UNIVERSIDAD DE COSTA RICA

SISTEMA DE ESTUDIOS DE POSGRADO

“DESARROLLO DE UN PROGRAMA DE AUDITORÍA PARA LA EVALUACIÓN DEL SISTEMA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DEL BANCO POPULAR, DE CONFORMIDAD CON LOS MARCOS DE REFERENCIA: ISO/IEC 27001 Y COBIT”

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

GERARDO ZÚÑIGA HERNÁNDEZ

Ciudad Universitaria Rodrigo Facio, Costa Rica

2015

Dedicatoria

A mi preciosa y amada hija Paola, quien en cada momento me llena de felicidad y me recuerda que, a pesar de todo, la familia y en especial los hijos tienen absoluta prioridad y merecen que les dediquemos el mayor tiempo posible, y que esto no lo reemplaza ningún regalo material.

A ella, le dedico todo el esfuerzo y la dedicación que he puesto en esta etapa, en procura de seguir creciendo profesional, espiritual y emocionalmente, con la finalidad de brindarle un mejor futuro.

Agradecimientos

A Dios por brindarme la salud, la sabiduría y la confianza para seguir creciendo integralmente.

A mi amada esposa, Tanya Garbanzo Bolívar, quien me ha brindado el apoyo y la comprensión para culminar con éxito esta etapa de mi vida.

Al Banco Popular que me brinda el sustento económico y la inspiración para desarrollar este trabajo, en procura de generar valor para el mejoramiento de la entidad.

En especial a la Auditoría Interna del Banco Popular, por apoyarme en mi crecimiento profesional y por haberme brindado la oportunidad de formar parte del equipo de auditores de tecnologías de información.

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

_____

Dr. Sergio Espinoza Guido
Profesor Guía

_____

MSc. Cilliam Cuadra Chavarría
Lector Académico

_____

Lic. Marco Antonio Chaves Soto, MBA.
Lector de Empresa

_____

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

_____

Gerardo Zúñiga Hernández
Sustentante

Tabla de Contenidos

Dedicatoria ii

Agradecimientos iii

Hoja de Aprobación iv

Tabla de Contenidos v

Resumen vii

Lista de Tablas viii

Lista de Figuras ix

Lista de Abreviaturas x

CAPÍTULO I: INTRODUCTORIO 1

1 Introducción 2

2 Justificación 4

3 Objetivos 5

4 Alcance 6

5 Marco teórico 6

6 Procedimiento Metodológico 8

7 Contenido Capitulario 9

CAPÍTULO II: CONOCIMIENTO DEL PROCESO 10

1 Aspectos generales del Banco Popular 11

2 Gestión de la seguridad de la información en el Banco Popular 12

3 COBIT 5 - APO13 Gestionar la Seguridad 19

CAPÍTULO III: PROGRAMA DE AUDITORÍA 29

1 Programa de auditoría del Proceso APO13 COBIT 5 30

Etapa A Determine el alcance de la evaluación de auditoría 31

Etapa B Comprender los habilitadores, establecer criterios adecuados de evaluación y realizar la evaluación la Seguridad.....35
CAPÍTULO IV: RESULTADOS DE LA EVALUACIÓN **52**
1 Resultados de la evaluación del proceso APO13 Gestionar la Seguridad.....53
CAPÍTULO V: INFORME DE AUDITORÍA.....**78**
1. Resultados: Observaciones y Recomendaciones 79
A. Se carece de un perfil de riesgos de seguridad de la información alineado a la norma IEC/ISO 27001 79
B. El diseño de la política de seguridad de la información dificulta el logro de los objetivos 81
C. La gestión de seguridad de la información carece de estructuras organizativas completas y de un adecuado ámbito de control y poder de decisión 84
2. Conclusiones.....86
REFERENCIA CONSULTADA.....88

Resumen

La gestión de riesgos y amenazas que atenten contra los activos de información de las empresas y, en especial, de instituciones financieras, requiere de la implementación y mantenimiento de un sistema gestor de la seguridad de la información, siendo este el medio que permita generar valor, en torno al nivel requerido de seguridad para mantener la integridad, disponibilidad y confiabilidad de los datos.

En el presente trabajo se desarrolla una evaluación de auditoría basada en riesgos, en la cual, se aborda el tema de gestión de seguridad de la información en el Banco Popular, desde una perspectiva estratégica y de gobierno, según el enfoque del proceso *APO13 Gestionar la Seguridad de COBIT 5.*

Si bien la entidad bancaria se encuentra desarrollando un plan del sistema gestor de la seguridad de la información con un horizonte de 5 años, que busca alinear la gestión de la seguridad de la información a las prácticas recomendadas en los dominios de la norma ISO 27001, el presente trabajo tiene como propósito analizar la gestión de la seguridad de la información en el Banco, con los recursos, estructuras organizacionales, marcos normativos y otros elementos vigentes durante el período de la evaluación, considerando los 7 habilitadores de COBIT 5 para el proceso APO13, y sus dimensiones comunes, es decir, las metas, interesados, ciclo de vida, y las buenas prácticas aplicables.

Los resultados obtenidos permiten concluir que se requiere la definición y actualización periódica de un perfil de riesgos de la seguridad de la información, el cual se utilice como un instrumento base para dirigir las estrategias e iniciativas de la seguridad de la información, aunado a una revisión integral de las estructuras organizativas requeridas para dirigir las actividades estratégicas y de gobierno de la seguridad de la información, las cuales, en la actualidad, carecen de la visibilidad suficiente para generar valor y coadyuvar a la protección de los activos de información del Banco.

Lista de Tablas

Tabla 1 – Inventario de Riesgos de la Seguridad de la Información del Banco Popular 17

Tabla 2 – Prácticas de Gestión del Proceso APO13 de COBIT 5 19

Tabla 3 – Metas del Proceso APO13 de COBIT 5 21

Tabla 4 – Mapeo de COBIT 4.1 con COBIT 5.....21

Tabla 5 – Comparación de estructuras organizativas COBIT 5 y Banco Popular 23

Tabla 6 – Mapeo de metas de TI del Proceso APO13 con objetivos del PETI del Banco Popular 25

Lista de Figuras

Figura 1 - Estructuras Organizacionales del Banco Popular relacionadas con la Gestión de Seguridad de la Información 15
Figura 2 - Matriz RACI - Proceso APO13 COBIT 5 22
Figura 3 - Matriz RACI - del Proceso DS5 conforme estructura del Banco Popular 23
Figura 4 - Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y el Proceso APO13 24
Figura 5 - Mapeo entre las Metas Corporativas de COBIT 5 y las Metas relacionadas con TI en Proceso APO13 26
Figura 6 - Proceso de Aseguramiento/auditoría según COBIT for Assurance 27
Figura 7- Enfoque genérico del programa de auditoría 30
Figura 8 Metas que forman parte del Alcance de la Evaluación 57

Lista de Abreviaturas

- ISO: Organización Internacional de Estandarización
- BYOD: Traer tu propio dispositivo (Bring Your Own Device)
- CISM: Certificación en Gestión de la Seguridad de la Información
- SUGEF: Superintendencia General de Entidades Financieras
- COBIT: Objetivos de Control para la información y tecnologías relacionadas
- APO: Domino de COBIT 5 – Alinear, planificar y organizar
- DSS: Domino de COBIT 5 – Entregar, dar servicio y soporte
- GPO's: Objetos de directiva de grupo en el Active Directory
- PKI: Infraestructura de llave pública
- SGSI: Sistema gestor de la seguridad de la información
- CISO: Director de Gestión de la Seguridad de la Información
- RACI: Modelo de roles y responsabilidades: R(responsable), A (quien rinde cuentas), C (consultado), I (informado)
- PETI: Plan Estratégico de Tecnología de Información

CAPÍTULO I
INTRODUCTORIO

1. Introducción

Según la Norma ISO/IEC 27002: *“La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada”; por tanto,* siendo la confianza la base del negocio bancario, la seguridad de la información, definida como el conjunto de medidas implementadas en una organización para mantener la integridad, confiabilidad y disponibilidad de la información, constituye un pilar fundamental de la banca, para la adecuada protección de uno de sus activos más importantes, como lo es la información, además de asegurar la continuidad del negocio y maximizar el retorno de la inversión, principalmente ante dos circunstancias actuales: el avance tecnológico y la delincuencia informática.

En primer lugar, el auge de nuevas tendencias tecnológicas, como los servicios en la nube, BYOD y la banca móvil, han borrado las fronteras de las redes de datos empresariales, obligando a las áreas de tecnología de información a replantear su visión de la seguridad de la información, para que sus infraestructuras tecnológicas adquieran la capacidad de adaptarse a este nuevo nivel de acceso y consumo de datos.

Por otra parte, el crecimiento exponencial de nuevas amenazas a través de Internet por medio de métodos cada vez más sofisticados de propagación de código malicioso, mantiene en alerta a las entidades financieras, al ser objetivos atractivos para los delincuentes informáticos que buscan sustraer información sensible de las bases de clientes y de los productos y servicios bancarios, principalmente lo relativo a los datos de los titulares de las tarjetas de crédito.

Para las organizaciones, “*lograr los niveles adecuados de seguridad de la información a un costo razonable requiere una buena planificación, una estrategia efectiva y una administración capaz. La gestión del programa de seguridad de la información es un requerimiento continuo y constante que sirve para proteger los activos de información, cumplir con las obligaciones regulatorias y minimizar*

posibles exposiciones legales y de responsabilidad civil." (ISACA - CISM, 2011, pág. 156)

Este sistema de gestión de la seguridad de la información constituye "la parte del sistema de gestión global, basada en un enfoque hacia los riesgos de un negocio, para establecer, implementar, operar, dar seguimiento, revisar, mantener y mejorar la seguridad de la información". (ISO/IEC 27002, p.9).

Desde de un punto de vista normativo, en nuestro país las entidades financieras supervisadas por la Superintendencia de Entidades Financieras deben acatar de manera obligatoria lo dispuesto en el acuerdo SUGEF 14-09 *Reglamento sobre la Gestión de la Tecnología de Información*, que establece en su artículo N°20. Estándar de seguridad lo siguiente:

> Sin menoscabo de los objetivos de control de los procesos aplicables de Cobit®, la entidad debe velar que el estándar, en materia de seguridad, permita implementar métodos de autenticación para el acceso lógico a los sistemas y servicios informáticos, consecuentes con la criticidad y el valor de los datos y servicios a proteger, debiendo considerar en particular la mejores prácticas en relación con la banca electrónica y otros servicios financieros por Internet.

En el caso particular de las entidades financieras del sector público costarricense, las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la Contraloría General de la República, plantean en el apartado 1.4 Gestión de la Seguridad de la Información que:

> La organización debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa.

Es por esta razón que la evaluación periódica de la efectividad y suficiencia del programa de gestión de la seguridad de la información en las entidades financieras representa una actividad fundamental para las auditorías de

tecnologías de información, en su función asesora y fiscalizadora en procura de coadyuvar conforme a sus competencias, en la mejora constante de los sistemas de control interno de las organizaciones.

2. Justificación

El interés profesional de desarrollar este proyecto, basado en la evaluación de un programa de gestión de la seguridad de la información, radica en la oportunidad de aplicar las técnicas y conocimientos adquiridos durante la Maestría Profesional en Auditoría de Tecnologías de Información en un tema que constituye la base para la especialización en el campo de la auditoría de la seguridad de la información, como área técnica especializada de gran interés que constituye todo un reto para los auditores en la era tecnológica actual.

El Banco Popular como una de las entidades líderes en la prestación de productos y servicios en el sector financiero costarricense, en cumplimiento de la normativa aplicable en materia de seguridad de la información, debe conocer y gestionar los riesgos y amenazas que atenten contra sus activos de información; esto a través de la implementación y seguimiento de un plan de gestión de la seguridad de la información.

Por tanto, este proyecto pretende mediante la aplicación de una metodología de auditoría basada en riesgos el desarrollo y aplicación de un programa de auditoría para la evaluación del sistema para la gestión de la seguridad de la información del Banco Popular, el cual sirva de base para evaluaciones futuras del nivel de madurez de la seguridad de la información que la entidad vaya adquiriendo en el tiempo.

3. Objetivos

Objetivo General

Evaluar por medio de una auditoría basada en riesgos que el sistema de gestión de la seguridad de la información del Banco Popular garantiza, de una manera razonable, la confidencialidad, integridad y disponibilidad de la información, dentro de los niveles de apetito de riesgo aprobados.

Objetivos específicos

- Verificar si se cuenta con el apoyo gerencial para obtener acceso a los recursos requeridos para implementar las iniciativas y estrategias que demanda un sistema de gestión de la seguridad de la información.

- Determinar si la infraestructura tecnológica que soporta el sistema para la gestión de la seguridad de la información controla los eventos de seguridad en tiempo real, que permita adoptar las medidas oportunas en caso de amenazas e incidentes.

- Evaluar la suficiencia de los procesos implementados para monitorear la eficacia continua de los programas de concientización organizacional en torno a la seguridad de la información, que permitan una mitigación de las amenazas que puedan generar las acciones del personal o factores externos.

- Determinar si el sistema de gestión de la seguridad de la información se encuentra alineado con la gestión de riesgos de la tecnología de la información definidos en la Institución.

4. Alcance

El proyecto se enfocará en la ejecución de una auditoría por riesgos para evaluar la suficiencia y eficacia del sistema de gestión de la seguridad de la información que actualmente se está implementado en el Banco Popular, verificando su alineación con los requerimientos del negocio, su relación con el apetito de riesgo establecido y su alcance para la protección de los activos de información, considerando las iniciativas de inversión y procesos en operación durante el período 2013-2014.

5. Marco teórico

Para implementar un sistema de gestión de la seguridad de la información, la utilización de un marco de estándares como ISO/IEC 27001 o COBIT pueden servir como una guía práctica para que las entidades desarrollen requisitos de seguridad e implementen prácticas de gestión de seguridad, ayudando de esta manera a fortalecer sus mecanismos de control de la seguridad de la información, mediante la generación de valor de las inversiones y recursos orientados a este fin, alineados al cumplimiento de objetivos estratégicos y apetito de riesgo.

COBIT 5 es un marco de negocio para el gobierno y la gestión de las tecnologías de información, desarrollado por ISACA, el cual incorpora las ideas más recientes en las técnicas de gobierno y de gestión empresarial, y proporciona principios globalmente aceptados, prácticas, herramientas analíticas y modelos para ayudar a aumentar la confianza y el valor de los sistemas de información. Así mismo, integra principios de otros marcos principales, normas y recursos, incluyendo Val IT de ISACA y Risk IT, ITIL® y las normas internacionales ISO. (http://cobitonline.isaca.org/about)

Referente a la seguridad de la información, el modelo de referencia de proceso de COBIT 5 incluye en el dominio: *Alinear, Planificar y Organizar*, el proceso *APO13*

Gestionar la Seguridad, proceso que incluye la definición, operación y supervisión de un sistema para la gestión de la seguridad de la información, con el propósito de mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa. Desde un punto de vista operativo, en el dominio: *Entregar, dar Servicio y Soporte*, COBIT 5 incorpora el proceso *DSS05 Gestionar los Servicios de Seguridad*, el cual incluye la protección de la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Estableciendo y manteniendo los roles de seguridad y privilegios de acceso de la información y realizando la supervisión de la seguridad, con el propósito de minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos que puedan ocurrir.

Por su parte, el estándar para la seguridad de la información ISO/IEC 27001 Tecnología de la información —Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos) y el estándar de control asociado ISO/IEC 27002 proporcionan un marco ampliamente aceptado para la gestión de la seguridad de la información. En este marco se especifican los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información según el famoso “Ciclo de Deming”: PDCA - acrónimo de Plan, Do, Check, Act (PHVA - Planificar, Hacer, Verificar, Actuar).

La norma internacional ISO/IEC 27001-2008 se divide en 11 Dominios de Control: A.5 Política de Seguridad, A.6 Organización de Seguridad de la Información, A.7 Gestión de Activos, A.8 Seguridad en Recursos Humanos, A.9 Seguridad Física y Ambiental, A.10 Gestión de operaciones y Comunicaciones, A.11 Control de Acceso, A.12 Adquisición, desarrollo y mantenimiento de Sistemas, A.13 Gestión de Incidentes de Seguridad de la Información, A.14 Gestión de la Continuidad del Negocio y A.15 Cumplimiento.

Conforme lo señala la norma internacional ISO/IEC 27001, la auditoría del sistema de gestión de la seguridad de la información debe determinar si los objetivos de control, los controles, los procesos y los procedimientos cumplen con los

requerimientos de esta norma y regulaciones relacionadas; además, si el sistema de gestión fue diseñado e implementado conforme los requisitos identificados de la seguridad de la información y se mantiene operando de manera eficaz y acorde a lo esperado.

6. Procedimiento metodológico

La aplicación de una metodología de auditoría basada en riesgos supone que el auditor desarrolle su plan de trabajo basado en una valoración de los riesgos de la entidad, considerando los criterios que fueron utilizados por la alta dirección de la organización para establecer su apetito de riesgo, haciendo especial énfasis en los procesos que representen una mayor amenaza para el cumplimiento de los objetivos estratégicos de la entidad bancaria, en lo relativo a la seguridad de la información.

Como marcos de trabajo se ha seleccionado la más reciente revisión del Marco de Trabajo de Referencia para el Gobierno y Administración de la Tecnología de Información Empresarial COBIT 5 y la Norma Internacional ISO/IEC 27001.

En la ejecución del trabajo de campo se desarrollará una guía de pruebas específica para la evaluación del sistema de gestión de la seguridad de la información del Banco Popular, alineada a los objetivos de la evaluación, utilizando como documento base la guía genérica de aseguramiento de auditoría del proceso de COBIT 5, APO13 Gestionar la seguridad.

Esta guía será utilizada como una herramienta de comprobación del nivel de madurez actual de la entidad bancaria, respecto a la implementación del sistema de gestión de la seguridad de la información, cuyos resultados permitirán establecer las recomendaciones que agreguen valor a la Institución.

7. Contenido capitulario

El presente proyecto está conformado por cinco capítulos que contienen la siguiente información:

Capítulo I, Introductorio: se inicia con una introducción del tema de estudio, su justificación, objetivo general y objetivos específicos, alcance de la auditoría y el fundamento teórico que dará sustento a los criterios desarrollados en el programa de auditoría sobre el sistema de gestión de la seguridad de la información.

Capítulo II, Conocimiento del Proceso: este capítulo contiene una reseña general del Banco Popular, destacando el diagnóstico de la situación actual entorno a la implementación del sistema de gestión de la seguridad de la información, así como una descripción de los principales procesos a evaluar y aspectos generales de las principales áreas auditadas que serán consideradas en el desarrollo del programa de auditoría.

Capítulo III, Programa de Auditoría: describe y desarrolla un programa de auditoría basado en la guía genérica de aseguramiento de auditoría del proceso de COBIT 5, APO13 Gestionar la seguridad.

Capítulo IV, Resultados de la evaluación: describe los resultados obtenidos en la ejecución del programa de auditoría.

Capítulo V, Informe final del programa de auditoría: corresponde a la comunicación de los principales hallazgos obtenidos como resultado de la aplicación del programa de auditoría, junto con las recomendaciones pertinentes para la implementación de mejoras al sistema de gestión de la seguridad de la información del Banco Popular.

CAPÍTULO II
CONOCIMIENTO DEL PROCESO

1. Aspectos generales del Banco Popular

El Banco Popular y de Desarrollo Comunal es una institución de Derecho Público no estatal, con personería jurídica y patrimonio propio, con plena autonomía administrativa y funcional, así lo indica el artículo 2 de su Ley Orgánica. (1969, p.1). Además, está sujeto a la fiscalización de la Superintendencia General de Entidades Financieras (SUGEF) y de la Contraloría General de la República (CGR). Para Fonrouge (citado por Escoto Leiva, 2001): “los entes públicos no estatales son ‘órganos’ que colaboran en las funciones del Estado, pero segregados de la administración general” (…), son creados por ley, actúan según las normas del derecho público y tienen a su cargo la ejecución de cometidos públicos, cuya finalidad justifica su régimen particular. (p.46).

Conforme con lo señalado en el artículo 47 de la Ley Orgánica del Banco, la entidad forma parte del Sistema Bancario Nacional y tiene las mismas atribuciones, responsabilidades y obligaciones que les corresponden a los bancos, de conformidad con lo establecido en la Ley Orgánica del Banco Central, la Ley Orgánica del Sistema Bancario Nacional y las demás leyes aplicables. Por tanto, debe mantener indicadores de desempeño y gestión de alta calidad y un efectivo nivel de seguridad en las transacciones que realizan sus clientes.

La entidad posee el 100% de las acciones de capital de las siguientes sociedades: Popular Sociedad de Fondos de Inversión. S.A., Popular Valores Puesto de Bolsa, S.A., Operadora de Planes de Pensiones Complementarias, S.A. y Popular Sociedad Agencia de Seguros, S.A. Estas subsidiarias en conjunto con el Banco Popular integran el Conglomerado Financiero Banco Popular.

El Banco Popular posee una alta orientación hacia la economía social, con la finalidad de fomentar el ahorro y satisfacer las necesidades de crédito de la clase trabajadora; de esta forma, uno de sus objetivos es promover el crecimiento económico y social de forma sostenible de personas, grandes empresas, instituciones, mipymes y organizaciones sociales del país.

La orientación de la política general del Banco corresponde a la Asamblea de los Trabajadores, su definición a la Junta Directiva Nacional y la administración a la Gerencia General Corporativa.

Los resultados del Sistema Financiero Nacional, al cierre del 2014, muestran que el Banco Popular obtuvo el tercer lugar en utilidad total, con una rentabilidad sobre el patrimonio del 7%, la cual se encuentra dentro de la media del mercado financiero. También posee el tercer lugar en activo total y el segundo lugar en patrimonio. Esto demuestra su solidez financiera y su alto nivel de suficiencia patrimonial con respecto a la competencia.

Actualmente, la entidad se encuentra en un período de transición de su infraestructura tecnológica, en donde, su Core Bancario será actualizado a una plataforma de avanzada, mediante la cual, espera brindar más y mejores productos y servicios con un alto valor percibido para sus clientes. Por otra parte, la entidad está finalizando la construcción e implementación de un centro de procesamiento de datos primario de alta tecnología, certificado TIER III por el Uptime Institute, ubicándose como una de las instalaciones para el procesamiento de datos de misión crítica más seguras y eficientes de la región.

2. Gestión de la seguridad de la información en el Banco Popular

La Política de Seguridad de la Información del Banco define la seguridad de la información "*como el conjunto de medidas preventivas y reactivas que permitan resguardar y proteger la información, con el fin de preservar las siguientes características:*

- *Confidencialidad: aseguramiento de que la información sea accesible sólo por quienes están autorizados para ello.*

- *Integridad: salvaguardia de la exactitud y totalidad de la información y de los métodos de procesamiento de la información, así como de las modificaciones realizadas por entes debidamente autorizados.*

- *Disponibilidad: aseguramiento de que los usuarios autorizados tengan acceso oportuno a la información y sus métodos de procesamiento."*

Al respecto, la Dirección de Gestión del Banco es la responsable de documentar un Plan de Gestión de Seguridad de la Información, velar por su correcta planificación, ejecución, seguimiento, mejora y actualizarlo: el cual debe incluir todos los principios de seguridad del Banco (Integridad, disponibilidad y confidencialidad), así como las estrategias por implementar para lograr esos principios.

El alcance de la seguridad de la información se estipula en el *Reglamento de Seguridad de la Información del Conglomerado Financiero Banco Popular y de Desarrollo Comunal* e indica lo siguiente:

> *"ARTÍCULO 6.- Alcance de la Seguridad de la Información*
>
> *La Seguridad de la Información cubre todas las áreas del Conglomerado con la finalidad de proteger los activos de información, tanto en formato físico como digital, así como las tecnologías utilizadas para su almacenamiento y procesamiento frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, autenticidad, responsabilidad, no repudiación y confiabilidad de la información."*

Así mismo, el ámbito de regulación, control y monitoreo de la seguridad de la información se establece en el Artículo 4 del mismo Reglamento e incluye lo siguiente:

1. Calidad de la información
2. Programa de Seguridad de la Información
3. Protección de la información del Conglomerado
4. Gestión de riesgos de seguridad
5. Gestión de cumplimiento de seguridad
6. Gestión de identidad y de accesos
7. Gestión de vulnerabilidades y amenazas
8. Gestión de activos de información
9. Gestión de continuidad del negocio

10. Gestión de incidentes
11. Gestión física y de ambiente
12. Gestión de aplicaciones
13. Capacitación y concienciación de seguridad
14. Capital Humano.

En 2010, se establecieron las responsabilidades para atender de manera integral los elementos relacionados con la seguridad de la información, a fin de dar cumplimiento a leyes y regulaciones de seguridad de la información; asignándose la función de Seguridad de la Información al Proceso de Gestión Estratégica Tecnológica Corporativa. Posteriormente, producto de un proceso de reorganización implementado en 2013, la Dirección de Gestión a través de la Unidad de Continuidad del Negocio asume dicha función.

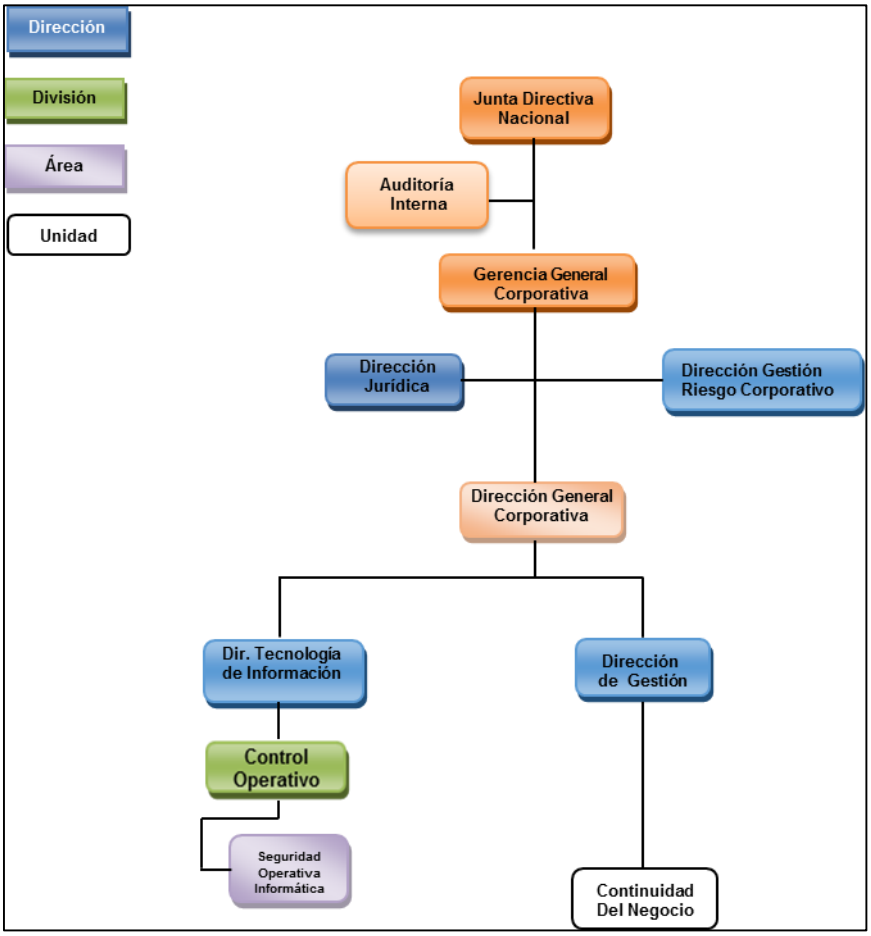
La Dirección de Tecnología de Información del Banco cuenta con un área técnica especializada en la función de seguridad informática, encargada de la gestión operativa de los servicios de seguridad de la información, cuya finalidad consiste en garantizar razonablemente la integridad de los datos, mediante la protección y monitoreo de la infraestructura tecnológica, el análisis de vulnerabilidades y la atención de incidentes de seguridad.

Los servicios más representativos que gestiona el Área de Seguridad Operativa Informática se indican a continuación:

a. Protección contra *software* malicioso
b. Análisis de vulnerabilidades *web*
c. Monitoreo de sistemas de prevención/detección de intrusiones (IPS/IDS)
d. Filtrado de navegación *web*
e. Filtrado de correo SMTP
f. Definición y mantenimiento de políticas de la red (GPO’s)
g. Gestión de la infraestructura de llave pública (PKI)
h. Gestión de identidades y accesos
i. Asesoría en aspectos de definición de controles de seguridad de la información.

Las áreas funcionales del Banco con responsabilidades directas entorno al sistema de gestión de la seguridad de la información, son la Unidad de Continuidad del Negocio y el Área de Seguridad Operativa Informática, las cuales se ubican en la estructura organizacional como se muestra a continuación:

Figura 1 - Estructuras Organizacionales del Banco Popular relacionadas con la Gestión de Seguridad de la Información



Fuente: Estructura Organizacional Banco Popular 2015

Así mismo, otras áreas del Banco poseen roles que brindan soporte a diversos procesos de la seguridad de la información, entre ellas se menciona a la Dirección de Gestión de Riesgo Corporativo, División de Seguridad Bancaria, División de Infraestructura y Proyectos, Dirección de Capital Humano, División de Operación de la Producción y el Área de Atención al Cliente Interno, además de las áreas del negocio propietarias de activos de información.

El Banco cuenta con reglamentos, directrices, políticas y guías que conforman la normativa interna relacionada con la seguridad de la información. En orden jerárquico se cuenta con un Reglamento Corporativo de Seguridad de la Información, una Política General de Seguridad de la Información y normativa específica que regula diversos procesos y actividades de la entidad, entre las cuales, se mencionan las siguientes:

- Directriz de Clasificación de la información
- Directriz de integridad y calidad de la información
- Directriz del sistema de gestión de la seguridad de la información
- Directriz para administración de dispositivos móviles
- Directriz de control de acceso a terceros
- Política para manejo de incidentes de seguridad de la información
- Política para publicaciones en redes sociales y blogs
- Política de protección física de equipos de cómputo
- Política de acceso y uso de Internet
- Política de uso de antivirus
- Política de uso del correo electrónico
- Política de utilización de la red para la transmisión de datos
- Política de gestión de parches y actualizaciones
- Política para gestión de accesos físicos
- Política de administración del *Firewall*
- Política de certificados digitales
- Política de sistema de detección de intrusos
- Políticas de horarios y acceso físico
- Política de seguridad en equipos de redes

La Dirección de Riesgo Corporativo del Banco es la responsable de gestionar el desarrollo de las actividades propias de la gestión de riesgos de seguridad de la información, entre las cuales, realizar la valoración integral de riesgos, la cual considera la identificación de eventos de seguridad y las debilidades asociadas a

los sistemas de información. La matriz de valoración de riesgos vigente incluye los siguientes eventos:

Tabla 1 – Inventario de Riesgos de la Seguridad de la Información del Banco Popular

No.	Nombre del evento
SI-15	Pérdidas por transacciones fraudulentas debido a la falta de educación de los clientes en la identificación de técnicas de ingeniería social.
SI-16	Pérdidas por transacciones fraudulentas a causa de suplantación de identidad del cliente.
SI-7	Pérdidas por el pago de demandas a causa de uso de *software* no autorizado, no licenciado y archivos no autorizados
SI-1	Pérdidas por demandas en la existencia de abuso de los privilegios de acceso a la información para beneficio propio debido a debilidades/ausencia de mecanismos de control.
SI-12	Pérdidas por intromisiones debido a debilidades en el proceso de manejo de incidentes de seguridad informática.
SI-18	Pérdidas por transacciones fraudulentas a causa de falta de educación de los usuarios con respecto a políticas de seguridad (compartir claves, no bloqueo de computadores).
SI-21	Pérdidas por demandas de robo o divulgación de información de los clientes al suministrar datos reales para desarrollos
SI-9	Pérdidas por intromisiones a causa de acceso a sitios *web* no seguros.
SI-17	Pérdidas por transacciones fraudulentas a causa de vulnerabilidades en los mecanismos de seguridad en los sistemas, tales como sistemas operativos y aplicaciones.
SI-20	Pérdidas por intromisiones a causa de vulnerabilidades sobre el uso de dispositivos móviles con acceso a la red del Banco.
SI-22	Pérdidas por demandas de robo o divulgación de información de los clientes al utilizar servicios en la nube.
SI-3	Pérdidas por demandas en la existencia de robo, alteración o destrucción de información a causa de suplantación de identidad.
SI-8	Pérdidas por intromisiones en los dispositivos y equipos por aprovechamiento de las vulnerabilidades.
SI-10	Pérdidas por intromisiones en los dispositivos y equipos a causa de una mala configuración de estos.
SI-13	Pérdidas por intromisiones por la ausencia de mecanismos de prevención y detección a causa de concentración de funciones del personal.
SI-6	Pérdidas por denegación del servicio a causa de explotación de vulnerabilidades.
SI-2	Pérdidas por demandas en la existencia de robo, alteración o destrucción de información por falta de una adecuada administración de usuarios y cuentas.
SI-4	Pérdidas por demandas en la existencia de robo, alteración o destrucción de información a causa de vulnerabilidades de los sistemas operativos, herramientas y aplicativos.
SI-5	Pérdidas por demandas en la existencia de robo o divulgación de información de los clientes por ausencias de políticas de clasificación de la información.

SI-11	Pérdidas por intromisiones a causa de un deficiente monitoreo de la red y de los equipos.
SI-19	Pérdidas por interrupción de servicios por daños intencionales en los dispositivos o equipos a causa de ataques de personal interno y debilidades en la gestión de accesos.
SI-14	Pérdidas por transacciones fraudulentas a causa de la ausencia de políticas de seguridad en los desarrollos.

Fuente: Taller de revaloración de riesgos 2013. Proceso Administración de la Seguridad de la Información

En 2011, por medio de una licitación abreviada, el Banco contrató los servicios de un consultor para la elaboración de un plan de gestión de seguridad de la información en concordancia con la norma ISO/IEC 27001. Conforme a los resultados presentados por el contratista, se generaron 26 iniciativas para ser implementadas a un horizonte de 5 años. Adicionalmente, presentó los siguientes entregables:

a. Diagnóstico del contexto y situación actual, así como del nivel de madurez del SGSI del Banco.
b. Recomendaciones, planes de acción y propuestas de mejora para mejorar en el corto plazo el SGSI del Banco.
c. Propuesta de una Política de Seguridad de la información institucional basada en la Norma ISO/IEC 27001 e ISO/IEC 27002. Procedimientos y plantillas de procesos generales de seguridad de la información y calidad de la información.
d. Propuesta de un Plan de Gestión de la Seguridad de la Información, según el estándar internacional ISO/IEC 272001 e ISO/IEC 272002.
e. Propuesta de estructura administrativa de la unidad de la Seguridad de la información en el Banco.

El desarrollo de un Programa Corporativo de Seguridad de la Información, alineado a las mejores prácticas en Gestión de la Seguridad de la Información, de conformidad con ISO/IEC27000 y COBIT, es una iniciativa a cargo de la Dirección de Gestión, con el patrocinio de la Gerencia General Corporativa.

Al respecto, conforme lo señalado en el capítulo 7 del Reglamento de Seguridad Informática del Conglomerado Financiero Banco Popular, "*le corresponde a la Gerencia General Corporativa o Gerencias Generales promover la divulgación de*

las disposiciones de Seguridad de la Información a todos los usuarios, así como proveer los recursos necesarios para gestionar el Sistema de Gestión de Seguridad de la Información en todas sus fases."

3. COBIT 5 - APO13 Gestionar la Seguridad

COBIT 5 incorpora en su dominio: *Alinear, Planificar y Organiza*r, el proceso *APO13 Gestionar la Seguridad,* el cual incluye la definición, operación y supervisión de un sistema para la gestión de la seguridad de la información. Este marco de negocio para el gobierno y gestión de las tecnologías de información, se alinea con otros estándares y marcos de referencia relevantes, tal como a la norma internacional ISO/IEC 27001 y, por tanto, permite al auditor usar COBIT 5 y las herramientas de soporte publicadas por ISACA como el marco integrador y la base para el desarrollo de evaluaciones al sistema de gestión de la seguridad de la información. Por tanto, a pesar que el Banco Popular aplique en este momento el marco de referencia de COBIT 4.0 para cumplir con aspectos regulatorios de la normativa SUGEF 14-09, no resultaría adecuado evaluar la Gestión de la Seguridad de la Información con ese marco de referencia, puesto que el proceso *DS5 Garantizar la Seguridad de los sistemas* se basa en aspectos más operativos que estratégicos, asignando la responsabilidad a la Dirección de TI y no a la figura de un CISO, tal y como se establece en COBIT 5.

El proceso APO13 Gestionar la Seguridad de COBIT 5, se compone de 3 prácticas claves de gestión, con la siguiente estructura:

Tabla 2 – Prácticas de Gestión del Proceso APO13 de COBIT 5

Práctica de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
APO13.01 Establecer y mantener un SGSI. Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineados con los requerimientos de negocio y la gestión de seguridad en la	Fuera del Ámbito de COBIT	Enfoque de seguridad de la empresa	Política de SGSI	Interno
			Declaración de alcance del SGSI	APO01.02 DSS06.03

empresa.				
Actividades				
1. Definir el alcance y los límites del SGSI en términos de las características de la empresa, la organización, su localización, activos y tecnología. Incluir detalles de y justificación para cualquier exclusión del alcance.				
2. Definir un SGSI de acuerdo con la política de empresa y alineada con la empresa, la organización, su localización, activos y tecnología.				
3. Alinear el SGSI con el enfoque global de la gestión de la seguridad en la empresa.				
4. Obtener autorización de la dirección para implementar y operar o cambiar el SGSI.				
5. Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.				
6. Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información.				
7. Comunicar el enfoque de SGSI.				
Práctica de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información. Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio.	APO02.04	Diferencias y cambios necesarios para alcanzar la capacidad objetivo	Plan de tratamiento de riesgos de seguridad de la información	Todo EDM Todo APO Todo BAI Todo DSS Todo MEA
	APO03.02	Descripciones de dominios de partida y definición de arquitectura	Casos de negocio de seguridad de información	APO02.05
	APO12.05	Propuestas de proyectos para reducir el riesgo		
Actividades				
1. Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura de la empresa. Asegurar que el plan identifica las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, las responsabilidades y las prioridades asociadas para gestionar los riegos identificados de seguridad de información.				
2. Mantener un inventario de componentes de la solución implementados para gestionar los riesgos relacionados con la seguridad como parte de la arquitectura de la empresa.				
3. Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad de la información, sustentados en casos de negocio adecuados que incluyan consideren la financiación la asignación de roles y responsabilidades.				
4. Proporcionar información para el diseño y desarrollo de prácticas de gestión y soluciones seleccionadas en base al plan de tratamiento de riesgos de seguridad de información.				
5. Definir la forma de medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizar estas mediciones para evaluar la efectividad y producir resultados reproducibles y comparables.				
6. Recomendar programas de formación y concienciación en seguridad de la información.				
7. Integrar la planificación, el diseño, la implementación y la supervisión de los procedimientos de seguridad de información y otros controles que permitan la prevención y detección temprana de eventos de seguridad, así como la respuesta a incidentes de seguridad.				
Práctica de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
APO13.03 Supervisar y revisar el SGSI. Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir	DSS02.02	Incidentes clasificados y priorizados y requerimientos de servicios	Informes de auditoría del SGSI	MEA02.01
			Recomendaciones para mejorar el SGSI	Interno

recurrencias. Promover una cultura de seguridad y de mejora continua.				
Actividades				
1. Realizar revisiones periódicas del SGSI, incluyendo aspectos de políticas, objetivos y prácticas de seguridad del SGSI. Considerar los resultados de auditorías de seguridad, incidentes, resultados de mediciones de efectividad, sugerencias y retroalimentación de todas las partes interesadas.				
2. Realizar auditorías internas al SGSI a intervalos planificados.				
3. Realizar revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI.				
4. Proporcionar información para el mantenimiento de los planes de seguridad para que consideren las incidencias de las actividades de supervisión y revisión periódica.				
5. Registrar las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI.				

Fuente: COBIT 5. Procesos Catalizadores

Los objetivos y metas del proceso APO13 Gestionar la Seguridad son los siguientes:

Tabla 3 – Metas del Proceso APO13 de COBIT 5

Meta del Proceso	**Métricas Relacionadas**
1. Está en marcha un sistema que considera y trata efectivamente los requerimientos de seguridad de la información de la empresa.	• Número de roles de seguridad claves claramente definidos • Número de incidentes relacionados con la seguridad
2. Se ha establecido, aceptado y comunicado por toda la empresa un plan de seguridad.	• Nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa • Número de soluciones de seguridad que se desvían del plan • Número de soluciones de seguridad que se desvían de la arquitectura de la empresa
3. Las soluciones de seguridad de la información están implementadas y operadas de forma consistente en toda la empresa.	• Número de servicios con alineamiento confirmado al plan de seguridad • Número de incidentes de seguridad causados por la no observancia del plan de seguridad • Número de soluciones desarrolladas con alineamiento confirmado al plan de seguridad

La normativa SUGEF 14-09, Reglamento sobre la gestión de la tecnología de información, evalúa la gestión de TI basada en el marco conceptual de la versión 4.0 de Cobit; por tanto, en términos de la gestión de seguridad de la información, al Banco le corresponde contar con un nivel de madurez 3, en el proceso *DS5 Garantizar la seguridad de los sistemas*, el cual, como se indicó anteriormente, corresponde a funciones y actividades más operativas.

Los objetivos de control del proceso DS5 Garantizar la seguridad de los sistemas, de la versión COBIT 4.1 que fueron cubiertos por el proceso APO13 Gestionar la Seguridad de COBIT 5, son los siguientes:

Tabla 4 – Mapeo de COBIT 4.1 con COBIT 5

Objetivo de Control de COBIT 4.1*	Cubierto en COBIT 5 por:
DS5.1 Administración de la Seguridad de TI	APO13.01; APO13.03
DS5.2 Plan de Seguridad de TI	APO13.02

*Nota: El Proceso DS5 Garantizar la seguridad de los sistemas de la versión COBIT 4.0 a la versión COBIT 4.1, no sufrió modificaciones importantes.
Fuente: COBIT 5. Procesos Habilitadores.

Respecto a las metas del proceso DS5 Garantizar la seguridad de los sistemas, en lo relacionado con el proceso APO13 de COBIT 5, no se evidenció en el Banco, la existencia de métricas de desempeño del proceso para los objetivos de control DS5.1 y DS5.2.

La designación de roles y responsabilidades, descritas en la matriz RACI (Responsable de que se haga, Responsable de la verificación, Consultado e Informado para una tarea), del proceso APO13 de COBIT 5, es la siguiente:

Figura 2 - Matriz RACI - Proceso APO13 COBIT 5

Prácticas de Gestión Clave	Director General Ejecutivo (CEO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los procesos de negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Director de Riesgo	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura Empresarial	Comité de Riesgos Corporativos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración de TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad del Negocio	Gestor de Privacidad de la información
APO13.01 Establecer y mantener un SGSI.	C	C	C	I	C	I	I	C	A	C	C	C	C	R	I	I	I	R	I	R	C	C
APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	C	C	C	C	C	I	I	C	A	C	C	C	C	R	C	C	C	R	C	R	C	C
APO13.03 APO13.03 Supervisar y revisar el SGSI.			C	C	C		R		A			C	C	R	R	R	R	R	R	R	R	R

Fuente: COBIT 5. Procesos Catalizadores

Conforme la matriz RACI descrita en el proceso APO13, la responsabilidad por la rendición de cuentas en cuanto a la gestión de la seguridad de la información le

corresponde al Director de Seguridad de la Información (CISO), figura que actualmente no existe en la estructura organizacional del Banco.

Así mismo, en el marco de trabajo de COBIT 4.0, en la matriz RACI del proceso DS5 Garantizar la seguridad de los sistemas, no existe la figura del CISO, por tanto, la responsabilidad sobre la definición y mantenimiento de un plan de seguridad de TI le corresponde al Director de Tecnología de Información (CIO). Esta situación, se refleja en la matriz RACI diseñada por el Banco, como parte de los insumos para el cumplimiento de la normativa SUGEF 14-09, en donde la gestión del proceso DS5 y la definición del plan de seguridad de TI, se visualizó como labores operativas y quedaron a cargo de áreas dentro de la Dirección de TI, tal y como se detalla en la matriz adjunta:

Figura 3 - Matriz RACI - del Proceso DS5 conforme estructura del Banco Popular

	Actividades	Dirección Tecnología Información	División Control Operativo	División Desarrollo	División Operación Producción	Área Aseg de Calidad	Área Admón Sourcing	Área Atención Cliente Interno	Área Seguridad Operativa Informática	Gestor de la Seguridad Informática	Área Desarrollo Sistemas	Área Admón y Des Proyectos	Área Investigación Tecnológica	Área Redes y Telecomunic	Área Soporte Técnico	Área Manten Sistemas	Área Cómputo	CITI	División Gestión Talento Humano	Cliente interno/ Usuario
Planificar el Proceso de Garantizar la Seguridad de los sistemas																				
1.1	Revisar y generar directrices, políticas e indicadores de gestión	R	I	I	I	I	I	I	A	R	I	I	I	I/C	I/C	I	I/C	R		
1.2	Revisar documentación base del proceso	R	I	I	I	I	I	I	A	R	I	I	I	I/C	I/C	I	I/C	R		
	Definir y mantener un plan de seguridad de TI																			
2.1	Elaboración del plan de seguridad de TI.	I	A/C	I/C	I/C	I/C	I	I/C	R		I/C	I/C	I/C	I/C	I/C		I/C	R		
2.2	Seguimiento del plan de seguridad de TI	I	A/C						R											
2.3	Actualizar el Plan de Seguridad de TI	I	A/C	I/C	I/C	I/C	I	I/C	R		I/C	I/C	I/C	I/C	I/C		I/C	R		
	Reportar el Desempeño del Proceso.																			
7.1	Generar informes de resultados	I	I						A	R										

*Una gráfica RACI identifica quién es **R**esponsable, a quién debe rendir cuentas (**A**), quién debe ser **C**onsultado y/o **I**nformado*

Fuente: Proceso Garantizar la Seguridad de los Sistemas. Banco Popular. Mayo 2014

A continuación, se presenta un mapeo entre las estructuras organizativas definidas en COBIT 5 y la estructura organizativa del Banco:

Tabla 5 – Comparación de estructuras organizativas COBIT 5 y Banco Popular

Roles y Estructuras Organizativas de COBIT 5	Estructura Organizacional del Banco Popular
Director General Ejecutivo (CEO)	Gerencia General Corporativa
Director de Operaciones (COO)	Subgerencia General de Negocios / Operaciones
Ejecutivos de negocio	Gerentes y coordinadores de Centros de Negocios
Propietarios de los procesos de negocio	Jefaturas de direcciones, divisiones y áreas
Comité Ejecutivo Estratégico	Comité Gerencial Ejecutivo

Comité Estratégico (Desarrollo/Proyectos)	Comité Gerencial Ejecutivo/ Comité de apoyo a proyectos
Oficina de Gestión de Proyectos	Oficina de Proyectos Corporativa
Director de Riesgo	Dirección de Riesgo Corporativo
Director de Seguridad de la Información (CISO)	Dirección de Gestión
Consejo de Arquitectura Empresarial	Foro de Arquitectura
Comité de Riesgos Corporativos	Comité de Riesgos
Cumplimiento Normativo (Compliance)	Comité de Cumplimiento
Auditoría	Auditoría Interna
Director de Informática/Sistemas (CIO)	Dirección de Tecnología de Información
Jefe de Arquitectura del Negocio	Área de Arquitectura Empresarial
Jefe de Desarrollo	División de Desarrollo de Servicios
Jefe de Operaciones TI	División de Operación de Servicios
Jefe de Administración de TI	División de Control Operativo
Gestor de Servicio (Service Manager)	División de Servicio al Cliente
Gestor de Seguridad de la Información	Área de Seguridad Operativa Informática
Gestor de Continuidad del Negocio	Unidad de Continuidad del Negocio
Gestor de Privacidad de la información	Unidad de Continuidad del Negocio

Conforme el principio "las empresas existen para crear valor para sus accionistas", COBIT 5 desarrolló el concepto de "cascada de metas", con la finalidad de traducir las necesidades de las partes interesadas en metas corporativas, metas relacionadas con la TI y metas asociadas a los habilitadores. De esta forma COBIT 5 define 17 objetivos genéricos, asociados a dimensiones del Cuadro de Mando Integral (CMI. En inglés: Balanced Scorecard, BSC) y relacionados a metas de TI.

En la siguiente matriz se visualiza la relación entre las metas genéricas relacionadas con la TI y el proceso APO13 Gestionar la Seguridad, en donde, la relación "P" indica relación primaria y "S" una relación secundaria:

Figura 4 - Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y el Proceso APO13

	Meta relacionada con las TI						
	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Riesgos de negocio relacionados con las TI gestionados	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio.	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Disponibilidad de información útil y relevante para la toma de decisiones
	02	04	06	07	08	10	14
Proceso COBIT 5 APO13	Financiera			Cliente		Interna	
Gestionar la Seguridad	P	P	P	S	S	P	P

Si bien las metas genéricas propuestas en COBIT no producen una relación directa de mapeo con los objetivos estratégicos de TI del Banco, se puede efectuar una relación basada en iniciativas y actividades para realizar, y de esta forma construir un mapeo, tal y como se muestra a continuación:

Tabla 6 – Mapeo de metas de TI del Proceso APO13 con objetivos del PETI del Banco Popular

Meta relacionada con las TI (Proceso APO13)		Objetivo Estratégico de TI del Banco	
02	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	**3**	Promover una eficiente gestión de servicios de TI.
04	Riesgos de negocio relacionados con las TI gestionados		
06	Transparencia de los costes, beneficios y riesgos de las TI	**1**	Optimizar la eficiencia de los recursos de TI
10	Seguridad de la información, infraestructura de procesamiento y aplicaciones	**4**	Optimizar la plataforma tecnológica
14	Disponibilidad de información útil y relevante para la toma de decisiones	**3**	Promover una eficiente gestión de servicios de TI.

Las metas relacionadas con las TI, que afectan el cumplimiento de las metas genéricas corporativas, se resumen en la siguiente matriz, en la cual, se puede observar que objetivos, tales como: el cumplimiento de regulaciones externas, la salvaguarda de activos, la continuidad y disponibilidad de los servicios, y la toma

de decisiones basada en información integral, forman parte de la gestión de la seguridad de la información.

Figura 5 - Mapeo entre las Metas Corporativas de COBIT 5 y las Metas relacionadas con TI en Proceso APO13

			Meta Corporativa														
			Valor para las partes interesadas de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activo)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basadas en información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Cumplimiento con las políticas internas	Personas preparadas y motivadas
			1	2	3	4	5	7	8	9	10	11	12	13	15	16
Meta relacionada con las TI (Proceso APO13)			Financiera									Interna				Aprend. y crecimiento
Financiera	02	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P									P	
Financiera	04	Riesgos de negocio relacionados con las TI gestionados			P	S		P	S		P			S	S	S
Financiera	06	Transparencia de los costes, beneficios y riesgos de las TI	S		S		P			S	P		P			
Interna	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones			P	P		P							P	
Interna	14	Disponibilidad de información útil y relevante para la toma de decisiones	S	S	S	S		P		P		S				

ISACA publicó guías profesionales de aseguramiento, basadas en el marco de trabajo de COBIT 5, y en *COBIT 5 for Assurance,* las cuales le ofrecen al auditor una guía más detallada y práctica para el desarrollo de evaluaciones, con una orientación sobre la planificación, determinación del alcance, y la ejecución de los procedimientos de control utilizando una hoja de ruta (*road map*, palabras en inglés). Estas guías hacen referencia explícita a los siete habilitadores de COBIT 5:

1. Principios, Políticas y Marcos de Referencia
2. Procesos
3. Estructuras Organizativas
4. Cultura, Ética y Comportamiento
5. Información
6. Servicios, Infraestructura y Aplicaciones

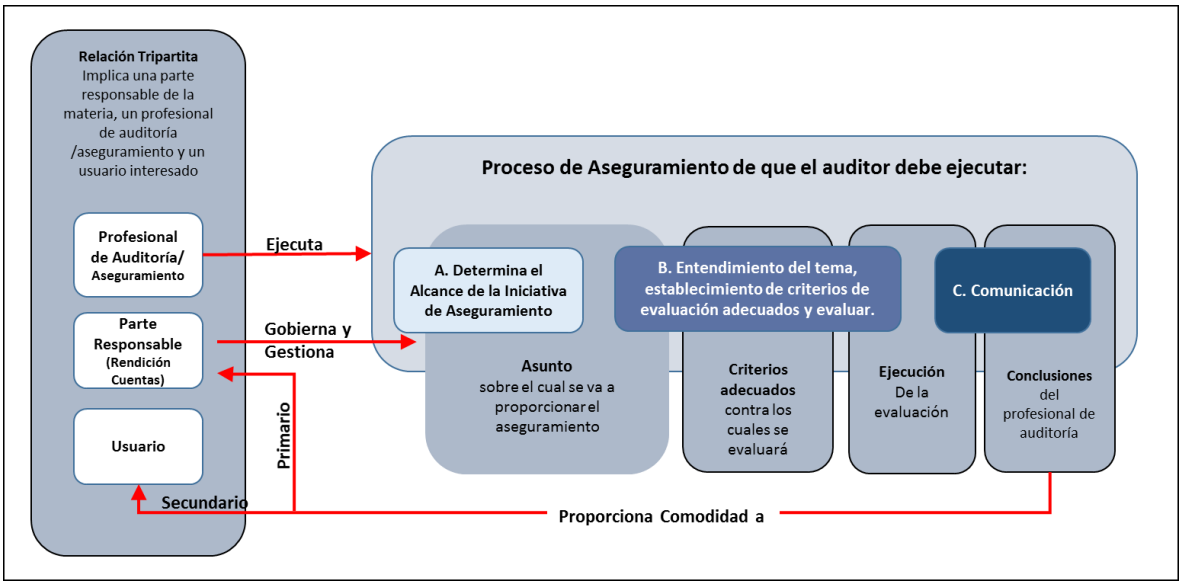
7. Personas, Habilidades y Competencias.

Tal y como lo señala COBIT 5 for Assurance: *"las evaluaciones no se concentran en el proceso, sino que también se incluyen las 4 dimensiones del modelo habilitador: (Partes interesadas, metas, ciclo de vida y buenas prácticas), para cubrir todos los aspectos que contribuyen a la realización de cada habilitador."* Procedimiento en el cual, se referencia la cascada de metas de COBIT 5.

Así, por ejemplo, se asegura que los procesos incluyan las actividades de aseguramiento específico, las estructuras organizacionales apoyen el cumplimiento de metas, en materia de cultura, ética y conducta que los factores contribuyan al éxito de la gobernanza y la gestión del aseguramiento, que los Servicios, Infraestructura y Aplicaciones, cuenten con las capacidades requeridas para proporcionar una seguridad y funciones relacionadas a la organización y que las personas posean las habilidades y competencias para el cumplimiento de metas.

Para COBIT 5 for Assurance, aseguramiento significa que, en virtud de una relación de responsabilidad entre dos o más partes, un profesional de auditoría y aseguramiento podrá emitir una comunicación escrita que exprese una conclusión acerca de los temas evaluados a la parte responsable. De esta forma, las guías de aseguramiento de los procesos de COBIT 5, buscan que un auditor ejecute un proceso con los siguientes componentes:

Figura 6 - Proceso de Aseguramiento/auditoría según COBIT for Assurance



Fuente: COBIT 5 for Assurance

El programa de auditoría está basado en la guía de auditoria del proceso APO13 Gestión de la seguridad de COBIT 5, el cual, se divide en 3 secciones:

> *Etapa A- Determinar el Alcance de la iniciativa de aseguramiento. En este proceso el auditor define el alcance de la evaluación, en términos de COBIT 5 y su cascada de metas.*
>
> *Etapa B- Entender los habilitadores de COBIT 5, establecer los criterios de evaluación adecuados y realizar la evaluación.*
>
> *Etapa C- Comunicar los resultados de las evaluaciones. El auditor comunica las observaciones a las partes interesadas del proceso. Incluye la documentación de las debilidades encontradas y su comunicación eficaz y eficiente, con el fin de aplicar las mejoras necesarias.*

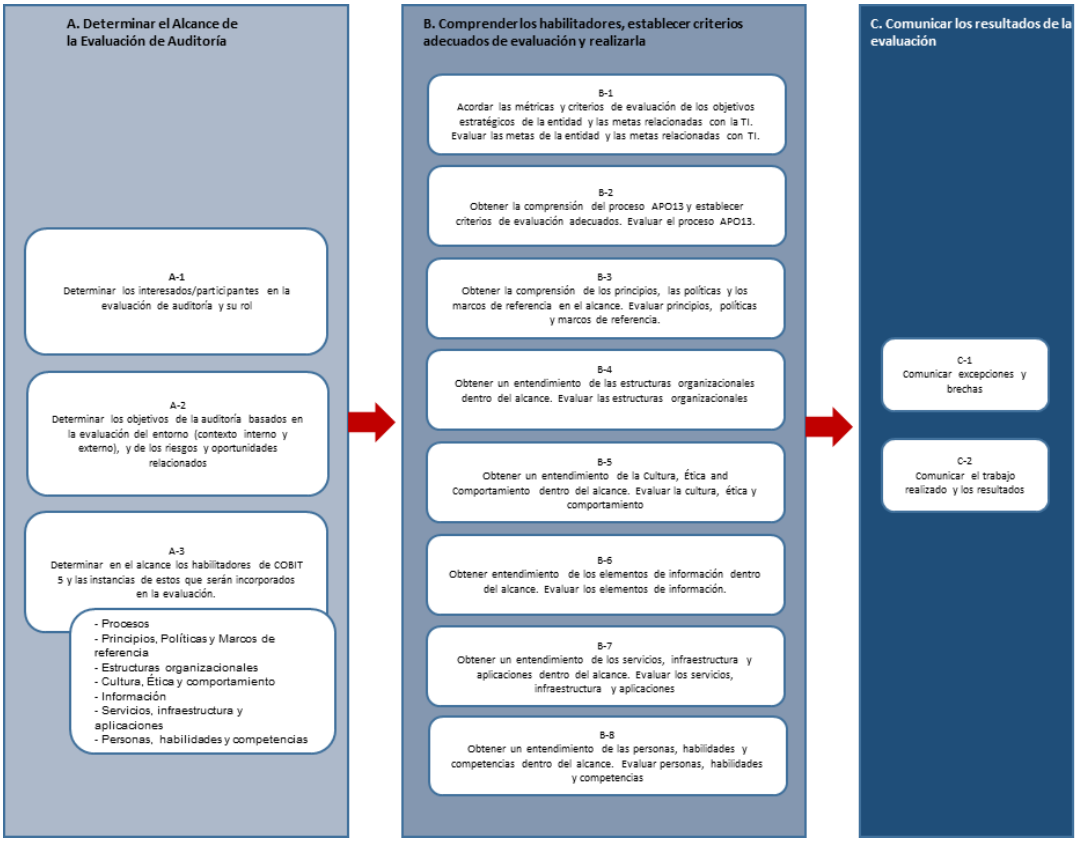
En el siguiente capítulo, se desarrolla la guía de auditoría del proceso APO13 Gestión de la seguridad de COBIT 5, adaptada según la realidad y características del Banco Popular.

CAPÍTULO III
PROGRAMA DE AUDITORÍA

1. Programa de auditoría del Proceso APO13 Gestionar la Seguridad – COBIT 5

La guía de auditoría del proceso APO13 Gestionar la Seguridad se basa en el enfoque genérico del documento *COBIT 5 for Assurance*. El programa se personalizó, de acuerdo con el alcance previsto en la evaluación del sistema de gestión de la seguridad de la información del Banco Popular, en donde se consideró a los interesados, objetivos, habilitadores y algunas de sus dimensiones comunes. El enfoque genérico del programa de auditoría se visualiza a continuación:

Figura 7- Enfoque genérico del programa de auditoría



Fuente: COBIT for Assurance

A continuación, se desarrolla el programa de auditoría del proceso *APO13 Gestionar la seguridad*.

Etapa A—Determine el alcance de la evaluación de auditoría					
Ref.	**Programa de Auditoría**	**Guía de orientación**		**Referencia Cruzada**	**Comentario**
A-1	Determinar los interesados/participantes en la evaluación de auditoría y su rol				
A-1.1	Identificar los usuarios interesados en el informe de auditoría y su participación en el proceso de evaluación.	**Usuarios interesados en el informe de auditoría**	*Describir las áreas auditadas*	**A-1.1.Cap. IV**	
A-1.2	Identificar las partes interesadas, responsables y encargados del proceso para evaluar.	**Partes encargadas de rendición de cuentas y responsables del proceso para evaluar.**	*Describir las partes encargadas de rendición de cuentas y responsables del proceso para evaluar; COBIT 5 incluye una descripción resumida de un amplio conjunto de roles que se pueden utilizar como punto de partida para este paso de auditoría (COBIT 5 Marco de trabajo, anexo 6, p.76); COBIT 5 for Assurance también proporciona una descripción resumida de un amplio conjunto de roles de aseguramiento, consulte la sección 2A, capítulo 4, p.37.*	**A-1.2. Cap. IV**	
A-2	Determinar los objetivos de la auditoría basados en la evaluación del entorno (contexto interno y externo), y de los riesgos y oportunidades relacionados.	Objetivos de la auditoría son esencialmente una expresión más detallada y concreta de esos objetivos estratégicos de la entidad relacionada con el proceso para evaluar. Objetivos estratégicos de la entidad se pueden formular en términos de los objetivos empresariales genéricos (COBIT 5 Marco de Trabajo) o pueden ser expresados más específicamente. **Objetivos de la auditoría pueden expresarse utilizando los objetivos empresariales genéricos de COBIT 5, los objetivos relacionados con la TI (que se relacionan más con la tecnología), objetivos de información o cualquier otro conjunto de metas específicas.**			

Etapa A—Determine el alcance de la evaluación de auditoría				
Ref.	**Programa de Auditoría**	**Guía de orientación**	**Referencia Cruzada**	**Comentario**
A-2.1	Comprender la estrategia y las prioridades de la entidad	*Indague con la Gerencia General o mediante la documentación disponible (Plan estratégico corporativo o informes anuales de gestión) sobre la estrategia de la entidad y las prioridades para el próximo período, verificando si el proceso para evaluar es relevante para la entidad.*	**A-2.1. Cap. IV**	
A-2.2	Comprender el contexto interno de la entidad	*Identificar todos los factores ambientales internos que pueden influir* ***en el rendimiento del proceso en revisión****.*	**A-2.2. Cap. IV**	
A-2.3	Comprender el contexto externo de la entidad	*Identificar todos los factores ambientales externos que pueden influir* ***en el rendimiento del proceso en revisión****.*	**A-2.3. Cap. IV**	
A-2.4	Dado el objetivo general de la evaluación, traduzca las prioridades estratégicas identificadas en metas específicas para la evaluación.	Las siguientes metas se pueden conservar como metas clave que deben apoyar la estrategia y prioridades de la entidad.		
		Metas Clave Metas empresariales: • EG07 Continuidad y disponibilidad del servicio de negocio • EG15 Cumplimiento con las políticas internas Metas relacionadas a las TI: • ITG10 Seguridad de la información, infraestructuras de procesamiento y aplicaciones • ITG14 Disponibilidad de información útil y relevante para la toma de decisiones	**A-2.4. Cap. IV**	Se delimitó el alcance a las metas relacionadas a las TI que forman parte de la dimensión de procesos internos y las metas empresariales prioritarias asociadas.
A-2.5	<u>Definir</u> los límites organizacionales de la evaluación	*Describir los límites organizacionales de la evaluación de auditoría, es decir, delimitar la revisión a los entes de mayor relevancia de la organización para la evaluación. Los otros aspectos para delimitar el alcance son identificados durante la fase A-3.*	**A-2.5. Cap. IV**	

Etapa A—Determine el alcance de la evaluación de auditoría				
Ref.	**Programa de Auditoría**	**Guía de orientación**	**Referencia Cruzada**	**Comentario**
A-3	Determinar en el alcance los **habilitadores de COBIT 5** y las instancias de estos que serán incorporados en la evaluación.	El alcance de este programa de auditoría es el proceso *APO13 Gestionar la Seguridad*. Sin embargo, según el modelo habilitador COBIT 5, todos los habilitadores relacionados tendrán también que ser considerados para su inclusión en el ámbito de aplicación, algunos considerando todas las dimensiones y otros en forma parcial.		
A-3.1	Definir el **proceso** en el alcance de la revisión	El siguiente proceso como se define en el documento *COBIT 5: Procesos Habilitadores,* está en el ámbito de esta evaluación de auditoría: ***APO13 Gestionar la Seguridad.***		
A-3.2	Definir los habilitadores relacionados. Habilitadores relacionados incluyen: • Principios, Políticas y Marcos de Referencia • Estructuras organizativas • Cultura, ética y comportamiento • Información • Servicios, infraestructura y aplicaciones • Personas, habilidades y competencias	**Principios, Políticas y Marcos de Referencia**: En el contexto de la revisión de este proceso, y teniendo en cuenta los objetivos identificados en A-2.4, los siguientes principios, políticas y marcos podrían ser considerados en el alcance de la revisión: • *Política de Seguridad de la Información del Banco Popular, vigente a febrero 2014.* **Estructuras organizativas:** Con base en el proceso que se evalúa, las siguientes estructuras organizativas y funciones se consideran parte del alcance de este programa de auditoría, en donde, conforme los recursos disponibles, se determinará cuáles aspectos serán revisados con mayor detalle: • Dirección de Tecnología de Información o **Área de Seguridad Operativa Informática** • Dirección de Gestión o **Unidad de Continuidad del Negocio** **Cultura, ética y comportamiento:** En el contexto de la evaluación al proceso APO13, el siguiente comportamiento en toda la empresa está incluido dentro del alcance: • *Las personas respetan la importancia de las políticas y los principios de seguridad de la información.* **Elementos de información:** Con base en el proceso APO13, el siguiente elemento de información es		

Etapa A—Determine el alcance de la evaluación de auditoría				
Ref.	**Programa de Auditoría**	**Guía de orientación**	**Referencia Cruzada**	**Comentario**
A-3.2 Cont.		considerado dentro del alcance de este programa de auditoría. • *Perfil de Riesgos de Seguridad de la Información del Banco Popular* **Servicios, infraestructura y aplicaciones** En el contexto de la evaluación al proceso APO13, y teniendo en cuenta los objetivos identificados en A-2.4, los siguientes servicios e infraestructura o aplicaciones relacionadas podrían ser considerados en el alcance de la revisión: • *Servicios e infraestructura tecnológica para la protección contra* software *malicioso (malware)* **Personas, habilidades y competencias:** En el contexto de la evaluación al proceso APO13, teniendo en cuenta los procesos clave y los principales roles, los siguientes conjuntos de habilidades se incluyen en el alcance**:** • <u>Formulación de la estrategia de seguridad de la información</u> a. **Experiencia**. Amplia experiencia en seguridad de la información y gestión empresarial de TI (recomendado), incluyendo: - Experiencia en definición de estrategias de seguridad de la información y gobernanza en el sector financiero - Experiencia en la creación e implementación de estrategias y principios, prácticas y actividades de seguridad de la información - Amplio conocimiento de todas las funciones de seguridad de la información (Referencia Norma ISO 27002) y cómo se relacionan con el negocio. b. **Cualificaciones.** CISM • <u>Operaciones de Seguridad de la Información</u> a. **Experiencia**. Experiencia técnica en seguridad de la información (recomendado), incluyendo: - Sólida experiencia en seguridad de la información. - Conocimiento técnico práctico de todas las funciones de seguridad de la información en una entidad financiera y la		

Etapa A—Determine el alcance de la evaluación de auditoría				
Ref.	**Programa de Auditoría**	**Guía de orientación**	**Referencia Cruzada**	**Comentario**
		comprensión de cómo se alinean con los objetivos de negocio **b. Formación/Cualificaciones.** - Experiencia en la aplicación de las directivas del programa de gestión de seguridad de la información para la protección de los activos de información del Banco y reducción al mínimo del riesgo de pérdidas - CRISC, CISSP - Certificaciones específicas de la infraestructura de seguridad implementada en la entidad.		

Etapa B— Comprender los habilitadores, establecer criterios adecuados de evaluación y realizar la evaluación						
Ref.	**Procedimientos de auditoría**				**Referencia cruzada**	**Comentario**
B-1	**Establecer las métricas y criterios de evaluación de las metas clave de la entidad y las metas relacionadas con la TI, relacionadas con el proceso APO13** **Evaluar las metas de la entidad y las metas relacionadas con la TI.**					
B-1.1	Las siguientes métricas y valores esperados se definieron para las metas clave de la entidad, definidos en la etapa A-2.4.					
	Meta empresarial	**Métrica**	**Resultado Esperado (Ex)**	**Prueba de Auditoría**		
	EG07 Continuidad y disponibilidad del servicio de negocio	• Número de interrupciones en el servicio al cliente provocando incidentes significativos	*Ninguna interrupción del servicio al cliente en el último año, provocada por un incidente de seguridad de la información.*	*En este paso, las métricas relacionadas para cada meta se revisarán y se hará una evaluación de si se alcanzan los criterios definidos.*	**B-1.1. Cap. IV**	
	EG15 Cumplimiento con las políticas internas	• El número de incidentes relacionados con el incumplimiento de la política de Seguridad de la Información del Banco • Porcentaje de los interesados que comprenden la Política de Seguridad de la	*Registro de los incidentes presentados por el incumplimiento de la Política de Seguridad de la Información y detalle de las sanciones aplicadas* *90% de evaluaciones*	*En este paso, las métricas relacionadas para cada meta se revisarán y se hará una evaluación de si se alcanzan los criterios definidos.*		

<table>
<tr><th colspan="7">Etapa B— Comprender los habilitadores, establecer criterios adecuados de evaluación y realizar la evaluación</th></tr>
<tr><th>Ref.</th><th colspan="4">Procedimientos de auditoría</th><th>Referencia cruzada</th><th>Comentario</th></tr>
<tr><td></td><td></td><td>Información del Banco</td><td>ganadas en el último año por el personal sobre el conocimiento de la Política de Seguridad de la Información</td><td></td><td></td><td></td></tr>
<tr><td rowspan="4">B-1.2</td><td colspan="4">Las siguientes métricas y valores esperados se definieron para las principales metas relacionadas con TI definidas en la etapa A-2.4.</td><td></td><td></td></tr>
<tr><td>Métricas relacionadas con TI</td><td>Métricas</td><td>Resultado Esperado (Ex)</td><td>Prueba de Auditoría</td><td></td><td></td></tr>
<tr><td>ITG10 Seguridad de la información, infraestructuras de procesamiento y aplicaciones</td><td>• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o daño de imagen
• Número de servicios de TI con los requisitos de seguridad pendientes</td><td>Ningún incidente de seguridad causante de pérdidas financieras para el Banco en el último año, producto de malware.

Ningún servicio crítico de TI y/o negocio sin la protección antimalware.</td><td>En este paso, las métricas relacionadas para cada meta se revisarán y se hará una evaluación de si se alcanzan los criterios definidos.</td><td>B-1.2. Cap. IV</td><td></td></tr>
<tr><td>ITG14 Disponibilidad de información útil y relevante para la toma de decisiones</td><td>• Número de incidentes en los procesos de negocio causados por la indisponibilidad de la información</td><td>Ningún incidente de seguridad de la información en el último año que afectara los procesos de negocio y la integridad, confiabilidad y disponibilidad de la información.</td><td>En este paso, las métricas relacionadas para cada meta se revisarán y se hará una evaluación de si se alcanzan los criterios definidos.</td><td>B-1.2. Cap. IV</td><td></td></tr>
</table>

<table>
<tr><th colspan="6">Etapa B— Comprender los habilitadores, establecer criterios adecuados de evaluación y realizar la evaluación</th></tr>
<tr><th>Ref.</th><th colspan="3">Procedimientos de auditoría</th><th>Referencia cruzada</th><th>Comentario</th></tr>
<tr><td>B-2</td><td colspan="3">Obtener la comprensión del proceso APO13 y establecer criterios de evaluación adecuados.

Evaluar el proceso APO13 Gestionar la Seguridad.</td><td></td><td></td></tr>
<tr><td>B-2.1</td><td colspan="3">Comprender el propósito del proceso.</td><td></td><td></td></tr>
<tr><td></td><td colspan="3">El propósito del proceso APO13, conforme lo declara COBIT 5 es:
“Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa”.</td><td></td><td></td></tr>
<tr><td>B-2.2</td><td colspan="3">Comprender las metas del Proceso y métricas relacionadas y definir los valores esperados (criterios), y evaluar si se alcanzan las metas del Proceso (resultados), es decir, evaluar la efectividad del Proceso.</td><td></td><td></td></tr>
<tr><td></td><td colspan="3">El proceso APO13 Gestionar la Seguridad tiene definidas 3 metas genéricas de proceso, tal y como se describe en COBIT 5: Procesos habilitadores, capítulo 5, p. 113. No obstante, para efectos de esta evaluación, se limitará a la evaluación de las métricas asociadas a una de las metas genéricas del proceso que mantiene mayor relación con la situación actual de implementación del sistema de gestión de seguridad de la información en el Banco.</td><td></td><td></td></tr>
<tr><td></td><td>Metas del Proceso</td><td>Métricas relacionadas</td><td>Criterios / Valor Esperado</td><td>Prueba de Auditoría</td><td></td></tr>
<tr><td></td><td>Está en marcha un sistema que considera y trata efectivamente los requerimientos de seguridad de la información de la entidad.</td><td>• Número de roles claves de seguridad claramente definidos</td><td>Para todos los roles definidos en la matriz RACI del proceso APO13 con (A) y (R), exista en el Banco una asociación clara del mismo nivel jerárquico recomendado.</td><td>En este paso, las métricas relacionadas para cada meta se revisarán y se hará una evaluación de si se alcanzan los criterios definidos.</td><td>B-2.2. Cap. IV</td><td></td></tr>
<tr><td></td><td colspan="2">El proceso APO13 Gestionar la seguridad es descrito en COBIT 5: Procesos habilitadores.

El proceso requiere de una serie de prácticas de gestión que deberán implementarse, como se describe en la descripción del proceso de la misma guía.</td><td colspan="2">Cada práctica se lleva a cabo normalmente a través de una serie de actividades, y un proceso bien diseñado implementará todas estas prácticas y actividades. Para efectos de la evaluación, serán consideradas aquellas actividades clave en cada una de las 3 prácticas de gestión del Proceso APO13.</td><td></td><td></td></tr>
</table>

Etapa B— Comprender los habilitadores, establecer criterios adecuados de evaluación y realizar la evaluación				
Ref.	**Procedimientos de auditoría**		**Referencia cruzada**	**Comentario**
	Referencia a la práctica del proceso	**Prueba de Auditoría**		
B-2.2 Cont.	APO13.01 Establecer y mantener un SGSI.	Evaluar mediante la aplicación de técnicas de auditoría adecuadas (entrevista, observación, testeo), si la práctica de gestión se aplique con eficacia a través de las siguientes actividades (controles) típicos: 1. Definir el alcance y los límites del SGSI en términos de las características del Banco, la organización, su localización, activos y tecnología. Incluir detalles y justificación para cualquier exclusión del alcance. 2. Alinear el SGSI con el enfoque global de la gestión de la seguridad en el Banco. 3. Obtener autorización de la Gerencia General Corporativa para implementar y operar o cambiar el SGSI. 4. Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información. 5. Comunicar el enfoque de SGSI. Compare la matriz RACI que se incluye en el proceso de referencia en COBIT 5: Procesos habilitadores con los actuales encargados de rendición de cuentas y responsables de esta práctica y evalúe si • La rendición de cuentas y la responsabilidad son asignadas y asumidas. • La rendición de cuentas y la responsabilidad son asignadas en el nivel adecuado en la organización.	**B-2.2. Cap. IV**	
	APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Evaluar mediante la aplicación de técnicas de auditoría adecuadas (entrevista, observación, testeo), si la práctica de gestión se aplique con eficacia a través de las siguientes actividades (controles) típicos: 1. Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura del Banco. 2. Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad de la información, sustentados en casos de negocio adecuados que consideren la financiación la asignación de roles y responsabilidades. 3. Definir la forma de medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizar estas mediciones para evaluar la efectividad y producir resultados reproducibles y comparables. 4. Recomendar programas de formación y concienciación en seguridad de la información. Compare la matriz RACI que se incluye en el proceso de referencia en COBIT 5: Procesos habilitadores con los actuales encargados de rendición de cuentas y responsables de esta práctica y evalúe si	**B-2.2. Cap. IV**	

Etapa B— Comprender los habilitadores, establecer criterios adecuados de evaluación y realizar la evaluación				
Ref.	**Procedimientos de auditoría**		**Referencia cruzada**	**Comentario**
B-2.2 Cont.		• La rendición de cuentas y la responsabilidad son asignadas y asumidas. • La rendición de cuentas y la responsabilidad son asignadas en el nivel adecuado en la organización.		
	APO13.03 Supervisar y revisar el SGSI.	Evaluar mediante la aplicación de técnicas de auditoría adecuadas (entrevista, observación, testeo), si la práctica de gestión se aplica con eficacia a través de las siguientes actividades (controles) típicos: 1. Realizar revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI. 2. Registrar las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI. Compare la matriz RACI que se incluye en el proceso de referencia en COBIT 5: Procesos habilitadores con los actuales encargados de rendición de cuentas y responsables de esta práctica y evalúe si • La rendición de cuentas y la responsabilidad son asignadas y asumidas. • La rendición de cuentas y la responsabilidad son asignadas en el nivel adecuado en la organización.	**B-2.2. Cap. IV**	

<table>
<tr><th colspan="6">Etapa B— Comprender los habilitadores, establecer criterios adecuados de evaluación y realizar la evaluación</th></tr>
<tr><th>Ref.</th><th colspan="3">Procedimientos de auditoría</th><th>Referencia cruzada</th><th>Comentario</th></tr>
<tr><td>B-3</td><td colspan="3">Obtener la comprensión de los principios, las políticas y los marcos de referencia en el alcance.

Evaluar principios, políticas y marcos de referencia.</td><td></td><td></td></tr>
<tr><td>B-3.1</td><td colspan="3">Comprender el contexto de la Política de Seguridad de la Información del Banco Popular</td><td>B-3.1. Cap. IV</td><td></td></tr>
<tr><td>B-3.2</td><td colspan="3">Comprender las partes interesadas de la Política de Seguridad de la Información del Banco Popular. Las partes interesadas en la política incluye: quienes establecen la política y los que deben cumplirla.</td><td>B-3.2. Cap. IV</td><td></td></tr>
<tr><td>B-3.3</td><td colspan="3">Evaluar si se logran las metas (resultados) de la Política de Seguridad de la Información del Banco, es decir, evaluar su efectividad.</td><td>B-3.3. Cap. IV</td><td></td></tr>
<tr><td></td><td>Meta</td><td>Criterio</td><td>Prueba de Auditoría</td><td></td><td></td></tr>
<tr><td></td><td>Integralidad</td><td>El conjunto de requisitos de la Política de Seguridad de la Información del Banco es exhaustivo en su cobertura.</td><td>• Verifique que el conjunto de requisitos establecidos en la Política de Seguridad de la Información del Banco es exhaustivo en su cobertura.</td><td></td><td></td></tr>
<tr><td></td><td>Flexibilidad</td><td>El conjunto de requisitos de la política es flexible. Está estructurado de tal manera que es fácil añadir o realizar actualizaciones como las circunstancias lo requieren.</td><td>• Verifique la flexibilidad de los requisitos y cláusulas establecidas en la Política de Seguridad de la Información, es decir, que están estructuradas de tal manera que es fácil añadir o actualizar como las circunstancias lo requieren.</td><td></td><td></td></tr>
<tr><td></td><td>Disponibilidad</td><td>Las políticas están disponibles para todos los interesados.
Las políticas son fáciles de navegar y tener una estructura lógica y jerárquica.</td><td>• Verifique que la Política de Seguridad de la Información está disponible para todos los interesados.
• Verifique que la Política de Seguridad de la Información es fácil de navegar y tiene una estructura lógica y jerárquica.</td><td></td><td></td></tr>
</table>

<table>
<tr><th colspan="5">Etapa B— Comprender los habilitadores, establecer criterios adecuados de evaluación y realizar la evaluación</th></tr>
<tr><th>Ref.</th><th colspan="3">Procedimientos de auditoría</th><th>Referencia cruzada</th><th>Comentario</th></tr>
<tr><td>B-3.5</td><td colspan="3">Comprender las buenas prácticas relacionadas con los principios, las políticas y los marcos de referencia y los resultados esperados. Evaluar el diseño de la Política de Seguridad de la Información.

El auditor, mediante el uso de técnicas adecuadas de auditoría evalúa los siguientes aspectos de la Política de Seguridad de la Información del Banco Popular</td><td>B-3.4. Cap. IV</td><td></td></tr>
<tr><td></td><td>Buena práctica</td><td>Criterio</td><td>Prueba de Auditoría</td><td></td><td></td></tr>
<tr><td></td><td>Alcance y vigencia</td><td>El alcance se describe y la fecha de validez se indica.</td><td>• Verifique que se describa el alcance de la Política y que se indique la fecha de validez.</td><td></td><td></td></tr>
<tr><td></td><td>Excepción y escalamiento</td><td>• El procedimiento de excepción y de escalamiento se explica y se conoce comúnmente.
• El procedimiento de excepción y escalamiento no se ha convertido en un estándar de facto.</td><td>• Verifique que el procedimiento de excepción y escalamiento se describe, explica y se conoce comúnmente.
• A través de la observación de una muestra representativa, compruebe que la excepción y el procedimiento de escalamiento no se ha convertido en un procedimiento estándar de facto.</td><td></td><td></td></tr>
<tr><td>B-3.5
Cont.</td><td>Cumplimiento</td><td>• El mecanismo de verificación del cumplimiento y de las consecuencias del no cumplimiento se describe claramente y se aplica.</td><td>• Verifique que el mecanismo de comprobación del cumplimiento y las consecuencias del no cumplimiento de la Política de Seguridad de la Información se describen claramente y se hacen cumplir.</td><td></td><td></td></tr>
</table>

<table>
<tr><th colspan="5">Etapa B— Comprender los habilitadores, establecer criterios adecuados de evaluación y realizar la evaluación</th></tr>
<tr><th>Ref.</th><th>Procedimientos de auditoría</th><th>Referencia cruzada</th><th>Comentario</th></tr>
<tr><td>B-4</td><td>Obtener un entendimiento de las estructuras organizacionales dentro del alcance.

Evaluar las estructuras organizacionales</td><td></td><td></td></tr>
<tr><td>B-4.2</td><td><u>Comprender</u> todos los interesados de las siguientes estructuras organizativas:
- Área de Seguridad Operativa Informática
- Unidad de Continuidad del Negocio (actividades de Seguridad de la información)

Determinar mediante la revisión de documentación (políticas, gestión de comunicaciones, etc.) los interesados clave de la función, es decir:

• Titular de la función y / o miembros de las Estructuras Organizacionales
• Otros interesados clave afectados por las decisiones de la función de las Estructuras Organizativas</td><td>B-4.2. Cap. IV</td><td></td></tr>
<tr><td>B-4.4</td><td><u>Evaluar</u> el diseño de las dos estructuras organizativas mencionadas en el punto B-4.2, es decir, evaluar el grado en que se espera se apliquen buenas prácticas.
<table>
<tr><th>Buena práctica</th><th>Criterio</th><th>Prueba de Auditoría</th></tr>
<tr><td>Principios operativos</td><td>• Principios operativos están documentados.</td><td>• Verificar si los principios operativos están debidamente documentados.</td></tr>
<tr><td>Composición</td><td>La composición de la estructura organizativa es equilibrada y completa, es decir, todos los interesados requeridos están lo suficientemente representados.</td><td>• Evaluar si la composición de la estructura organizativa es equilibrada y completa, es decir, todos los interesados requeridos están lo suficientemente representados.</td></tr>
<tr><td>Ámbito de control</td><td>• El ámbito de control de la Estructura Organizativa está definido.
• El ámbito de control es adecuado, es decir, la estructura organizativa tiene el derecho de tomar todas las decisiones que debería.</td><td>• Compruebe si se ha definido el ámbito del control de la Estructura Organizativa.
• Evaluar si el ámbito de control es adecuado, es decir, la estructura organizativa tiene el derecho de tomar todas las decisiones que debería.</td></tr>
<tr><td>Nivel de autoridad / poder de decisión</td><td>• El poder de decisión de la Estructura organizativa está definido y documentado.
• Se respeta y cumple el poder de decisión de la Estructura Organizativa.</td><td>• Verificar que el poder de decisión de la estructura organizativa está definido y documentado.
• Verificar que el poder de decisión de la estructura organizativa se cumple y respeta.</td></tr>
</table>
</td><td>B-4.4. Cap. IV</td><td></td></tr>
</table>

<table>
<tr><th colspan="5">Etapa B— Comprender los habilitadores, establecer criterios adecuados de evaluación y realizar la evaluación</th></tr>
<tr><th>Ref.</th><th colspan="3">Procedimientos de auditoría</th><th>Referencia cruzada</th><th>Comentario</th></tr>
<tr><td rowspan="4">B-4.5</td><td colspan="3">Evaluar la medida en la que se gestiona el ciclo de vida de las estructuras organizativas descritas en el punto B-4.2.</td><td>B-4.5. Cap. IV</td><td></td></tr>
<tr><td>Elemento del ciclo de vida</td><td>Criterio</td><td>Prueba de Auditoría</td><td></td><td></td></tr>
<tr><td>Mandato</td><td>• La estructura organizacional está formalmente establecida.</td><td>• Verifique a través de entrevistas y observación que la estructura organizacional está formalmente establecida.</td><td></td><td></td></tr>
<tr><td>Monitoreo</td><td>• El desempeño de la estructura organizativa y de sus miembros debe ser monitoreado y evaluado con regularidad por evaluadores competentes e independientes.</td><td>• Verifique si el desempeño de la estructura organizativa y de sus miembros se supervisa y evalúa con regularidad por asesores competentes e independientes.</td><td></td><td></td></tr>
</table>

Etapa B— Comprender los habilitadores, establecer criterios adecuados de evaluación y realizar la evaluación				
Ref.	**Procedimientos de auditoría**		**Referencia cruzada**	**Comentario**
B-5	**Obtener un entendimiento de la cultura, ética y comportamientos dentro del alcance** **Evaluar la cultura, ética y comportamiento**			
B-5.3	Comprender las metas para el comportamiento definido en el alcance de la evaluación, que indica lo siguiente: - *La gente respeta la importancia de las políticas y los principios de seguridad de la información.* Evaluar si los resultados del comportamiento deseado se cumplen, es decir, evaluar su eficacia.			
	Definir lo que constituye comportamientos deseados y no deseados.	Los comportamientos están asociados a las personas y las estructuras organizativas de las que forman parte, por tanto, mediante el uso de técnicas adecuadas de auditoría, el auditor debe: • Identificar las personas que deben cumplir con los comportamientos que se examinan. • Identificar las Estructuras organizativas involucradas. • Evaluar si los comportamientos deseados se pueden observar.		
	Comportamiento deseado (Meta de comportamiento)	**Prueba de Auditoría**		
	La importancia de la política de seguridad de la información es reconocida por los funcionarios del Banco. A nivel organizacional, la política de seguridad de la información es respaldada por la alta dirección, y la aprobación, revisión y comunicación de políticas se produce sobre una base regular. A nivel individual, las personas han leído y entendido la política.	• Verificar mediante entrevista a los encargados de las estructuras organizativas con roles de responsabilidad y rendición de cuentas en la gestión de la seguridad de la información si consideran que la Política de Seguridad de la Información influye en el comportamiento deseado	**B-5.3. Cap. IV**	

Etapa B— Comprender los habilitadores, establecer criterios adecuados de evaluación y realizar la evaluación					
Ref.	**Procedimientos de auditoría**			**Referencia cruzada**	**Comentario**
			del personal, respecto a los aspectos culturales y de control relacionados con la seguridad de la información. Indague sobre el criterio de estos encargados, respecto al entendimiento de la Política de Seguridad de la Información por parte de los funcionarios de la entidad.		
B-5.5	Evaluar el diseño de la Cultura, Ética y Conducta, es decir, evaluar en qué medida se aplican buenas prácticas.				
	Buena Práctica	**Criterio**	**Prueba de Auditoría**		
	Comunicación y aplicación de normas	Existencia y calidad de la información	Aplicar técnicas de auditoría apropiados para evaluar si la buena práctica se aplica adecuadamente, es decir, se cumplen los criterios de evaluación.	**B-5.5. Cap. IV**	
	Incentivos	Existencia y aplicación de recompensas e incentivos apropiados (BSC).			

<table>
<tr><th colspan="6">Etapa B— Comprender los habilitadores, establecer criterios adecuados de evaluación y realizar la evaluación</th></tr>
<tr><th>Ref.</th><th colspan="3">Procedimientos de Auditoría</th><th>Referencia Cruzada</th><th>Comentarios</th></tr>
<tr><td>B-6</td><td colspan="3">Obtener entendimiento de los elementos de información dentro del alcance

Evaluar los elementos de información.</td><td></td><td></td></tr>
<tr><td>B-6.1</td><td colspan="3">Comprender el contexto del elemento de Información:

• Perfil de Riesgos de Seguridad de la Información del Banco Popular

a. ¿Dónde y cuándo se utiliza?
b. ¿Para qué se utiliza?
c. Comprender la conexión con otros habilitadores en el alcance, por ejemplo:
○ ¿Utilizado por cuáles procesos?
○ ¿Qué estructuras Organizativas están involucradas (véase también B-4.2)?
○ ¿Qué servicios / aplicaciones están involucrados?</td><td>B-6.1. Cap. IV</td><td></td></tr>
<tr><td>B-6.3

.</td><td colspan="3"><u>Evaluar</u> si se alcanzan los criterios de calidad de los elementos de Información (resultados), es decir, evaluar la efectividad del elemento de Información seleccionado.</td><td></td><td></td></tr>
<tr><td></td><td colspan="2">Aproveche el modelo COBIT 5 habilitador información, el cual está centrado en la descripción de metas de calidad para seleccionar los criterios más relevantes de calidad de información del elemento de información a la mano.</td><td>El auditor mediante el uso de técnicas apropiadas de auditoría, verifica y evalúa los criterios de calidad en el ámbito de aplicación.</td><td>B-6.3. Cap. IV</td><td></td></tr>
<tr><td></td><td>Dimensión de calidad</td><td>Descripción</td><td>Prueba Auditoría</td><td></td><td></td></tr>
<tr><td></td><td>Objetividad</td><td>El grado en que la información es objetiva, sin prejuicios e imparcial</td><td>Determine si el perfil de riesgos de seguridad de la información fue diseñado utilizando criterios objetivos, en cuanto a eventos de riesgo y su frecuencia.</td><td></td><td></td></tr>
<tr><td></td><td>Relevancia</td><td>El grado en que la información es aplicable y útil para la tarea a realizar</td><td rowspan="2">Indague con el encargado del Área de Seguridad Informática si considera relevantes y completos los criterios indicados en el perfil de riesgos de la seguridad de la información.</td><td></td><td></td></tr>
<tr><td></td><td>Completitud</td><td>El grado en que la información no tiene carencias y es de la suficiente profundidad y amplitud para la tarea por realizar</td><td></td><td></td></tr>
<tr><td></td><td>Comprensibilidad</td><td>El grado en que la información sea fácil de comprender</td><td>Determine si el lenguaje utilizado en el perfil de riesgos de seguridad de la información es comprensible para todas las partes interesadas.</td><td></td><td></td></tr>
</table>

Etapa B— Comprender los habilitadores, establecer criterios adecuados de evaluación y realizar la evaluación					
Ref.	**Procedimientos de Auditoría**			**Referencia Cruzada**	**Comentarios**
	Disponibilidad	El grado en que la información está disponible cuando se requiera, o que es rápida y fácilmente recuperable.	Verifique si el perfil de riesgos de seguridad de la información está disponible para todas las partes interesadas.		

Etapa B— Comprender los habilitadores, establecer criterios adecuados de evaluación y realizar la evaluación					
Ref.	**Procedimientos de Auditoría**			**Referencia Cruzada**	**Comentarios**
B-7	**Obtener un entendimiento de los servicios, infraestructura y aplicaciones dentro del alcance.** **Evaluar los servicios, infraestructura y aplicaciones**				
B-7.1	Comprender el contexto del servicio de protección contra *software* malicioso *Comprender el contexto organizacional y tecnológico de este servicio.* *Consulte el paso A-2.2 y A-2.3 y reutilice esa información para comprender la importancia del servicio de protección contra software malicioso.*			**B-7.1. Cap. IV**	
B-7.3	Comprender las metas principales del servicio de protección contra *software* malicioso, las métricas relacionadas y los resultados esperados. *Evaluar si se logran los resultados de las metas* del servicio de protección contra *software* malicioso*, es decir, evaluar su eficacia.*			**B-7.3. Cap. IV**	
	Meta	**Criterio**	**Prueba de Auditoría**		
	Descripción del servicio	• El servicio se describe con claridad. • El servicio está disponible para todos los posibles interesados • Verificar la eficacia del servicio en la reducción de incidentes de seguridad de la información	• Evaluar la calidad de la descripción del Servicio y del servicio ofrecido. • Verificar la accesibilidad del servicio a todos los posibles interesados. • Verificar si el servicio de protección contra *software* malicioso permite mantener bajo control los incidentes de seguridad de la información, basados en *software* malicioso.		

<table>
<tr><th colspan="6">Etapa B— Comprender los habilitadores, establecer criterios adecuados de evaluación y realizar la evaluación</th></tr>
<tr><th>Ref.</th><th colspan="3">Procedimientos de Auditoría</th><th>Referencia cruzada</th><th>Comentarios</th></tr>
<tr><td>B-8</td><td colspan="3">Obtener un entendimiento de las personas, habilidades y competencias dentro del alcance.

Evaluar personas, habilidades y competencias</td><td></td><td></td></tr>
<tr><td>B-8.3</td><td colspan="3">Evaluar si se logran los resultados de las Personas, Habilidades y Competencias, para las estructuras organizativas definidas en el alcance, es decir, evaluar la eficacia de las personas, habilidades y competencias.

Para la formulación de la estrategia de seguridad de la información, los siguientes objetivos y criterios asociados se pueden abordar.</td><td>B-8.3. Cap. IV</td><td></td></tr>
<tr><td></td><td>Meta</td><td>Criterio</td><td>Prueba de Auditoría</td><td></td><td></td></tr>
<tr><td></td><td>Experiencia</td><td>Experiencia en definición de estrategias de seguridad de la información y gobernanza en el sector financiero

Experiencia en la creación e implementación de estrategias y principios, prácticas y actividades de seguridad de la información

Amplio conocimiento de todas las funciones de seguridad de la información (Referencia Norma ISO 27002) y cómo se relacionan con el negocio.</td><td rowspan="3">Aplicar técnicas de auditoría apropiadas para evaluar si se logran las metas de las personas, Habilidades y Competencias, es decir, que se cumplan los criterios de evaluación.</td><td></td><td></td></tr>
<tr><td></td><td>Calificación</td><td>CISM</td><td></td><td></td></tr>
<tr><td></td><td>Conocimiento</td><td>Capacidad para:
• Definir una estrategia de seguridad de la información que está alineado con la estrategia de la empresa
• Desarrollar políticas de seguridad de la información y elaborar indicadores para medir efectivamente el conocimiento de las políticas:</td><td></td><td></td></tr>
</table>

Etapa B— Comprender los habilitadores, establecer criterios adecuados de evaluación y realizar la evaluación					
Ref.	**Procedimientos de Auditoría**			**Referencia cruzada**	**Comentarios**
		• tendencias de seguridad de la información, servicios y disciplinas • Los requisitos legales y reglamentarios que afectan a la seguridad de información			
	Habilidades técnicas	Amplio conocimiento de la gestión de identidades de acceso, gestión de amenazas y vulnerabilidad, la arquitectura de seguridad de la información y protección de datos			
	Habilidades de comportamiento	• líder reconocido con excelentes habilidades de comunicación y capacidad de interactuar con todos los niveles de la empresa • Orientación de negocios • Pensamiento estratégico de alto nivel • Un entendimiento del panorama general			
	Para la ***operación de seguridad de la información***, los siguientes objetivos y criterios asociados se pueden abordar.			**B-8.3. Cap. IV**	
	Meta	**Criterio**	**Prueba de Auditoría**		
	Experiencia	- Sólida experiencia técnica en seguridad de la información - Conocimiento técnico práctico de todas las funciones de seguridad de la información en una entidad financiera y la comprensión de cómo se alinean con los objetivos de negocio			

Etapa B— Comprender los habilitadores, establecer criterios adecuados de evaluación y realizar la evaluación					
Ref.	**Procedimientos de Auditoría**			**Referencia cruzada**	**Comentarios**
	Educación	Experiencia en la aplicación de las directivas del programa de gestión de seguridad de la información para la protección de los activos de información del Banco y reducción al mínimo del riesgo de pérdidas			
	Calificación	- CRISC, CISSP - Certificaciones específicas de la infraestructura de seguridad implementada en la entidad.			
	Conocimiento	• programas de seguridad de la información Gestión de equipo, políticas, procedimientos y normas que se relacionan con las actividades empresariales • Monitoreo de registro, registro la agregación y análisis de registros.			
	Habilidades técnicas	Amplia experiencia respeto de las operaciones informáticas El conocimiento profundo de los sistemas Windows® / UNIX® funcionamiento, métodos de autenticación, cortafuegos, *routers*, servicios *web*, etc.			
	Habilidades de comportamiento	• Competencia en la gestión de proyectos y personal • Mentalidad analítica, orientación detalle • Habilidades de comunicación y facilitación fuertes • Habilidades de gestión del tiempo fuerte			

Etapa B— Comprender los habilitadores, establecer criterios adecuados de evaluación y realizar la evaluación				
Ref.	**Procedimientos de Auditoría**		**Referencia cruzada**	**Comentarios**
B-8.5	Evaluar el diseño de **personas, habilidades y competencias**, es decir, evaluar en qué medida se aplican las buenas prácticas esperadas.		**B-8.5. Cap. IV**	
	Buena práctica	**Prueba Auditoría**		
	Las habilidades y competencias están definidas.	• Determinar que un inventario de habilidades y competencias se mantiene por unidad organizacional, función de trabajo e individual. • Evaluar el análisis de la brecha entre el portafolio requerido de Habilidades y Competencias y el inventario actual de las habilidades y capacidades.		
	Los niveles de habilidades están definidos.	• Evaluar la flexibilidad y el rendimiento de conocer el desarrollo de habilidades para hacer frente a las brechas identificadas entre los niveles de habilidad necesarios y actuales.		

La etapa C, en la cual se documentan los resultados y se exponen los hallazgos encontrados en el estudio de auditoría, forma parte integral de los capítulos IV y V.

CAPÍTULO IV
RESULTADOS DE LA EVALUACIÓN

1. Resultados de la evaluación del proceso APO13 Gestionar la Seguridad

Producto de la ejecución del programa de auditoría, descrito en el capítulo III, cuya estructura se fundamenta en la guía genérica de auditoría del proceso APO13 Gestionar la Seguridad, a continuación se detallan los resultados obtenidos, en donde en la etapa A se determinó el alcance de la evaluación y en la etapa B se comprendieron y evaluaron cada uno de los habilitadores relacionados con el proceso de gestión de la seguridad de la información, conforme al alcance definido y los componentes de las dimensiones comunes, a saber: interesados, metas, ciclo de vida y buenas prácticas, según lo establece COBIT.

A. Determine el alcance de la evaluación de auditoría

A-1.1 Identificar los usuarios interesados en el informe de auditoría y su participación en el proceso de evaluación.

Partes Interesadas Banco	**Participación en evaluación**
Gerencia General Corporativa	Le corresponde patrocinar la implementación de las iniciativas del sistema de gestión de la seguridad de la información del Banco. Se evaluará su participación y apoyo en la gestión de la seguridad de la información y es un usuario interesado en conocer los resultados generales de la auditoría.
Subgerencia General de Negocios	Por la importancia que implica el manejo de la información como uno de los recursos críticos del negocio bancario, a estas instancias les interesa
Subgerencia General de Operaciones	
Dirección General Corporativa	

Dirección de Riesgo Corporativo	conocer los resultados de la auditoría y gestionar mejoras en los roles que tienen a cargo, respecto a los controles implementados sobre la seguridad de la información.
Dirección Tecnología de Información Área Seguridad Operativa Informática	Estas dependencias son responsables del diseño, desarrollo, implementación y monitoreo continuo de herramientas para el control de la seguridad de la información en la infraestructura tecnológica. Son áreas auditadas dentro de la evaluación.
Dirección de Gestión Unidad de Continuidad del Negocio	Al mantener algunas de las funciones de gestión estratégica de la seguridad de la información, además de ser los fiscalizadores de las iniciativas del Plan de gestión de la seguridad de la información que el Banco está implementando, les corresponde un rol de áreas auditadas dentro de la evaluación.

A-1.2 Identificar las partes interesadas, responsables y encargados del proceso a evaluar

Conforme la descripción de los roles y estructuras organizativas de COBIT 5 relacionadas con la Gestión de la Seguridad de la Información los encargados en el Banco que se asocian a los roles definidos en el proceso APO13, referentes a responsable de ejecución (R) y responsable de rendición de cuentas (A) son los siguientes:

Estructura organizativa Banco	**Rol en el Banco**	**Descripción del rol asociado en COBIT 5**
Dirección de Gestión Unidad de Continuidad del Negocio	R	Director de Seguridad de la Información (CISO). El ejecutivo de mayor cargo responsable de todos los aspectos de la seguridad de la información de la empresa, en todas sus formas. Importante aclarar, que el rol de CISO no está formalmente establecido en el Banco, y que la Dirección de Gestión, a través

		de la Unidad de Continuidad del Negocio asume algunas responsabilidades de este rol.
División de Control Operativo	A	Jefe de Administración de TI. Un miembro de la gerencia responsable de los registros relacionados con TI y responsable de soportar las cuestiones administrativas de TI.
Área de Seguridad Operativa Informática	R	Gerente de Seguridad de la Información. Un individuo que gestiona, diseña, supervisa y/o evalúa la seguridad de la información de la empresa.
CITI (Comité interno de Tecnología de Información), conformado por la Dirección de TI y las jefaturas de División de esa Dirección	R	Comité de dirección de TI. Un comité a nivel de dirección ejecutiva que ayuda en la realización de la estrategia de TI, supervisa la gestión del día a día en la entrega de servicios de TI y proyectos de TI, y se centra en aspectos de implementación.

A-2.1 Comprender la estrategia y las prioridades de la entidad

Conforme la revisión del Plan Estratégico de Tecnología de Información del Banco Popular para el período 2013-2015, se determinó que uno de los objetivos estratégicos contiene una actividad y métricas asociadas para dar seguimiento a la implementación del Plan de Seguridad de la Información, siendo responsables la Dirección de TI y la Dirección de Gestión.

A-2.2 Comprender el contexto interno de la entidad

Los factores ambientales internos del Banco Popular que pueden influir en el rendimiento del proceso de Gestión de la Seguridad de la Información son los siguientes:

Factor Interno	Descripción
Renovación de plataforma tecnológica del Core Bancario	Este proyecto consume gran parte de los recursos técnicos de la Dirección de TI, modifica procesos, procedimientos actuales, y posee la prioridad total por encima de proyectos como la implementación del sistema

	de gestión de la seguridad de la información.
Renovación de infraestructura de servidores en ambiente de producción	Este proyecto agrega nuevas oportunidades/amenazas a la infraestructura tecnológica actual, incorpora en gran medida elementos de virtualización, consolidación de infraestructura, e implementación de modelos de tercerización, basados en servicios administrados.
Implementación y puesta en operación de Centro de Procesamiento de Datos primario del Banco.	Incorpora una serie de mejoras en términos de seguridad de la información, principalmente en la seguridad física y la continuidad del servicio. No obstante, su operación demanda cambios en los procesos y procedimientos actuales e incorpora modelos de tercerización, basados en servicios administrados.
Implementación de los procesos de la normativa SUGEF14-09. (COBIT 4.0)	Este proceso demanda recursos de distintas áreas de la Dirección de TI y conlleva el rediseño de procesos y procedimientos, para cumplir los objetivos de mantener un nivel de madurez 3, en los procesos COBIT 4.0, conforme lo establece la normativa de SUGEF. Este proceso es prioritario sobre las iniciativas del sistema de gestión de seguridad de la información.
Desarrollo del plan del sistema de gestión de la seguridad de la información	El desarrollo de las iniciativas que contempla el proyecto del sistema de gestión de seguridad de la información facilitará al Banco el desarrollo y mantenimiento de un razonable nivel de madurez, en los distintos dominios de la norma ISO 27001. Es un proceso que requiere ser revalidado para efectuar los ajustes que sean requeridos, dado el plazo acordado por la Administración de 5 años para la implementación de todas las iniciativas.
Estructura organizacional de la Dirección de TI, pendiente de reajustarse.	Conforme lo indicado en el Plan Estratégico de Tecnología de Información del Banco Popular para el período 2013-2015, dada la estrategia definida se deberá realizar ajustes a la estructura organizacional de la Dirección de TI, con el objetivo de orientarla a un enfoque de servicios. No obstante, dadas las prioridades en la ejecución de otros proyectos de mayor impacto para el Banco, como lo es la actualización del Core Bancario, la reestructuración de la Dirección de TI se ha postergado.

A-2.3 Comprender el contexto externo de la entidad

Respecto a los factores externos que afectan la implementación del sistema de gestión de la seguridad de la información en el Banco Popular, los más representativos se relacionan con normas, políticas y procedimientos regulatorios que se requieran implementar en las entidades del sector financiero, por ejemplo: los requisitos de PCI-DSS, regulaciones emitidas por la Contraloría General de la República e inclusive el mismo cumplimiento de niveles de madurez de la normativa SUGEF 14-09.

A su vez, el incremento exponencial de amenazas a la seguridad de la información para la consecución de delitos informáticos, constituye un elemento que requiere de atención especial, principalmente en el sector financiero, el cual es sumamente atractivo para los delincuentes.

A-2.4 Dado el objetivo general de la evaluación, traduzca las prioridades estratégicas identificadas en metas específicas para la evaluación.

Figura 8 Metas que forman parte del Alcance de la Evaluación

Mapeo entre las Metas Corporativas de COBIT 5 y las Metas relacionadas con TI en Proceso APO13 delimitado al Alcance de la Evaluación			Meta Empresarial	
			Continuidad y disponibilidad del servicio de negocio	Cumplimiento con las políticas internas
			7	15
Meta relacionada con las TI (Proceso APO13)				
Interna	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones	P	P
	14	Disponibilidad de información útil y relevante para la toma de decisiones	P	

Fuente: COBIT 5, Marco de Referencia

Se delimita el alcance de la evaluación a las metas relacionadas con la TI de la dimensión de procesos internos y a las metas empresariales prioritarias asociadas a esas metas de TI. Considerando como temas prioritarios para el sistema de

gestión de la seguridad de la información, la seguridad de infraestructura, procesamiento y aplicaciones y la disponibilidad de información integra y útil para el negocio bancario.

A-2.5 Definir los límites organizacionales de la evaluación

Las áreas auditadas que serán consideradas en el programa de auditoría son el Área de Seguridad Operativa Informática de la Dirección de Tecnología de Información y la Unidad de Continuidad del Negocio de la Dirección de Gestión, ambas como áreas que les corresponde la responsabilidad y rendición de cuentas en cuanto a la gestión de la seguridad de la información del Banco.

B Comprender los habilitadores, establecer criterios adecuados de evaluación y realizar la evaluación la Seguridad

B-1.1 Las siguientes métricas y valores esperados se definieron para las metas clave de la entidad, definidos en la etapa A-2.4.

Métrica	Resultado esperado	Resultado Prueba Auditoría
Número de interrupciones en el servicio al cliente provocando incidentes significativos	Ninguna interrupción del servicio al cliente en el último año, provocada por un incidente de seguridad de la información.	Los resultados de un informe de la Auditoría Interna del Banco de finales del 2014 sobre Servicios de Seguridad, indican que en el último año no se han detectado incidentes de seguridad significativos que interrumpan el servicio al cliente. Si bien, se han registrado infecciones por código malicioso en equipos de usuario final, el alcance del ataque ha sido reducido a un máximo de 5

		equipos y no ha ocasionado problemas en los servicios. Las causas de estas infecciones se originan por la falta de actualización de la consola *antimalware* en los equipos infectados.
• El número de incidentes relacionados con el incumplimiento de la política de Seguridad de la Información del Banco • Porcentaje de los interesados que comprenden la Política de Seguridad de la Información del Banco	Registro de los incidentes presentados por el incumplimiento de la Política de Seguridad de la Información y detalle de las sanciones aplicadas 90% de evaluaciones ganadas en el último año por el personal sobre el conocimiento de la Política de Seguridad de la Información	Se consultó mediante correo electrónico a la jefatura de la Unidad de Continuidad del Negocio, como área que diseñó la Política de Seguridad de la Información del Banco e indicó que no se cuenta con información sobre las métricas de evaluación indicadas. En términos generales la política se diseñó y publicó pero no se generan actividades para evaluar su comprensión y cumplimiento.

Las siguientes métricas y valores esperados se definieron para las principales metas relacionadas con TI definidas en la etapa A-2.4.

Métrica	Resultado esperado	Resultado Prueba Auditoría
• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o daño de imagen • Número de servicios de TI con los requisitos de seguridad pendientes	Ningún incidente de seguridad causante de pérdidas financieras para el Banco en el último año, producto de *malware.* Ningún servicio crítico de TI y/o negocio sin la protección *antimalware.*	Según un informe de la Auditoría Interna del Banco de finales del 2014, las infecciones por *malware* en equipos de cómputo de la red de datos del Banco han sido reducidos y no han ocasionado problemas en los servicios, ni en los procesos de negocio.
Número de incidentes en los	Ningún incidente de seguridad	

procesos de negocio causados por la indisponibilidad de la información	de la información en el último año que afectara los procesos de negocio y la integridad, confiabilidad y disponibilidad de la información.	En el mismo informe si se detectaron al menos 10 equipos sin la protección *antimalware*, por tanto, la Auditoría Interna emitió una recomendación para el Área de Seguridad Operativa Informática para que se cerciore de que todos los equipos conectados a la red de datos cuenten con protección activa y con las firmas actualizadas.

B-2.2 Para todos los roles definidos en la matriz RACI del proceso APO13 con (A) y (R), verifique que exista en el Banco una asociación clara del mismo nivel jerárquico recomendado.

Estructuras organizacionales COBIT 5	**Estructuras organizacionales Banco**	**Equivalencia**
Oficina de Gestión de Proyectos	Oficina de Administración de Proyectos	Sí
Director de Seguridad de la Información (CISO)	El Banco no tiene definida esta función	NO
Director de Informática (CIO)	Dirección de Tecnología de Información	Sí
Jefe de Arquitectura del Negocio	Área de Arquitectura Empresarial	Sí
Jefe de Desarrollo	División de Desarrollo de Servicios	Sí
Jefe de Operaciones de TI	División de Operación de Servicios	Sí
Jefe de Administración de TI	División de Control Operativo	Sí
Gestión de Servicio (Service Manager)	División de Gestión de Servicios	Sí
Gestor de Seguridad de la Información	Área de Seguridad Operativa Informática	NO
Gestor de Continuidad del Negocio	Unidad de Continuidad del Negocio	Sí
Gestor de Privacidad de la Información	Unidad de Continuidad del Negocio	NO

La figura de Director de Seguridad de la Información, conocido como CISO no existe en la estructura organizacional del Banco, si bien la Dirección de Gestión, por medio de la Unidad de Continuidad del Negocio ha asumido algunas actividades estratégicas de gestión de la seguridad de la información, mediante el diseño de normativa y la fiscalización del plan de seguridad de la información, es claro que a falta de esa figura, la visión de la seguridad de la información se enfoca en aspectos de orden operativo, en donde es el Área de Seguridad Operativa Informática de la Dirección de TI, quien tiene mayor visibilidad en la población bancaria, con el riesgo de considerarse los procedimientos de control establecidos como privativos, al carecer de un proceso paralelo de culturización. Por otra parte, si bien el rol de gestión de seguridad de la información cuenta con un área afín en el Banco, se considera que el nivel jerárquico es menor en el Banco al recomendado por el marco de referencia COBIT, el cual establece una gerencia de gestión de la seguridad de la información encargada de la gestión, diseño, supervisión y evaluación de la seguridad de la información de la empresa.

B-2.2 Prácticas del Proceso APO13. Cuestionarios aplicados a uno de los funcionarios de la Unidad de Continuidad del Negocio, encargado de la gestión de seguridad de la información.

APO13.01 Establecer y mantener un Sistema de Gestión de la Seguridad de la Información

1. ¿Se definió el alcance y los límites del Sistema de Gestión de la Seguridad de la Información, conforme las características del Banco, su estructura organizacional, activos de información y tecnología?

Sí. El trabajo realizado por la empresa consultora para el diseño del plan del sistema de gestión de la seguridad de la información contempló la revisión de la situación actual de la entidad respecto a la gestión de la seguridad de la información, además se realizaron inventarios de activos de información, infraestructura y estructuras organizacionales, incorporando el diseño de un plan de cierre de brechas.

2. ¿Se alineó el Sistema de Gestión de Seguridad de la Información con el enfoque global de la gestión de la seguridad en el Banco?

Sí. A la División de Seguridad Bancaria le fueron designadas responsabilidades en una de las iniciativas para la implementación del plan de gestión de la seguridad de la

información. Actualmente, el enfoque global de seguridad de la información posee un nivel básico de madurez.

3. ¿Al implementar cambios en el Sistema de Gestión de la Seguridad de la Información, se requiere la autorización de la Gerencia General Corporativa u otra instancia, por ejemplo la Dirección de TI?

Sí. Todo lo relacionado con los cambios en la gestión de la seguridad de la información es aprobado por la Dirección de Gestión, quien soporta sus decisiones en el criterio que emita la Unidad de Continuidad del Negocio. Por otra parte, los cambios al proyecto del plan de gestión de la seguridad de la información son revisados y aprobados por un comité gerencial ejecutivo.

4. ¿Fueron definidos y comunicados los roles y las responsabilidades de la gestión de la seguridad de la información en el Banco?

Sí. Existe un acuerdo de división de funciones entre la Dirección de Gestión y la Dirección de TI. Se considera que si están claros los roles y responsabilidades, no obstante, en la práctica no se participa en todas las decisiones relacionadas con la seguridad de la información a la Dirección de Gestión.

5. ¿Fue comunicado y comprendido el enfoque del Sistema de Gestión de la Seguridad de la Información y su alineación con la estrategia del Banco?

Sí. Se ha realizado procesos de divulgación de la estructura actual, por medio de comunicación masiva a través de correos electrónicos, además en reuniones presenciales y por medio de video conferencia con jefaturas de diversas áreas del negocio y soporte del Banco se han brindado detalles del plan de seguridad de la información y del rol que asume la Dirección de Gestión.

APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.

1. ¿Se formuló y mantiene un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura tecnológica del Banco?

No. Se trabaja con un inventario de riesgos sobre la seguridad de la información que fueron levantados por el consultor y sobre este inventario se desarrolla un plan de cierre de brechas. Sin embargo, la entidad no cuenta con un perfil de riesgos de la seguridad de la información como lo define COBIT.

2. ¿Se han desarrollado propuestas para implementar el plan de tratamiento de riesgos de seguridad de la información, sustentados en casos de negocio adecuados?

No. Tal y como se indicó en la pregunta anterior, el Banco no cuenta con un perfil de riesgos de seguridad de la información como lo define COBIT. Inclusive se determinó

que los eventos de riesgos de seguridad de la información identificados por la Dirección de Riesgos Corporativa no concuerdan con los riesgos identificados por el consultor, ni tampoco están siendo considerandos en el desarrollo del plan de gestión de la seguridad de la información. Con el desarrollo de las iniciativas del plan de seguridad de la información, se espera el cierre de las brechas identificadas por el consultor.

3. ¿Se han establecido métricas para la medición de la efectividad de las prácticas de gestión relacionadas con el Sistema de Gestión de la Seguridad de la Información?

No. Como parte del plan de gestión de la seguridad de la información se diseñaron algunos indicadores, no obstante, no se han aplicado hasta el momento, ya que forma parte de los procesos aún en desarrollo.

4. ¿Qué programas de formación y concienciación en seguridad de la información han sido recomendados e implementados?

Se ha realizado publicaciones masivas a través de correo electrónico institucional, y boletines internos del Banco como parte de un plan de concientización sobre seguridad de la información. Así mismo, se han desarrollado varias videoconferencias a jefaturas de la entidad enfocadas en dar a conocer aspectos relevantes de la política de seguridad de la información del Banco. También existe una iniciativa como parte del plan de gestión de la seguridad de la información para generar programas de formación y concientización.

APO13.03 Supervisar y revisar el Sistema de Gestión de la Seguridad de la Información.

1. ¿Se han realizado revisiones del Sistema de Gestión de la Seguridad de la Información para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en sus procesos?

No. Puesto que el plan con horizonte a cinco años para el desarrollo del sistema de gestión de la seguridad de la información se encuentra en proceso de implementación y únicamente se está revisando el alcance y estado del proyecto de forma anual.

2. ¿Se mantiene un registro de las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del Sistema de Gestión de la Seguridad de la Información?

No. En este momento no se aplica. La revisión se enfoca en la medición y revisión de los riesgos del proyecto de implementación del plan de gestión de la seguridad de la información y no del sistema de gestión como tal.

¿La rendición de cuentas y la responsabilidad en las actividades relacionadas con el Sistema de Gestión de la Seguridad de la Información han sido asignadas?

Sí. Las responsabilidades han sido asignadas, pero se requiere un mayor nivel de madurez para una ejecución efectiva y consistente en la Institución.

¿Considera usted que la rendición de cuentas y la responsabilidad son asignadas en el nivel adecuado en el Banco?

No. A pesar de encontrarse en un nivel de Dirección, las actividades estratégicas de gestión de la seguridad de la información, no cuentan con el nivel adecuado de visibilidad en la Institución.

B-3.1 Comprender el contexto de la Política de Seguridad de la Información del Banco Popular

La Política de Seguridad de la Información del Banco Popular se establece con el fin de alinear el Sistema de Gestión de la Seguridad de la Información a marcos regulatorios, así como de actualizar la normativa vigente de acuerdo con la evolución de la tecnología en el entorno actual. De esta forma, según se indica en la política, el Banco define esquemas de protección de su información para reducir la probabilidad de acceso no autorizado, divulgación, mal uso o alteración de sus sistemas e información, de acuerdo con la norma ISO 27001.

La propuesta de la Política de Seguridad de la Información del Banco Popular fue uno de los entregables que desarrolló el consultor contratado para el desarrollo del Plan de Seguridad de la Información del Banco.

B-3.2 Comprender las partes interesadas de la Política de Seguridad de la Información del Banco Popular. Las partes interesadas en la política incluye: quienes establecen la política y los que deben cumplirla.

Conforme el alcance definido en la Política de Seguridad de la Información del Banco Popular las partes interesadas incluyen a toda la población del Banco y todo personal externo que interactúe con activos de información del Banco, ya sea digital o impresa. Los cuales deben acatar los lineamientos indicados en la política.

Así mismo, se indica que es responsabilidad de la Dirección de Gestión validar la política de seguridad de la información y sus actualizaciones y a la Gerencia General Corporativa le corresponde su aprobación.

B-3.3 Evaluar si se logran las metas (resultados) de la Política de Seguridad de la Información del Banco, es decir, evaluar su efectividad.

Prueba de Auditoría	Resultado
Verifique que el conjunto de requisitos establecidos en la Política de Seguridad de la Información del Banco es exhaustivo en su cobertura.	**Insatisfactorio.** Se evidenció que la Política cubre los dominios de la norma ISO 27001, por tanto, la distribución de roles y responsabilidades si es exhaustiva en la cobertura de cada dominio. Sin embargo, muchas de las actividades señaladas son generales, situación que puede afectar la medición de su cumplimiento, así como de su grado de madurez.
Verifique la flexibilidad de los requisitos y clausulas establecidas en la Política de Seguridad de la Información, es decir, que están estructuradas de tal manera que es fácil añadir o actualizar como las circunstancias lo requieren.	**Satisfactorio**. Al ser una política institucional, la actualización de sus contenidos debe ser aprobada por la Gerencia General. Además, según se evidenció, la política se diseñó en términos generales que no hacen mención a infraestructuras tecnológicas específicas u otros habilitadores o tendencias que puedan variar en el tiempo, por tanto, su contenido puede ser actualizado, sin mayor dificultad.
Verifique que la Política de Seguridad de la Información está disponible para todos los interesados.	**Satisfactorio**. La Política de Seguridad de la Información está publicada como uno de los capítulos del Manual de Políticas y procedimientos Institucionales, y es accesible desde la Intranet del Banco. No obstante, al ser parte de un manual de políticas generales de la Institución podría perder visibilidad.
Verifique que la Política de Seguridad de la Información es fácil de navegar y tiene una estructura lógica y jerárquica.	**Insatisfactorio**. En términos generales, la política fue diseñada considerando cada uno de los dominios de la norma ISO 27001, por tanto, la distribución de responsabilidades y roles se realiza por cada uno de los dominios. Esta forma de organización es compleja y difícil de navegar si un usuario desea conocer cuáles son todas sus responsabilidades, puesto que tendría que extraer de cada dominio lo correspondiente y verificar que

Prueba de Auditoría	Resultado
	inclusive no existan casos en donde una actividad no contradiga otra. Por tanto, también su actualización, debe ser realizada cuidadosamente.

B-3.5 Comprender las buenas prácticas relacionadas con los principios, las políticas y los marcos de referencia y los resultados esperados. Evaluar el diseño de la Política de Seguridad de la Información.

Prueba de Auditoría	Resultado
Verifique que se describa el alcance de la Política y que se indique la fecha de validez.	**Satisfactorio**. Según se evidenció en el apartado 3 de la Política se establece su alcance, así mismo, al formar parte del Manual de Políticas Institucionales, no se lleva un detalle de fecha de validez individualizado por política, sino para todo el documento, así como también del control de cambios.
Verifique que el procedimiento de excepción y escalamiento se describe, explica y se conoce comúnmente.	**Insatisfactorio**. No se evidenció la existencia de procedimientos de excepción o escalamiento en la Política de Seguridad de la Información del Banco.
A través de la observación de una muestra representativa, compruebe que la excepción y el procedimiento de escalamiento no se han convertido en un procedimiento estándar de facto.	No aplica, dado el resultado de la prueba anterior.
Verifique que el mecanismo de comprobación del cumplimiento y las consecuencias del no cumplimiento de la Política de Seguridad de la Información se describen claramente y se hacen cumplir.	**Insatisfactorio**. El apartado sexto de la Política establece que en caso de incumplimiento por parte de los funcionarios y funcionarias o terceros, se exponen a las acciones administrativas o legales que correspondan; no obstante, la política no es clara en cuanto a sanciones o penalidades específicas, así mismo, no señala cómo se medirá el cumplimiento de la Política. Por otra parte, se evidenciaron casos en donde la responsabilidad de ejecutar una actividad en particular no es clara, tal y como se muestra en el

Prueba de Auditoría	Resultado
	siguiente ejemplo, en el cual, la responsabilidad sobre la omisión de la instrucción no está definida, lo que dificulta la rendición de cuentas: "*En caso de que cualquier equipo del Banco necesite ser trasladado fuera de las instalaciones por mantenimiento, se debe realizar las acciones necesarias para salvaguardar la información del Banco".* En general, no se indica quién debe actuar y cuáles acciones se deben ejecutar.

B-4.2 Comprender todos los interesados las siguientes estructuras organizativas:

- Área de Seguridad Operativa Informática
- Unidad de Continuidad del Negocio (actividades de Seguridad de la información).

Determinar mediante la revisión de documentación (políticas, gestión de comunicaciones, etc.) los interesados clave de la función, es decir:

- Titular de la función y / o miembros de las Estructuras Organizacionales
- Otros interesados clave afectados por las decisiones de la función de las Estructuras Organizativas.

La Unidad de Continuidad del Negocio, forma parte de la Dirección de Gestión. Según se evidenció en el Manual de la Organización, esta Unidad tiene a cargo además de la administración del Sistema de Gestión de la Continuidad del Negocio del Banco, la administración del Sistema de Gestión de Seguridad de la Información del Banco, mediante la aplicación del estándar ISO-27001. Las acciones y actividades que ejecute esta Unidad respecto a la gestión de la seguridad de la información afecta a todo el Banco. En este manual se mencionan las funciones generales asignadas a esta Unidad, respecto a la gestión de la seguridad de la información.

El Área de Seguridad Operativa Informática es un área técnica que forma parte de la División de Control Operativo y esta a su vez de la Dirección de Tecnología de Información. Su objetivo es planear, coordinar y administrar los servicios de Seguridad de la Información en el Banco, con el fin de garantizar una seguridad razonable en todas las operaciones realizadas. Su enfoque es operativo y los controles y procedimientos que aplique a la infraestructura tecnológica afecta las operaciones y procesos del negocio.

B-4.4 El diseño de las dos estructuras organizativas se evalúa a continuación:

Prueba de Auditoría	**Resultado**
Verificar si los principios operativos están debidamente documentados.	**Satisfactorio**. Según se verificó ambas estructuras organizativas cuentan con procedimientos operativos documentados y actualizados.
Evaluar si la composición de la estructura organizativa es equilibrada y completa, es decir, todos los interesados requeridos están lo suficientemente representados.	**Insatisfactorio**. Área de Seguridad Operativa Informática: Cuenta con una estructura organizativa que incluye al jefe del área y técnicos encargados de la gestión de los servicios de seguridad. Sin embargo, según se evidenció esta Área también tiene a cargo otras actividades no relacionadas con la seguridad de la información, por ejemplo la administración de la infraestructura de comunicación unificada. Unidad de Continuidad del Negocio: Cuenta con un jefe de unidad y personal que administra la gestión de continuidad y la gestión de seguridad de la información. Sobre estas estructuras es importante agregar que al separarse en direcciones distintas la función estratégica y de gobierno de seguridad de la función de gestión operativa de la seguridad de la información, la comunicación y control es más complejo, así mismo, al no existir formalmente una estructura de gestión de la seguridad de la información, esta función pierde visibilidad y la gestión de la seguridad se centra en la función operativa.
Compruebe si se ha definido el ámbito del control de la Estructura Organizativa. Evaluar si el ámbito de control es adecuado, es decir, la estructura organizativa tiene el derecho de tomar todas las decisiones que debería.	**Insatisfactorio**. En términos de la gestión estratégica de la seguridad de la información, la estructura actual dificulta la independencia y control de esta función, al ser administrada desde una estructura organizacional que además de estar ubicada en una posición que no es estratégica, tiene que distribuir sus recursos entre otras funciones como la continuidad del negocio y privacidad de la

Prueba de Auditoría	**Resultado**
	información, además pertenece a una Dirección que también tiene diversas actividades no relacionadas con la seguridad de la información. Del mismo modo, el Área de Seguridad de la Información pertenece a la División de Control Operativo y esta a su vez reporta a la Dirección de Tecnología de Información, por tanto, el ámbito de control de esta Área se ve limitado a las decisiones que tome tanto la Dirección de TI como sus divisiones, siendo los temas de seguridad parte de un portafolio de iniciativas, proyectos y otras prioridades que debe atender la estructura de tecnología de información del Banco.
Verificar que el poder de decisión de la estructura organizativa está definido y documentado, además que se cumple y respeta.	**Insatisfactorio**. Respecto al poder de decisión, según se evidenció, una de las conclusiones de la consultoría en el diagnóstico de la situación actual respecto a la gestión de la seguridad de la información indica que "*Aunque los límites entre la Dirección de Gestión Corporativa y Tecnologías de Información están establecidos, falta que la función de Seguridad de la información (Dirección de Gestión Corporativa) se apropie de las responsabilidades implantadas, actividad necesaria para garantizar un adecuado gobierno de la seguridad de la información". Sobre esta posición es importante, agregar que la Dirección de Gestión delegó en la Unidad de Continuidad del Negocio la administración de la gestión de seguridad de la información y que la estructura actual no brinda el suficiente poder de decisión a esta Unidad para gestionar los temas de seguridad de la información.*

B-4.5 Evaluar la medida en la que se gestiona el ciclo de vida de las estructuras organizativas descritas en el punto B-4.2.

Prueba de Auditoría	Resultado
Verifique a través de observación que la estructura organizacional está formalmente establecida.	**Insatisfactorio**. Conforme la revisión de la estructura organizacional y el Manual de la Organización se determinó que la función de seguridad de la información a nivel estratégico en el Banco Popular no está formalmente establecida en la estructura organizacional; como se ha indicado, la Dirección de Gestión a través de la Unidad de Continuidad del Negocio asume algunas funciones. En el ámbito operativo, la gestión de los servicios de seguridad de la información está formalmente establecida en el organigrama institucional, representado en el Área de Seguridad Operativa Informática.
Verifique si el desempeño de la estructura organizativa y de sus miembros se supervisa y evalúa con regularidad por asesores competentes e independientes.	**Satisfactorio**. Únicamente la Auditoría Interna del Banco mantiene una función de verificación independiente y objetiva sobre la gestión que realizan las distintas dependencias de la entidad, a través de la ejecución de estudios de auditoría por riesgos. En el caso de entes externos, la SUGEF tiene a cargo la auditoría del cumplimiento de la normativa 14-09, no obstante, se fundamenta en el marco de referencia de COBIT 4.0; por tanto, la gestión de seguridad de la información, se evalúa en un ámbito operativo más que de gobierno. Por otra parte, la norma ISO 27001 no es de cumplimiento mandatorio para el Banco, únicamente es un marco de referencia, el cual está siendo utilizado para estructurar el plan de gestión de la seguridad de la información.

B-5.3 Evaluar si los resultados del comportamiento deseado se cumplen, es decir, evaluar su eficacia.

Comportamiento: *"La gente respeta la importancia de las políticas y los principios de seguridad de la información".*

Prueba de Auditoría	Resultado
Verificar mediante entrevista a los encargados de las estructuras organizativas con roles de responsabilidad y rendición de cuentas en la gestión de la seguridad de la información si consideran que la Política de Seguridad de la Información influye en el comportamiento deseado del personal, respecto a los aspectos culturales y de control relacionados con la seguridad de la información. Indague sobre el criterio de estos encargados, respecto al entendimiento de la Política de Seguridad de la Información por parte de los funcionarios de la entidad.	Preguntas a uno de los funcionarios de la Unidad de Continuidad del Negocio, encargado de funciones relacionadas con la gestión de la seguridad de la información: 1. ¿Considera usted que la Política de Seguridad de la Información influye en el comportamiento deseado del personal, y brinda insumos para propiciar una cultura de seguridad de la información? Sí. Considero que influye, a pesar que falta divulgación de la política en la totalidad de la población bancaria, la política es una base y representa la herramienta principal de trabajo en la que se fundamenta la gestión de la seguridad de la información. 2. ¿Se promueve a nivel institucional, la cultura de la seguridad de la información y la comprensión de las responsabilidades de la Política de Seguridad de la Información? Sí. A la fecha se han realizado videoconferencias con jefaturas del Banco para explicar aspectos generales de la Política de Seguridad de la Información, basados principalmente en una explicación de responsabilidades. No obstante, se depende de las jefaturas para el traslado de estos conocimientos a su personal. Por otra parte, también se está realizando un levantado de los propietarios de los datos, con la finalidad de poder explicarles su rol y responsabilidades, respecto a la seguridad de la información.

	3. ¿Considera que la Política de Seguridad de la Información es entendible por la Población bancaria? Sí. Se considera que la Política es comprensible, no obstante, es importante agregar que está orientada a responsabilidades por apartados y no por actores, lo que podría dificultar su revisión. A pesar de ello, no se ha recibido retroalimentación para mejorar o modificar el esquema actual de la Política.

B-5.5 Evaluar el diseño de la Cultura, Ética y Conducta, es decir, evaluar en qué medida se aplican buenas prácticas.

Prueba de Auditoría	Resultados
¿Verifique mediante consulta al encargado de la Unidad de Continuidad del Negocio si se aplican métricas para medir la calidad de la comunicación e información brindada a la población bancaria sobre la gestión de la seguridad de la información?	Conforme lo indicado en entrevista realizada con uno de los funcionarios de la Unidad de Continuidad del Negocio, en la actualidad no se realiza mediciones. El diseño de métricas forma parte de una de las iniciativas del plan de gestión de la seguridad de la información que se encuentra en desarrollo. Por otra parte, a la fecha no se conocen necesidades específicas o retroalimentación sobre la gestión de seguridad de la información en el Banco.
¿Verifique mediante consulta al encargado de la Unidad de Continuidad del Negocio si en las herramientas de evaluación y pago de incentivos al personal del Banco se ha contemplado incluir temas de gestión de la seguridad de la información, tal y como se evalúan otras metas y objetivos estratégicos?	Conforme lo indicado en entrevista realizada con uno de los funcionarios de la Unidad de Continuidad del Negocio, la inclusión de evaluaciones sobre el tema de seguridad de la información no ha sido aceptada hasta la fecha, dado el mismo desconocimiento sobre la importancia de la gestión de la seguridad de la

	información. Se ha considerado incluir algunos puntos de control en evaluaciones de control interno y riesgo operativo, pero aún se encuentra en revisión. Así mismo, el funcionario argumentó que el enfoque actual se basa en orientación general sobre la Política de Seguridad y no una capacitación formal y completa.

B-6.1 Comprender el contexto del elemento de Información: Perfil de Riesgos de Seguridad de la Información del Banco Popular

Prueba de Auditoría	Resultado
¿Verifique dónde y cuándo se utiliza el perfil de riesgos de seguridad de la información?	**Insatisfactorio**. Según se determinó el inventario de eventos de riesgos relacionados con la seguridad de la información diseñado por la Dirección de Riesgos Corporativos no fue utilizado por la Dirección de Gestión para el diseño del Plan de Gestión de la Seguridad de la Información, en su lugar, la empresa consultora, construyó su propio inventario de riesgos y los utilizó para establecer sus análisis y conclusiones.
¿Consulte al encargado de la Unidad de Continuidad del Negocio que estructuras organizacionales participan en el diseño y actualización del perfil de riesgos de la seguridad de la información del Banco?	No se aplica. Tal y como se indicó en la pregunta anterior, en el Banco hasta la fecha no se diseña un perfil de riesgos de la seguridad de la información.
¿Determine con el encargado de la Unidad de Continuidad del Negocio si el perfil actual de riesgos de la seguridad de la información está alineado con norma ISO 27001?	**Insatisfactorio**. No se evidenció la existencia de un perfil de riesgos de la seguridad de la información. El inventario de eventos relacionados con la seguridad de la información, no está alineado a la norma ISO 27001.

B-6.3 Evaluar si se alcanzan los criterios de calidad del perfil de riesgos de la seguridad de la información del Banco Popular

Prueba de Auditoría	Resultados
Solicite el perfil de riesgos de la Seguridad de la Información del Banco y determine si fue diseñado utilizando criterios objetivos, en cuanto a eventos de riesgo y su frecuencia.	**Insatisfactorio**. Se obtuvo evidencia de un inventario de riesgos relacionados con seguridad de la información, el cual fue desarrollado por la Dirección de Administración del Riesgo Corporativo. Contiene un listado de 22 tipos de eventos de riesgos, los cuales no se alinean con la norma ISO 27001. Ni se utilizan como base para el desarrollo del plan del sistema de gestión de la seguridad de la información.
Determine si el lenguaje utilizado en el perfil de riesgos de seguridad de la información es comprensible para todas las partes interesadas.	No aplica. No obstante, considerando que no se evidenció la existencia de un perfil de riesgos, sino de un inventario de eventos, se considera que el vocabulario utilizado para describir cada uno es simple y no técnico.
Verifique si el perfil de riesgos de seguridad de la información está disponible para todas las partes interesadas.	No aplica**.** No se evidenció la existencia de un perfil de riesgos de la seguridad de la información. Por otra parte, el inventario de eventos de riesgo que la Dirección de Riesgos relaciona con la gestión de seguridad de la información, está disponible para consulta de las áreas fiscalizadoras y con roles en este proceso y se solicita a la Dirección de Riesgo Corporativo. Así mismo, el inventario de riesgos diseñado por el consultor para el desarrollo del plan del sistema de gestión de la seguridad de la información está disponible para la Dirección de Gestión y la Unidad de Continuidad del Negocio, así como para otras áreas del Banco que lo requieran como la Auditoría Interna.

B-7.1 Comprender el contexto organizacional y tecnológico del servicio de protección contra *software* malicioso

Uno de los servicios de seguridad de la información que le permiten al Banco un mayor control sobre incidentes y amenazas de código malicioso es la plataforma empresarial *antimalware* y *Firewall* que se ejecuta una infraestructura cliente-servidor y protege a equipos de misión crítica y de usuario final, a través de un agente instalado en cada equipo.

La administración de este servicio es responsabilidad del Área de Seguridad Operativa Informática, lo cual incluye mantener la aplicación *antimalware* funcionando adecuadamente y con las últimas firmas publicadas por el proveedor del servicio, así como realizar el monitoreo regular, verificando que el agente se encuentre activo en todos los equipos. Sin embargo, también los usuarios tienen la responsabilidad de verificar que sus equipos cuentan con la protección *antimalware* activa y con las últimas actualizaciones, según lo indicado por el Área de Seguridad Operativa Informática.

B-7.3 Evaluar si se logran los resultados de las metas del servicio de protección contra *software* malicioso, es decir, evaluar su eficacia.

Prueba de Auditoría	Resultado
Evaluar la calidad de la descripción del Servicio y del servicio ofrecido.	**Satisfactorio**. El servicio *antimalware*, conocido por la población bancaria como "antivirus" es una de las aplicaciones de seguridad informática más reconocidas por los funcionarios, dado el uso de este tipo de herramientas en el ámbito personal. Por otra parte, su funcionalidad, instalación y actualización no requiere de la intervención del usuario, e inclusive las políticas automatizadas de grupo aplicadas a cada usuario de la red de datos no permiten que un funcionario realice modificaciones a la consola *antimalware* de su equipo de cómputo. Es importante mencionar que no se realizan verificaciones con otras herramientas del mercado, por tanto, técnicamente se desconoce si existen amenazas que el sistema *antimalware* actual no esté detectando.
Verificar la accesibilidad del servicio a todos los posibles interesados.	**Satisfactorio**. El servicio *antimalware* es accesible a todos los equipos conectados a la red de datos del Banco, inclusive su instalación es un requisito obligatorio para que un equipo se pueda agregar al dominio corporativo.
Verificar si el servicio de protección contra *software* malicioso permite mantener bajo control los incidentes de seguridad de la información, basados en *software* malicioso.	**Satisfactorio**. De acuerdo con lo indicado en una evaluación de la Auditoría Interna del último año, los incidentes de seguridad informática relacionados con *software* malicioso no son representativos y no han ocasionado mayores problemas en los servicios ofrecidos.

B-8.3 Evaluar si se logran los resultados de las Personas, Habilidades y Competencias, para las estructuras organizativas definidas en el alcance

Prueba de Auditoría	Resultado
Verifique mediante la revisión del Manual de Puestos del Banco que los requisitos para los puestos relacionados con la formulación de la estrategia de seguridad de la información en las metas relacionadas con la experiencia, calificación, conocimiento, habilidades técnicas y de conocimiento es congruente con los requisitos genéricos indicados en la guía de evaluación.	**Insatisfactorio**. Respecto al perfil de la Dirección de Gestión según la revisión del Manual de Puestos se evidenció que no se exige conocimientos en gestión de seguridad de la información, gobernanza de TI o aspectos técnicos de infraestructura de seguridad de la información. Por otra parte, en la Unidad de Continuidad del Negocio, a pesar de contar con 2 funcionarios que desarrollan a tiempo completo actividades relacionadas con la gestión de la seguridad de la información, los perfiles de sus puestos son más genéricos en el Manual de Puestos del Banco y no contemplan por ejemplo la necesidad de contar con certificaciones en seguridad de la información.
Verifique mediante la revisión del Manual de Puestos del Banco que los requisitos para los puestos relacionados con la operación de la gestión de seguridad de la información en las metas relacionadas con la experiencia, calificación, conocimiento, habilidades técnicas y de conocimiento es congruente con los requisitos genéricos indicados en la guía de evaluación.	**Insatisfactorio**. Existen diferencias con respecto al perfil genérico de la operación de la gestión de seguridad de la información. En cuanto al conocimiento específico no se exige certificaciones de seguridad de la información, por tanto, únicamente se puede medir mediante la aplicación de prueba técnica interna. Así mismo, la experiencia que se solicita en tópicos de seguridad de la información es interna. Respecto a la capacitación requerida, se indican temas generales y no específicos, por ejemplo no se solicita capacitación formal sobre las tecnologías e infraestructura de seguridad que se mantiene implementada en el Banco. Finalmente, en cuanto a las habilidades y competencias se solicitan como deseables y no fuertes como lo indica la guía.

B-8.5 Evaluar en qué medida se aplican las buenas prácticas esperadas.

Prueba de Auditoría	Resultados
Determinar que un inventario de habilidades y competencias se mantiene en las unidades con responsabilidades en la gestión de la seguridad de la información	Según lo señalado en una entrevista efectuada con un funcionario de la Unidad de Continuidad del Negocio, debido al desarrollo del plan del sistema de gestión de la seguridad de la información y por recomendaciones de la Auditoría Interna, se ha iniciado un proceso de revisión y ajuste de los perfiles actuales relacionados con la gestión de la seguridad de la información; proceso en el cual, se determinaron las habilidades y competencias requeridas.
Determinar si las jefaturas de las unidades relacionadas con la gestión de la seguridad de la información, realizan evaluaciones de análisis de brechas entre el portafolio requerido de Habilidades y Competencias y el inventario actual de las habilidades y capacidades.	Según lo señalado en una entrevista efectuada con un funcionario de la Unidad de Continuidad del Negocio, como parte del desarrollo del plan del sistema de gestión de la seguridad de la información, si se han determinado las brechas de conocimientos y habilidades requeridas.
Indague si existen planes de acción y métricas de rendimiento para desarrollar las habilidades y competencias requeridas para la gestión de la seguridad de la información, conforme a las brechas identificadas.	Según lo argumentado en entrevista realizada con un funcionario de la Unidad de Continuidad del Negocio, actualmente se reciben algunas capacitaciones relacionadas con la gestión de la seguridad de la información, no obstante, agrega que el Área encargada de los procesos de capacitación en el Banco les ha denegado capacitaciones especializadas y certificaciones en seguridad de la información y solo permite la participación en talleres y cursos de menor costo y alcance, lo que no permite desarrollar plenamente las capacidades y conocimientos del personal interno. Esta situación también se presenta en la Dirección de Tecnología de Información.

CAPÍTULO V
INFORME DE AUDITORIA

1. Resultados: Observaciones y Recomendaciones

En este capítulo se presente el informe de auditoría, en el cual, se exponen los resultados de la evaluación de la suficiencia y eficacia del sistema de gestión de la seguridad de la información que actualmente está implementado en el Banco Popular, conforme el enfoque que brinda la guía de auditoría del proceso APO13 Gestionar la Seguridad.

Los aspectos evaluados se relacionan con el establecimiento, efectividad y suficiencia de los procedimientos de control definidos para gestionar la seguridad de la información, en términos de estrategia y gobierno, garantizando de una manera razonable, la confidencialidad, integridad y disponibilidad de la información, dentro de los niveles de apetito de riesgo aprobados por el Banco.

Como resultado del análisis efectuado, a continuación se describen los principales hallazgos y recomendaciones.

A. Se carece de un perfil de riesgos de seguridad de la información alineado a la norma IEC/ISO 27001

La gestión de seguridad de la información en el Banco Popular no está alineada a un perfil de riesgos de seguridad de la información.

Se determinó que la Dirección de Riesgos Corporativa posee un inventario de eventos de riesgos relacionados con la seguridad de la información que no está alineado a la norma IEC/ISO 27001, ni es utilizado por la Dirección de Gestión ni la Dirección de TI, como parte de sus funciones relacionadas con la gestión de la seguridad de la información.

Según se evidenció, el proyecto para la implementación de un plan del sistema gestor de la seguridad de la información a cargo de la Dirección de Gestión, utiliza como base un inventario de riesgos elaborado por la empresa consultora que

participó en el desarrollo de ese proyecto, cuyas iniciativas tratan de cerrar las brechas identificadas; no obstante, ese inventario de riesgos no es considerado como oficial por las estructuras organizacionales que actualmente poseen un rol en la gestión de la seguridad de la información, por tanto, fuera del proyecto no se considera su utilización ni actualización.

Al no contar con un perfil de riesgos de la seguridad de la información, que se revise y ajuste periódicamente, la entidad carece de un enfoque global de apetito de riesgo, no aplica métricas ni planes de mejora y la implementación de herramientas de control se basa en criterios subjetivos de las áreas de toma de decisiones y no en función de atender riesgos de mayor criticidad.

Al respecto, la más reciente revisión del Marco de Trabajo de Referencia para el Gobierno y Administración de la Tecnología de Información Empresarial COBIT, recomienda la aplicación de la siguiente buena práctica:

> *APO12.03 Mantener un perfil de riesgo.*
>
> *Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados.*

Esta situación obedece a que la función de seguridad de la información en el Banco no ha sido considerada desde un punto de vista estratégico y de gobierno, sino operativo, lo que ha limitado el diseño e implementación de un perfil de riesgos que contenga atributos del riesgo, escenarios, actividades de control y apetito de riesgo deseado por la entidad respecto a la seguridad de la información.

La falta de un proceso institucional de valoración del riesgo de seguridad de la información que sea actualizable y revisable periódicamente, no permite desarrollar una adecuada gestión estratégica de la seguridad de la información con un enfoque de extremo a extremo en el Banco, lo que contribuye al riesgo de disponer de recursos limitados para la ejecución de actividades de menor impacto y criticidad y no enfocar los esfuerzos en reducir los principales riesgos que afectan la seguridad de la información.

Recomendaciones

Para: Dirección de Riesgos Corporativa

1. Diseñar, implementar y mantener actualizado un perfil de riesgos de seguridad de la información, alineado a la norma IEC/ISO 27001, en el cual, participen las estructuras organizacionales que cuentan con roles de rendición de cuentas y responsabilidad entorno al sistema de gestión de la seguridad de la información.

Para: Dirección de Gestión

2. Conforme los resultados obtenidos del perfil de riesgos de seguridad de la información, formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura del Banco.

B. El diseño de la política de seguridad de la información dificulta el logro de los objetivos

La revisión de la Política de la Información del Banco Popular evidenció que su estructura es compleja y difícil de navegar. Si un funcionario desea conocer cuáles son todas sus responsabilidades, debe extraer de cada dominio lo correspondiente y verificar inclusive que no existan casos en donde una actividad no contradiga otra. Por tanto, también su actualización, debe ser realizada cuidadosamente.

Las actividades señaladas en la Política son generales, situación que puede afectar la medición de su cumplimiento, así como de su grado de madurez

Se evidenciaron al menos dos casos en donde la Política no es clara en la delimitación de la responsabilidad y rendición de cuentas, tal y como se indica en el siguiente ejemplo, en el cual, la responsabilidad sobre la omisión de la instrucción no está definida, lo que dificulta la rendición de cuentas: *“En caso de*

que cualquier equipo del Banco necesite ser trasladado fuera de las instalaciones por mantenimiento, se debe realizar las acciones necesarias para salvaguardar la información del Banco". En general, no se indica quién y cuáles acciones se deben ejecutar.

Así mismo, la Política carece de un mecanismo de comprobación de su cumplimiento y las consecuencias del no cumplimiento de esta no se describen claramente. El apartado sexto de la Política establece que en caso de incumplimiento por parte de los funcionarios y funcionarias o terceros, se exponen a las acciones administrativas o legales que correspondan; no obstante, la política no es clara en cuanto a sanciones o penalidades específicas.

La norma INTE ISO IEC 27002:2009 Tecnología de la información - Código de prácticas para la gestión de la seguridad de la información, en su apartado 5.1 Política de seguridad de la información, establece lo siguiente:

> *5.1.2 Revisión de la política de seguridad de la información*
>
> *La política de seguridad de la información debería revisarse a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia, y eficacia continuas.*
>
> *La política de seguridad de la información debería tener un propietario con responsabilidad de gestión aprobada para el desarrollo, la revisión, y la evaluación de la política de seguridad. La revisión debería incluir la evaluación de las oportunidades de mejora de la política de seguridad de la información de la organización y el enfoque a la gestión de la seguridad de la información en respuesta a cambios en el ambiente de la organización, a las circunstancias del negocio, a las condiciones legales, o al ambiente técnico.*
>
> *La revisión de la política de seguridad de la información debería tomar en cuenta los resultados de las revisiones por la dirección. Debería haber procedimientos definidos de la revisión por la dirección, incluyendo un calendario o un período para la revisión.*
>
> *Las entradas para la revisión por la dirección deberían incluir información sobre:*
>
> *a) retroalimentación de las partes interesadas;*
>
> *b) cumplimiento de la política de seguridad de la información y del desempeño de procesos.*

La falta de mecanismos de medición de la efectividad de la Política y de su nivel de conocimiento y aceptación en la población bancaria, se considera una de las principales causas que limitan a la Dirección de Gestión la obtención de retroalimentación y aplicación de mejoras en esta herramienta, que es considerada la base para el desarrollo del sistema gestor de la seguridad de la información en el Banco. Por otra parte, la Política de Seguridad de la Información fue diseñada considerando cada uno de los dominios de la norma IEC/ISO 27001; por tanto, la distribución de responsabilidades y roles se realiza por cada uno de los dominios.

Una Política de Seguridad de la Información con una estructura compleja y difícil de actualizar no contribuye a mejorar el nivel de culturización y enfoque hacia la seguridad de la información en la población bancaria; por tanto, no se estaría logrando el impacto esperado y, con ello, se afecta directamente el nivel de madurez esperado en relación con la gestión de la seguridad de la información.

Recomendación

Para: Dirección de Gestión

1. Implementar métricas e indicadores para determinar la eficiencia de la Política de Seguridad de la Información, en términos de su contribución a los objetivos y metas del negocio relacionadas con la gestión de la seguridad de la información. Sobre los resultados obtenidos, ejecutar las acciones de mejora necesarias.

C. La gestión de seguridad de la información carece de estructuras organizativas completas y de un adecuado ámbito de control y poder de decisión

En el Banco no existe formalmente una estructura organizativa de gestión de la seguridad de la información. Actualmente, la Dirección de Gestión asume algunas responsabilidades de gestión estratégica de la seguridad, siendo la Unidad de Continuidad del Negocio quien ejecuta estas funciones y reporta a dicha Dirección. No obstante, la figura de Dirección de la Seguridad de la Información, conocida como CISO, tal cual la describe COBIT no forma parte de la estructura de la entidad.

Desde la Unidad de Continuidad del Negocio, se dificulta la independencia y control de la función de seguridad de la información, al no estar ubicada en una posición estratégica, y además compartir recursos entre otras funciones como la continuidad del negocio. Por otra parte, pertenece a una Dirección que también tiene diversas actividades no relacionadas con la seguridad de la información.

Igualmente, en el caso del Área de Seguridad Operativa Informática, que tiene a cargo la gestión operativa de seguridad informática, se ve limitado a las decisiones que tome tanto la Dirección de TI como sus divisiones, siendo los temas de seguridad de la información parte de un portafolio de iniciativas, proyectos y otras prioridades que debe atender la estructura de tecnología de información del Banco.

Dentro de las estructuras organizativas relacionadas con la gestión de seguridad de la información se evidenciaron debilidades en cuanto a la composición de los perfiles de competencias y habilidades que se requieren para la gestión de la seguridad de la información, en donde, por ejemplo, a una Dirección de Gestión no se le exige ningún conocimiento sobre seguridad de la información.

Al respecto, la más reciente revisión del Marco de Trabajo de Referencia para el Gobierno y Administración de la Tecnología de Información Empresarial COBIT, recomienda la aplicación de la siguiente buena práctica:

> EDM01.03 Supervisar el sistema de gobierno.
>
> *Supervisar la ejecución y la efectividad del gobierno de TI de la empresa. Analizar si el sistema de gobierno y los mecanismos implementados (incluyendo estructuras, principios y procesos) están operando de forma efectiva y proporcionan una supervisión apropiada de TI.*

Las situaciones expuestas se dan a consecuencia de la falta de madurez del proceso de seguridad de la información en el Banco, aunado a la falta de exigibilidad tanto de certificaciones para el personal en tópicos de seguridad de la información, así como de un conocimiento experto en las herramientas que adquiere la entidad para la prevención de incidentes de seguridad de la información. Por otra parte, se carece de procesos formales de formación al considerarse de alto costo económico para la entidad.

La falta de visibilidad y de poder de decisión de la función estratégica de seguridad de la información afecta el mantenimiento de un nivel de madurez aceptable y continúa dando a este tema un enfoque operativo, siendo el Área de Seguridad Operativa Informática de la Dirección de Tecnología de Información, la estructura organizativa que reconoce la población bancaria, en cuanto a los temas de seguridad informática.

Así mismo, la gestión de seguridad de la información enfocada únicamente a los controles automatizados, aunado a la falta de procesos de formación continuos en competencias y habilidades, limita la capacidad de respuesta de la entidad ante incidentes de seguridad, provocados por el desconocimiento, la falta de cultura y precaución de los usuarios que acceden a la red de datos del Banco, o bien, que tienen acceso a información sensible en cualquier formato sea digital o impreso.

Recomendaciones

Para: Dirección General Corporativa

1. Realizar un análisis para determinar cuáles deben ser las estructuras organizativas en el Banco que soporten al sistema gestor de seguridad de la información, tanto la gestión estratégica como operativa, conforme las mejores prácticas recomendadas por los marcos de referencia COBIT y la norma ISO 27001. De acuerdo con los resultados obtenidos del análisis, proponer los ajustes en la estructura organizacional que se consideren necesarios.

2. Determinar cuáles son las habilidades, competencias y conocimientos requeridos para mantener una adecuada administración del sistema gestor de la seguridad de la información. Conforme los resultados obtenidos, determinar las brechas existentes y realizar los ajustes que corresponda.

2. Conclusiones

La aplicación de la guía de auditoría del proceso APO13 Gestionar la Seguridad permite al auditor la ejecución de una evaluación exhaustiva y completa de un proceso, que para este trabajo corresponde al APO13, considerando a cada uno de los 7 habilitadores de COBIT 5, a saber: 1. Principios, Políticas y Marcos de Referencia; 2. Procesos; 3. Estructuras organizativas; 4. Cultura, Ética y Comportamiento; 5. Información; 6. Servicios, Infraestructura y Aplicaciones; y 7. Personas, Habilidades y Competencias. Este análisis se realiza considerando por cada habilitador las dimensiones comunes, las cuales contemplan: las partes interesadas, las metas, el ciclo de vida y las buenas prácticas aplicables a cada habilitador. Si bien, para efectos de esta investigación, no fueron considerados todos las dimensiones en cada habilitador, en algunos casos por duplicidad y en otros por limitaciones al alcance previsto en la evaluación, el proceso seguido

permitió el conocimiento y análisis del estado actual del sistema de gestión de la seguridad de la información del Banco y poder generar oportunidades de mejora, basadas en la revisión de habilitadores clave, tales como los marcos de referencia, las estructuras organizativas y las competencias y habilidades requeridas.

Los resultados obtenidos en el presente trabajo permiten concluir que el Banco Popular debe mejorar el enfoque estratégico y de gobierno que se le brinda a la gestión de la seguridad de la información. Si bien el proyecto actual de implementación de un plan del sistema gestor de la seguridad de la información cuenta con el apoyo de la Gerencia General Corporativa, se determinó que se requiere una revisión y ajustes a las estructuras organizativas que administran las funciones de gobierno, estrategia y gestión operativa de la seguridad de la información.

Es importante que el Banco no se limite a la implementación de herramientas que brinden protección a la seguridad perimetral de la red de datos, puesto que si bien no se determinaron incidentes de seguridad significativos en el último año, esta situación puede dar una falsa sensación de seguridad, al no ser considerada la seguridad de la información como un proceso integral y estratégico más que operativo, que incluye todo tipo de información y en cualquier formato, ya sea digital, o impreso.

La implementación de programas de concientización organizacional de mayor impacto en torno a la seguridad de la información, así como métricas de evaluación periódicas que permitan a las estructuras organizativas responsables del sistema gestor de la seguridad de la información el poder determinar las brechas y su tratamiento, representan aspectos de mejora para ser tratados por la entidad.

Finalmente, a falta de un perfil de riesgos de la seguridad de la información, que brinde una visión global y sea revisable y ajustable periódicamente, los esfuerzos para mantener y mejorar el nivel de madurez, en torno a la gestión de la seguridad de la información, pueden ser insuficientes e imprecisos, respecto a la realidad interna y externa de la entidad.

REFERENCIA CONSULTADA

Contraloría General de la República (2007). Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE).

Escoto Leiva, R. (2001). *Banca Comercial*. San José, Costa Rica: EUNED.

INTE ISO 27001:2008. Tecnología de la información —Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos.

INTE ISO IEC 27002:2009. Tecnología de la información - Código de prácticas para la gestión de la seguridad de la información.

ISACA (2014). Align, Plan and Organise. APO13 Manage Security Audit/Assurance Program.

ISACA (2014). COBIT 5, for Assurance.

ISACA - CISM. (2011). Manual de Preparación al Examen CISM® 2012. Estados Unidos.

ISACA. (2012). COBIT 5: Procesos Catalizadores. Estados Unidos.

Ley Nº 4351. *Ley Orgánica del Banco Popular y de Desarrollo Comunal* (1969).

Política de Seguridad de la Información del Banco Popular y de Desarrollo Comunal.

Reglamento de Seguridad de la Información del Conglomerado Financiero Banco Popular y de Desarrollo Comunal.

SUGEF 14-09 (2009). Reglamento sobre la Gestión de la Tecnología de Información

www.bancopopularcr.com