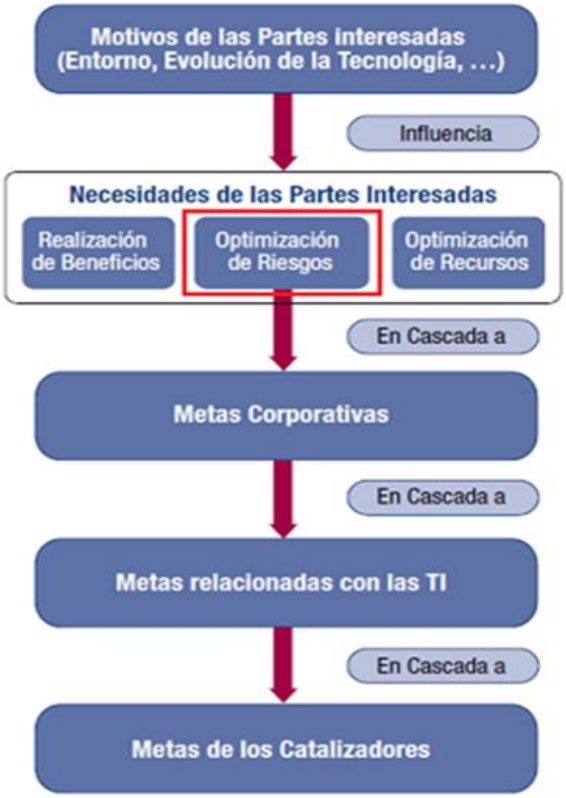

Figura 3. Cascada de Metas de COBIT 5
Tomado de: ISACA, 2012

Principio 2. Cubrir la empresa de Extremo-a-Extremo.- COBIT 5 para Seguridad de la Información cubre a todas las partes interesadas, funciones y procesos que forman parte de la empresa y son relevantes para la seguridad de la información.

Principio 3. Aplicar un Marco de Referencia Único Integrado.- COBIT 5 para Seguridad de la Información reúne conocimientos previamente distribuidos entre los diferentes marcos y modelos de ISACA (COBIT, BMIS, Risk IT, Val IT) con guías de otros importantes estándares relacionados con la seguridad de la información, tales como la serie ISO/IEC 27000, el Estándar de Buenas Prácticas para Seguridad de la Información de ISF y el SP800-53A del U.S. National Institute of Standards and Technology (NIST).

Principio 4. Hacer Posible un Enfoque Holístico.- COBIT 5 define un conjunto de habilitadores para apoyar la implementación de un sistema de gobierno de

la seguridad de la información y gestión global para las TI y la información de la empresa. (ver figura 4).

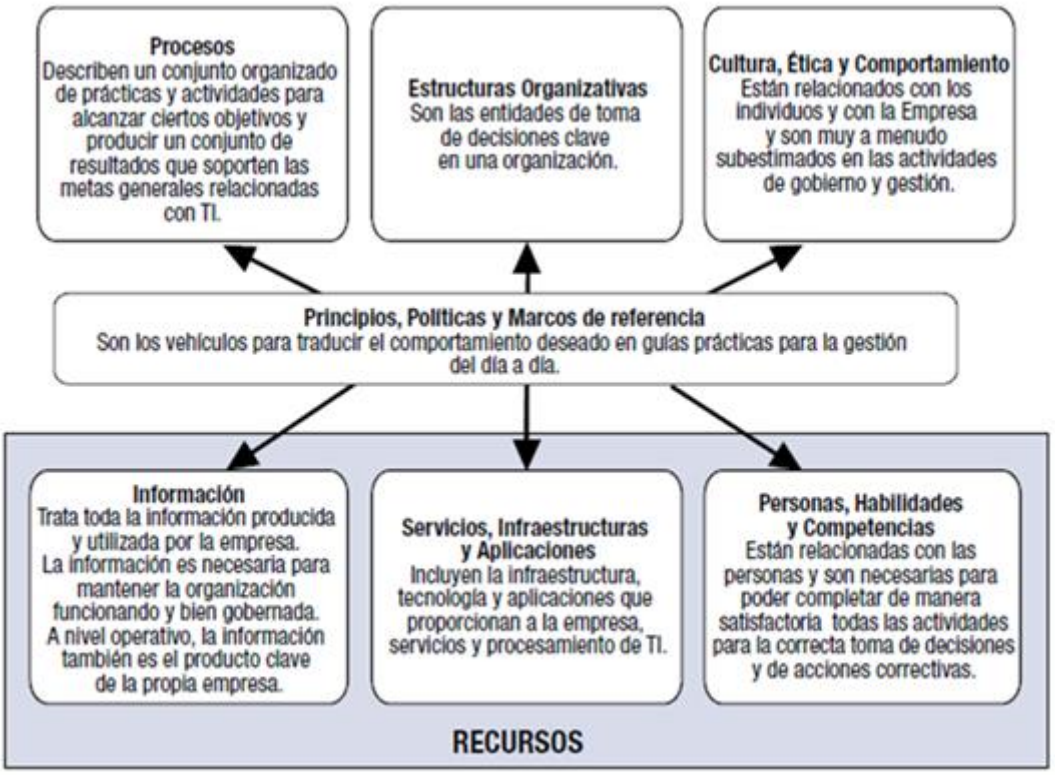

Figura 4. Catalizadores de COBIT 5
Tomado de: ISACA, 2012

Principio 5. Separar el Gobierno de la Gestión.- Los diferentes roles del gobierno y gestión de la seguridad de la información se hacen visibles mediante el modelo de procesos de COBIT 5, que incluye procesos de gestión y procesos gobierno, cada grupo con sus propias responsabilidades. (ver figura 5)

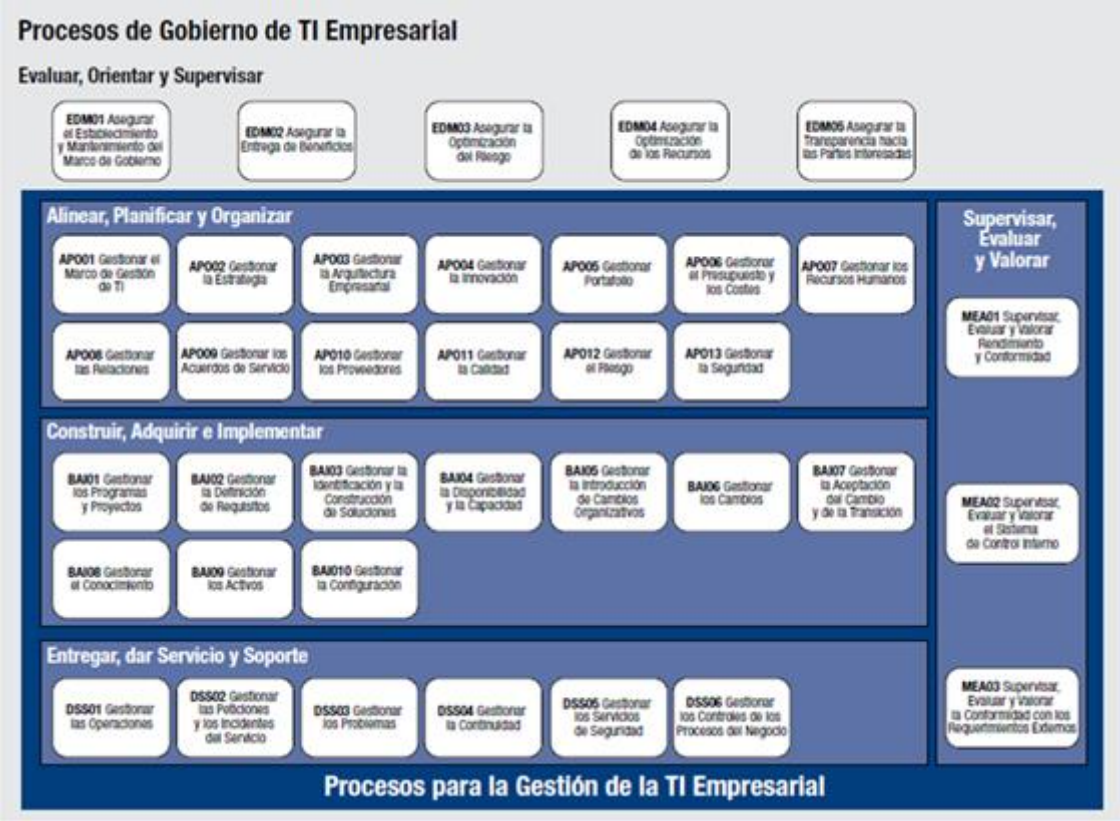

Figura 5. Modelo de Referencia de Procesos de COBIT 5
Tomado de: ISACA, 2012

"COBIT 5 para seguridad de la información puede ayudar a las empresas a reducir sus perfiles de riesgo a través de la adecuada administración de la seguridad. La información específica y las tecnologías relacionadas son cada vez más esenciales para las organizaciones, pero la seguridad de la información es esencial para la confianza de los accionistas", dijo Greg Grocholski, CISA, presidente internacional de ISACA y el auditor jefe de Dow Chemical.

1.6.2 COSO

Marco Integrado de Control Interno, creado en 1985 por la National Commission on Fraudulent Financial Reporting (Treadway Commission). La primera versión COSO I, publicada en 1992 permitía establecer, monitorear, evaluar y reportar acerca del control interno.

La versión COSO II, publicada en el año 2004 se enfoca a la gestión de los riesgos mediante técnicas como la gestión de un portafolio de riesgos.

Control Interno es un proceso llevado a cabo por el Consejo de Administración, la Gerencia y otro personal de la Organización, diseñado para proporcionar una garantía razonable sobre el logro de objetivos relacionados con operaciones, reporte y cumplimiento (COSO & PWC, 2014, p. 4).

COSO 2013 a través de la implantación de 5 componentes, garantiza la efectividad y eficiencia de las operaciones, confiabilidad de la información financiera, cumplimiento de las leyes y normas que sean aplicables y salvaguardia de los recursos. (ver figura 6)

Figura 6. Marco Integrado de Control Interno
Tomado de: COSO & PWC, 2014

El control interno consta de cinco componentes integrados. El Marco establece un total de diecisiete principios que representan los conceptos fundamentales asociados a cada componente (ver figura 7). Dado que estos principios proceden directamente de los componentes, una entidad puede alcanzar un control interno efectivo aplicando todos los principios, los que son aplicables a los objetivos operativos, de información y de cumplimiento. (Gobierno de Chile, sf.)

Figura 7. Principios de un control interno efectivo
Adaptado de: Gobierno de Chile, sf

COSO es un documento que contiene los principales lineamientos para lograr la implementación y gestión de un sistema de control. Puede considerarse como una ampliación de lo que contiene la serie de normas ISO 27000, buscando llevar la gestión de seguridad a todos los niveles de la organización. (Gutiérrez, 2013).

Algunos de los beneficios de utilizar el estándar COSO

- Promueve la gestión de riesgos en todos los niveles de la organización y establece directrices para la toma de decisiones de los directivos para el control de los riesgos y la asignación de responsabilidades.
- Ayuda a la integración de los sistemas de gestión de riesgos con otros sistemas que la organización tenga implantados.
- Ayuda a la optimización de recursos en términos de rentabilidad.
- Mejora la comunicación en la organización.

1.6.3 ITIL V.3

ITIL® desarrollada a finales de 1980, puede ser definido como un conjunto de buenas prácticas destinadas a mejorar la gestión y provisión de servicios TI. Su

objetivo último es mejorar la calidad de los servicios TI ofrecidos, evitar los problemas asociados a los mismos y en caso de que estos ocurran ofrecer un marco de actuación para que estos sean solucionados con el menor impacto y a la mayor brevedad posible. (Osiatis, 2011). La última versión lanzada en julio del 2007 se centra en el ciclo de vida del servicio (ver figura 8), que tiene por objetivo ofrecer una visión global de la vida de un servicio desde su diseño hasta su eventual abandono sin por ello ignorar los detalles de todos los procesos y funciones involucrados en la eficiente prestación del mismo.

El Ciclo de Vida del Servicio consta de cinco fases:

Estrategia del Servicio: En esta fase, la gestión de servicios no sólo es vista como una capacidad sino como un activo estratégico.

Diseño del Servicio: En esta fase se diseña los servicios de TI en base a arquitecturas, procesos, políticas y documentación para transformar los objetivos estratégicos en portafolios de servicios.

Transición del Servicio: En esta fase los servicios que han sido diseñados se integran al entorno de producción y se encuentran accesibles.

Operación del Servicio: El objetivo es asegurar que los servicios operen efectiva y eficientemente, según los niveles de calidad acordados.

Mejora Continua del Servicio: El objetivo de esta fase es mantener alineados los servicios con las necesidades del negocio que cambian constantemente, buscando la manera de mejorar la efectividad y la eficiencia de las actividades que se realizan en dichos servicios.

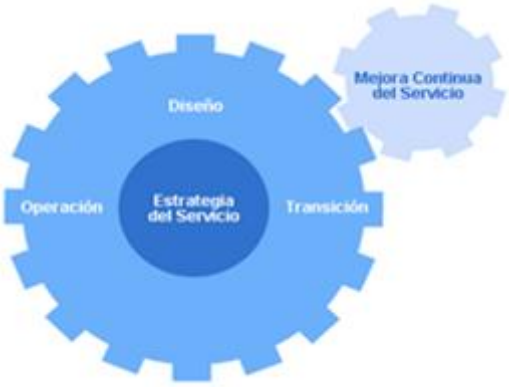

Figura 8. Ciclo de vida del servicio
Tomado de: Osiatis, 2011

Para una mejor administración del ciclo de vida de los servicios de TI se tiene un conjunto de procesos en cada fase del ciclo de vida (ver figura 9) y que sirven para planificar, entregar y dar soporte a los servicios.

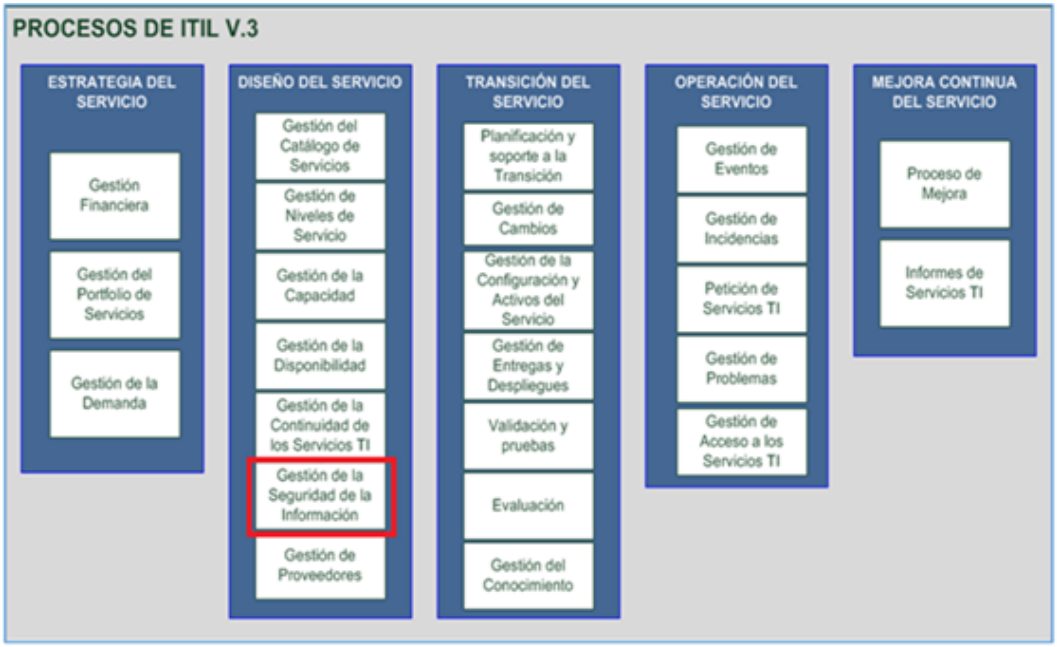

Figura 9. Procesos de ITIL V.3
Adaptado de: Osiatis, 2011

Los principales objetivos de la Gestión de la Seguridad se resumen en:

- Diseñar una política de seguridad, en colaboración con clientes y proveedores, correctamente alineada con las necesidades del negocio.

- Asegurar el cumplimiento de los estándares de seguridad acordados en los SLAs.
- Minimizar los riesgos de seguridad que amenacen la continuidad del servicio.

Los principales beneficios de una correcta Gestión de la Seguridad son (Osiatis, 2011):

- Se evitan interrupciones del servicio causadas por virus, ataques informáticos, etcétera.
- Se minimiza el número de incidentes.
- Se tiene acceso a la información cuando se necesita y se preserva la integridad de los datos.
- Se preserva la confidencialidad de los datos y la privacidad de clientes y usuarios.
- Se cumplen los reglamentos sobre protección de datos.
- Mejora la percepción y confianza de clientes y usuarios en lo que respecta a la calidad del servicio.

La Gestión de la Seguridad se relaciona con otros procesos de ITIL (Ríos, 2014, p. 40) con el objetivo de que éstos conozcan los estándares de seguridad asociados a cada servicio y para que se establezcan y cumplan los requisitos de seguridad necesarios para el correcto funcionamiento del negocio. (Osiatis, 2011).

- Gestión de la Disponibilidad: Para garantizar la disponibilidad del servicio se previene incurrir en incidencias de seguridad.
- Gestión de Cambios: Con una efectiva gestión de cambios se minimiza los riesgos de seguridad.
- Gestión de la Continuidad: Al garantizar la inmediata recuperación de los servicios de TI tras un desastre, se minimiza los riesgos de seguridad.

- Gestión de los Niveles de Servicio: La gestión de la seguridad se implementa en los SLAs, OLAs y UCs.
- Gestión de Incidentes: A través de este proceso se gestionan las incidencias de seguridad para lo cual debe existir una comunicación eficaz.
- Gestión de Configuraciones: Una inadecuada gestión de la configuración puede acarrear problemas de seguridad, los mismos que deben ser evitados o mitigados.
- Gestión de Versiones: Las nuevas versiones deben ser evaluadas para evitar problemas de continuidad o disponibilidad del servicio y monitorizadas por la Gestión de la Seguridad.

Es necesario que la Gestión de la Seguridad: (Osiatis, 2011).

- Establezca una clara y definida política de seguridad que sirva de guía a todos los otros procesos.
- Elabore un Plan de Seguridad que incluya los niveles de seguridad adecuados tanto en los servicios prestados a los clientes como en los acuerdos de servicio firmados con proveedores internos y externos.
- Implemente el Plan de Seguridad.
- Monitorice y evalúe el cumplimiento de dicho plan.
- Supervise proactivamente los niveles de seguridad analizando tendencias, nuevos riesgos y vulnerabilidades.
- Realice periódicamente auditorías de seguridad.

1.6.4 ISO27001

ISO/IEC 27000, 27001, 27002 y 27005 son un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un Marco de Gestión de la Seguridad de la Información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. (Arévalo, 2015, p. 2).

ISO 27001 es una norma internacional que describe cómo gestionar la seguridad de la información en una empresa. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. La última revisión fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013.

ISO / IEC 27001:2013 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI), en el contexto de la organización. También incluye los requisitos para la evaluación y tratamiento de los riesgos de seguridad de información adaptados a las necesidades de la organización. (ISO, 2013).

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo de mejora continua PDCA (Plan-Do-Check-Act). (ISO 27000, 2012, p.7)

- Plan (planificar): establecer el SGSI.
- Do (hacer): implementar y utilizar el SGSI.
- Check (verificar): monitorizar y revisar el SGSI.
- Act (actuar): mantener y mejorar el SGSI.

La ISO / IEC 27001:2013 está organizado en base a 14 dominios de seguridad, 35 objetivos de control y 114 controles. (ver figura 10). (AENOR, 2012, p. 42)

Figura 10. Sistema de Gestión de la Seguridad de la Información ISO 27001
Adaptado de: AENOR, 2012

1.6.5 ISO31000

La norma ISO 31000 desarrollada en el año 2009, establece principios y guías para el diseño, implementación y mantenimiento de la gestión de riesgos en forma sistemática y transparente de toda forma de riesgo en cualquier contexto. (Ormella, 2014, p.1).

Lo que se incorpora a la norma ISO 31000 es el nuevo concepto de riesgo, el mismo que se define en términos del efecto de la incertidumbre en los objetivos.

La definición de riesgo en este contexto, se refiere a situaciones negativas que provocan pérdidas, como a situaciones positivas que constituyen oportunidades.

Para una efectiva gestión de riesgos, la ISO 31000 se compone de tres elementos:

- Principios de la gestión de riesgos, cuyo objetivo es alinearse al contexto y al perfil de riesgos de la organización.

- Marco de trabajo para la gestión de riesgos, cuyo objetivo es integrar el proceso de gestión de riesgos al gobierno corporativo. (ver figura 11)

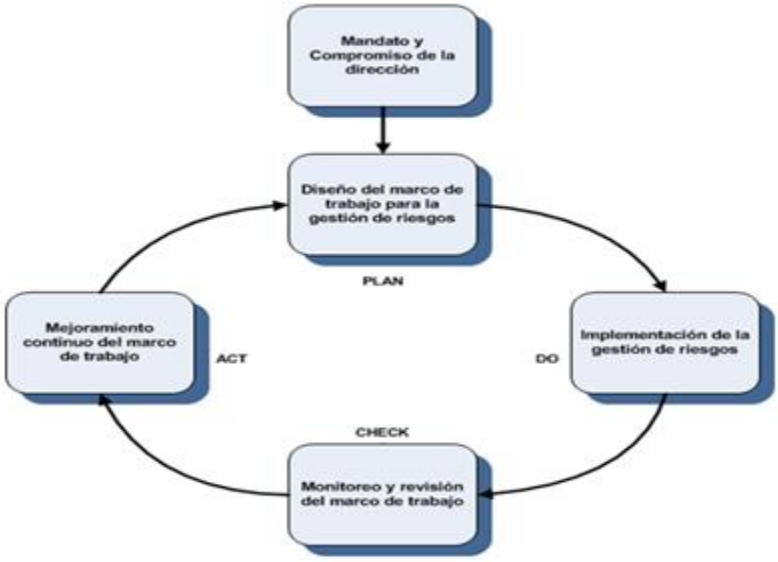

Figura 11. Marco de Trabajo de la ISO 31000
Adaptado de: Ormella, 2014

- Procesos de gestión de riesgos, compuesto por tres etapas: establecimiento del contexto, valuación de riesgos y tratamiento de riesgos. (ver figura 12)

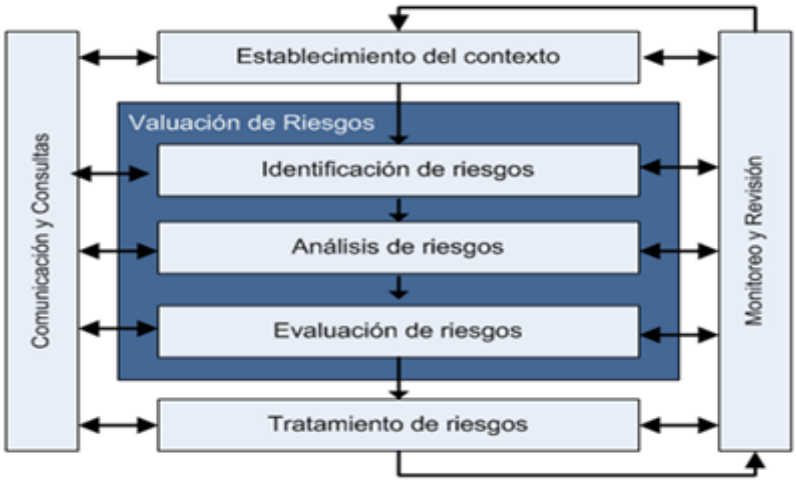

Figura 12. Procesos de la ISO 31000
Adaptado de: Ormella, 2014

Los beneficios de implementar ISO31000 (ICONTEC, 2011) son:

- Fomentar una gestión proactiva libre de riesgo.
- Mejorar la identificación de oportunidades y amenazas.
- Cumplir con las exigencias legales y reglamentarias, además de las normas internacionales.
- Aumentar la seguridad y confianza y mejorar la prevención de pérdidas y manejo de incidentes.
- Mejorar el aprendizaje organizacional.
- Mejorar la eficiencia y eficacia operacional.

1.6.6 EGSI

En base al Acuerdo Ministerial 166 de septiembre de 2013, la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación desarrolla el Esquema Gubernamental de Seguridad de la Información (EGSI), basado en la norma técnica ecuatoriana INEN ISO/IEC 27002, para implementar controles de seguridad en todas las entidades públicas que dependen de la Función Ejecutiva.

El EGSI establece un conjunto de directrices prioritarias para la Gestión de la Seguridad de la Información e inicia un proceso de mejora continua en las instituciones de la Administración Pública.

.

La implementación del EGSI incrementará la seguridad de la información en las entidades públicas, así como en la confianza de los ciudadanos en la Administración Pública. (Lexis, 2013, p. 4).

En la tabla 1, se hace un comparativo de los estándares, normas y marcos de referencia analizados para el desarrollo del tema.

En base al análisis, la presente investigación se centra en tres prácticas y estándares específicos, los que están siendo ampliamente adoptados a nivel

global (COBIT 5, ITIL v3 e ISO 27001), los mismos que se adaptarán a lo establecido en el EGSI.

Tabla 1.

Comparativo entre normas, estándares y marcos de referencia para la gestión de seguridad de la información

	COSO	COBIT5	ITIL V.3	ISO 270001	ISO 31000	EGSI
Objetivo	Mejora el control interno de la organización	Ayudar a las empresas a reducir sus perfiles de riesgo a través de una adecuada administración de la seguridad.	Ofrece una visión global de la vida de un servicio desde su diseño hasta su eventual abandono	Proporcionan un marco de Gestión de la Seguridad de la Información utilizable por cualquier tipo de organización.	Establece principios y guías para el diseño, implementación y mantenimiento de la Gestión de Riesgos.	Establece un conjunto de directrices prioritarias para la Gestión de la Seguridad de la Información e inicia un proceso de mejora continua en las instituciones de la Administración Pública
Área de aplicación	Toda la organización	Entorno TI	Entorno TI	Entorno TI	Toda la organización	Entorno TI
Beneficios	Gestión de los riesgos mediante técnicas como la gestión de un portafolio de riesgos	Mantener los riesgos relacionados con TI en un nivel aceptable	Diseñar una política de seguridad, en colaboración con clientes y proveedores, correctamente alineada con las necesidades del negocio	La seguridad de la información esté garantizada en la organización	Fomentar una gestión proactiva libre de riesgo.	La implementación reduce significativamente amenazas, riesgos y vulnerabilidades relacionadas a la gestión de la información.
	Gestión de seguridad a todos los niveles de la organización	Cumplir con las constantemente crecientes leyes, regulaciones, acuerdos contractuales y políticas aplicables	Asegurar el cumplimiento de los estándares de seguridad acordados en los SLAs.	Desarrolla una adecuada gestión de los riesgos	Mejorar la identificación de oportunidades y amenazas	Ayuda a establecer un proceso de mejora continua en la gestión de la

						seguridad de la información.
		Contempla de forma específica la seguridad de la información como uno de sus objetivos	Minimizar los riesgos de seguridad que amenacen la continuidad del servicio	Credibilidad y confianza entre nuestros clientes	Cumplir con las exigencias legales y reglamentarias, además de las normas internacionales	Increment a la cultura de los servidores públicos en cuanto al manejo de la información.
		Más completo dentro de su ámbito		Reducción de los costes vinculados a los incidentes de seguridad de la información	Aumenta la seguridad y confianza y mejora la prevención de pérdidas y manejo de incidentes	
				Sensibilización del personal en relación a la aplicación adecuada de las medidas de seguridad		
Procesos	5 componentes y 17 principios enfocados a la gestión de riesgos	37 procesos de seguridad de la información	8 procesos de seguridad de la información	14 dominios de seguridad de la información, 35 objetivos de control y 114 controles	3 elementos enfocados a la gestión de riesgos	11 dominios de seguridad de la información y 139 controles
Concienciación	Uno de los componentes de control interno "Ambiente de Control" influye en la concientización de los funcionarios de una empresa respecto al control	Como una buena práctica se propone que las políticas de seguridad de la empresa deben considerar como contenido de gran importancia el tema de la cultura y concienciación en seguridad de la información. El material para concienciación es un catalizador clave para la seguridad de la información y se debe considerar dentro del catálogo de servicios de la empresa.	En todo el proceso de gestión de la seguridad se tienen programas de formación los cuales son evaluados y medidos sus resultados.	La formación y concientización del personal es contemplada en el objetivo de control A.8.2.2 Concienciación, formación y capacitación en seguridad de la información.	La norma ayuda a concientizar a la empresa de la importancia de identificar y tratar los riesgos de toda la organización	El tema de concientización es abordado en 6 de los dominios de seguridad

Adaptado de: ISACA,2012; ISO27001,2013; Osiatis,2011; LEXIS,2013; Gutiérrez,2013 y Ormella,2014

2. CAPÍTULO II. ANÁLISIS DE LA SITUACIÓN ACTUAL

2.1 Estrategia de la Empresa

Los avances de las Tecnologías de Información y Comunicación, han obligado a que los ejecutivos de las empresas: directores generales (CEO), directores de tecnologías de la información (CIO) y directores de seguridad de la información (CISO), estén más conscientes de la importancia que tiene la seguridad de la información en la empresa como parte de su estrategia. Conocer la estrategia de la Institución Financiera permitirá a través de una alineación con sus objetivos estratégicos garantizar la confidencialidad, integridad y disponibilidad de la información desde que se crea hasta que se destruye.

2.1.1 Misión

Gestionar la liquidez de la economía ecuatoriana, mediante la instrumentación de las políticas monetaria, crediticia, cambiaria y financiera, para alcanzar el Buen Vivir.

2.1.2 Visión

Ser una institución innovadora en la gestión de la liquidez, incluyente en la prestación de servicios financieros, reconocida por sus aportes al desarrollo del país y referente del nuevo rol de Banca Central.

2.1.3 Principios y Valores

Los principios y valores que rigen el marco estratégico de la Institución Financiera son los siguientes:

- Respeto: Involucra la consideración de la dignidad de la persona, los derechos y libertades que le son inherentes, el trato con la ciudadanía y los colaboradores de la Institución Financiera.
- Transparencia: Significa el ejercicio de una conducta clara y evidente que se comprende sin duda ni ambigüedad de la que se puede dar cuenta en todo momento; cumpliendo con la reserva y confidencialidad que requiere la información sujeta a sigilo bancario o estadístico y acatando el deber de rendir cuentas a la ciudadanía.
- Integridad: Comprende las cualidades personales de honestidad, probidad, sinceridad y ausencia de conductas corruptibles, evitando todo comportamiento que pueda reflejarse negativamente en su persona o en la Institución.
- Profesionalismo y actitud de servicio: Implica poseer y demostrar actitudes que pongan en evidencia el compromiso con las necesidades de la población, orientando el servicio y la satisfacción de los clientes internos y externos como prioridad; involucra el ejercicio eficiente.

2.1.4 Objetivos Estratégicos

Los objetivos estratégicos que contribuyen a cumplir la misión de la Institución financiera son:

- Programar y regular la liquidez de la economía, mediante el monitoreo de la actividad económica, generación de estadísticas de síntesis macroeconómica, evaluación del riesgo sistémico, generación de propuestas de regulación monetaria y financiera y la instrumentación de políticas de integración monetaria y financiera regional, para aportar al cumplimiento de los objetivos de desarrollo y a la sostenibilidad del sistema monetario y financiero.
- Instrumentar operaciones de las políticas de gestión de la liquidez mediante la gestión de reservas, operaciones de liquidez doméstica y seguridad financiera que optimicen las inversiones realizadas y procuren

un balance equilibrado entre riesgo y rendimiento para el fortalecimiento económico y su sostenibilidad.

- Prestar servicios para la canalización de los flujos de liquidez de la economía de manera oportuna, eficiente, eficaz, segura, con calidad y calidez a través del Sistema Nacional de Pagos, el suministro de medios de pago y la prestación de servicios de banca central, fomentando la inclusión financiera de la población.
- Mejorar la eficacia y el desempeño de la gestión de los recursos humanos institucionales, como pilar fundamental de mejora continua.
- Maximizar la eficiencia operacional de la gestión institucional, a través del mejoramiento de procesos y la atención oportuna al ciudadano y usuario de los servicios.
- Optimizar las finanzas institucionales tanto de la programación y ejecución del gasto corriente como de inversión, que permita cumplir con los objetivos institucionales.

2.2 Análisis FODA

El análisis FODA permitirá obtener un diagnóstico preciso de la situación estratégica de la Institución Financiera.

Tabla 2.

Análisis FODA

Fortalezas	***Debilidades***
• Ser ente regulador del Sistema Financiero • Ser administrador del Sistema de Pagos • Ofrecer estadísticas económicas • Institución con Recursos propios • Autonomía jurídica • Gestión técnica y administrativa con patrimonio propio	• Alta rotación de personal (personas a contrato) • Personal jerárquico cambiante (tema político) • Falta de cumplimiento de la planificación institucional • Baja calidad de investigaciones por personal desmotivado • Bajo nivel de tecnología en la

	presentación de los servicios a los usuarios • Nivel de sueldos bajos
Oportunidades	***Amenazas***
• Compromiso de presupuesto anual	• Cambios constantes a la Ley • Incertidumbre laboral del personal

2.3 Estructura organizacional de la Institución Financiera

Para el cumplimiento de su misión, visión y objetivos, la Institución Financiera ha diseñado una estructura organizacional basada en procesos (ver figura 13), los que se clasifican, en función de su contribución a la Institución, en:

- Procesos Gobernantes: Aquellos que proporcionan directrices, políticas, planes estratégicos para la dirección y control de la Institución.
- Procesos Sustantivos: Aquellos que realizan las actividades esenciales para proveer los servicios y lo productos que ofrece a sus clientes una Institución. Los procesos sustantivos se enfocan a cumplir la misión de la Institución.
- Procesos Transversales: Aquellos procesos que de manera independiente asesoran y aseguran el cumplimiento efectivo de las políticas y estrategias relacionadas con la calidad de los productos o servicios
- Procesos Adjetivos: Aquellos que proporcionan productos o servicios a los procesos gobernantes y sustantivos.

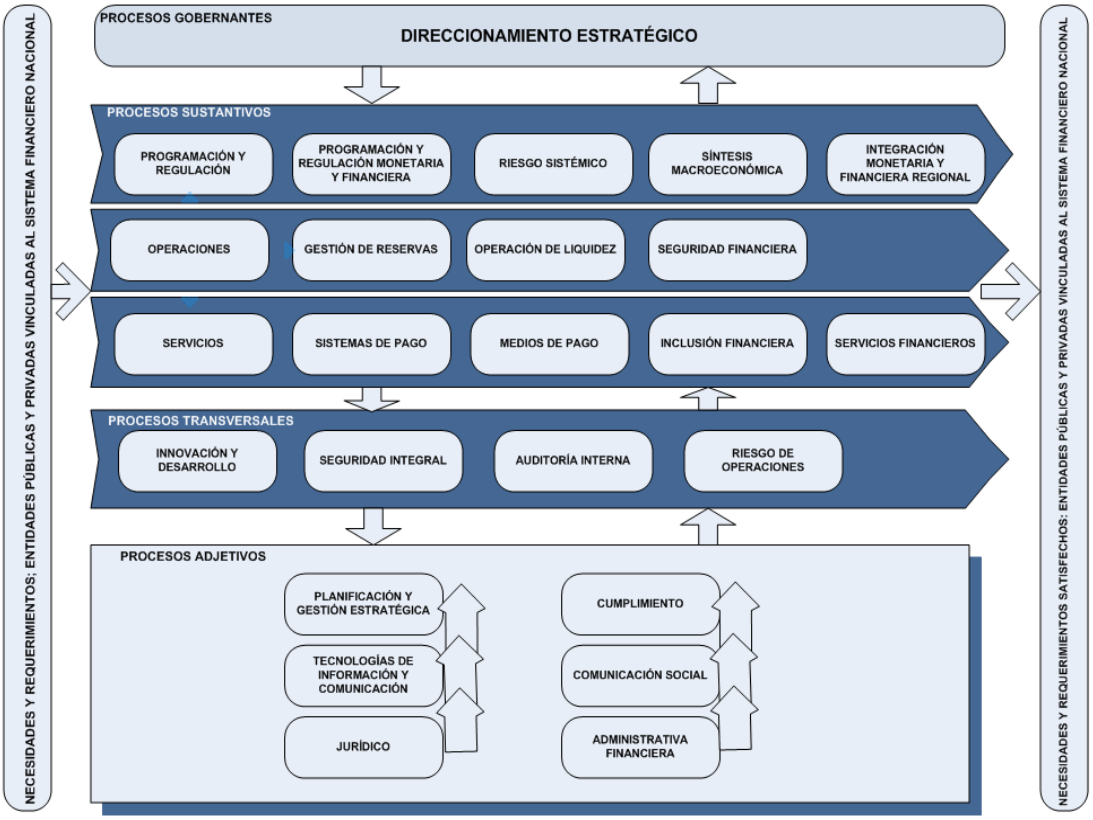

Figura 13. Estructura organizacional de la Institución Financiera

Ésta estructura está representada gráficamente a través del organigrama de la Institución Financiera (ver figura 14)

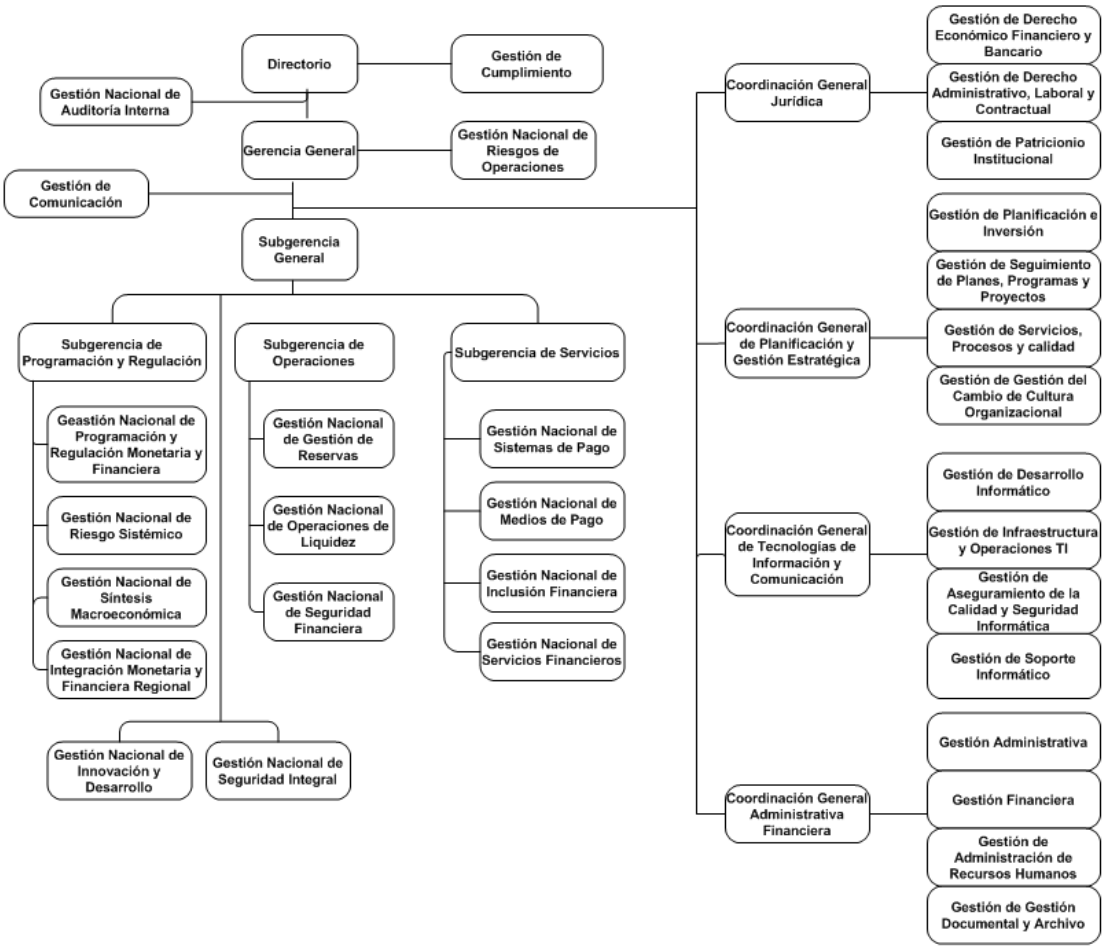

Figura 14. Organigrama de la Institución Financiera

2.4 Gestión Nacional de Auditoría Interna.

La Gestión Nacional de Auditoría Interna tiene como misión evaluar el funcionamiento del sistema de control interno y la utilización de los recursos públicos; asesorar en el ámbito de control para la mejora de los procesos; y, verificar el cumplimiento de las leyes aplicables y la normativa legal vigente, a fin de proveer una garantía razonable acerca de la eficiencia y eficacia de las operaciones, salvaguarda de los activos y de la información y adecuada presentación de los estados financieros.

2.5 Gestión Nacional de Riesgos de Operaciones.

La Gestión Nacional de Riesgos de Operaciones tiene como misión fomentar la seguridad y eficiencia institucional mediante la identificación, medición, monitoreo, control/mitigación de los riesgos a los que están expuestas las operaciones de la Institución; promover la seguridad y el buen funcionamiento de los sistemas de pago del país; y monitorear permanentemente el cumplimiento de las políticas emitidas por la Institución Financiera.

2.6 Gestión Nacional de Seguridad Integral.

La Gestión Nacional de Seguridad Integral tiene como misión gestionar la seguridad integral de la Institución a través de la identificación y mitigación de los factores de inseguridad de la custodia y transporte de valores, los sistemas de información, la infraestructura y el personal, para asegurar el funcionamiento y la integridad de los activos tangibles e intangibles de la Institución.

Una de las gestiones internas es la Gestión de Seguridad de la Información, cuyos productos y servicios son los siguientes:

1) Reporte de políticas de seguridad de la información y de seguridad transaccional.
2) Estudios análisis, y reportes de vulnerabilidades de la estructura tecnológica.
3) Manual de seguridad de la información.
4) Reportes de evaluación de controles.
5) Informes y reportes sobre incidentes relacionados con la seguridad de la información.
6) Informes de niveles de clasificación de la información y controles asociados.
7) Reglamento de uso de recursos de información y comunicaciones.
8) Reportes de vulnerabilidades de seguridad de la información.
9) Niveles de clasificación de la información.

El Artículo No. 1 del Acuerdo Ministerial 166, Registro Oficial Suplemento 88 del 25 de septiembre de 2013, dispone a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información y la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

En base al Artículo No. 2, la implementación del EGSI se realizará en cada institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en Gestión de Seguridad de la Información.

2.7 Coordinación General de Tecnologías de Información y Comunicación.

La Coordinación General de Tecnologías de Información y Comunicación tiene como misión contribuir al logro de los objetivos estratégicos de la Institución Financiera mediante la provisión de productos y servicios de tecnologías de información y comunicación seguras, eficientes y de vanguardia, elevando el nivel de competitividad e incrementando su prestigio y credibilidad frente a usuarios externos e internos. En el organigrama (ver figura 15.), está compuesta por cuatro gestiones:

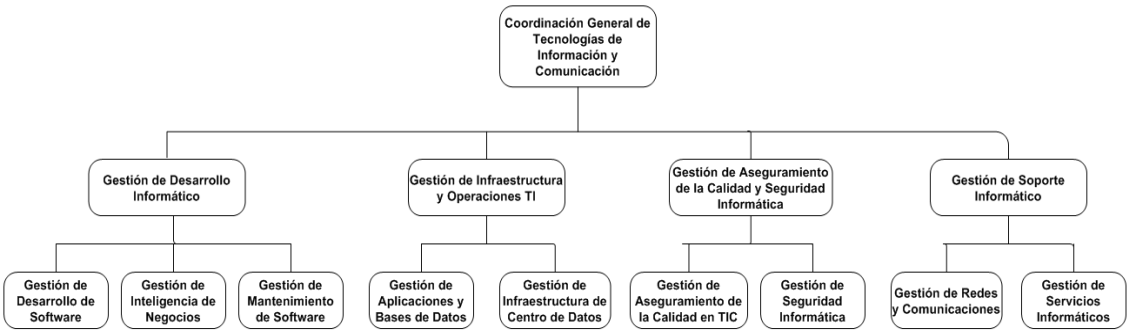

Figura 15. Organigrama de la Coordinación General de Tecnologías de la Información y Comunicación.

2.7.1 Gestión de Infraestructura y Operaciones de TI

La Gestión de Infraestructura y Operaciones de TI tiene como misión implementar proyectos de infraestructura, bases de datos, aplicaciones y sistemas de capa media, administrar la infraestructura tecnológica y herramientas de monitoreo de la Institución para garantizar el acceso, la disponibilidad, capacidad de procesamiento y contingencia de las TIC de la Institución Financiera.

Una de las gestiones internas es la Gestión de Aplicaciones y Bases de Datos cuyos productos y servicios son los siguientes:

1. Informe de pruebas de alta disponibilidad de base de datos y capa media
2. Proyectos de plataformas de software de base de datos y capa media
3. Planes de aseguramiento y disponibilidad de infraestructura tecnológica que incluye la instalación, configuración y administración de capa media, base de datos, repositorios, entre otros recursos tecnológicos requeridos para el servicio de los sistemas informáticos
4. Manuales, procedimientos y estándares de operación y monitoreo de bases de datos, servidores de aplicaciones web
5. Reporte de alertas y eventos del monitoreo de los servicios de TIC
6. Informes periódicos de desempeño y capacidad de base de datos y capa media
7. Reporte de estado de las réplicas de datos a sitios contingentes e interoperabilidad
8. Inventario de aplicaciones en ambientes de producción

2.8 Estudio de los informes de auditoría interna y externa desde el 2010 al 2014

En base a las estadísticas que se muestran en las Figuras 16, 17 y 18,se evidencia tanto para la auditoría interna como externa, que el porcentaje de

cumplimiento de las recomendaciones cada vez disminuye dentro del período comprendido entre el 2010 al 2014.

RECOMENDACIONES POR AÑO – AUDITORÍA INTERNA
DESDE: 2010 HASTA: 2014

Año	Total de Recomendaciones	En Proceso	Cumplidas	Incumplidas	% de Cumplimiento
2010	65	0	61	4	93.85
2011	110	0	100	10	90.91
2012	50	0	48	2	96.00
2013	150	0	70	80	46.67
2014	100	25	10	65	10.00
Totales	475	25	289	161	60.84

Figura 16. Recomendaciones por año – Auditoría Interna

RECOMENDACIONES POR AÑO – AUDITORÍA EXTERNA
DESDE: 2010 HASTA: 2014

Año	Total de Recomendaciones	En Proceso	Cumplidas	Incumplidas	% de Cumplimiento
2010	10	0	5	5	50.00
2011	7	0	7	0	100.00
2012	30	0	16	14	53.33
2013	15	0	10	5	66.67
2014	8	0	5	3	62.50
Totales	70	0	43	27	61.43

Figura 17. Recomendaciones por año – Auditoría Externa

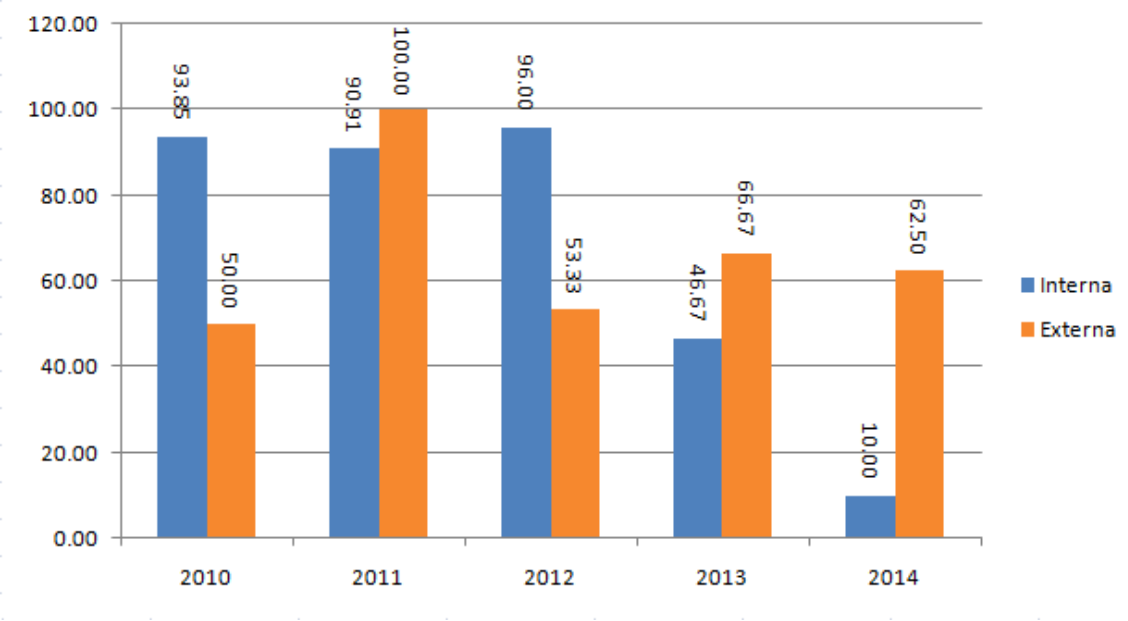

Figura 18. Porcentaje de recomendaciones Cumplidas

2.9 Identificación de problemas recurrentes y categorización de sus niveles de impacto

A continuación parte de los problemas identificados dentro de la Coordinación General de Tecnologías de Información y Comunicación categorizados en base a la experiencia del autor y a la importancia que tiene dentro del Sistema de Gestión de la Seguridad de la Información cuyo objetivo es contribuir al cumplimiento de los objetivos estratégicos de la Institución.

Tabla 3.

Problemas recurrentes y categorización de sus niveles de impacto

Problema	Importancia
Ausencia de procedimientos o procedimientos desactualizados en lo que tiene que ver con la seguridad de la información	Media
No existen métricas ni una evaluación periódica del desempeño y eficacia del sistema de gestión de seguridad de la información que establezcan acciones de mejora continua	Alta
Falta de concienciación y conocimiento en temas de seguridad de la información por parte de todos los funcionarios de la institución	Alta
No se aíslan los datos sensibles en los ambientes de desarrollo y pruebas (son los mismos de producción)	Media
No se cuenta con un proceso de gestión de incidentes de seguridad de la información	Alta
No se tiene claramente definido los roles y responsabilidades de la seguridad de la información	Alta
Los niveles de seguridad de los usuarios no están de acuerdo con la norma establecida para la creación de usuarios	Baja
Alta rotación de personal, personal nuevo no tiene una inducción apropiada sobre los procedimientos establecidos	Media
No existe un registro de los cambios de la configuración	Media
Falta de seguimiento a los incidentes de seguridad	Alta

3. CAPÍTULO III. ANÁLISIS DE CAUSAS RAÍZ E IDENTIFICACIÓN DE LA BRECHA CON LAS MEJORES PRÁCTICAS

3.1 Análisis y recolección de información

El objetivo de este análisis es identificar el nivel de cumplimiento de la Institución Financiera con relación a las directrices y objetivos de control del EGSI desarrollado en base al Acuerdo No. 166 de la Secretaría Nacional de la Administración Pública (SNAP) y en base al análisis de las causas raíz, definir acciones que permitan cerrar las brechas identificadas y permitan mejorar la capacidad de gestión de la seguridad de la información.

El análisis de brechas se realizó con la firma auditora Deloitte, a través de entrevistas a los funcionarios de la Dirección Nacional de Riesgos de Operaciones, Unidad de Vigilancia y Protección Física, Dirección de Administración del Talento Humano, Coordinación General de Tecnologías de

Información y Comunicación y Dirección Administrativa y a la revisión de documentación de procedimientos y políticas con el personal entrevistado de la Institución Financiera. Se basó en los 11 dominios del EGSI (Lexis, 2013, p. 4):

- Política de Seguridad de la Información.
- Organización de la Seguridad de la Información.
- Gestión de los Activos.
- Seguridad de los Recursos Humanos.
- Seguridad Física y del Entorno.
- Gestión de Comunicaciones y Operaciones.
- Control de Acceso.
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
- Gestión de los Incidentes de la Seguridad de la Información.
- Gestión de la Continuidad del Negocio.
- Cumplimiento.

Para el diagnóstico se utilizó un Modelo Genérico de Cumplimiento con opción de respuestas SI/NO. Dicho modelo establece seis posibles niveles de cumplimiento de acuerdo con los criterios generales mencionados a continuación:

Valor	Escala	Detalle
0	**No existe**	No existen directrices o no hay evidencia de su existencia.
1	**Inicial**	Las directrices no están estructuradas o son intuitivas, se aplican enfoques de forma individual o por caso.
2	**Repetible**	Las directrices siguen un enfoque similar de actividades que son ejecutadas por diferentes personas que desarrollan la misma tarea, no existe entrenamiento y sensibilización formal de las actividades comunes.
3	**Definido**	Las directrices se han estandarizado, documentado y comunicado. Existe entrenamiento disponible pero no se aplica en forma obligatoria. En la ejecución de los procesos es poco probable que se generen desviaciones.
4	**Administrado**	Las directrices se monitorean y se miden. Se identifican acciones de mejora que se aplican de forma irregular. Se utilizan herramientas en el proceso de forma limitada.
5	**Optimizado**	Las directrices siguen las buenas prácticas y se evidencia una mejora continua, se ejecutan acciones preventivas y correctivas y se mide la eficacia de su aplicación. Se aplican y utilizan herramientas para automatización de las directrices.

Figura 19. Niveles del Modelo Genérico de Cumplimiento
Adaptado de: CMM por Deloitte, 2014

El nivel de cumplimiento por cada dominio y subdominio se representará a través de un gráfico araña.

3.1.1 Política de Seguridad de la Información

En base al Anexo A, el cual contiene las preguntas que se plantearon para evaluar cada uno de los controles y las respectivas respuestas dadas por los funcionarios entrevistados, se tiene que la Institución Financiera se encuentra en el nivel 'Inicial (1)', de acuerdo al nivel de cumplimiento frente al Anexo 1 del Esquema Gubernamental de Seguridad de la Información (EGSI). El nivel de cumplimiento general del dominio se obtiene en base al promedio de cada subdominio que a su vez es el promedio de cada directriz.

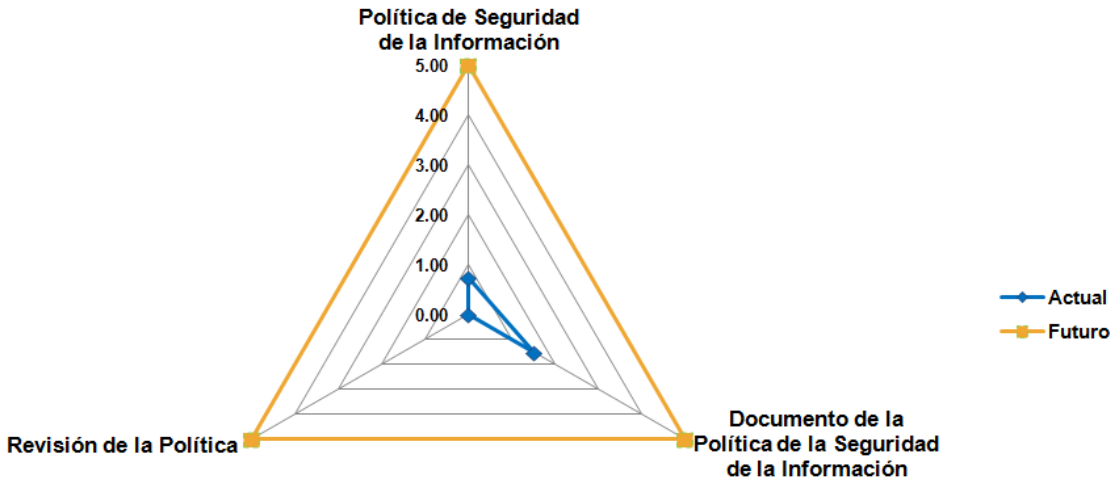

Figura 20. Nivel de cumplimiento de la Institución Financiera -Dominio 1: Política de Seguridad de la Información

3.1.2 Organización de la Seguridad de la Información

En base al Anexo B, el cual contiene las preguntas que se plantearon para evaluar cada uno de los controles y las respectivas respuestas dadas por los funcionarios entrevistados, se tiene que la Institución Financiera se encuentra en el nivel 'Repetible (2)', de acuerdo al nivel de cumplimiento frente al Anexo 1 del Esquema Gubernamental de Seguridad de la Información (EGSI). El nivel

de cumplimiento general del dominio se obtiene en base al promedio de cada subdominio que a su vez es el promedio de cada directriz.

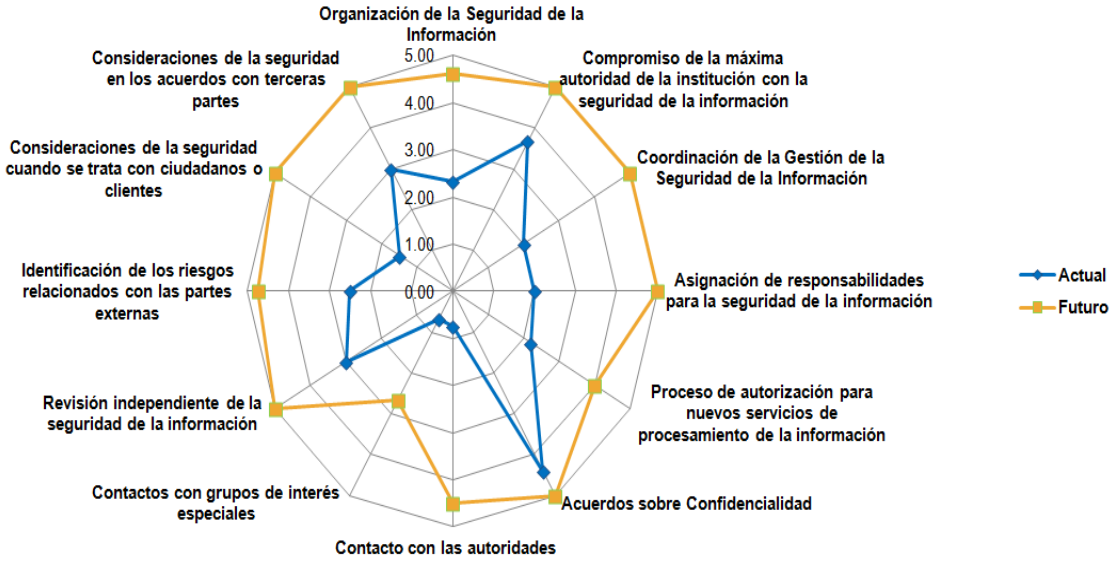

Figura 21. Nivel de cumplimiento de la Institución Financiera -Dominio 2: Organización de la Seguridad de la Información

3.1.3 Gestión de los Activos

En base al Anexo C, el cual contiene las preguntas que se plantearon para evaluar cada uno de los controles y las respectivas respuestas dadas por los funcionarios entrevistados, se tiene que la Institución Financiera se encuentra en el nivel ‘Definido (3)’, de acuerdo al nivel de cumplimiento frente al Anexo 1 del Esquema Gubernamental de Seguridad de la Información (EGSI). El nivel de cumplimiento general del dominio se obtiene en base al promedio de cada subdominio que a su vez es el promedio de cada directriz.

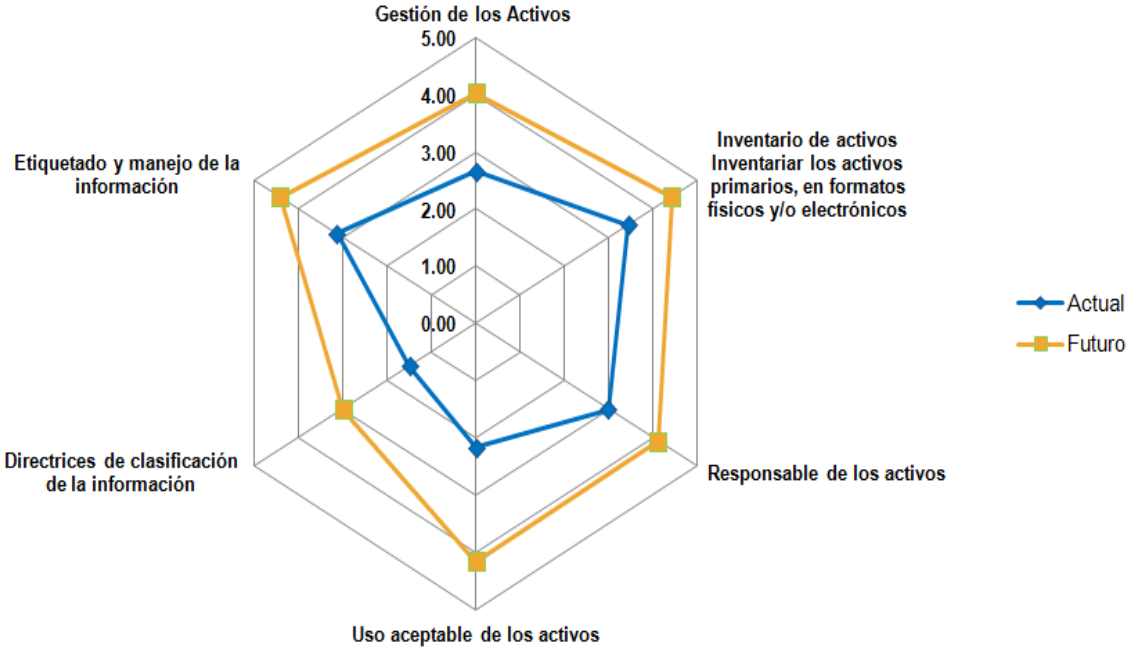

Figura 22. Nivel de cumplimiento de la Institución Financiera -Dominio 3: Gestión de los Activos

3.1.4 Seguridad de los Recursos Humanos

En base al Anexo D, el cual contiene las preguntas que se plantearon para evaluar cada uno de los controles y las respectivas respuestas dadas por los funcionarios entrevistados, se tiene que la Institución Financiera se encuentra en el nivel 'Repetible (2)', de acuerdo al nivel de cumplimiento frente al Anexo 1 del Esquema Gubernamental de Seguridad de la Información (EGSI). El nivel de cumplimiento general del dominio se obtiene en base al promedio de cada subdominio que a su vez es el promedio de cada directriz.

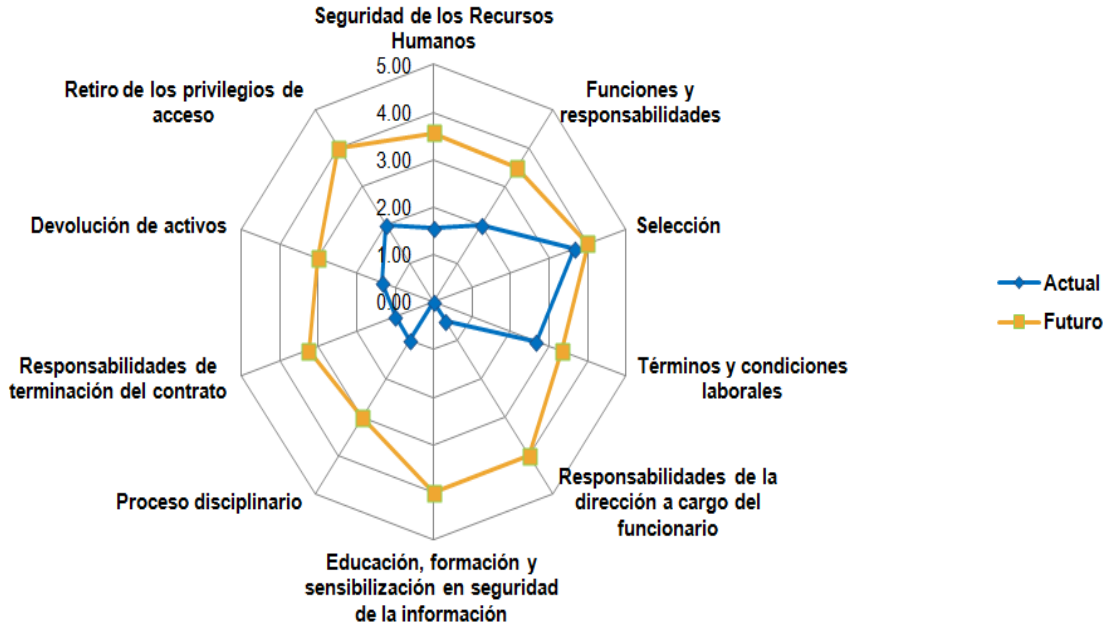

Figura 23. Nivel de cumplimiento de la Institución Financiera -Dominio 4: Seguridad de los Recursos Humanos

3.1.5 Seguridad Física y del Entorno

En base al Anexo E, el cual contiene las preguntas que se plantearon para evaluar cada uno de los controles y las respectivas respuestas dadas por los funcionarios entrevistados, se tiene que la Institución Financiera se encuentra en el nivel 'Definido (3)', de acuerdo al nivel de cumplimiento frente al Anexo 1 del Esquema Gubernamental de Seguridad de la Información (EGSI). El nivel de cumplimiento general del dominio se obtiene en base al promedio de cada subdominio que a su vez es el promedio de cada directriz.

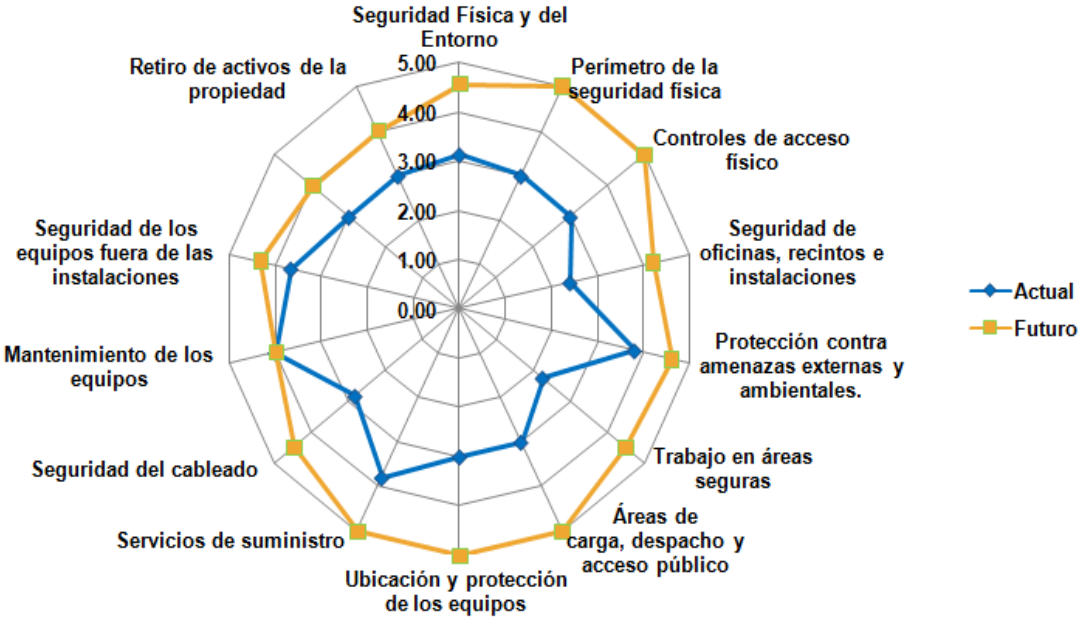

Figura 24. Nivel de cumplimiento de la Institución Financiera -Dominio 5: Seguridad Física y del Entorno

3.1.6 Gestión de Comunicaciones y Operaciones

En base al Anexo F, el cual contiene las preguntas que se plantearon para evaluar cada uno de los controles y las respectivas respuestas dadas por los funcionarios entrevistados, se tiene que la Institución Financiera se encuentra en el nivel 'Definido (3)', de acuerdo al nivel de cumplimiento frente al Anexo 1 del Esquema Gubernamental de Seguridad de la Información (EGSI). El nivel de cumplimiento general del dominio se obtiene en base al promedio de cada subdominio que a su vez es el promedio de cada directriz.

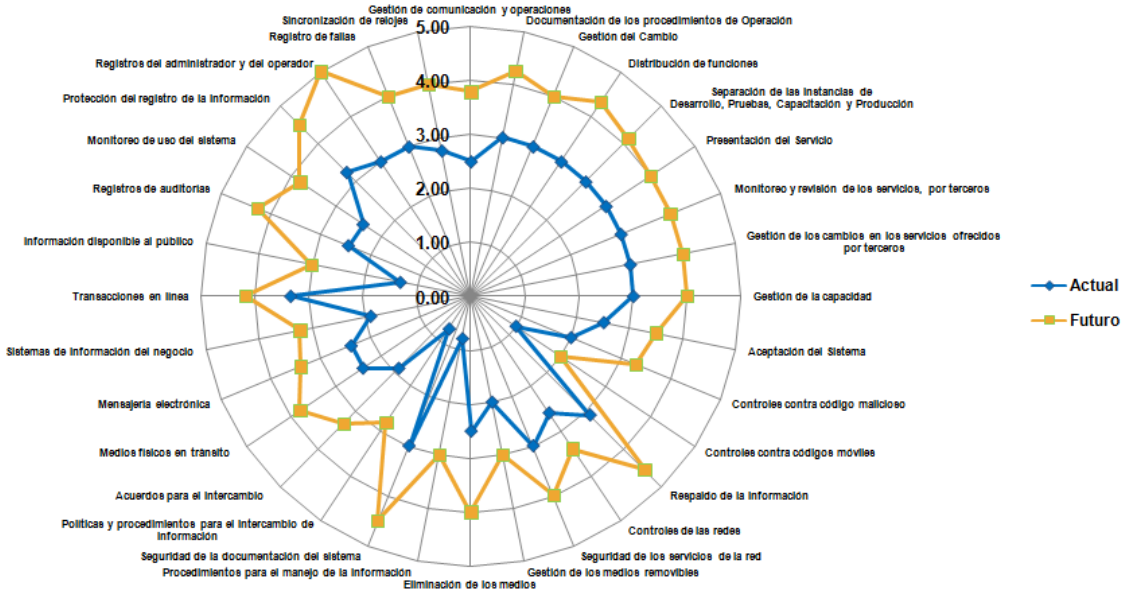

Figura 25. Nivel de cumplimiento de la Institución Financiera -Dominio 6: Gestión de Comunicaciones y Operaciones

3.1.7 Control de Acceso

En base al Anexo G, el cual contiene las preguntas que se plantearon para evaluar cada uno de los controles y las respectivas respuestas dadas por los funcionarios entrevistados, se tiene que la Institución Financiera se encuentra en el nivel ‘Repetible (2)’, de acuerdo al nivel de cumplimiento frente al Anexo 1 del Esquema Gubernamental de Seguridad de la Información (EGSI). El nivel de cumplimiento general del dominio se obtiene en base al promedio de cada subdominio que a su vez es el promedio de cada directriz.

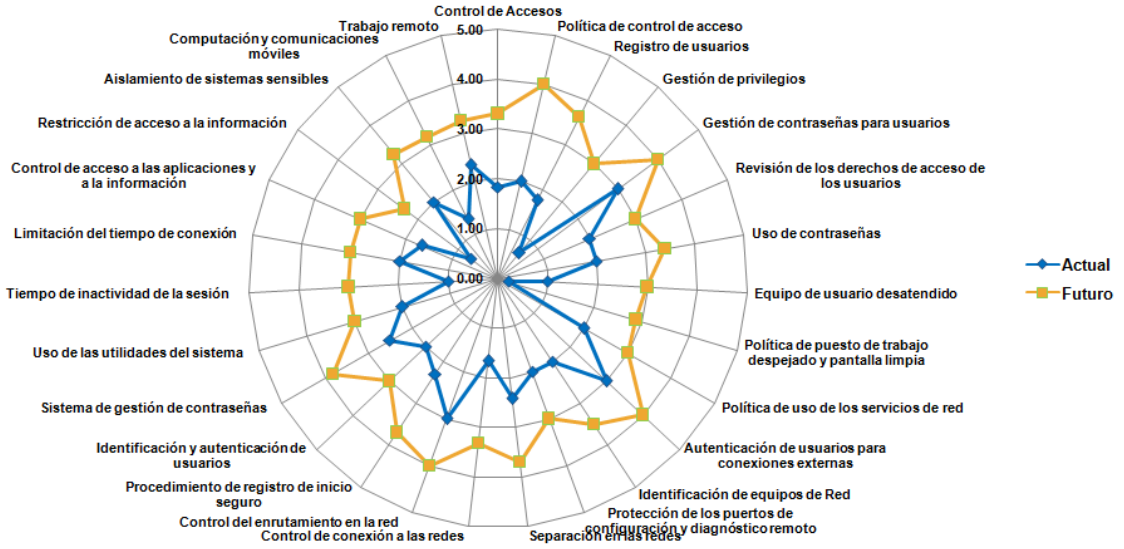

Figura 26. Nivel de cumplimiento de la Institución Financiera -Dominio 7: Control de Acceso

3.1.8 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

En base al Anexo H, el cual contiene las preguntas que se plantearon para evaluar cada uno de los controles y las respectivas respuestas dadas por los funcionarios entrevistados, se tiene que la Institución Financiera se encuentra en el nivel 'Repetible (2)', de acuerdo al nivel de cumplimiento frente al Anexo 1 del Esquema Gubernamental de Seguridad de la Información (EGSI). El nivel de cumplimiento general del dominio se obtiene en base al promedio de cada subdominio que a su vez es el promedio de cada directriz.

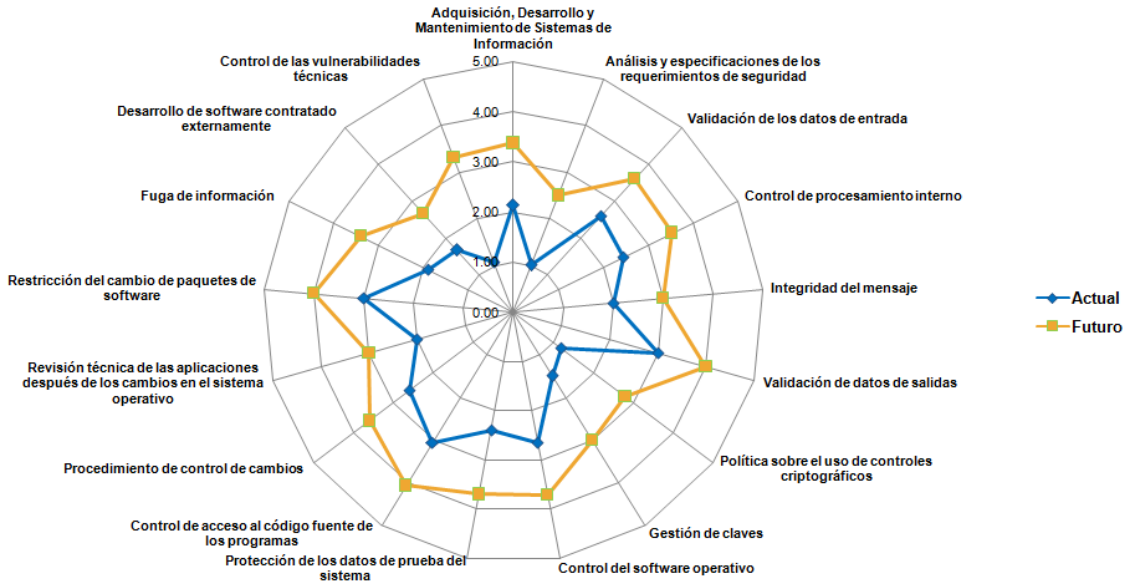

Figura 27. Nivel de cumplimiento de la Institución Financiera -Dominio 8: Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

3.1.9 Gestión de los Incidentes de la Seguridad de la Información

En base al Anexo I, el cual contiene las preguntas que se plantearon para evaluar cada uno de los controles y las respectivas respuestas dadas por los funcionarios entrevistados, se tiene que la Institución Financiera se encuentra en el nivel 'Inicial (1)', de acuerdo al nivel de cumplimiento frente al Anexo 1 del Esquema Gubernamental de Seguridad de la Información (EGSI). El nivel de cumplimiento general del dominio se obtiene en base al promedio de cada subdominio que a su vez es el promedio de cada directriz.

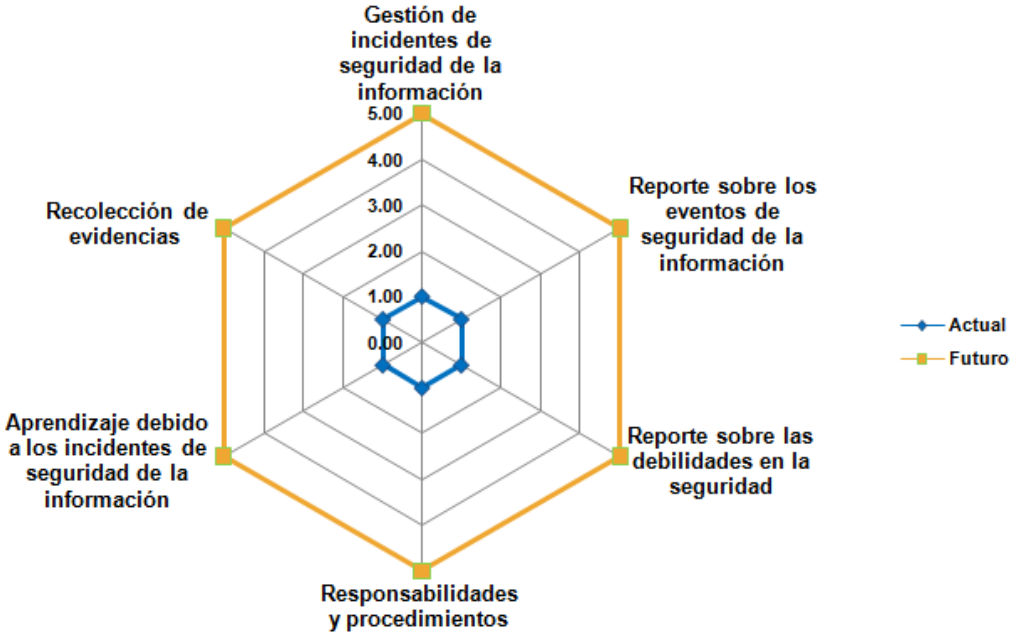

Figura 28. Nivel de cumplimiento de la Institución Financiera -Dominio 9: Gestión de Incidentes de Seguridad de la Información

3.1.10 Gestión de la Continuidad del Negocio

En base al Anexo J, el cual contiene las preguntas que se plantearon para evaluar cada uno de los controles y las respectivas respuestas dadas por los funcionarios entrevistados, se tiene que la Institución Financiera se encuentra en el nivel 'Definido (3)', de acuerdo al nivel de cumplimiento frente al Anexo 1 del Esquema Gubernamental de Seguridad de la Información (EGSI). El nivel de cumplimiento general del dominio se obtiene en base al promedio de cada subdominio que a su vez es el promedio de cada directriz.

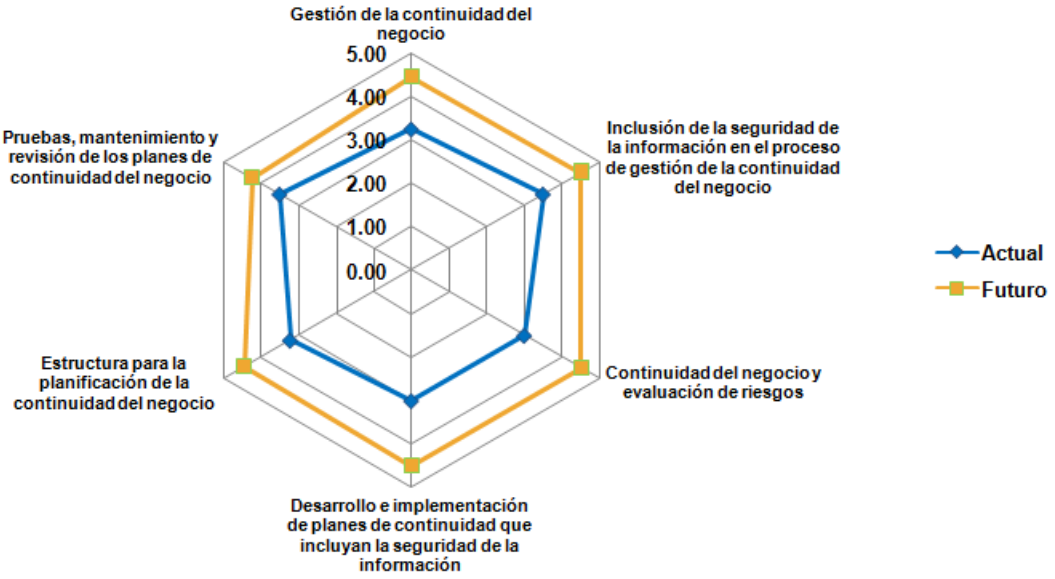

Figura 29. Nivel de cumplimiento de la Institución Financiera -Dominio 10: Gestión de la Continuidad del Negocio

3.1.11 Cumplimiento

En base al Anexo K, el cual contiene las preguntas que se plantearon para evaluar cada uno de los controles y las respectivas respuestas dadas por los funcionarios entrevistados, se tiene que la Institución Financiera se encuentra en el nivel 'Definido (3)', de acuerdo al nivel de cumplimiento frente al Anexo 1 del Esquema Gubernamental de Seguridad de la Información (EGSI). El nivel de cumplimiento general del dominio se obtiene en base al promedio de cada subdominio que a su vez es el promedio de cada directriz.

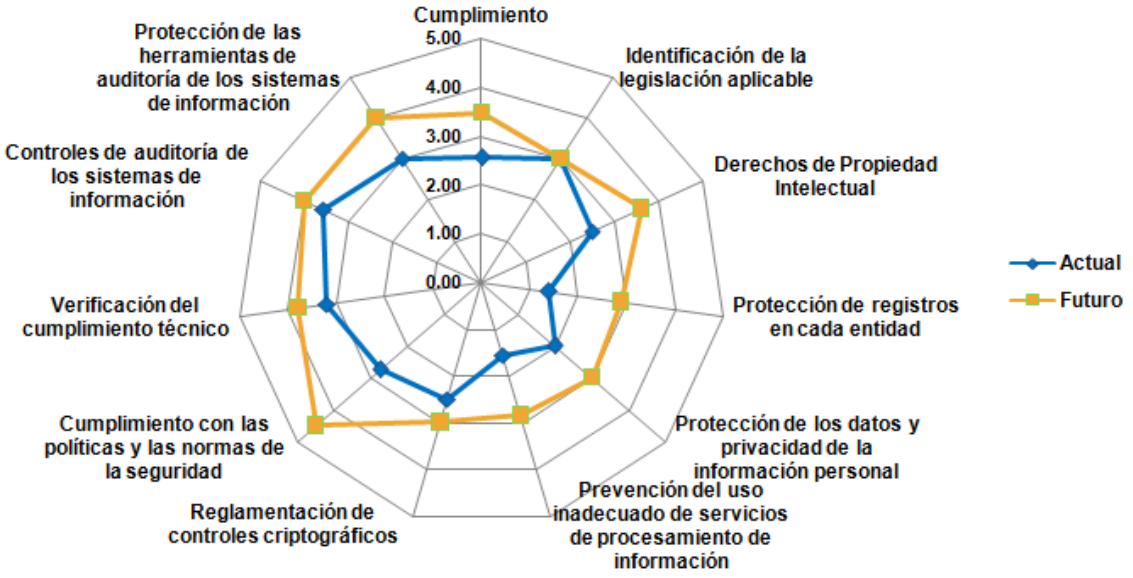

Figura 30. Nivel de cumplimiento de la Institución Financiera -Dominio 11: Cumplimiento

3.2 Identificación y análisis de riesgos

El objetivo del análisis de riesgos es determinar aquellos recursos involucrados en la gestión de la información (procesos, documentos físicos y electrónicos, software, hardware, personas, instalaciones físicas) que requieren protección, para lo cual se deben identificar las vulnerabilidades que los debilitan y las amenazas que podrían explotar dichas vulnerabilidades, con el fin de valorar el nivel de riesgo al que están expuestos. Con el resultado de este análisis la alta gerencia define si los riesgos deben ser aceptados, mitigados, transferidos o evitados. (GU-003, 2016)

3.2.1 Metodología de evaluación de riesgos

La evaluación de riesgos se basará en la Guía Metodológica para Clasificación de Activos de Información y Análisis de Riesgos de la Seguridad de la Información (GU-003), aprobada en el mes de octubre de 2016 por la Institución Financiera y que se basa en la norma NTE INEN-ISO/IEC 27005:2012 Gestión de Riesgo en la Seguridad de la Información y se enfocará

en la Coordinación General de Tecnologías de la Información y Comunicación. La Guía Metodológica consta de las siguientes actividades:

a. Identificar los activos de información
b. Clasificar los activos de información
c. Determinar los activos de información críticos
d. Identificación de universo de amenazas y vulnerabilidades
e. Análisis y evaluación de riesgos de la seguridad de la información

3.2.1.1 Identificar los activos de información

La identificación de los activos de información se realiza de acuerdo a la siguiente clasificación de tipos de activos definida en la metodología, para el proceso de la Coordinación General de Tecnologías de la Información y Comunicación.

- Archivo digital: políticas, procedimientos, manuales, reglamentos, registros y otros archivos en formato electrónico.
- Archivo físico: políticas, procedimientos, manuales, reglamentos y registros en formato físico.
- Hardware: servidores, equipos de redes, equipos de telecomunicaciones, entre otros.
- Software: aplicativos, sistemas de información, bases de datos, sistemas de toma de decisiones, software de equipos de redes, software de equipos de telecomunicaciones, entre otros.
- Personas: personal clave que desempeñe o acumule conocimientos especializados.
- Instalaciones físicas: entorno físico que alberga los servicios e instalaciones

Tabla 4.
Activos de Información de la Coordinación General de Tecnologías de Información y Comunicación

No	Nombre del Activo	Descripción del Activo	Tipo de activo
A1	Centro de Datos	Centro principal y alterno de procesamiento donde reside la infraestructura para soportar la operación del negocio	Instalaciones físicas
A2	Área de Consolas	Instalación física donde están ubicados las consolas de administración de la infraestructura	Instalaciones físicas
A3	Cintoteca	Instalación física donde se almacenan las cintas de respaldo	Instalaciones físicas
A4	Racks de comunicaciones	Soporte Metálico que aloja equipamiento de comunicaciones	Instalaciones físicas
A5	Red LAN	Red LAN corporativa de la Institución	Hardware
A6	Red WAN	Red WAN de la Institución	Hardware
A7	Red WIFI	Red Wifi utilizada por los equipos móviles para acceder a los recursos de la red de la Institución	Hardware
A8	Equipos de redes	Equipos que facilitan el uso de una red informática	Hardware
A9	Equipos de comunicaciones	Equipos que gestionan las comunicaciones	Hardware
A10	Equipos de seguridad perimetral	Equipos informáticos destinados a proteger la seguridad perimetral de la entidad	Hardware
A11	Servidores de bases de datos	Servidores que soportan los motores e instancias de bases de datos	Hardware
A12	Servidores de aplicaciones	Servidores que soportan las aplicaciones y sistemas de información	Hardware
A13	Servidores de Correo	Servidores que soporta el servicio de correo electrónico de la Institución	Hardware
A14	Servidores de Backup	Servidores para el respaldo de información de la Institución	Hardware
A15	Servidores de Directorio Activo	Servidores para la administración los inicios de sesión en los equipos conectados a la red	Hardware
A16	Servidor de Archivos	Almacenamiento de los documentos electrónicos que manejan las áreas de la entidad	Hardware
A17	SAN	Red de área de almacenamiento donde reside la información de la entidad	Hardware
A18	Computadores de escritorio	Computadores de escritorio asignados a los colaboradores de la entidad	Hardware
A19	Portátiles	Computadores portátiles de la entidad	Hardware
A20	Impresoras/fotocopiadoras/fax	Impresoras de la entidad ubicada en diferentes áreas	Hardware
A21	Medios extraíbles	Cintas, CD-ROM, DVD, discos duros portátiles, dispositivos de almacenamiento PC Card, dispositivos de almacenamiento USB etc.	Hardware
A22	Software de aplicación de usuario final	Aplicaciones de usuario final (ofimáticas)	Software
A23	Herramientas de Desarrollo	Aplicaciones que apoyan en el desarrollo de aplicaciones	Software

A24	Sistema de Control de Accesos	Sistema que gestiona los sistemas y los usuarios de la Institución	Software
A25	Sistema de Gestión de TI	Sistema para gestión de servicios de TI, gestión de incidentes y cambios y gestión de configuración	Software
A26	Sistema Monitoreo de servicios	Sistema de monitoreo de servicios	Software
A27	Sistema de Gestión Base de Datos	Sistema de gestión y administración de las bases de datos de la entidad	Software
A28	Sistema de Control de Versiones	Sistema de administración para el control de versionamiento de software	Software
A29	Sistema de administración Directorio activo	Sistema de administración de inicios de sesión en los equipos conectados a la red	Software
A30	Herramienta de Virtualización	Herramienta utilizada para la virtualización de servidores	Software
A31	Antivirus	Software de administración de seguridad para el control de virus	Software
A32	Sistema administración de la SAN	Sistema para administrar la SAN	Software
A33	Sistemas desarrollados por la Institución	Corresponde a los aplicativos que soportan el core del negocio de la Institución	Software
A34	Sistema de Gestión Documental	Sistema de Gestión documental de la Institución	Software
A35	Sistema de Gestión de Calidad	Aplicativo para el Sistema de Gestión de Calidad	Software
A36	Página WEB	Página Web de la Entidad	Software
A37	Intranet	Intranet de la Entidad	Software
A38	Manuales técnicos de administración	Corresponde a los documentos, manuales y procedimientos relacionadas con la administración de la plataforma	Archivo físico
A39	Bitácora de control de acceso al centro de datos	Registro de acceso al centro de datos	Archivo físico
A40	Políticas, procedimientos, manuales	Políticas, procedimientos, manuales	Archivo físico
A41	Políticas, procedimientos, manuales	Políticas, procedimientos, manuales	Archivo digital
A42	Plan estratégico de tecnología	Documento que contiene el plan estratégico de tecnología	Archivo digital
A43	Log de evento de seguridad	Log que contiene los registros de los eventos de seguridad y de los eventos de administración sobre las aplicaciones	Archivo digital
A44	Administradores de los servicios	Personal que administra los servicios de TI	Personas
A45	Proveedores	Personal que brinda el soporte	Personas

3.2.1.2 Clasificación y ponderación de los activos de información

Para clasificar los activos de información se considera los siguientes criterios:

- Nivel de importancia de la información producida o contenida: crítica, esencial, no esencial

- Nivel de sensibilidad de la información producida o contenida: confidencial, reservada, privada o no reservada, pública.

a) **Nivel de importancia**

i. **Crítica**: La información deberá ser clasificada como crítica si es necesaria para la continuidad de un proceso crítico de la Institución Financiera o si es requerida por la Ley. Es mandatorio preservar su disponibilidad ya que la afectación a la Institución Financiera es directa.

ii. **Esencial**: La información deberá ser clasificada como esencial si las siguientes condiciones son verdaderas:

- La información deberá estar disponible y puede ser reconstruida en caso de pérdida.
- La reconstrucción o recuperación de la información podría no ser lograda en el tiempo definido por la Institución Financiera como ventana de tiempo máximo tolerable, sin que la Institución se vea afectado ya sea legal, operacional o económicamente.

iii. **No Esencial**: Toda aquella información que no es considerada crítica o esencial, pero es útil en el desarrollo de las tareas habituales del personal.

- No Esencial 
- Esencial 
- Crítica 

b) Nivel de sensibilidad

i. **Confidencial:** Toda aquella información personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos

personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República.

ii. **Reservada:** Toda aquella información que requiere de acceso autorizado ya que su tratamiento no adecuado puede presentar riesgos importantes para la Institución Financiera, y que está catalogada como tal en la norma interna aprobada por la Gerencia General, deberá cumplir con las medidas de seguridad establecidas en las Normas de Seguridad de la Información de la Institución Financiera, en cuanto a rotulado, uso, publicación externa, reclasificación, almacenamiento, reproducción, envío, impresión, reutilización de medios digitales, cifrado, según corresponda.

iii. Privada o no reservada (Información de acceso autorizado): Toda aquella información cuyo acceso deberá ser expresamente autorizado por el Responsable del activo de información y restringido a un grupo reducido de usuarios que la necesite para el desarrollo de sus tareas habituales. Puede presentar riesgos para la Institución Financiera si es conocida por personal no autorizado, deberá cumplir con las medidas de seguridad establecidas en las Normas de Seguridad de la Información de la Institución Financiera, en cuanto a rotulado, uso, publicación externa, reclasificación, almacenamiento, reproducción, envío, impresión, reutilización de medios digitales, cifrado, según corresponda.

iv. Pública: La información que está catalogada como tal en la Ley Orgánica de Transparencia y Acceso a la Información Pública, y no expone a la Institución Financiera a pérdidas financieras, de imagen, o perjuicios de cualquier tipo, ni que viole algún derecho de privacidad individual. No representa riesgo significativo para la Institución Financiera y tiene requerimientos de control limitados, ya que no es necesario establecer restricciones especiales más allá de las

consideraciones establecidas en la Ley sobre su buen uso y conservación.

- Pública 
- Privada 
- Reservada 
- Confidencial 

Para la ponderación de los activos de información se determina, en términos cualitativos, el nivel de impacto que tendría la Institución Financiera, por la pérdida de cualquiera de los atributos de la seguridad de la información: confidencialidad, integridad y disponibilidad sobre los atributos estratégicos identificados en la metodología para la clasificación de activos de información y análisis de riesgos de la seguridad de la información. La determinación de los atributos estratégicos de la Institución Financiera es una actividad que forma parte de la alineación estratégica de la seguridad de la información con los procesos de la Institución, considerando los elementos misión, visión, principios y valores; y, objetivos estratégicos.

Tabla 5.

Atributos estratégicos de la Institución Financiera

Atributo	Descripción
AE1	Cumplimiento de objetivos
AE2	Reputacional
AE3	Patrimonial
AE4	Continuidad de los Servicios

Tomado de: GU-003,2016

Para evaluar el impacto sobre los atributos estratégicos en caso que el evento de riesgo llegara a materializarse, se consideran los siguientes criterios de evaluación:

Impacto en el Cumplimiento de Objetivos: La materialización del riesgo podría ocasionar incumplimiento de la Institución Financiera con los objetivos establecidos en la ley y demás cuerpos normativos.

Tabla 6.

Criterios de evaluación para el atributo (AE1): Cumplimiento de Objetivos

Escalas/Impacto		Cumplimiento de Objetivos
5	Muy Alta	Incumplimiento de los objetivos establecidos en la Ley
4	Alta	Incumplimiento parcial de los objetivos establecidos en la Ley o incumplimiento de los objetivos institucionales
3	Media	Errores o retrasos significativos en el desarrollo de las funciones vinculadas a la Ley o incumplimiento parcial de los objetivos
2	Baja	Cumplimiento de los objetivos establecidos en la Ley y/o institucionales, aunque la calidad y rapidez en el desarrollo de las funciones pueden verse alteradas
1	Muy baja	Cumplimiento de los objetivos establecidos en la Ley y/o institucionales, pueden producirse alteraciones en algún proceso

Tomado de: GU-003,2016

Impacto Reputacional (Imagen): La materialización del riesgo podría ocasionar impacto a la imagen de la Institución Financiera.

Tabla 7.

Criterios de evaluación para el atributo (AE2): Reputacional

Escalas/Impacto		Reputacional(Imagen)	
5	Muy Alta	La ocurrencia del riesgo generaría: - Cobertura de los medios de comunicación (prensa, televisión, radio e internet) a nivel internacional o regional - Impacto de largo plazo en la imagen de la Institución Financiera	Reputación afectada más de 6 meses
4	Alta	La ocurrencia del riesgo generaría: - Cobertura de los medios de comunicación (prensa, televisión, radio e internet) a nivel local - Impacto de mediano plazo en la imagen de la Institución Financiera	Reputación afectada entre 3 meses y 6 meses
3	Media	La ocurrencia del riesgo generaría: - Cobertura de los medios de comunicación (prensa, televisión, radio e internet) - Impacto pasajero en la imagen de la Institución Financiera	Reputación afectada entre 1 mes y 3 meses
2	Baja	La ocurrencia del riesgo generaría cobertura en algún medio de comunicación (prensa, televisión, radio e internet) a nivel local, con acusaciones puntuales que afecten la imagen de la Institución Financiera	Reputación afectada entre 1 semana y 1 mes
1	Muy baja	Rumores que no generarían impacto en la reputación e imagen de la Institución Financiera	Reputación afectada menos de 1 semana

Tomado de: GU-003,2016

Impacto Patrimonial: La materialización del riesgo podría ocasionar incumplimiento de las operaciones de la Institución Financiera, generando una pérdida patrimonial a la Entidad.

Tabla 8.

Criterios de evaluación para el atributo (AE3): Patrimonial

Escalas/Impacto		Patrimonial
5	Muy Alta	Daño patrimonial igual o superior a USD 1'000.000
4	Alta	Daño patrimonial igual o superior a USD 100.000 e inferior a USD 1'000.000
3	Media	Daño patrimonial igual o superior a USD 10.000 e inferior a USD 100.000
2	Baja	Daño patrimonial igual o superior a USD 1.000 e inferior a USD 10.000
1	Muy baja	Daño patrimonial inferior a USD 1.000

Tomado de: GU-003,2016

Impacto en la Continuidad de los Servicios: La materialización del riesgo podría ocasionar interrupciones de los servicios que ofrece la Institución Financiera.

Tabla 9.

Criterios de evaluación para el atributo (AE4): Continuidad de los Servicios

Escalas/Impacto		Continuidad de los Servicios
5	Muy Alta	El tiempo máximo en que el servicio debe ser recuperado es inferior a 1 hora
4	Alta	El tiempo máximo en que el servicio debe ser recuperado es igual o superior a 1 hora e inferior a 4 horas
3	Media	El tiempo máximo en que el servicio debe ser recuperado es igual o superior a 4 hora e inferior a 1 día
2	Baja	El tiempo máximo en que el servicio debe ser recuperado es igual o superior a 1 día e inferior a 3 días
1	Muy baja	El tiempo máximo en que el servicio debe ser recuperado es igual o superior a 3 días e inferior a 5 días

Tomado de: GU-003,2016

El impacto total del activo de información será calculado mediante el promedio de las calificaciones registradas para ese activo.

Los niveles de impacto definidos son los siguientes:

Muy Bajo1	Bajo2	Medio3	Alto4	Muy alto5

De acuerdo a la metodología para clasificación de activos de información y análisis de riesgos de la seguridad de la información, en el Anexo L se tiene la valoración del nivel de criticidad de los activos de información de la Coordinación General de Tecnología de la Información y Comunicación de la Institución Financiera.

3.2.1.3 Determinar los activos de información críticos

Los activos de información críticos son aquellos identificados con un nivel de importancia esencial o crítica y nivel de sensibilidad confidencial, reservada o privada, y que cumplan con un nivel de impacto medio, alto y muy alto como resultado de la ponderación. A estos activos se aplica el análisis y evaluación de riesgos de seguridad de la información. (Anexo M).

3.2.1.4 Identificación de universo de amenazas y vulnerabilidades

Una parte vital del Análisis de Riesgos es la identificación de amenazas y vulnerabilidades a las cuales está expuesto el activo de información, para lo cual se debe realizar una revisión de amenazas y vulnerabilidades, en intervalos planeados, considerando los diferentes cambios que pueden afectar a la Institución Financiera, tales como:

- Reformas a la normativa legal que aplica a la Institución Financiera
- Decretos Ejecutivos, Resoluciones de la Junta de Política y Regulación Monetaria y Financiera; y demás normativas
- Nuevos procesos y productos
- Cambios tecnológicos, entre otros

El resultado de esta identificación genera la Matriz de Amenazas y Vulnerabilidades por tipo de activo de información de la Institución Financiera (Software, Hardware, Archivo físico, Archivo digital, Personas, Instalaciones físicas), y se relaciona con los controles establecidos en el EGSI.

Tabla 10.
Amenazas y Vulnerabilidades por tipo de activo de información y principio afectado

Tipo de Activo	Amenaza	Vulnerabilidad	Principios afectados		
			C	I	D
Hardware Software	R1.nterrupciones de los servicios	Falta de mantenimiento de equipos Configuración inadecuada y falta de capacidad de los ambientes No existe o no se aplica procedimiento de control de cambios Ataque de Virus			X
Instalaciones físicas	R2.Robo de equipos	Ausencia o inadecuada aplicación de políticas y normas de seguridad Gestión inadecuada de vigilancia física No se realiza un inventario permanente de activos físicos Ubicación física de los equipos			X
Software Archivo físico Archivo digital	R3.Robo de información	Inadecuada administración de seguridad Ausencia o inadecuada plataforma de seguridad perimetral Ausencia o inadecuada aplicación de políticas y normas de seguridad Administración o asignación inadecuada de roles y permisos Inadecuado mecanismo de cifrado No se cuenta con logs de eventos de seguridad	X		X
Hardware Software	R4.Abuso de privilegios de acceso	Cuentas de usuario sin auditar Contraseñas no seguras No se cuenta con logs de eventos de seguridad Administración o asignación inadecuada de roles y permisos Ausencia o inadecuada aplicación de políticas y normas de seguridad	X	X	
Hardware Software Archivo físico Archivo digital	R5.Cambios no autorizados de la configuración	No existe o no se aplica procedimiento de control de cambios Ausencia o inadecuada aplicación de política y normas de seguridad Administración o asignación inadecuada de roles y permisos Inexistencia de respaldos de información No se realiza monitoreo periódico de		X	

		la disponibilidad de los servicios			
Instalaciones físicas Hardware Software Archivo físico Archivo digital	R6.Acceso no autorizado	Ausencia o inadecuada aplicación de política y normas de seguridad Ausencia o inadecuada plataforma de seguridad perimetral Administración o asignación inadecuada de roles y permisos Ausencia de una configuración segura de la red Contraseñas no seguras	X	X	
Instalaciones físicas Hardware Software Archivo físico Archivo digital	R7.Ataques internos/externos	Inadecuada administración de seguridad Ausencia o inadecuada plataforma de seguridad perimetral Ausencia de una configuración segura de la red Falta de seguridad de los componentes de red	X		X
Hardware Software	R8.Cambios de privilegios sin autorización	No existe o no se aplica procedimiento de control de cambios Inadecuada administración de seguridad Administración o asignación inadecuada de roles y permisos Contraseñas no seguras Ausencia o inadecuada aplicación de políticas y normas de seguridad	X	X	X
Instalaciones físicas	R9.Desastres naturales	Ausencia de un plan de continuidad de negocio Falta de capacitación del personal ante desastres naturales Ubicación física de los equipos Ubicación física del centro de cómputo No existe seguridad física Falta de mantenimiento de las instalaciones físicas			X
Software Archivo físico Archivo digital	R10.Divulgación de información de autenticación	Inadecuada administración de seguridad Contraseñas no seguras Ausencia o inadecuada aplicación de políticas y normas de seguridad Administración o asignación inadecuada de roles y permisos Inadecuado mecanismo de cifrado	X		

Personas	R11.Errores de los administradores	Ausencia de capacitación permanente Ausencia o inadecuado procedimiento de control de cambios Desmotivación del personal	X	X	X
Software	R12.Instalación de software no autorizado	Ausencia o inadecuada aplicación de políticas y normas de seguridad Inadecuada administración o asignación de roles y permisos No se cuenta con un control para instalación de software		X	X
Software	R13.Interceptación no autorizada de información en tránsito	Ausencia o inadecuada aplicación de políticas y normas de seguridad Inadecuada mecanismo de cifrado No se tiene un monitoreo permanente Administración o asignación inadecuada de roles y permisos	X		
Software	R14.Suplantación de identidad de usuarios	Contraseñas no seguras Cuentas de usuario sin auditar Ausencia o inadecuada plataforma de vigilancia física Inadecuado mecanismo de cifrado	X	X	
Hardware Software	R15.Mal uso de sistemas para generar fraudes	Inadecuada administración de seguridad Cuentas de usuario sin auditar No se cuenta con logs de eventos de seguridad Administración o asignación inadecuada de roles y permisos Ausencia o inadecuada aplicación de políticas de seguridad Corrupción de funcionarios	X	X	
Hardware Software	R16.Mal uso de sistemas que generan interrupción	Inadecuada administración de seguridad Cuentas de usuario sin auditar No se cuenta con logs de eventos de seguridad Administración o asignación inadecuada de roles y permisos Ausencia o inadecuada aplicación de política y normas de seguridad Ausencia de transferencia de conocimientos			X

Adaptado de: MAGERIT, 2012; Advisera - 27001 Academy

3.2.1.5 Análisis y evaluación de riesgos de la seguridad de la información

A través del análisis y evaluación de riesgos de la seguridad de la información, podemos determinar los riesgos a los cuales están expuestos los activos de información de la Institución Financiera y definir el tratamiento adecuado para aquellos eventos de riesgo que registren niveles medio, alto y muy alto; para aquellos riesgos de nivel bajo la metodología considera aceptados por los responsables de los activos de información.

Para determinar el impacto que pueden tener las pérdidas de confidencialidad, integridad y disponibilidad sobre los activos de información, se utilizó los niveles de impacto definidos para la ponderación y clasificación de los activos de información.

Para determinar la probabilidad de ocurrencia de una amenaza sobre cada uno de los activos, se utilizó los siguientes criterios de valoración:

- Controles y Mitigación: Qué tanto se encuentra expuesta la Institución Financiera a la amenaza a causa de falta de medidas de mitigación o fallas en las que se encuentran establecidas.
- Probabilidad de Ocurrencia de Amenaza: Frecuencia con la cual se han presentado causas potenciales de incidentes que podrían tener efectos adversos o negativos sobre los activos de información de la Institución Financiera.

Tabla 11.

Criterios de Evaluación de Vulnerabilidad

Escalas / Probabilidad		Descripción
5	Muy Alta	Los controles no operan o no existen.
4	Alta	Los controles son detectivos, pero no preventivos, no existe reporte efectivo.
3	Media	Los controles son detectivos, pero no preventivos y hay reporte efectivo.
2	Baja	Los controles son apropiadamente detectivos y preventivos pero no hay reporte efectivo.
1	Muy baja	Los controles son apropiadamente detectivos y preventivos, existe reporte efectivo.

Tomado de: GU-003,2016.

El nivel de riesgo inherente es igual al nivel de probabilidad de ocurrencia x el nivel de impacto total.

Para establecer el nivel de riesgo, se utilizó los siguientes criterios de valoración en base a las siguientes relaciones de la matriz de calor de riesgos.

Tabla 12.

Niveles de Riesgo

Nivel de riesgo	Impacto	Probabilidad
Alto	5	1 - 2 -3 - 4 - 5
	4	3 - 4 - 5
Medio	4	1 – 2
	3	2 – 3 – 4 - 5
	2	5
Bajo	3	1
	2	1 - 2 – 3 – 4
	1	1 - 2 - 3 - 4 - 5

Tomado de: GU-003,2016.

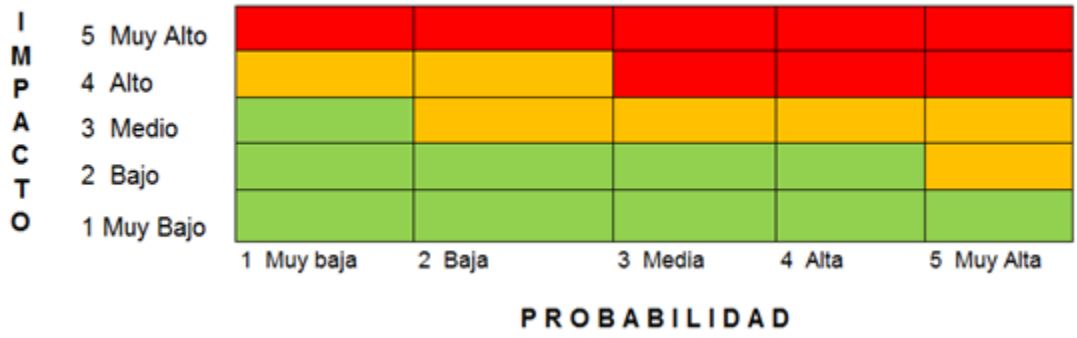

Figura 31. Mapa de Calor de Riesgos

- Nivel bajo.- Los eventos de riesgo ubicados en este nivel, se consideran tolerables y no exigen elaboración de planes de administración de riesgos.

- Nivel medio.- Para los eventos de riesgo ubicados en este nivel, se considera elaborar medidas de mitigación a fin de disminuir el riesgo a niveles más bajos.

- Nivel alto.- Para los eventos de riesgo ubicados en este nivel, se requiere de acciones inmediatas para disminuir el riesgo, compartir el riesgo o inclusive evitarlo o solicitarán al Comité de Seguridad de la Información la aceptación de los riesgos en caso de requerirlo.

En el Anexo N se muestra el resultado del proceso de valoración del riesgo para una amenaza/vulnerabilidad en particular asociada a los activos de información de la Coordinación General de Tecnologías de la Información y Comunicación.

Basados en el resultado del proceso de valoración del riesgo se tiene la siguiente matriz de riesgo inherente

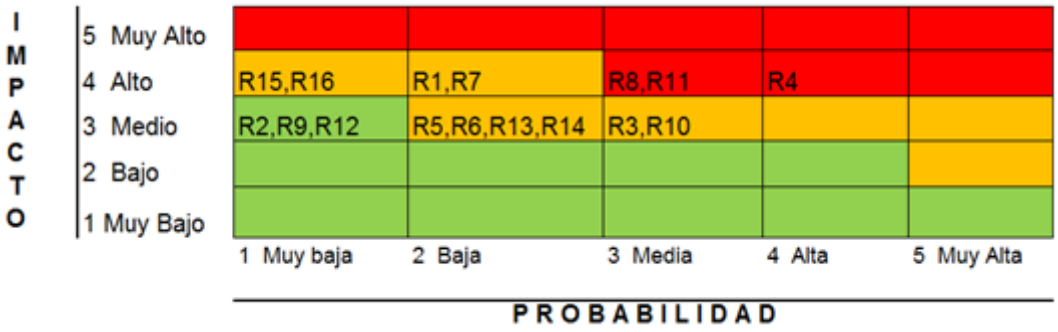

Figura 32. Mapa de Riesgo Inherente

3.2.1.6 Identificación de controles

Se ha identificado una serie de controles muchos de ellos establecidos en el EGSI, con el fin de minimizar o eliminar la probabilidad de materialización de una amenaza sobre las vulnerabilidades existentes, por cada tipo de activo de información.

Tabla 13.

Identificación de controles por tipo de activo de información

No.	Tipo de Activo	Amenaza	Vulnerabilidad	Descripción del Control
1	Hardware Software	Interrupciones de los servicios	Falta de mantenimiento de equipos Configuración inadecuada y falta de capacidad de los ambientes No existe o no se aplica procedimiento de control de cambios Ataque de Virus	Se cuenta con una plataforma en alta disponibilidad Se cuenta con un Plan de continuidad de los servicios de TI Se cuenta con suministro de energía sin interrupción Se cuenta con un procedimiento formal de control de cambios de hardware y software Se cuenta con una gestión de la capacidad
2	Instalaciones físicas	Robo de equipos	Ausencia o inadecuada aplicación de políticas y normas de seguridad Gestión inadecuada de vigilancia física No se realiza un inventario permanente de activos físicos Ubicación física de los equipos	Se cuenta con controles de acceso físico Se cuenta con reglamentos y normas de seguridad de instalaciones y oficina Se dispone de un sistema de vigilancia Se cuenta con pólizas de seguro contra robos

3	Software Archivo físico Archivo digital	Robo de información	Inadecuada administración de seguridad Ausencia o inadecuada plataforma de seguridad perimetral Ausencia o inadecuada aplicación de políticas y normas de seguridad Administración o asignación inadecuada de roles y permisos Inadecuado mecanismo de cifrado No se cuenta con logs de eventos de seguridad	Se cuenta con un esquema de seguridad basado en roles y permisos Existen controles contra virus y código malicioso Se monitorea y supervisa el trabajo de los proveedores de servicios Se cuenta con un mecanismo de cifrado de la información Se tiene una política de control de acceso a la información Existe una política sobre dispositivos móviles
4	Hardware Software	Abuso de privilegios de acceso	Cuentas de usuario sin auditar Contraseñas no seguras No se cuenta con logs de eventos de seguridad Administración o asignación inadecuada de roles y permisos Ausencia o inadecuada aplicación de políticas y normas de seguridad	Existe un procedimiento de revisión periódica de privilegios de acceso Se cuenta con un esquema de seguridad basado en roles y permisos Se tiene una política de control de acceso a la información
5	Hardware Software Archivo físico Archivo digital	Cambios no autorizados de la configuración	No existe o no se aplica procedimiento de control de cambios Ausencia o inadecuada aplicación de política y normas de seguridad Administración o asignación inadecuada de roles y permisos Inexistencia de respaldos de información No se realiza monitoreo periódico de la disponibilidad de los servicios	Se cuenta con un procedimiento formal de control de cambios de hardware y software Se cuenta con un esquema de seguridad basado en roles y permisos Existen registros de auditoría sobre los cambios en la configuración Existe un procedimiento de monitoreo periódico de la disponibilidad de los servicios El acceso a los recursos se controla a través de Active Directory
6	Instalaciones físicas Hardware Software Archivo físico Archivo digital	Acceso no autorizado	Ausencia o inadecuada aplicación de política y normas de seguridad Ausencia o inadecuada plataforma de seguridad perimetral Administración o asignación inadecuada de roles y permisos Ausencia de una configuración segura de la red Contraseñas no seguras	Existen controles de acceso físico Se cuenta con un esquema de seguridad basado en roles y permisos El acceso a los recursos se controla a través de Active Directory Existe política de seguridad sobre gestión de contraseñas de usuario Existe un procedimiento de revisión periódica de privilegios de acceso

7	Instalaciones físicas Hardware Software Archivo físico Archivo digital	Ataques internos/externos	Inadecuada administración de seguridad Ausencia o inadecuada plataforma de seguridad perimetral Ausencia de una configuración segura de la red Falta de seguridad de los componentes de red	Existe un sistema de detección de intrusos Existe un proceso de monitoreo continuo de posibles ataques Existe un sistema correlacionador de eventos
8	Hardware Software	Cambios de privilegios sin autorización	No existe o no se aplica procedimiento de control de cambios Inadecuada administración de seguridad Administración o asignación inadecuada de roles y permisos Contraseñas no seguras Ausencia o inadecuada aplicación de políticas y normas de seguridad	Se cuenta con un procedimiento formal de control de cambios de hardware y software Se cuenta con un esquema de seguridad basado en roles y permisos Se realiza revisión periódica de privilegios de acceso
9	Instalaciones físicas	Desastres naturales	Ausencia de un plan de continuidad de negocio Falta de capacitación del personal ante desastres naturales Ubicación física de los equipos Ubicación física del centro de cómputo No existe seguridad física Falta de mantenimiento de las instalaciones físicas	Se cuenta con un plan de continuidad de servicios de TI Se cuenta con mantenimiento permanente de las instalaciones físicas Se capacita al personal sobre desastres naturales
10	Software Archivo físico Archivo digital	Divulgación de información de autenticación	Inadecuada administración de seguridad Contraseñas no seguras Ausencia o inadecuada aplicación de políticas y normas de seguridad Administración o asignación inadecuada de roles y permisos Inadecuado mecanismo de cifrado	Existe política de seguridad sobre gestión de contraseñas de usuario Se cuenta con un esquema de seguridad basado en roles y permisos Se firman acuerdos de confidencialidad
11	Personas	Errores de los administradores	Ausencia de capacitación permanente No existe o no se aplica procedimiento de control de cambios Desmotivación del personal	Existe un plan de capacitación permanente Se cuenta con un procedimiento formal de control de cambios de hardware y software

12	Software	Instalación de software no autorizado	Ausencia o inadecuada aplicación de políticas y normas de seguridad Inadecuada administración o asignación de roles y permisos No se cuenta con un control para instalación de software	Se cuenta con un esquema de seguridad basado en roles y permisos Se realizan inventarios de activos de software Existe una administración de políticas a través del Active Directory
13	Software	Interceptación no autorizada de información en tránsito	Ausencia o inadecuada aplicación de políticas y normas de seguridad Inadecuada mecanismo de cifrado No se tiene un monitoreo permanente Administración o asignación inadecuada de roles y permisos	Se establecen protocolos seguros en la comunicación Se cuenta con una adecuada seguridad de cableado
14	Software	Suplantación de identidad de usuarios	Contraseñas no seguras Cuentas de usuario sin auditar Ausencia o inadecuada plataforma de vigilancia física Inadecuado mecanismo de cifrado	Se utilizan programas de seguridad de protección de equipos Existe política de seguridad sobre gestión de contraseñas de usuario Existe concientización en los usuarios sobre el uso de correo e internet
15	Hardware Software	Mal uso de sistemas para generar fraudes	Inadecuada administración de seguridad Cuentas de usuario sin auditar No se cuenta con logs de eventos de seguridad Administración o asignación inadecuada de roles y permisos Ausencia o inadecuada aplicación de políticas de seguridad Corrupción de funcionarios	Se cuenta con un esquema de seguridad basado en roles y permisos Existe un monitoreo continuo de privilegios de acceso Existe concienciación sobre seguridad de la información
16	Hardware Software	Mal uso de sistemas que generan interrupción	Inadecuada administración de seguridad Cuentas de usuario sin auditar No se cuenta con logs de eventos de seguridad Administración o asignación inadecuada de roles y permisos Ausencia o inadecuada aplicación de política y normas de seguridad Ausencia de transferencia de conocimientos	Se cuenta con un esquema de seguridad basado en roles y permisos Se cuenta con una plataforma en alta disponibilidad Se cuenta con un Plan de continuidad de los servicios de TI

Con el objetivo de determinar el nivel de desplazamiento que estos controles pueden genera sobre el mapa de calor de riesgo inherente, lo cual determina,

el mapa de calor del riesgo residual, se ha procedido a valorar la efectividad de los controles estableciendo los niveles de impacto y probabilidad de materialización de la amenaza, de acuerdo a los criterios establecidos anteriormente.

En el Anexo O se muestra el resultado del proceso de valoración del riesgo que se realizó con los controles identificados obteniendo la siguiente matriz de riesgo residual.

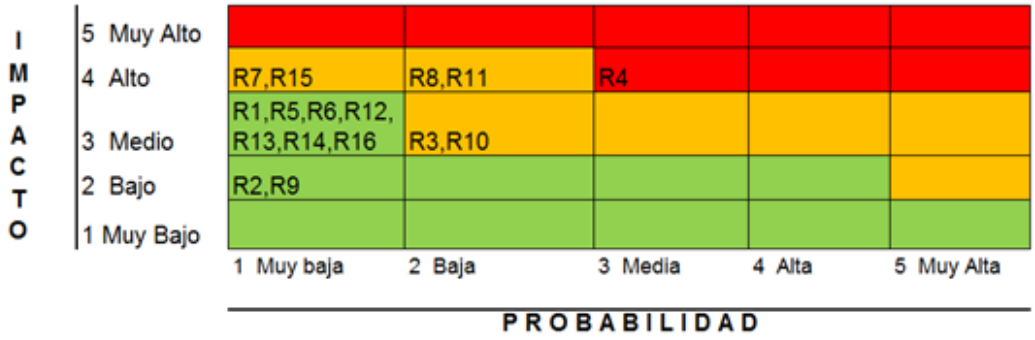

Figura 33. Mapa de Riesgo Residual

3.2.1.7 Plan de Tratamiento de Riesgos

El Plan de tratamiento de Riesgos busca gestionar el riesgo residual resultado de la valoración de riesgos realizado por la Institución Financiera, mediante la implementación de controles que permitirán mitigar, transferir o aceptar los riesgos ubicados en un nivel medio y alto.

La selección y priorización de controles se basará en aquellos dominios de control cuya brecha de cumplimiento es mayor y aquellos riesgos que se considera deben ser mitigados en base al siguiente resumen.

Tabla 14.

Resumen de cumplimiento de objetivos de control

OBJETIVOS DE CONTROL	NIVEL DE CUMPLIMIENTO	# RIESGOS ASOCIADOS
Política de Seguridad de la Información	1	11
Organización de la Seguridad de la Información	2	11
Gestión de los Activos	3	6
Seguridad de los Recursos Humanos	2	11
Seguridad Física y del Entorno	3	7
Gestión de Comunicaciones y Operaciones	2	9
Control de Acceso	2	11
Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	2	4
Gestión de los Incidentes de la Seguridad de la Información	1	16
Gestión de la Continuidad del Negocio	3	3
Cumplimiento	3	12

Promedio de cumplimiento de la Institución Financiera frente al Acuerdo No.166 es de **2 – Repetible.**

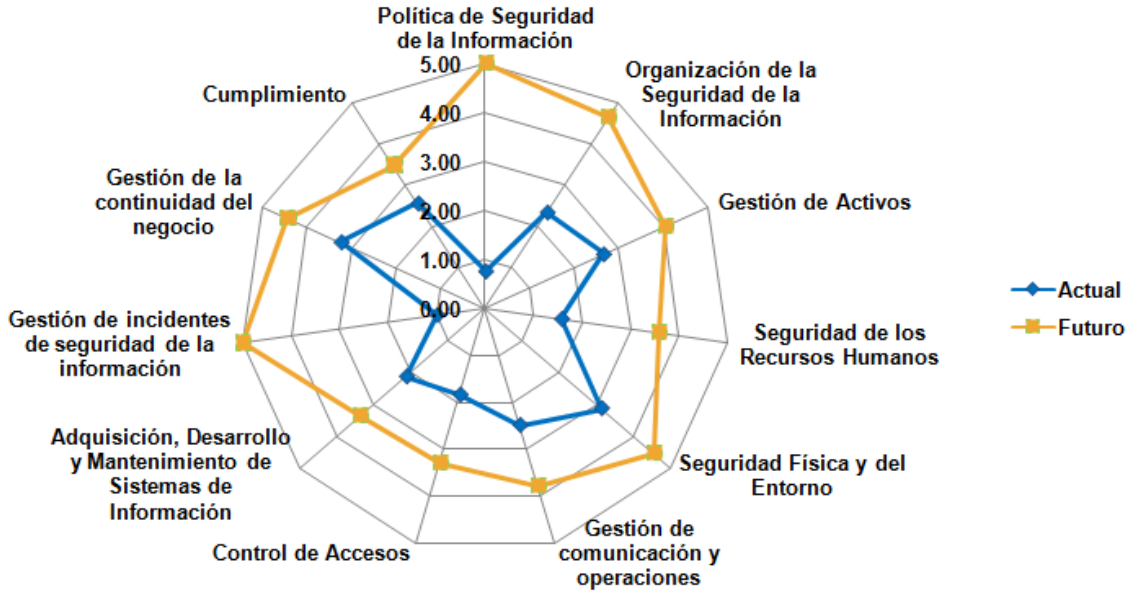

Figura 34. Resumen del nivel de cumplimiento de la Institución para cada dominio y la meta sugerida.

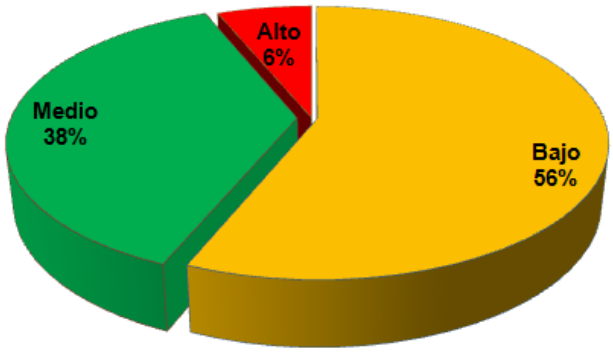

Figura 35. Resumen de distribución de riesgo residual

En base al análisis de la situación actual de la Institución frente a la seguridad de la información, los planes de acción se centrarán en los siguientes dominios:

- Política de Seguridad de la Información
- Organización de la Seguridad de la Información.
- Seguridad de los Recursos Humanos
- Control de Acceso
- Gestión de los Incidentes de la Seguridad de la Información.

Con el fin de integrar procesos, objetivos de control y controles en un modelo de solución que busca mejorar la capacidad de gestión de la seguridad de la información y cerrar las brechas identificadas en el análisis realizado del nivel de cumplimiento de la Institución Financiera con relación a las directrices y objetivos de control del Acuerdo No. 166 de la Secretaría Nacional de la Administración Pública (SNAP), se realizará un mapeo entre normas y mejores prácticas utilizadas en el desarrollo del presente trabajo y se obtendrá el documento de declaración de aplicabilidad.

Tabla 15.

Mapeo Normas y Mejores Prácticas

Cláusula **Objetivo de control / Control**

	ISO27001:2013	EGSI	COBIT 5.	ITIL V. 3
	Todo	Todo	APO13 Gestionar la seguridad	Gestión de la Seguridad de la Información (SD)
A.5	**Políticas de seguridad de la información**	**Política de Seguridad de la Información**		
A.5.1	Dirección de la gestión de seguridad de la información	Documento de la Política de la Información	EDM01 Asegurar el establecimiento y mantenimiento del marco de gobierno	Gestión de la Seguridad de la Información (SD)
A.5.1.1	Políticas para seguridad de la información	Revisión de la Política	APO01 Gestionar el Marco de Gestión de TI	
A.5.1.2	Revisión de las políticas para seguridad de la información			
A.6	**Organización de la seguridad de la información**	**Organización de la Seguridad de la Información**	Catalizador Estructura Organizacional	
			APO01 Gestionar el Marco de Gestión de TI	
A.6.1	Organización interna	Compromiso de la máxima autoridad de la institución con la seguridad de la información	APO08 Gestionar las relaciones	
A.6.1.1	Roles y responsabilidades para seguridad de la información	Coordinación de la gestión de la Seguridad de la Información		Gestión de la Seguridad de la Información (SD)
A.6.1.2	Segregación de funciones	Asignación de responsabilidades para la		

		seguridad de la información		
A.6.1.3	Contacto con autoridades	Responsabilidades del Oficial de Seguridad de la Información		Gestión de la Seguridad de la Información (SD) Gestión de Incidentes (SO)
A.6.1.4	Contacto con grupos de especial interés	Responsabilidades del Responsable de Seguridad del Área de Tecnologías de la Información		
A.6.1.5	Seguridad de la información en la gestión de proyectos	Proceso de autorización para nuevos servicios de procesamiento de la información		Gestión de Cambios (ST)
A.6.2	Dispositivos móviles y teletrabajo	Acuerdos sobre confidencialidad		
A.6.2.1	Política de dispositivos móviles	Contacto con las autoridades		Gestión de la Seguridad de la Información (SD) Gestión de Proveedores (SD) Gestión de Accesos(SO)
A.6.2.1	Teletrabajo	Contactos con grupos de intereses especiales		Gestión del Catálogo de Servicios (SD) Gestión del Nivel de Servicio (SD) Gestión de Accesos (SO)
		Revisión independiente de la seguridad de la información		
		Identificación de los riesgos relacionados con las partes externas	APO12 Gestionar el Riesgo	
		Consideraciones de la seguridad cuando se trata		

		con ciudadanos o clientes		
		Consideraciones de la seguridad en los acuerdos con terceras personas		
A.7	**Seguridad de los recursos humanos**	**Seguridad de los Recursos Humanos**	APO07 Gestionar los recursos humanos	Competencias y Habilidades para la Gestión del Servicios (SAT)
A.7.1	Antes del empleo	Funciones y responsabilidades		Marco de Competencias y Habilidades (SAT)
A.7.1.1	Investigación	Selección		Formación (SAT)
A.7.1.2	Términos y condiciones del empleo	Términos y condiciones laborales		
A.7.2	Durante el empleo	Responsabilidades de la dirección a cargo del funcionario		
A.7.2.1	Responsabilidades de la administración	Educación, Formación y sensibilización en seguridad de la información		
A.7.2.2	concienciación, educación y formación en seguridad de la información	Proceso disciplinario		
A.7.2.3	Proceso disciplinario	Responsabilidades de terminación del contrato		
A.7.3	Terminación y cambio de empleo	Devolución de Activos		
A.7.3.1	Responsabilidades en la terminación o cambio de empleo	Retiro de los privilegios de acceso		
A.8	**Gestión de activos**	**Gestión de los Activos**	BAI09 Gestionar los activos	Gestión de la configuración y activos del servicio (ST)
A.8.1	Responsabilidad por los	Inventario de Activos	BAI10 Gestionar la	

	activos	Primarios	Configuración	
A.8.1.1	Inventario de activos	Inventario de Activos de Soporte de Hardware		
A.8.1.2	Propiedad de los activos	Inventariar los Activos de Soporte de Software		
A.8.1.3	Uso aceptable de los activos	Inventariar los Activos de Soporte de Redes		
A.8.1.4	Devolución de activos	Inventariar los Activos referentes a la estructura organizacional		
A.8.2	Clasificación de información	Responsable de los activos		
A.8.2.1	Clasificación de información	Uso aceptable de los activos		
A.8.2.2	Etiquetado de la información	Directrices de clasificación de la información		
A.8.2.3	Manejo de activos	Etiquetado y manejo de la información		
A.8.3	Manejo de medios			
A.8.3.1	Gestión de soportes extraíbles			
A.8.3.2	Eliminación de medios			
A.8.3.3	Transporte físico de medios			
A.9	**Control de acceso**	**Control de Acceso**	DSS05 Gestionar los Servicios de Seguridad	
A.9.1	Requisitos de negocio de control de acceso	Política de control de acceso		
A.9.1.1	Política de control de accesos	Registro de usuarios		Gestión de la Seguridad de la Información (SD) Gestión de Accesos (SO)
A.9.1.2	Acceso a las redes y servicios de red	Gestión de privilegios		Gestión de Accesos (SO)
A.9.2	Gestión de accesos de	Gestión de contraseñas		

	usuario	para usuarios		
A.9.2.1	Registro y eliminación de usuarios	Revisión de los derechos de acceso de los usuarios		Gestión de Accesos (SO)
A.9.2.2	Provisión de acceso a usuarios	Uso de contraseñas		
A.9.2.3	Gestión de derechos de acceso privilegiados	Equipo de usuario desatendido		
A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	Política de puesto de trabajo despejado y pantalla limpia		Gestión de Accesos (SO)
A.9.2.5	Revisión de derechos de acceso a usuarios	Política de uso de los servicios de red		Gestión de Cambios (ST) Gestión de Accesos (SO)
A.9.2.6	Remoción o ajuste de derechos de acceso	Autenticación de usuarios para conexiones externas		
A.9.3	Responsabilidades de usuario	Identificación de los equipos en las redes		
A.9.3.1	Uso de información secreta de autenticación	Protección de los puertos de configuración y diagnóstico remoto		
A.9.4	Control de acceso a sistemas y aplicaciones	Separación en las redes		
A.9.4.1	Restricción a información de acceso	Control de conexión a las redes		Gestión de Accesos (SO)
A.9.4.2	Procedimientos seguros de inicio de sesión	Control de enrutamiento en la red		
A.9.4.3	Sistema de gestión de contraseñas	Procedimiento de registro de inicio seguro		
A.9.4.4	Uso de programas de utilidad privilegiados	Identificación y autenticación de usuarios		
A.9.4.5	Control de acceso al código fuente de los programas	Sistema de gestión de contraseñas		
		Uso de las utilidades del		

		sistema		
		Tiempo de inactividad de la sesión		
		Limitación del tiempo de conexión		
		Control de acceso a las aplicaciones y a la información		
		restricción de acceso a la información		
		Aislamiento de sistemas sensibles		
		Computación y comunicaciones móviles		
		Trabajo remoto		
A.10	**Criptografía**			
A.10.1	Controles criptográficos			
A.10.1.1	Política de uso de controles criptográficos			
A.10.1.2	Manejo de llaves criptográficas			Gestión de Niveles de Servicio (SD) Gestión de Proveedores (SD)
A.11	**Seguridad física y ambiental**	**Seguridad Física y del Entorno**	DSS05 Gestionar los Servicios de Seguridad	
A.11.1	Áreas seguras	Perímetro de la seguridad física		
A.11.1.1	Perímetro de seguridad física	Controles de acceso físico		
A.11.1.2	Controles de ingreso físico	Seguridad de oficinas, recintos e instalaciones		
A.11.1.3	Asegurar oficinas, salas e instalaciones	Protección contra amenazas externas y		

		ambientales		
A.11.1.4	Protección contra amenazas externas y ambientales	Trabajo en áreas seguras		
A.11.1.5	Trabajo en áreas seguras	Áreas de carga, despacho y acceso público		
A.11.1.6	Áreas de entrega y carga	Ubicación y protección de los equipos		Gestión de la Configuración y Activos del Servicio (ST) Gestión de Accesos (SO)
A.11.2	Equipos	Servicios de suministro		
A.11.2.1	Ubicación y protección de equipos	Seguridad del cableado		Gestión de la Configuración y Activos del Servicio (ST)
A.11.2.2	Servicios de apoyo	Mantenimiento de los equipos		
A.11.2.3	Seguridad del cableado	Seguridad de los equipos fuera de las instalaciones		Gestión de la Configuración y Activos del Servicio (ST)
A.11.2.4	Mantenimiento de equipos	Seguridad en la reutilización o eliminación de los equipos		Gestión de la Configuración y Activos del Servicio (ST) Gestión de Incidentes (SO)
A.11.2.5	Retiro de activos	Retiro de activos de la propiedad		Gestión de cambios (ST) Gestión de la Configuración y Activos del Servicio (ST)
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones			Gestión de la Continuidad de los Servicios de TI (SD)
A.11.2.7	Eliminación segura o reutilización de los equipos			Gestión de cambios (ST)
A.11.2.8	Equipos de usuario desatendidos			Formación (TA)
A.11.2.9	Política de escritorios limpios y pantallas limpias			Formación (TA)
A.12	Seguridad de Operaciones	Gestión de Comunicaciones y	EDM05 Asegurar la transparencia hacia las partes	

		Operaciones	interesadas	
A.12.1	Procedimientos y responsabilidades operativas	Documentación de los procedimientos de operación		
A.12.1.1	Procedimientos operativos documentados	Gestión del Cambio		Mejora Continua del Servicio (MC)
A.12.1.2	Gestión del cambio	Distribución de funciones	BAI06 Gestionar los Cambios	Gestión del Cambio (ST)
A.12.1.3	Gestión de la capacidad	Separación de las instancias de desarrollo, pruebas, capacitación y producción	BAI04 Gestionar la Disponibilidad y Capacidad	Gestión de la Capacidad (SD) Gestión de Eventos (SO) Gestión de Incidentes (SO)
A.12.1.4	Separación de ambientes de desarrollo, pruebas y producción	Presentación del servicio		
A.12.2	Protección contra malware	Monitoreo y revisión de los servicios por terceros	DSS05 Gestionar los Servicios de Seguridad	
A.12.2.1	Controles contra malware	Gestión de los cambios en los servicios ofrecidos por terceros	DSS05 Gestionar los Servicios de Seguridad	Gestión de la Configuración y Activos del Servicio (ST)
A.12.3	Respaldos		DSS01 Gestionar las operaciones	Gestión de la Disponibilidad (SD) Gestión de la Continuidad de los Servicios de TI (SD)
A.12.3.1	Respaldo de información	Aceptación del sistema		
A.12.4	Registro y supervisión	Controles contra código malicioso		
A.12.4.1	Registro de eventos	Controles contra códigos móviles		Gestión de Eventos (SO)
A.12.4.2	Protección de información de bitácoras	Respaldo de la información		Gestión de Eventos (SO)
A.12.4.3	Registros de administrador y operador	Controles de las redes		Gestión de Eventos (SO)
A.12.4.4	Sincronización de relojes	Seguridad de los servicios		

		de la red		
A.12.5	Control de software operacional	Gestión de los medios removibles		
A.12.5.1	Instalación de software en sistemas operacionales	Eliminación de los medios		
A.12.6	Gestión de vulnerabilidades técnicas	Procedimientos para el manejo de la información		
A.12.6.1	Gestión de vulnerabilidades técnicas	Seguridad de la documentación del sistema		Mejora Continua del Servicios (MC)
A.12.6.2	Restricciones en la instalación de software	Políticas y procedimientos para el intercambio de información		
A.12.7	Consideraciones de auditoría a sistemas de información	Acuerdos para el intercambio		
A.12.7.1	Controles de auditoría a sistemas de información	Medios físicos en tránsito		
A.13	**Seguridad de las comunicaciones**	Mensajería electrónica	EDM05 Asegurar la transparencia hacia las partes interesadas MEA03 Supervisar, evaluar y valorar la conformidad con los requerimientos externos	Gestión de la Seguridad de la Información (SD)
A.13.1	Gestión de la seguridad de redes	Sistemas de información del negocio		
A.13.1.1	Controles de red	Transacciones en línea		
A.13.1.2	Seguridad de servicios de red	Información disponible al público		Gestión de Niveles de Servicio (SD)
A.13.1.3	Segregación en redes	Registro de auditorías		
A.13.2	Transferencia de información	Monitoreo de uso del sistema		Gestión de la disponibilidad (SD)
A.13.2.1	Políticas y procedimientos de transferencia de información	Protección del registro de la información		

A.13.2.2	Acuerdos sobre la transferencia de información	Registros del administrador y del operador		Gestión de Niveles de Servicio (SD) Gestión de Proveedores (SD)
A.13.2.3	Mensajería electrónica	Registro de fallas		
A.13.2.4	Acuerdos de confidencialidad o no revelación	Sincronización de relojes		
A.14	**Adquisición, desarrollo y mantenimiento de sistemas**	**Adquisición, Desarrollo y Mantenimiento de Sistemas de Información**	BAI03 Gestionar la Identificación y la construcción de soluciones	
A.14.1	Requisitos de seguridad en sistemas de información	Análisis y especificaciones de los requerimientos de seguridad		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Validación de datos de entrada		
A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Control de procesamiento interno		
A.14.1.3	Proteger las transacciones de servicios de aplicaciones	Integridad del mensaje		
A.14.2	Seguridad en los procesos de desarrollo y soporte	Validación de datos de salidas		
A.14.2.1	Política de desarrollo seguro	Política sobre el uso de controles criptográficos		
A.14.2.2	Procedimientos de control de cambios en sistemas	Gestión de claves		Gestión de Cambios (ST)
A.14.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma operativa	Control del software operativo		Gestión de Cambios (ST) Gestión de la Configuración y Activos del Servicio (ST)
A.14.2.4	Restricciones en cambios a paquetes de software	Protección de los datos de prueba del sistema		

A.14.2.5	Principios de ingeniería de sistemas seguros	Control de acceso al código fuente de los programas		Gestión de Cambios (ST) Gestión de la Configuración y Activos del Servicio (ST) Gestión de Accesos (SO)
A.14.2.6	Ambiente de desarrollo seguro	Procedimiento de control de cambios		
A.14.2.7	Desarrollo externalizado	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo		
A.14.2.8	Pruebas de seguridad de los sistemas	Restricción del cambio de paquetes de software		
A.14.2.9	Pruebas de aceptación de sistemas	Fuga de información		Gestión de Versiones y Despliegues (ST)
A.14.3	Datos de prueba	Desarrollo de software contratado externamente		
A.14.3.1	Protección de datos de prueba	Control de las vulnerabilidades técnicas		Gestión de la Configuración y Activos del Servicio (ST)
A.15	**Relaciones con proveedores**		APO10 Gestionar los proveedores	
A.15.1	Seguridad de la información en relaciones con proveedores			
A.15.1.1	Política de seguridad de la información para relaciones con proveedores			Gestión del Catálogo de Servicios (SD) Gestión de Proveedores (SD) Gestión de la continuidad de los Servicios de TI (SD) Gestión del Nivel de Servicio (SD) Gestión de Cambios (ST) Gestión de Problemas (SO)

A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores			
A.15.1.3	Cadena de abastecimiento de la tecnología de información y comunicaciones			
A.15.2	Gestión de la entrega de servicios de proveedores			
A.15.2.1	Monitoreo y revisión de servicios de proveedores			Gestión de Proveedores (SD)
A.15.2.2	Gestión de cambios a servicios de proveedores			Gestión del Cambio (ST)
A.16	**Gestión de incidentes de seguridad de la información**	**Gestión de los Incidentes de la Seguridad de la Información**	DSS02 Gestionar las peticiones y los incidentes del servicio	
A.16.1	Gestión de incidentes de seguridad de la información y mejoras	Reporte sobre los eventos de seguridad de la información		
A.16.1.1	Responsabilidades y procedimientos	Reporte sobre las debilidades en la seguridad		Gestión del Cambio (ST) Gestión de Incidentes (SO)
A.16.1.2	Reporte de eventos de seguridad de la información	Responsabilidades y procedimientos		Gestión de Incidentes (SO)
A.16.1.3	Reporte de debilidades de seguridad de la información	Aprendizaje debido a los incidentes de seguridad de la información		Gestión de Incidentes (SO)
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	Recolección de evidencias		
A.16.1.5	Respuesta a incidentes de seguridad de la información			
A.16.1.6	Aprender de incidentes de seguridad de la información			Gestión de Incidentes (SO) Gestión de Problemas (SO) Proceso CSI (MC)

A.16.1.7	Colección de evidencia			
A.17	Aspectos de seguridad de la información de la gestión de continuidad del negocio	Gestión de la Continuidad del Negocio	DSS04 Gestionar la continuidad	
A.17.1	Continuidad de la seguridad de la información	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio		Gestión de la Continuidad de los Servicios de TI (SD) Gestión de la Configuración y Activos del Servicio(ST)
A.17.1.1	Planear la continuidad de la seguridad de la información	Continuidad del negocio de riesgos		Gestión de la Continuidad de los Servicios de TI (SD)
A.17.1.2	Implementar la continuidad de la seguridad de la información	Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información		Gestión de la Continuidad de los Servicios de TI (SD)
A.17.1.3	Verificar, revisar y evaluar la continuidad de la seguridad de la información	Estructura para la planificación de la continuidad del negocio		
A.17.2	Redundancias	Pruebas, mantenimiento y revisión de los planes de continuidad del negocio		
A.17.2.1	Disponibilidad de las instalaciones de procesamiento de información			
A.18	**Cumplimiento**	**Cumplimiento**		
A.18.1	Cumplimiento con requerimientos legales y contractuales	Identificación de la legislación aplicable	MEA03 Supervisar, evaluar y valorar la conformidad con los requerimientos externos	
A.18.1.1	Identificación de legislación aplicable y requerimientos contractuales	Derechos de propiedad intelectual		
A.18.1.2	Derechos de propiedad intelectual	Protección de registros en cada entidad		

A.18.1.3	Protección de registros	Protección de los datos y privacidad de la información personal		
A.18.1.4	Privacidad y protección de información personal identificable	Prevención del uso inadecuado de servicios de procesamiento de información		
A.18.1.5	Regulación de controles criptográficos	Reglamentación de controles criptográficos		
A.18.2	Revisiones de seguridad de la información	Cumplimiento con las políticas y las normas de la seguridad		
A.18.2.1	Revisión independiente de seguridad de la información	Verificación del cumplimiento técnico		
A.18.2.2	Cumplimiento con políticas y estándares de seguridad	Controles de auditoría de los sistemas de información	MEA02 Supervisar, evaluar y valorar el sistema de control interno	
A.18.2.3	Revisión del cumplimiento técnico	Protección de las herramientas de auditoría de los sistemas de información	MEA03 Supervisar, evaluar y valorar la conformidad con los requerimientos externos	

Adaptado de: ISACA,2012; ISO27001,2013; Osiatis,2011; LEXIS,2013

Declaración de Aplicabilidad

El propósito de la Declaración de Aplicabilidad no solo es identificar los controles a ser implementados como parte del Plan de Tratamiento de Riesgos sino también actualizar las políticas, normas y documentos relacionados al Esquema Gubernamental de Seguridad de la Información (EGSI).

SI** → El control no será tomado en cuenta en base a análisis de situación actual de la Institución Financiera.

Tabla 16.

Declaración de Aplicabilidad

Control	Requerimiento	Aplica (SI/NO)	Si aplica: Documento de Referencia en el EGSI Si no aplica: Justificación para la exclusión	Promedio Nivel de cumplimiento
1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN				
1.1	Documento de la política de Seguridad de la Información	SI	Política de Seguridad de la Información Normativa de Seguridad de la Información.	**1**
1.2	Revisión de la Política	SI	Política de Seguridad de la Información. Normativa de Seguridad de la Información.	
2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN				
2.1	Compromiso de las Directivas con la Seguridad de la Información	SI	Política de Seguridad de la Información.	
2.2	Coordinación de la Seguridad la Información	SI	Manual de funciones de Seguridad de la Información.	**2**
2.3	Asignación de responsabilidades para la Seguridad de la Información	SI	Manual de funciones de Seguridad de la Información.	
2.4	Proceso de autorización para nuevos servicios de procesamiento de la información	SI	Normativa de autorización para nuevos servicios de procesamiento de la información.	

Control	Requerimiento	Aplica (SI/NO)	Si aplica: Documento de Referencia en el EGSI Si no aplica: Justificación para la exclusión	Promedio Nivel de cumplimiento
2.5	Acuerdos de confidencialidad	SI	Acuerdos de confidencialidad para funcionarios, servidores, trabajadores, pasantes y personal en general.	
2.6	Contacto con las autoridades	SI	Procedimiento de Administración de Eventos de Seguridad de la Información.	
2.7	Contacto con grupos de especial interés	SI	Normativa para mantener contacto con organizaciones de seguridad.	
2.8	Revisión independiente de la Seguridad de la Información	SI	Planificación anual de revisiones de Auditoría Interna.	
2.9	Identificación de los riesgos relacionados con las partes externas	SI	Normativa de gestión de Seguridad de la Información con terceros.	
2.10	Consideraciones de la seguridad cuando se trata con ciudadanos o clientes	SI	Normativa de gestión de Seguridad de la Información con terceros.	
2.11	Consideraciones de la seguridad en los acuerdos con terceras partes	SI	Acuerdos de confidencialidad con terceros.	
3. GESTIÓN DE LOS ACTIVOS				**3**
3.1	Inventario de activos	SI**	Está siendo aplicado.	
3.2	Responsable de los activos	SI**	Está siendo aplicado.	
3.3	Uso aceptable de los activos	SI**	Está siendo aplicado.	
3.4	Directrices de clasificación de la información	SI**	Está siendo aplicado.	
3.5	Etiquetado y manejo de la información	SI**	Está siendo aplicado.	
4. SEGURIDAD DE LOS RECURSOS HUMANOS				**2**
4.1	Funciones y responsabilidades	SI	Normas para la Seguridad de la Información. Reglamento Interno de Administración del Talento Humano.	

Control	Requerimiento	Aplica (SI/NO)	Si aplica: Documento de Referencia en el EGSI Si no aplica: Justificación para la exclusión	Promedio Nivel de cumplimiento
4.2	Selección	SI	Normas para la Seguridad de la Información. Reglamento Interno de Administración del Talento Humano.	
4.3	Términos y condiciones laborales	SI	Reglamento Interno de Administración del Talento Humano. Acuerdos de confidencialidad para funcionarios, servidores, trabajadores, pasantes y personal en general.	
4.4.	Responsabilidades de la dirección a cargo del funcionario	SI	Normas para la Seguridad de la Información. Acuerdos de confidencialidad para funcionarios, servidores, trabajadores, pasantes y personal en general. Reglamento Interno de Administración del Talento Humano.	
4.5	Educación, formación y sensibilización en Seguridad de la Información	SI	Plan de Sensibilización de Seguridad de la Información.	
4.6	Proceso disciplinario	SI	Guía para el Proceso Disciplinario por Faltas relacionadas con Seguridad de la Información.	
4.7	Responsabilidades de terminación del contrato	SI	Normas para la Seguridad de la Información. Acuerdos de confidencialidad para funcionarios, servidores, trabajadores, pasantes y personal en general.	
4.8	Devolución de activos	SI	Normas para la Seguridad de la Información. Instructivo de Gerencia para la Administración y Control de los Bienes Muebles y Equipos.	
4.9	Retiro de los privilegios de acceso	SI	Normas para la Seguridad de la Información. Normas de Identificación y Autenticación para acceso a aplicaciones.	
5. SEGURIDAD FÍSICA Y DEL ENTORNO				**3**
5.1	Perímetro de la seguridad física	SI**	Está siendo aplicado.	

Control	Requerimiento	Aplica (SI/NO)	Si aplica: Documento de Referencia en el EGSI Si no aplica: Justificación para la exclusión	Promedio Nivel de cumplimiento
5.2	Controles de acceso físico	SI**	Está siendo aplicado.	
5.3	Seguridad de oficinas, recintos e instalaciones	SI**	Está siendo aplicado.	
5.4	Protección contra amenazas externas y ambientales	SI**	Está siendo aplicado.	
5.5	Trabajo en áreas seguras	SI**	Está siendo aplicado.	
5.6	Áreas de carga, despacho y acceso público	SI**	Está siendo aplicado.	
5.7	Ubicación y protección de los equipos	SI**	Está siendo aplicado.	
5.8	Servicios de suministro	SI**	Está siendo aplicado.	
5.9	Seguridad del cableado	SI**	Está siendo aplicado.	
5.10	Mantenimiento de los equipos	SI**	Está siendo aplicado.	
5.11	Seguridad de los equipos fuera de las instalaciones	SI**	Está siendo aplicado.	
5.12	Seguridad en la reutilización o eliminación de los equipos	SI**	Está siendo aplicado.	
5.13	Retiro de activos de la propiedad	SI**	Está siendo aplicado.	
6. GESTIÓN DE COMUNICACIONES Y OPERACIONES				
6.1	Documentación de los procedimientos de Operación	SI**	Está siendo aplicado.	
6.2	Gestión del cambio	SI**	Está siendo aplicado.	
6.3	Distribución de funciones	SI**	Está siendo aplicado.	**3**
6.4	Separación de las instancias de Desarrollo, Pruebas, Capacitación y Producción.	SI**	Está siendo aplicado.	
6.5	Presentación del Servicio	SI**	Está siendo aplicado.	
6.6	Monitoreo y revisión de los servicios, por terceros	SI**	Está siendo aplicado.	

Control	Requerimiento	Aplica (SI/NO)	Si aplica: Documento de Referencia en el EGSI Si no aplica: Justificación para la exclusión	Promedio Nivel de cumplimiento
6.7	Gestión de los cambios en los servicios ofrecidos por terceros	SI**	Está siendo aplicado.	
6.8	Gestión de la capacidad	SI**	Está siendo aplicado.	
6.9	Aceptación del Sistema	SI**	Está siendo aplicado.	
6.10	Controles contra código malicioso	SI**	Está siendo aplicado.	
6.11	Controles contra códigos móviles	SI**	Está siendo aplicado.	
6.12	Respaldos de la información	SI**	Está siendo aplicado.	
6.13	Controles de la redes	SI**	Está siendo aplicado.	
6.14	Seguridades de los servicios de la red.	SI**	Está siendo aplicado.	
6.15	Gestión de los medios removibles	SI**	Está siendo aplicado.	
6.16	Eliminación de los medios	SI**	Está siendo aplicado.	
6.17	Procedimientos para el manejo de la información	SI**	Está siendo aplicado.	
6.18	Seguridad de la documentación del sistema	SI**	Está siendo aplicado.	
6.19	Políticas y procedimientos para el intercambio de información	SI**	Está siendo aplicado.	
6.20	Acuerdo para el intercambio	SI**	Está siendo aplicado.	
6.21	Medios físicos en tránsito	SI**	Está siendo aplicado.	
6.22	Mensajería electrónica	SI**	Está siendo aplicado.	
6.23	Sistemas de información del negocio	SI**	Está siendo aplicado.	
6.24	Transacciones en línea	SI**	Está siendo aplicado.	
6.25	Información disponible al público	SI**	Está siendo aplicado.	
6.26	Registro de auditoría	SI**	Está siendo aplicado.	
6.27	Monitoreo del uso del sistema	SI**	Está siendo aplicado.	
6.28	Protección del registro de la información	SI**	Está siendo aplicado.	

Control	Requerimiento	Aplica (SI/NO)	Si aplica: Documento de Referencia en el EGSI Si no aplica: Justificación para la exclusión	Promedio Nivel de cumplimiento
6.29	Registros del administrador y del operador	SI**	Está siendo aplicado.	
6.30	Registro de fallas	SI**	Está siendo aplicado.	
6.31	Sincronización de relojes	SI**	Está siendo aplicado.	
7. CONTROL DE ACCESO				
7.1	Política de control de acceso	SI	Normas para la Seguridad de la Información. Normas de Identificación y Autenticación para acceso a aplicaciones. Generación de Claves Cliente Servidor. Manual de procedimientos para la recepción del formulario y entrega de claves de acceso al Sistema Nacional de Pagos. Normativa de Administración de Cuentas de Usuarios y Accesos. Normativa de Administración de Cuentas de Máximos Privilegios y Contraseñas Asociadas. Procedimiento para Revisión de Privilegios de Accesos.	**2**
7.2	Registro de usuarios	SI	Normas para la Seguridad de la Información. Normas de Identificación y Autenticación para acceso a aplicaciones. Generación de Claves Cliente Servidor. Manual de procedimientos para la recepción del formulario y entrega de claves de acceso al Sistema Nacional de Pagos. Normativa de Administración de Cuentas de Usuarios y Accesos. Normativa de Administración de Cuentas de Máximos Privilegios y Contraseñas Asociadas. Procedimiento para Revisión de Privilegios de Accesos.	

Control	Requerimiento	Aplica (SI/NO)	Si aplica: Documento de Referencia en el EGSI Si no aplica: Justificación para la exclusión	Promedio Nivel de cumplimiento
7.3	Gestión de privilegios	SI	Normas para la Seguridad de la Información. Normas de Identificación y Autenticación para acceso a aplicaciones. Generación de Claves Cliente Servidor. Manual de procedimientos para la recepción del formulario y entrega de claves de acceso al Sistema Nacional de Pagos. Normativa de Administración de Cuentas de Usuarios y Accesos. Normativa de Administración de Cuentas de Máximos Privilegios y Contraseñas Asociadas. Procedimiento para Revisión de Privilegios de Accesos.	
7.4	Gestión de contraseñas para usuarios	SI	Normas para la Seguridad de la Información. Normas de Identificación y Autenticación para acceso a aplicaciones.	
7.5	Revisión de los derechos de acceso de los usuarios	SI	Procedimiento para Revisión de Privilegios de Accesos.	
7.6	Uso de contraseñas	SI	Normas para la Seguridad de la Información. Normas de Identificación y Autenticación para acceso a aplicaciones.	
7.7	Equipo de usuario desatendido	SI	Normas para la Seguridad de la Información. Normas de Identificación y Autenticación para acceso a aplicaciones.	
7.8	Política de puesto de trabajo despejado y pantalla limpia	SI	Normas para la Seguridad de la Información. Normas de Identificación y Autenticación para acceso a aplicaciones.	
7.9	Política de uso de los servicios de red	SI	Normativa de Administración de Seguridad de la Red Interna. Control de acceso remoto por VPN.	

Control	Requerimiento	Aplica (SI/NO)	Si aplica: Documento de Referencia en el EGSI Si no aplica: Justificación para la exclusión	Promedio Nivel de cumplimiento
7.10	Autenticación de usuarios para conexiones externas	SI	Normas para la Seguridad de la Información. Normativa de Administración de Seguridad de la Red Interna. Control de acceso remoto por VPN. Manual de procedimientos para la recepción del formulario y entrega de claves de acceso al Sistema Nacional de Pagos.	
7.11	Identificación de equipos de red	SI	Normativa de Administración de Seguridad de la Red Interna. Control de acceso remoto por VPN.	
7.12	Protección de los puertos de configuración y diagnóstico remoto	SI	Normativa de Administración de Seguridad de la Red Interna. Control de acceso remoto por VPN.	
7.13	Separación de redes	SI	Normativa de Administración de Seguridad de la Red Interna. Control de acceso remoto por VPN.	
7.14	Control de conexión a las redes	SI	Normativa de Administración de Seguridad de la Red Interna. Control de acceso remoto por VPN.	
7.15	Control del enrutamiento en la red	SI	Normativa de Administración de Seguridad de la Red Interna. Control de acceso remoto por VPN.	

Control	Requerimiento	Aplica (SI/NO)	Si aplica: Documento de Referencia en el EGSI Si no aplica: Justificación para la exclusión	Promedio Nivel de cumplimiento
7.16	Procedimiento de registro de inicio seguro	SI	Normas para la Seguridad de la Información. Normas de Identificación y Autenticación para acceso a aplicaciones. Generación de Claves Cliente Servidor. Manual de procedimientos para la recepción del formulario y entrega de claves de acceso al Sistema Nacional de Pagos. Normativa de Administración de Cuentas de Usuarios y Accesos. Normativa de Administración de Cuentas de Máximos Privilegios y Contraseñas Asociadas. Procedimiento para Revisión de Privilegios de Accesos.	
7.17	Identificación y autenticación de usuarios	SI	Normas para la Seguridad de la Información. Normas de Identificación y Autenticación para acceso a aplicaciones. Generación de Claves Cliente Servidor. Manual de procedimientos para la recepción del formulario y entrega de claves de acceso al Sistema Nacional de Pagos. Normativa de Administración de Cuentas de Usuarios y Accesos. Normativa de Administración de Cuentas de Máximos Privilegios y Contraseñas Asociadas. Procedimiento para Revisión de Privilegios de Accesos.	
7.18	Sistema de gestión de contraseña	SI	Normas para la Seguridad de la Información. Normas de Identificación y Autenticación para acceso a aplicaciones.	
7.19	Uso de las utilidades del sistema	SI	Instalación de software de usuario final.	
7.20	Tiempo de inactividad de la sesión	SI	Normas para la Seguridad de la Información.	

Control	Requerimiento	Aplica (SI/NO)	Si aplica: Documento de Referencia en el EGSI Si no aplica: Justificación para la exclusión	Promedio Nivel de cumplimiento
7.21	Limitación del tiempo de conexión	SI	Normas para la Seguridad de la Información.	
7.22	Control de acceso a las aplicaciones y a la información	SI	Normas para la Seguridad de la Información. Normas de Identificación y Autenticación para acceso a aplicaciones. Generación de Claves Cliente Servidor. Manual de procedimientos para la recepción del formulario y entrega de claves de acceso al Sistema Nacional de Pagos. Normativa de Administración de Cuentas de Usuarios y Accesos. Normativa de Administración de Cuentas de Máximos Privilegios y Contraseñas Asociadas. Procedimiento para Revisión de Privilegios de Accesos.	
7.23	Restricción de acceso a la información	SI	Normas para la Seguridad de la Información. Normas de Identificación y Autenticación para acceso a aplicaciones. Generación de Claves Cliente Servidor. Manual de procedimientos para la recepción del formulario y entrega de claves de acceso al Sistema Nacional de Pagos. Normativa de Administración de Cuentas de Usuarios y Accesos. Normativa de Administración de Cuentas de Máximos Privilegios y Contraseñas Asociadas. Procedimiento para Revisión de Privilegios de Accesos.	
7.24	Aislamiento de sistemas sensibles	SI	Normativa de aislamiento de sistemas sensibles.	
7.25	Computación y comunicaciones móviles	SI	Normativa para la administración de computación y comunicaciones móviles.	

Control	Requerimiento	Aplica (SI/NO)	Si aplica: Documento de Referencia en el EGSI Si no aplica: Justificación para la exclusión	Promedio Nivel de cumplimiento
7.26	Trabajo remoto	SI	Control de acceso remoto por VPN.	
8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN				**2**
8.1	Análisis y especificaciones de los requerimientos de seguridad	SI**	Está siendo aplicado.	
8.2	Validación de los datos de entrada	SI**	Está siendo aplicado.	
8.3	Control de procesamiento interno	SI**	Está siendo aplicado.	
8.4	Integridad del mensaje	SI**	Está siendo aplicado.	
8.5	Validación de datos de salidas	SI**	Está siendo aplicado.	
8.6	Política sobre el uso de controles criptográficos	SI**	Está siendo aplicado.	
8.7	Gestión de claves	SI**	Está siendo aplicado.	
8.8	Control del software operativo	SI**	Está siendo aplicado.	
8.9	Protección de los datos de prueba del sistema	SI**	Está siendo aplicado.	
8.10	Control de acceso al código fuente de los programas	SI**	Está siendo aplicado.	
8.11	Procedimiento de control de cambios	SI**	Está siendo aplicado.	
8.12	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo	SI**	Está siendo aplicado.	
8.13	Restricción del cambio de paquetes de software	SI**	Está siendo aplicado.	
8.14	Fuga de información	SI**	Está siendo aplicado.	
8.15	Desarrollo de software contratado externamente	SI**	Está siendo aplicado.	
8.16	Control de las vulnerabilidades técnica	SI**	Está siendo aplicado.	
9. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN				**1**

Control	Requerimiento	Aplica (SI/NO)	Si aplica: Documento de Referencia en el EGSI Si no aplica: Justificación para la exclusión	Promedio Nivel de cumplimiento
9.1	Reporte sobre los eventos de Seguridad de la Información	SI	Procedimiento de Administración de Eventos de Seguridad de la Información.	
9.2	Reporte sobre las debilidades en la seguridad	SI	Procedimiento de Administración de Eventos de Seguridad de la Información.	
9.3	Responsabilidades y procedimientos	SI	Procedimiento de Administración de Eventos de Seguridad de la Información.	
9.4	Aprendizaje debido a los incidentes de Seguridad de la Información	SI	Procedimiento de Administración de Eventos de Seguridad de la Información.	
9.5	Recolección de evidencias	SI	Procedimiento de Administración de Eventos de Seguridad de la Información.	
10. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO				
10.1	Inclusión de la Seguridad de la Información en el proceso de gestión de la continuidad	SI**	Está siendo aplicado.	**3**
10.2	Continuidad del negocio y evaluación de riesgos	SI**	Está siendo aplicado.	
10.3	Desarrollo e implementación de planes de continuidad que incluyan la Seguridad de la Información	SI**	Está siendo aplicado.	
10.4	Estructura para la planificación de la continuidad del negocio	SI**	Está siendo aplicado.	
10.5	Pruebas, mantenimiento y revisión de los planes de continuidad del negocio	SI**	Está siendo aplicado.	
11. CUMPLIMIENTO				
11.1	Identificación de la legislación aplicable	SI**	Está siendo aplicado.	**3**
11.2	Derechos de Propiedad Intelectual	SI**	Está siendo aplicado.	

Control	Requerimiento	Aplica (SI/NO)	Si aplica: Documento de Referencia en el EGSI Si no aplica: Justificación para la exclusión	Promedio Nivel de cumplimiento
11.3	Protección de registros en cada entidad	SI**	Está siendo aplicado.	
11.4	Protección de los datos y privacidad de la información personal	SI**	Está siendo aplicado.	
11.5	Prevención del uso inadecuado de servicios de procesamiento de información	SI**	Está siendo aplicado.	
11.6	Reglamentación de controles criptográficos	SI**	Está siendo aplicado.	
11.7	Cumplimiento con las políticas y las normas de la seguridad	SI**	Está siendo aplicado.	
11.8	Verificación del cumplimiento técnico	SI**	Está siendo aplicado.	
11.9	Controles de auditoría de los sistemas de información	SI**	Está siendo aplicado.	
11.10	Protección de las herramientas de auditoría de los sistemas de información	SI**	Está siendo aplicado.	

3.3 Normas de seguridad de la información basada en estándares ISO

Los controles que se deben aplicar como resultado del análisis de riesgo realizado correspondiente a las normas de seguridad de la información basada en el estándar ISO27001, serán los considerados en la Declaración de Aplicabilidad detallados en la tabla No. 15.

3.4 Análisis y selección de procesos de COBIT5 relacionados con la seguridad de la información

A continuación, se analizará la seguridad de la información a través de los 7 catalizadores que provee COBIT5, que se considera como un marco integrador único con el cual es posible alinear ISO e ITIL.

- **Principios, Políticas y Marcos de Referencia de la seguridad de la información**

Principios, que definen las reglas de la Institución con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información, así como garantizar la continuidad de los sistemas de información, minimizar los riesgos y asegurar el cumplimiento de los objetivos estratégicos institucionales.

Tabla 17.

Principios de la Seguridad de la Información

Área de Enfoque	Principios
Dar soporte al negocio	Centrarse en el negocio
	Dar calidad y valor a las partes interesadas
	Cumplir con los requisitos legales y regulatorios relevante
	Proporcionar información oportuna y exacta sobre el desempeño de la seguridad de la información
Defender el Negocio	Evaluar las amenazas actuales y futuras
	Promover la mejora continua en la seguridad de la información
	Adoptar una estrategia basada en el riesgo
	Proteger la información clasificada
	Concentrarse en las aplicaciones críticas para el negocio
	Desarrollar los sistemas de forma segura
Promover un comportamiento responsable en seguridad de la información	Actuar de manera profesional y ética
	Fomentar una cultura positiva de seguridad de la información

Adaptado de: ISACA, 2012.

Políticas, que proveen una guía más detallada de cómo poner en práctica los principios y cómo éstos influirán en la toma de decisiones. Las políticas se estructuran en tres grupos (ISACA, 2012):

- La Política de Seguridad de la Información escrita por la función de seguridad de la información, pero dirigida por la Dirección Ejecutiva

- Las políticas específicas de seguridad de la información dirigidas por la función de Seguridad de la Información
- Otras políticas que puedan relacionarse con la seguridad de la información, pero que están dirigidas por otras funciones de la empresa. En estas políticas, la seguridad de la información debería influir en el desarrollo para asegurar el logro de los requisitos de seguridad de la información.

Se puede considerar relevantes las siguientes políticas:

- Política de Seguridad de la información
- Política de Control de Acceso
- Política de Seguridad de la Información del Personal
- Política de Seguridad Física y Ambiental
- Política de Gestión de Incidentes
- Política de Continuidad de Negocio y Recuperación ante Desastres
- Política de Gestión de Activos
- Reglas de Comportamiento (uso aceptable)
- Política de Adquisición, Desarrollo de Software y Mantenimiento de Sistemas de Información
- Política de Gestión de Proveedores
- Política de Gestión de Comunicaciones y Operaciones
- Política de Cumplimiento
- Política de Gestión de Riesgos

Las políticas deberían estar alineadas con los principios, objetivos, estrategia y el apetito de riesgo generales de la Institución para adaptarse a su entorno.

Basados en la declaración de aplicabilidad, la Institución Financiera debe definir e implementar las siguientes políticas, normas y procedimientos:

- Política de Seguridad de la Información
- Manual de funciones de Seguridad de la Información

- Plan de sensibilización de Seguridad de la Información
- Política de Administración de Seguridad Integral
- Procedimiento de Administración de Eventos de Seguridad de la Información

- **Procesos**

La Institución debe implementar procesos de gobierno y procesos de gestión para proporcionar un gobierno y una gestión integral de la seguridad de la información.

El modelo de procesos, los procesos y sus partes interesadas documentados en matrices RACI. (ISACA, 2012)

De los 37 procesos de COBIT 5 se seleccionarán aquellos que se relacionan directamente con la gestión de la seguridad de la información y que resultan del mapeo realizado en la tabla 14.

- Evaluar, Orientar y Supervisar: EDM01 Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno, EDM03 Asegurar la optimización del riesgo, EDM04 Asegurar la optimización de los recursos.
- Alinear, Planificar y Organizar: APO01Gestionar el Marco de Gestión de TI, APO07 Gestionar los Recursos Humanos, APO08 Gestionar las Relaciones, APO12 Gestionar el Riesgo, APO13 Gestionar la Seguridad.
- Entregar, dar Servicio y Soporte: DSS02 Gestionar las Peticiones y los Incidentes del Servicio, DSS04 Gestionar la Continuidad, DSS05 Gestionar los Servicios de Seguridad
- Supervisar, Evaluar y Valorar: MEA01.- Supervisar, Evaluar y Valorar Rendimiento y Conformidad, MEA02- Supervisar, Evaluar y Valorar el Sistema de Control Interno, MEA03.- Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.

De esta selección de procesos, la Institución Financiera deberá implementar solo aquellos que no lo tenga implementado o aquellos que necesitan ser mejorados.

Para cada proceso se deben definir metas y métricas que especifican hasta donde las metas son alcanzadas. Como sugerencia se lista a continuación algunas métricas que se podría utilizar:

- Número de brechas de seguridad de la información relativas a no conformidades de los dominios de la EGSI.
- Nivel de satisfacción de las partes interesadas con las medidas de seguridad de la información existentes.
- Porcentaje de riesgo mitigado con controles de seguridad de la información
- Porcentaje de actividades de seguridad de la información alineadas con la estrategia de negocio.
- Porcentaje de empleados a los que se proporciona concienciación sobre seguridad de la información
- Número de incidentes de seguridad de la información abiertos y cerrados y sus niveles de riesgo.
- Número de incidentes relacionados con accesos no autorizados a la información.
- Porcentaje de los procesos de negocio que satisfacen los requerimientos de seguridad de la información definidos.
- Porcentaje de controles de seguridad de la información adecuadamente monitorizados con resultados informados y revisados.

- **Estructuras Organizativas**

Las estructuras organizativas, roles y responsabilidades sobre la seguridad de la información son elementos clave en la toma de decisiones de la Institución y serán claramente definidos en la propuesta de modelo de gestión de la seguridad de la información. (ISACA, 2012).

Una métrica sugerida para este catalizador: Porcentaje de empleados que han recibido y aceptado formalmente roles y responsabilidades de seguridad de la información.

- **Cultura, Ética y Comportamiento**

Comprende todas las actividades relacionadas con una cultura de seguridad de la información que influencie en las actitudes y comportamientos de las personas, así como también con el liderazgo del personal estratégico de la Institución que toma en consideración todos los requisitos de seguridad de la información al momento de toma de decisiones, crean conciencia y demuestren la importancia de la seguridad de la información.

La Institución Financiera debe desarrollar un programa de formación y concienciación en seguridad de la información en coordinación con el área de Talento Humano, el mismo que debe ser evaluado permanentemente.

- **Información**

La información es el catalizador clave para la seguridad de la información ya que puede ser utilizada por la máxima autoridad de la Institución Financiera como base para la toma de decisiones.

Para optimizar el desarrollo y la distribución de la información, a continuación se detallan los emisores y los destinatarios de cada tipo de información a través de un identificador que establece la relación con las partes interesadas.

A → Aprobador
O → Emisor
I → Informado del tipo de información
U → Usuario del tipo de información

Tabla 18.
Grupos de Interés para Información Relacionada con Seguridad de la Información

Parte Interesada	Tipo de Información									
	Estrategia de Seguridad de la Información	**Presupuesto de Seguridad de la Información**	**Plan de Seguridad de la Información**	**Políticas**	**Requerimientos de Seguridad de la Información**	**Material de Concienciación**	**Informes de Revisión de Seguridad de la Información**	**Catálogo de Servicios de Seguridad de la Información**	**Perfil de Riesgo de la Información**	**Cuadro de Mando de Seguridad de la Información**
Gerencia General	U			I		U	I		A	
Comité de Seguridad	A	O	A	U	U	I	U	I	U	U
Oficial de Seguridad	O	U	O	O	A	A	A	A	U	U
Coordinador General de Tecnologías de la Información y Comunicación	U	O	U	U	U	U	I		U	U
Director Administrativo		A		U		U			U	
Director de Administración del Talento Humano				U		U				
Director Nacional de Seguridad	O	U	O	O	A	A	A	A	U	U
Responsable Seguridad en TIC	U	U	U	O	U	O	O	O	O	O
Subgerencia				U	O	U		U	U	
Coordinaciones				U	O	U		U	U	
Direcciones				U	O	U		U	U	
Funcionarios				U						
Personal Externo				U		I				
Terceras Partes				U		I				
Proveedores						I				
SNAP		I				I	I			
Superintendencia de Bancos		I				I	I			
Contraloría General del Estado		I				I	I			
Otros Entes		I				I	I			

Adaptado de: ISACA, 2012.

- **Servicios, Infraestructura y Aplicaciones**

Es necesario capacidades de servicio que proporcionen a la Institución Financiera seguridad de la información y funcionalidades relacionadas. Los servicios no solo requieren infraestructura y aplicaciones, sino que se entregan mediante una combinación de otros catalizadores tales como procesos, información y estructuras organizativas. (ISACA, 2012)

Los servicios a implementar deben proporcionar: una arquitectura de seguridad, concienciación sobre seguridad, desarrollo alineado con los estándares de seguridad, evaluaciones de seguridad, pruebas de seguridad, servicios de monitorización y alerta para eventos relacionados con la seguridad, entre otros.

La Institución Financiera debe considerar dentro de su catálogo de servicios los siguientes:

- Servicios de Concienciación en Seguridad
- Servicios de Evaluación de la Seguridad
- Servicios de Acceso de Usuario y Derechos de Acceso
- Servicios de Respuesta a Incidentes
- Servicios de Pruebas de Seguridad
- Servicios de Monitorización y Mejora de la Seguridad de la Información

La infraestructura tecnológica con la que cuenta la Institución Financiera posee mecanismos de seguridad que garantizan la protección de la confidencialidad, integridad y disponibilidad de la información.

- **Personas, habilidades y competencias**

Las habilidades y competencias vinculados a grados de educación y cualificación, habilidades técnicas, niveles de experiencia, conocimiento, y

destrezas conductuales de las personas aseguran que se tomen decisiones correctas y que todas las actividades relaciones con la seguridad de la información se realicen satisfactoriamente. (ISACA, 2012).

Cada rol que la Institución Financiera defina para la seguridad de la información deben cumplir con ciertas habilidades y competencias, las mismas que pueden ser desarrolladas a través de formación o adquiridas a través de contratación.

3.5 Análisis y selección de procesos de ITIL relacionados con la Seguridad de la Información

Uno de los objetivos de ITIL al integrar la estrategia del negocio dentro del diseño del servicio, es manejar un nivel definido de seguridad de un servicio, incluido el manejo de la reacción ante incidentes de seguridad. (Osiatis, 2011)

Es a través de la Gestión de incidentes que ITIL se integrará a todos los procesos descritos anteriormente para mejorar la calidad de Gestión de la Seguridad de la Información de la Institución Financiera considerada en el análisis del presente trabajo de titulación.

En diciembre del 2016 se aprobó el procedimiento para la administración de incidentes de seguridad de la información, desarrollado en base a ITIL, un marco de trabajo que describe las mejores prácticas en la administración de servicios de TI, con las siguientes consideraciones:

- El procedimiento permitirá reportar, registrar, priorizar, escalar, investigar, solucionar y monitorear los incidentes de seguridad de la información de la Institución Financiera.
- Todo incidente de seguridad de la información deberá ser reportado al Oficial de Seguridad de la Información y de catalogarse con impacto alto, se informará al Comité de Seguridad de la Información y a la máxima autoridad según el caso.

- Los incidentes de seguridad de la información en la Institución Financiera, son gestionados por la Dirección de Aseguramiento de la Calidad y Seguridad Informática, cuando esos incidentes son de tipo tecnológico; y por las áreas competentes, en función del evento reportado.
- El Oficial de Seguridad de la Información deberá reportar oportunamente los incidentes identificados de seguridad de la información a la SNAP, si provocan indisponibilidad o falta de continuidad de los servicios críticos.

3.6 Integración de procesos en un modelo de solución

Como resultado del análisis de la situación actual realizado a la Institución Financiera tanto en el nivel de cumplimiento con relación a las directrices y objetivos de control del Acuerdo No. 166, como del análisis e identificación de riesgos a los cuales la Institución está expuesta, se establece la necesidad de mejorar el Sistema de Gestión de la Seguridad de la Información, para lo cual se propone en el siguiente capítulo un modelo de gestión basado en normas, estándares y buenas prácticas reconocidas a nivel mundial.

4. CAPÍTULO IV. MODELO DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El modelo propuesto se basa en los requerimientos de la norma ISO27001:2013 y el modelo de mejora continua PDCA que se encuentra embebido en la misma, y establece todos los procedimientos y políticas en relación a los objetivos de negocio de la Institución Financiera, con el fin de mantenerla en el mínimo nivel de exposición al riesgo y garantizando su confidencialidad, integridad y disponibilidad.

Se establece tres fases: Diagnóstico y Planificación, Implementación, Evaluación del Desempeño y Mejora Continua.

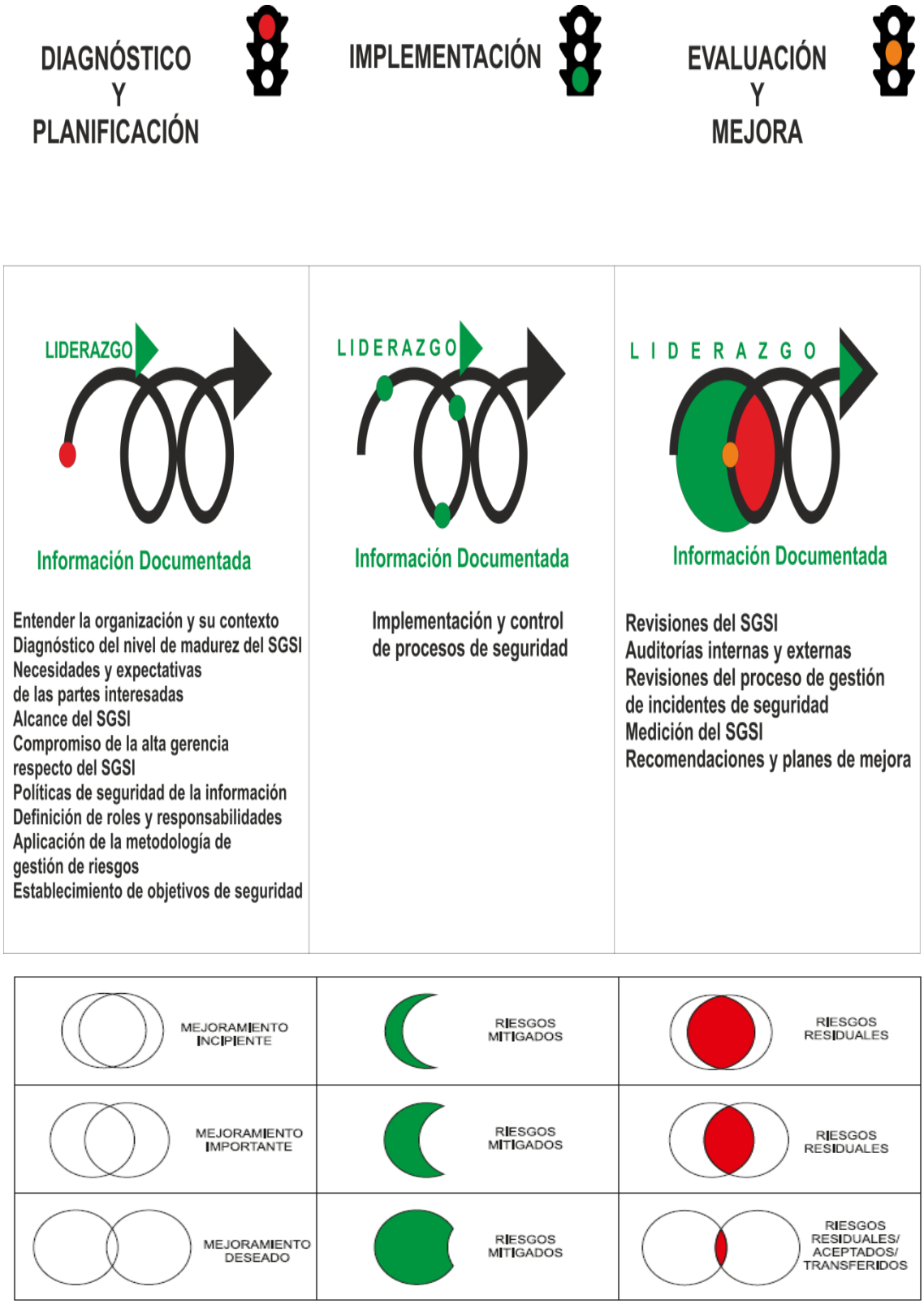

Figura 36. *Modelo de Gestión de la Seguridad de la Información*

4.1 FASE 1.- Diagnóstico y Planificación

4.1.1 Contexto de la organización

4.1.1.1 Conocimiento de la organización y su contexto

Para establecer, implementar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información con base en los objetivos y las necesidades propias de la Institución Financiera, es necesario tomar en cuenta factores específicos de los entornos internos y externos tales como:

- Estrategia de la Institución Financiera, en donde se especifique misión, visión, principios y valores y objetivos estratégicos
- Análisis FODA
- Estructura Organizacional
- Leyes, regulaciones y políticas aplicables, las cuales son de cumplimiento obligatorio para la Institución Financiera.
- Diagnóstico del nivel de madurez de la seguridad de la información actual de la Institución Financiera.

El conocimiento de la organización y de su contexto debe ser conocido por todos los funcionarios de la Institución

4.1.1.2 Conocimiento de las necesidades y expectativas de las partes interesadas

Tomando como referencia uno de los principios de COBIT 5, se recomienda utilizar la cascada de metas para traducir y concretar las necesidades y expectativas de las partes interesadas en metas operativas relacionadas con la seguridad de la información de la Institución, que deben satisfacerse.

Identificar y definir la función de las partes interesadas es una de las tareas de la Institución que tiene un papel clave en el Sistema de Gestión de Seguridad de la Información. (ISACA, 2012). Las partes interesadas de la Institución incluyen:

- Gerencia General
- Comité de Seguridad de la Información
- Oficial de Seguridad
- Responsable de la Seguridad de la Información en TIC
- Auditores internos y externos
- Proveedores
- Clientes
- Funcionarios
- Entes reguladores

4.1.1.3 Determinación del alcance

Para establecer el alcance, la Institución Financiera debe determinar los límites y la aplicabilidad de su Sistema de Gestión de Seguridad de la Información a través de la declaración de aplicabilidad definida en la tabla 15, que determina el ámbito en el que la Institución trabajará bajo los requisitos de la EGSI.

4.1.1.4 Sistema de Gestión de la Seguridad de la Información

La Institución Financiera debe establecer, implementar, mantener y mejorar de manera continua un Sistema de Gestión de la Seguridad de la Información en base al modelo propuesto. La Institución puede basarse en el proceso de COBIT5 -APO013. (ISACA, 2012).

4.1.2 Liderazgo

4.1.2.1 Liderazgo y compromiso

En base a COBIT 5, se puede definir tres niveles de liderazgo (ISACA, 2012):

- Máxima autoridad de la Institución Financiera – Gerente General
- Comité de Gestión de Seguridad de la Información (CSI) – Oficial de Seguridad, Coordinador General de Tecnologías de la Información y Comunicación, Director Administrativo, Director de Administración de Talento Humano, Director Nacional de Seguridad
- Responsables de la información, el nivel organizacional de los responsables de la información son los Subgerentes, Coordinadores y Directores de las Áreas de la Institución Financiera.

Estos niveles deben demostrar el liderazgo y compromiso con la seguridad de la información al:

- Disponer la implementación, operatividad, monitoreo, mantenimiento y mejoramiento del Esquema Gubernamental de Seguridad de la Información (EGSI) en la Institución.
- Gestionar la disponibilidad de recursos necesarios para el Sistema de Gestión de la Seguridad de la Información.
- Definir, mantener y gestionar la aprobación de la política y normas de seguridad de la información de la Institución.
- Asegurar el cumplimiento de la política y normas de seguridad de la información para garantizar la confidencialidad, la integridad y la disponibilidad de sus activos de información.
- Monitorear cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la Institución frente a incidentes de seguridad imprevistos.

- Revisar las métricas de seguridad y monitorear el cumplimiento de las metas definidas.
- Asignando roles y responsabilidades de la seguridad de la información,
- Siendo pieza fundamental en el cumplimiento de la seguridad de la información y dando ejemplo a los funcionarios de la Institución a fin de crear una verdadera cultura de seguridad

4.1.2.2 Política

Las políticas para la seguridad de la información son documentos que proporcionan las reglas para apoyar a los objetivos que la Institución se ha propuesto en materia de seguridad de la información y que permiten garantizar la integridad, confidencialidad y disponibilidad de la información. Las políticas deben tener los siguientes atributos (ISACA, 2012):

- Objetivo
- Alcance
- Responsabilidades

  Todos los funcionarios, personal externo, (auditores, consultores, contratistas, entre otros) y las terceras partes (proveedores, clientes, entre otros) de la Institución Financiera ejecutarán sus actividades considerando los lineamientos de la presente política.

  La Gerencia General, aprobará la política de seguridad de información y cualquier cambio y ajuste que se realice sobre ésta.

  Las Subgerencias, Coordinaciones Generales y Direcciones que componen la Entidad, formularán ajustes y mejoras a la política de seguridad de la información a través del Comité de Seguridad de la Información.

  El Comité de Seguridad de la Información realizará el control y seguimiento del cumplimiento de esta política.
- Base Legal
- Consideraciones

Esta política será revisada con regularidad como parte de un proceso de revisión gerencial, o cuando se identifiquen cambios en la Institución o, su estructura, sus objetivos o alguna condición que afecten la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos institucionales.

- Definiciones
- Incumplimientos

  Los funcionarios que incumplan la política serán sancionados de acuerdo a la normativa interna vigente.
- Referencias a otros documentos

4.1.2.3 Funciones, responsabilidades y autoridad de la organización

La máxima autoridad debe asegurar que las responsabilidades y autoridades para los roles definidos a la seguridad de la información sean asignados y comunicados, lo que va a permitir que todos los que conforman la Institución Financiera tengan la responsabilidad clara de la ejecución de un proceso o actividad y el reporte de sus resultados a la persona o personas adecuadas.

Se define el siguiente esquema de roles y responsabilidades.

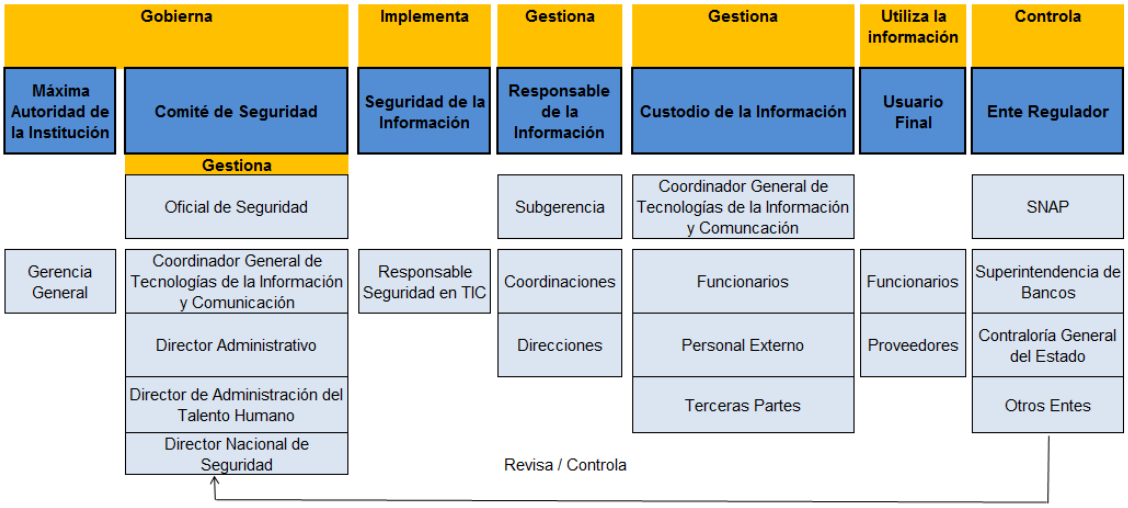

Figura 37. Roles y Responsabilidades de la Seguridad de la Información.

La máxima autoridad de la Institución Financiera dispondrá la implementación, operatividad, monitoreo, mantenimiento y mejoramiento del Esquema Gubernamental de Seguridad de la Información (EGSI) y gestionará los recursos necesarios para la administrar la Seguridad de la Información en la Institución.

El Comité de Gestión de Seguridad de la Información se enfocará en la definición de la estrategia de seguridad de la Institución Financiera, con base en las directrices del Anexo 1 del Acuerdo No. 166 de la Secretaría Nacional de la Administración Pública, publicado en el Segundo Suplemento del Registro Oficial No. 88, de 25 de septiembre de 2013 y efectuará el seguimiento al cumplimiento de las tareas de la gestión de la Seguridad de la Información de la Entidad.

El Oficial de Seguridad de la Información será el delegado por el Comité de Seguridad de la Institución Financiera para gestionar la implementación la estrategia de Seguridad de la Información en base a las directrices del Anexo 1 del Acuerdo No. 166 de la Secretaría Nacional de la Administración Pública. Es el encargado de dirigir el programa de Seguridad de la Información y tomar las decisiones que permitan gestionar la Seguridad de la Información.
El Responsable de Seguridad del Área de Tecnologías de Información, es un profesional de la Coordinación General de Tecnologías de Información y Comunicación que apoyará en la implementación de la estrategia de Seguridad de la Información, siendo responsable de la seguridad en la mencionada área.

Los Responsables de la información están encargados de definir y asegurar el cumplimiento de los requerimientos de seguridad de los activos de información que le sean asignados, así como de la clasificación, control y monitoreo del uso y gestión de los mismos. El nivel organizacional de los Responsables de la Información son los Subgerentes, Coordinadores y Directores de las Áreas de la Institución Financiera.

Los Custodios de la información corresponde a la Coordinación General de Tecnologías de la Información y Comunicación, funcionarios de las Subgerencias, Coordinaciones y Direcciones de la Institución Financiera, el personal externo, (auditores, consultores, contratistas, entre otros) y las terceras partes (proveedores, clientes, entre otros) que tienen la responsabilidad de gestionar la seguridad de los activos de información que le han sido asignados para su administración.

Los usuarios finales son todos los funcionarios, proveedores, terceras partes, u otra persona autorizada para utilizar la información de la Institución Financiera en el cumplimiento de sus funciones y/o la ejecución de sus actividades laborales cotidianas.

Los entes reguladores son instituciones encargadas de controlar, regular y supervisar al sistema financiera del país, adicionalmente, asegura que las instituciones controladas cumplan las leyes y protege a los usuarios para que de esta forma haya confianza en el sistema.

4.1.3 Planeación

La planificación del Sistema de Gestión de la Seguridad de la Información debe considerar el contexto de la organización, las necesidades y expectativas de las partes interesadas y la importancia que tiene, ya que de ello depende el éxito de su implementación; a través de acciones para enfrentar los riesgos y oportunidades y del establecimiento de objetivos de seguridad que puedan ser alcanzados.

4.1.3.1 Acciones para enfrentar los riesgos y las oportunidades

Se debe aplicar una Metodología de Gestión de Riesgos que contemple un proceso de evaluación de riesgos y un proceso de tratamientos de riesgos.

El proceso de evaluación de riesgos debe contemplar las siguientes actividades:

- Identificación de los riesgos asociados a la seguridad de la información
- Análisis de riesgos considerando probabilidad de ocurrencia e impacto sobre los activos de información.
- Evaluación de los riesgos en base a definición de criterios de aceptación y evaluación de riesgos.
- Priorización de los riesgos para ser considerados en el tratamiento de riesgos.
- Documentar el proceso de evaluación
- Asegurar que los resultados sean consistentes, validados y comparables

El proceso de tratamiento de riesgos debe contemplar las siguientes actividades:

- Seleccionar la opción de tratamiento de riesgos en base a resultados de la evaluación
- Determinar controles a ser implementados
- Elaborar la declaración de aplicabilidad
- Formular un plan te tratamiento de riesgo adecuado que permita mantener un nivel adecuado de apetito y tolerancia al riesgo de la Institución.
- Aprobar el plan de tratamiento con el propietario del riesgo
- Documentar el proceso de tratamiento de riesgo

La metodología de gestión de riesgos en la Institución debe ser aplicada de forma continua con el fin de cumplir con uno de los objetivos de gobierno que es la optimización del riesgo. (GU-003, 2016)

4.1.3.2 Objetivos de Seguridad de la información y planificación para alcanzarlos

Los objetivos de seguridad de la información deben ser: consistentes con la política de seguridad de la Institución Financiera, resultado de la evaluación y tratamiento de riesgos, medibles, comunicados y actualizados en el tiempo.

Al establecer los objetivos de seguridad considerar los siguientes atributos: descripción, recursos necesarios, responsables, planificación del cumplimiento del objetivo y como se evaluará el resultado.

4.1.4 Soporte

El Sistema de Gestión de la Seguridad de la Información de la Institución Financiera se fundamenta en el uso eficiente de los recursos, competencias, conciencia, comunicación e información documentada.

4.1.4.1 Recursos

La máxima autoridad de la Institución Financiera debe proveer los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de la Seguridad de la Información. En general cuando se habla de recursos se puede hablar de recursos humanos, servicios, infraestructura, aplicaciones e información.

4.1.4.2 Competencias

Basados en COBIT 5, para implementar con eficiencia una función de seguridad de la información las personas deben tener algunas de las siguientes habilidades y competencias (ISACA, 2012)

- Gobierno de seguridad de la información

- Formulación estratégica de seguridad de la información
- Gestión del riesgo de la información
- Desarrollo de la arquitectura de seguridad de la información
- Operaciones de seguridad de la información
- Evaluación, pruebas y cumplimiento de la información.

Para el esquema de roles establecido en la Institución Financiera, se definen las siguientes habilidades y competencias:

Tabla 19.

Habilidades y Competencias para cada rol de seguridad de la in información

Roles	Competencias
Máxima Autoridad de la Institución	Gobierno de la Seguridad de la Información
Comité de Seguridad de la Información	Estrategia de la Seguridad de la Información
Oficial de Seguridad	Gestión del riesgo de la información
Seguridad de la Información	Desarrollo de la arquitectura de seguridad de la información Operaciones de seguridad de la información
Responsable de la Información	Gestión del riesgo de la información
Custodio de la Información	Estrategia de la Seguridad de la Información Gestión del riesgo de la información
Usuario Final	Estrategia de la Seguridad de la Información Gestión del riesgo de la información
Ente Regulador	Evaluación, pruebas y cumplimiento de la información

4.1.4.3 Concientización

Basado en la práctica de Gestión APO01.04 - Comunicar los objetivos y la dirección de gestión (ISACA, 2012), la Institución Financiera a través de los expertos en seguridad de la información deben desarrollar un programa de formación y concienciación en seguridad de la información en coordinación con el área de Talento Humano que tiene la responsabilidad de incorporar, suministrar el material de concienciación y realizar las pruebas que evidencien

su comprensión y el Oficial de Seguridad que tiene la responsabilidad de que el programa se lleve a cabo.

El programa debe identificar los recursos a través de los cuales se impartirá la concienciación y el tipo de audiencia objetivo de este programa.

El material de concienciación debe actualizarse periódicamente y su eficiencia se puede medir a través del comportamiento de los individuos y de los efectos de dicho comportamiento en términos de incidencias e incumplimientos.

4.1.4.4 Comunicación

La Institución Financiera debe determinar la necesidad de comunicar interna y externamente aspectos relacionados con la seguridad de la información. A través de las comunicaciones se proporciona la conciencia y formación adecuada sobre seguridad de la información.

4.1.4.5 Documentación de la información

A lo largo de todas las fases del Sistema de Gestión de Seguridad de la Información se genera información documentada que la Institución estima relevante. Los documentos deben ser adecuadamente identificados, descritos, revisados y aprobados. Adicionalmente se deben asignar responsables de su control y actualización.

4.2 Fase2. Implementación

Para cumplir con los requisitos de seguridad y asegurar que el Sistema de Gestión de Seguridad de la Información logre los resultados esperados, la Institución Financiera debe planificar, implementar y controlar una serie de procesos que le permitirán implementar los planes de acción resultado de la evaluación y tratamiento de riesgos.

En base a los procesos considerados en las secciones 3.3, 3.4 y 3.5 y a la declaración de aplicabilidad, la Institución Financiera cuenta con una línea base para la implementación de los procesos de seguridad.

La Institución Financiera debe considerar realizar evaluaciones de riesgo de forma continua o cuando se presenten cambios que lo ameriten, manteniendo siempre información documentada y actualizada del proceso.

Se propone el siguiente plan de implementación que nos permitirá cerrar las brechas encontradas en el nivel de cumplimiento de los dominios del EGSI de la Institución Financiera.

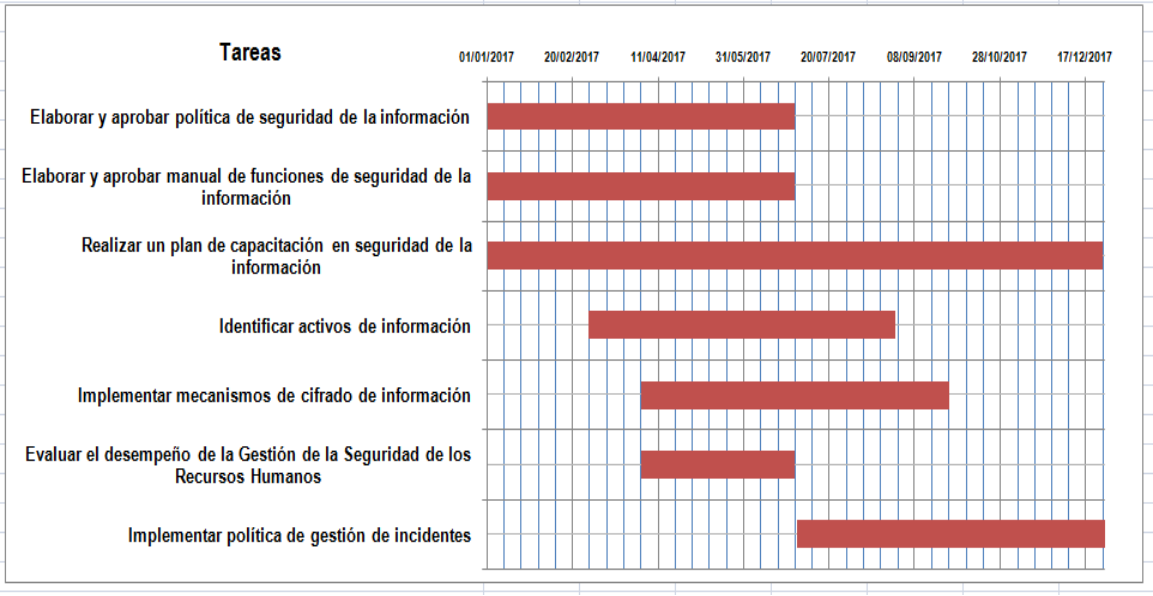

Figura 38. Plan de Implementación de dominios del EGSI

4.3 Fase 3. Evaluación del Desempeño y Mejora Continua

Las actividades de supervisión y revisión del Sistema de Gestión de la Seguridad de la Información son claves para el proceso de mejora continua del sistema.

Para evaluar el desempeño del Sistema de Gestión de la Seguridad de la Información se debe realizar las siguientes actividades.

- Realizar revisiones periódicas del Sistema de Gestión de la Seguridad de la Información, incluyendo aspectos de políticas, objetivos y prácticas de seguridad del sistema. En cada revisión considerar los resultados de auditorías internas y externas, incidentes de seguridad, mediciones de efectividad, sugerencias y retroalimentación de las partes interesadas. (ISACA, 2012). La Dirección de Riesgos a través del Oficial de Seguridad será la responsable de estas revisiones.
- Realizar auditoría internas y externas al Sistema de Gestión de la Seguridad de la Información a intervalos planificados, estas auditorías deben contar con los respectivos informes. (ISACA, 2012). La Dirección de Riesgos y Dirección de Auditoria serán las responsables.
- Realizar revisiones periódicas del Proceso de Gestión de Incidentes de Seguridad. El Oficial de Seguridad será el responsable de estas revisiones periódicas.
- Por lo menos una vez al año, la máxima autoridad deberá realizar revisiones del Sistema de Gestión de la Seguridad de la Información para asegurar su alcance sigue siendo el adecuado y que se identifican mejoras en el Sistema. (ISACA, 2012).
- Proporcionar información para el mantenimiento de los planes de seguridad para que se incluyan las incidencias de las actividades de supervisión y revisión periódica. (ISACA, 2012)
- Revisar las métricas de seguridad y monitorear el cumplimiento de las metas definidas. El Oficial de Seguridad reportará al Comité de Seguridad de la Información los resultados a fin de que se identifiquen mejoras en el proceso.

Como resultado del proceso de evaluación se debe emitir las recomendaciones de mejora del Sistema de Gestión de la Seguridad de la Información.

Al proponer un Modelo de Gestión de Seguridad de la Información basado en la norma ISO27001:2013, se garantiza la eficacia y eficiencia del sistema a través de la implementación del ciclo de mejora continua PDCA.

Tras el proceso de evaluación del desempeño del Sistema de Gestión de la Seguridad de la Información descrito en la fase 3, se tienen una serie de recomendaciones y planes de mejora, que constituyen insumos para volver a la fase de planificación; y, tomando en cuenta que como resultado del análisis y evaluación de riesgos siempre permanecen los riesgos residuales que deben ser revisados, el ciclo continúa y nunca dejará de fluir.

A través de la mejora continua, la Institución Financiera irá cubriendo las brechas identificadas en el análisis del nivel de cumplimiento con relación a las directrices y objetivos de control del Acuerdo No. 166 de la Secretaría Nacional de la Administración Pública (SNAP) realizado en la sección 3.1.

El modelo está planteado, la eficiencia y éxito del mismo depende principalmente del compromiso de la máxima autoridad de la Institución Financiera, a través de su apoyo e involucramiento y de la definición del ámbito de implementación por áreas.

5. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

En base a las recomendaciones emitidas por los organismos de control y/o la Dirección Nacional de Auditoría Interna de la Institución Financiera se identificaron una serie de problemas recurrentes, los mismos que en base a la experiencia del autor y a sus niveles de impacto dentro del Sistema de Gestión de la Seguridad de la Información se categorizaron con un nivel de importancia alta, media y baja. Entre los problemas con importancia alta se identificaron los siguientes: no existen métricas ni una evaluación periódica del desempeño y eficacia del sistema de gestión de seguridad de la información que establezcan acciones de mejora continua, falta de concienciación y conocimiento en temas de seguridad de la información por parte de todos los funcionarios de la institución, no se cuenta con un proceso de gestión de incidentes de seguridad de la información, no se tiene claramente definido los roles y responsabilidades respecto de la seguridad de la información. Estos problemas constituyen un primer diagnóstico de la situación actual de la Institución Financiera con relación a la seguridad de la información.

Para establecer de manera precisa las causas raíz de los problemas asociados al proceso de Gestión de la Seguridad de la Información, se realizó un análisis de brechas con el fin de identificar el nivel de cumplimiento de la Institución Financiera con relación a las directrices y objetivos de control del Esquema Gubernamental de Seguridad de la Información (EGSI), llegando a establecer un nivel de cumplimiento promedio de 2 – Repetible, que en base al Modelo Genérico de Cumplimiento significa que las directrices siguen un enfoque similar de actividades que son ejecutadas por diferentes personas que desarrollan la misma tarea y que no existe entrenamiento y sensibilización formal de las actividades comunes y se complementó con un análisis y evaluación de riesgos basados en la metodología aprobada por la Institución Financiera en el mes de octubre de 2016, con un resultado de 56% de riesgos

de nivel bajo, 38% de riesgos de nivel medio y 6% de riesgos de nivel alto. En base a este análisis se concluye que los planes de acción se deberán centrar en los siguientes dominios: Política de Seguridad de la Información, Organización de la Seguridad de la Información, Seguridad de los Recursos Humanos, Control de Acceso y Gestión de los Incidentes de la Seguridad de la Información.

En este sentido la Institución Financiera requiere contar con una Política de Seguridad, implementar un programa de culturización y concientización en Seguridad de la Información, establecer un proceso de gestión de incidentes y realizar de forma periódica el análisis y evaluación de riesgos.

Con el fin de integrar procesos, objetivos de control y controles en un modelo de solución que busca mejorar la capacidad de Gestión de la Seguridad de la Información y cerrar las brechas identificadas con relación al nivel de cumplimiento de la Institución Financiera con relación al EGSI, se realizó un mapeo de COBIT 5, ITIL v3 e ISO 27001, prácticas y estándares que están siendo ampliamente adoptados a nivel global y que fueron seleccionados a partir de un análisis comparativo de objetivos, áreas de aplicación, beneficios, procesos y concienciación. Como resultado de este mapeo se obtuvo el documento de Declaración de Aplicabilidad el mismo que servirá como línea base para la implementación del modelo propuesto.

Para mejorar la capacidad de gestión de la seguridad de la información, se propone un modelo que consta de tres fases: Diagnóstico y Planificación, Implementación y Evaluación y Mejora, el mismo que se desarrolló en base a los requerimientos de la norma ISO 27001:2013 y el modelo de mejora continua PDCA, cuya implementación mejorará la gestión de la calidad y fiabilidad de la información.

5.2 Recomendaciones

Se recomienda que la Institución Financiera en base al modelo propuesto, implemente rutinas, controles o metodologías que solucionen los problemas identificados y mejoren los niveles de cumplimiento de las recomendaciones emitidas por los organismos de control y/o la Dirección Nacional de Auditoría Interna, con el fin de obtener mayor eficiencia operacional y administrativa en el proceso de Gestión de la Seguridad de la Información.

Con el fin de cerrar las brechas identificadas en el nivel de cumplimiento de la Institución Financiera con relación a los objetivos de control del EGSI y mitigar los riesgos a los cuales está expuesta, se recomienda las siguientes acciones: realizar las gestiones necesarias a fin de agilizar el proceso de aprobación de la Política de Seguridad de la Información que ya se encuentra desarrollada, coordinar con la Dirección de Talento Humano la implementación de programas de concientización con el objetivo de mejorar la cultura de seguridad de los funcionarios de la Institución, continuar con el proceso de análisis y evaluación de riesgos iniciado en algunas direcciones e implementar el procedimiento de Gestión de Incidentes que se encuentra aprobado desde diciembre de 2016.

Se recomienda que la Institución Financiera tome como línea base para la implementación de los procesos de seguridad, los considerados en las secciones 3.3, 3.4 y 3.5.

Para el éxito en la implementación del modelo propuesto se recomienda que el Oficial de Seguridad garantice el compromiso de la máxima autoridad en actividades de supervisión y revisión del Sistema de Gestión de la Seguridad de la Información que son claves para una mejora continua.

REFERENCIAS

Arévalo, P. A. O. (2015). Gobierno de seguridad de la información, un enfoque hacia el cumplimiento regulatorio. Revista Tecnológica-ESPOL, 28(3).

Fernández, C. (2012). La norma ISO 27001 del Sistema de Gestión de la Seguridad de la Información, Recuperado el 9 de noviembre de 2016 de: http://www.aec.es/c/document_library/get_file?uuid=a89e72de-d92b-47cf-ba5e-5ea421fcbeb4&groupId=10128

Gutiérrez, C. (2013). COSO y el establecimiento de un sistema de control. Recuperado el 12 de noviembre de 2016 de: http://www.welivesecurity.com/la-es/2013/07/16/coso-y-el-establecimiento-de-un-sistema-de-control/.

ICONTEC, (2012). Boletín informático ICONTEC, Marzo 2011-nro.03 Artículo "Gestión de riesgos".

ISACA. (2008). Alineando COBIT®4.1, ITIL®V3 e ISO/IEC 27002 en beneficio de la empresa. Recuperado el 15 de junio de 2016 de: http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-COBIT-4-1-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa_res_Spa_0108.pdf).

ISACA. (2012). COBIT 5: Para la Seguridad de la Información, Estados Unidos.

ISO27001:2013, El Portal de ISO 27001. Recuperado el 9 de noviembre de 2016 de: www.iso27000.es

ISO27000 (2012). Sistema de Gestión de la Seguridad de la Información. Recuperado el 9 de noviembre de 2016 de: http://www.iso27000.es/download/doc_sgsi_all.pdf

Kosutic, D.Advisera-27001academy, Catalogue of threats & vulnerabilities. Recuperado el 15 de diciembre de 2016 de: https://advisera.com/27001academy/knowledgebase/threats-vulnerabilities/

MAGERIT. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos, Madrid.

Ormella, C. (2014). Norma ISO 31000 de Riesgos Corporativos. Recuperado el 12 de diciembre de 2016 de: http://www.criptored.upm.es/descarga/ISO_31000_riesgos_corporativos.pdf,

Osiatis. (2011). Curso ITIL Foundation. Recuperado el 17 de mayo de 2016 de: http://itilv3.osiatis.es/diseno_servicios_TI/gestion_seguridad_informacion/introduccion_objetivos.php

Ríos Huércano, S. (2014). Manual de ITIL V.3. Recuperado el 12 de diciembre de 2016 de: Biable Management, Excellence and Innovation: www.biable.es

ANEXOS

Anexo A - Política de seguridad de la información

Anexo B - Organización de la Seguridad de la Información

Anexo C - Gestión de los Activos

Anexo D - Seguridad de los Recursos Humanos

Anexo E - Seguridad Física y del Entorno

Anexo F - Gestión de Comunicaciones y Operaciones

Anexo G - Control de Accesos

Anexo H - Adquisición, desarrollo y mantenimiento de sistemas de información

Anexo I - Gestión de los Incidentes de la Seguridad de la Información

Anexo J - Gestión de la Continuidad del Negocio

Anexo K - Cumplimiento

Anexo L - Ponderación y Clasificación de los Activos de Información

Anexo M - Activos de Información Críticos

Anexo N - Análisis de Riesgo Inherente

Anexo O - Análisis de Riesgo Residual

Los anexos se incluyen en el CD que se adjunta a la presente tesis.