INFORME FINAL DE GESTIÓN

Nombre:	Jorge Mayorga Castillo
Dependencia:	División Control Operativo
Periodo de Gestión:	Mayo 2018 al 02 de setiembre del 2022
Destinatarios:	Rolando González Montero Dirección de TI Roger Granados Camacho
Firma:	JORGE FRANCISCO MAYORGA CASTILLO (FIRMA) Fecha: 2022.11.25 13:41:01 -06'00'
Fecha:	02/09/2022

INFORMACION DE USO PÚBLICO CBP- A1
La información contenida en este documento es de Uso Público y puede para darse a conocer al público en general a través de canales aprobados por el Conglomerado Banco Popular.

INDICE

Contenido

Presentación

Este documento tiene por objetivo presentar el estado de las actividades en curso de la División Control Operativo y sus áreas adscritas, a la fecha de 02 de setiembre del 2022.

Resultados de la gestión

Esta sección del informe deberá contener, al menos, información relativa a los siguientes aspectos:

Labor Sustantiva Institucional

La División Control Operativo de la Dirección de TI, del Banco Popular tiene por función sustantiva gestionar y velar por el cumplimiento normativo de TI al nivel institucional y brindar apoyo a las sociedades anónimas del Conglomerado Financiero. Asimismo, impulsar el correcto accionar administrativo y funcional de las áreas a cargo, las cuales proporcionan mecanismos de control mediante normativas que aseguren la operatividad de las plataformas tecnológicas del Banco.

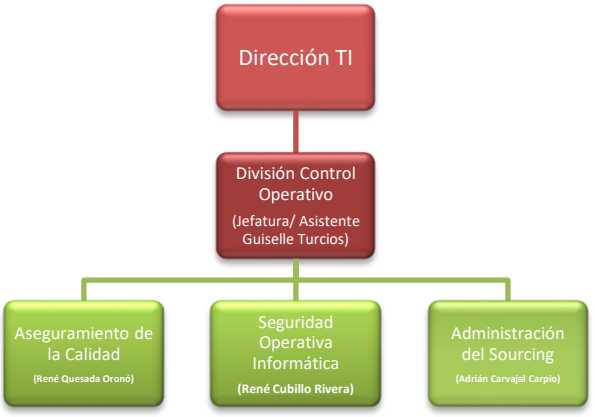
Controlar los procesos de cambios dados por adición de nuevos elementos, retiros, “upgrades” o modificaciones en el ambiente de Tecnología de Información. Ejercer el control y seguimiento del presupuesto y de los diferentes procesos de licitación relacionados con Tecnología de Información, con el fin de lograr que se cuente con los recursos necesarios en forma oportuna para apoyar las labores de todas las dependencias de la Dirección.

Planear, coordinar y administrar los servicios de ciberseguridad en la organización con el fin de garantizar una seguridad razonable en todas las operaciones realizadas, a través de la adquisición, implementación y uso de herramientas tecnológicas que impulsen el cumplimiento de los procesos, normas, reglas, políticas y estándares que aseguren una adecuada protección de los recursos informáticos. De manera que contribuya en el cumplimento de los objetivos del Plan Estratégico de TI, del Plan Estratégico Corporativo y acuerdos de nivel de servicio aplicables.

A continuación, los aspectos generales más relevantes:

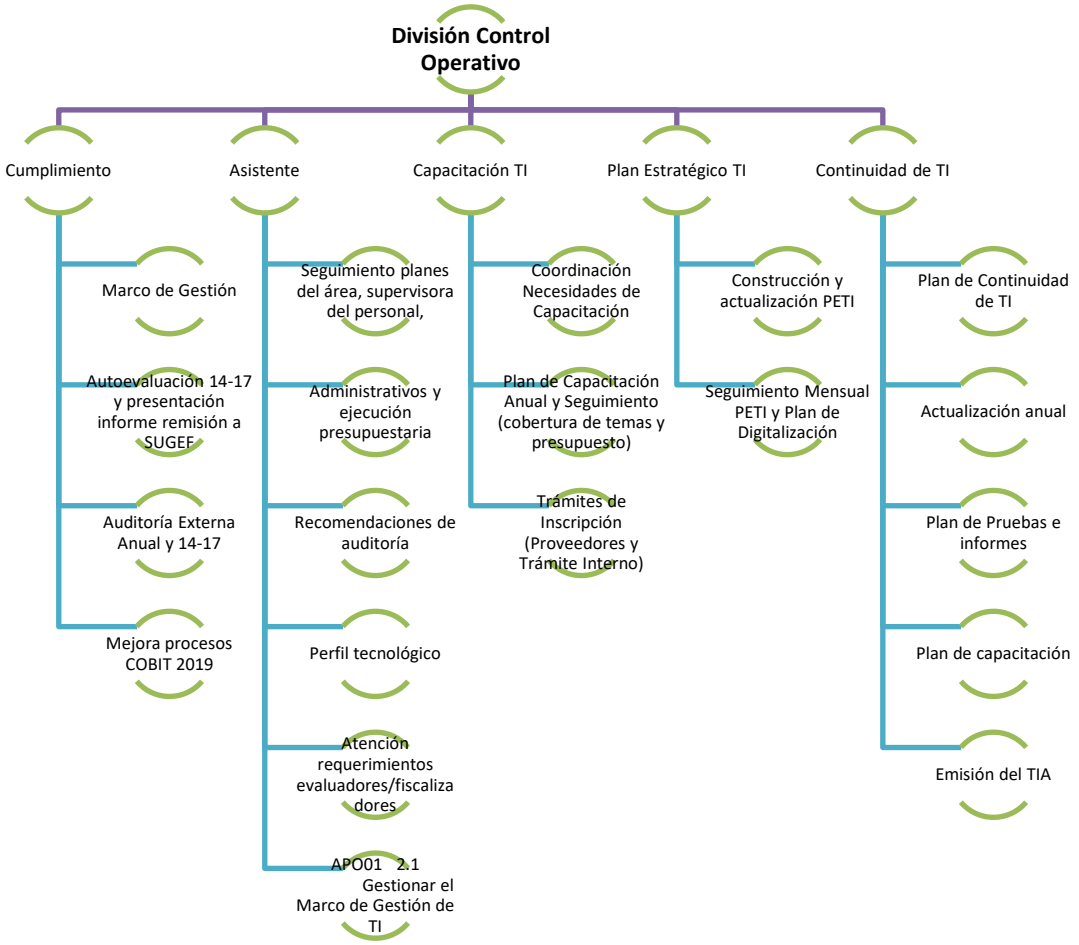
División Control Operativo

Estructura organizativa vigente de la DCO:



Adicionalmente a las áreas adscritas a la División, directamente dependen y se supervisan el siguiente personal:

Mediante su colaboración se atienen los siguientes aspectos generales:



Importante indicar que desde esta División se tenía la responsabilidad por ser la contraparte de TI con la Dirección Corporativa de Riesgos, en materia general de riesgos tecnológicos presentes en diferentes procesos y adquisiciones, no obstante, el único recurso que llevaba tales tareas se retiró por movilidad laboral, lo que hizo imposible su sustitución y por lo tanto imposibilitó continuar con dicha labor.

Actividades Planificadas 2022

Actividades Programadas	Horas	%
Cumplimiento Normativo 14-17	40	3.2%
Perfil Tecnológico	80	6.5%
Procesos responsabilidad de la DCO	86	7.0%
Contrataciones	75	6.1%
Continuidad de TI	220	17.8%
PETI - Plan de Digitalización y Tecnología: Seguimiento e Informe	93	7.5%
PETI - Plan de Digitalización y Tecnología: Revisión y Actualización	80	6.5%
Gestión de Indicadores Procesos Marco de Gestión de TI	70	5.7%
Cumplimiento Acuerdos Ganar - Ganar	25	2.0%
Plan de Capacitación y su seguimiento	90	7.3%
Atención entes evaluadores y reguladores Externos	28	2.3%
Recomendaciones y planes de acción - Seguimiento interno y registro	30	2.4%
Administrativas	186	15.0%
Otros	133	10.8%
	1236	

Actividades Cumplimiento Normativo:

Las actividades de cumplimiento están en línea con el Reglamento General de Gestión de TI, SUGEF 14-17, las cuales se programan anualmente respetando los plazos establecidos, en la siguiente tabla se presenta las actividades, su programación y estado vigente a la fecha del informe:

Nombre de tarea	Programación Anual	Comentarios	Estado al Final
SUGEF 14-17			
Actualización del Marco de Gestión de TI	IV semana de Mayo	Visto y aprobado en CETI y CCTI Pendiente JDN	Pendiente de aprobar, dado que al presentarse se presentaron dudas en el CETI, se coordinó con la empresa asesora contratada para dar una inducción del tema COBIT
Responsables asignados de cada	IV semana de Mayo		

aspecto del marco de gestión de TI			y 14-17. Pendiente de presentar al CETI.
Aprobación Resultados de la Autoevaluación de Procesos TI	II Semana de setiembre	Iniciado y en proceso, a la espera de los ajustes realizados por la Auditoría y Riesgo a los resultados obtenidos por los responsables de los procesos	Ajustes de Auditoría y Riesgos se comunicaron a los responsables de los procesos el 01/09/2022 inmediatamente fueron comunicados por la Auditoría
Remisión de Resultados de la Autoevaluación a la SUGEF	Último día hábil de setiembre (3)		Pendiente
Remisión del Perfil tecnológico	Primeros 10 días hábiles de enero	Cumplido oportunamente	
Auditoría Externa	Según lo solicite la SUGEF, periodicidad no menor a 2 años y no mayor a 4 años, se comunica oficialmente por la SUGEF con 9 meses de antelación a la presentación de los resultados.	Se presupuesta, sin embargo, la SUGEF no ha solicitado una nueva auditoría.	
Seguimiento Planes de acción de cierre de brechas	Periodicidad trimestral	Se coordina con la UTEG	Este aspecto se realiza por parte de la UTEG
Remisión del Plan de Acción cierre de brechas Auditoría Externa	20 días hábiles posteriores a la solicitud de la SUGEF		El plan de acción se emite 20 días posterior a la aprobación del informe de salida de la Auditoría Externa y debe establecer en el formato que la SUGEF tenga establecido

			al momento de su remisión.

En relación a lo indicado en la tabla anterior es importante considerar los siguientes aspectos:

- El marco de gestión corresponde con una tabla del perfil tecnológico, que entre sus campos incluye la información de aprobación de Junta Directiva: acta, fecha, etc. Razón por la cual se eleva anualmente para aprobación. Aunque no forma parte del marco de gestión, al presentar este para su aprobación se incluyen las áreas organizacionales responsables, si se presentan cambios, se debe indicar la motivación del indicado cambio.

- Con relación al proceso de autoevaluación, se indica que éste se planifica en cumplimiento con la normativa SUGEF 24-00 pero con la metodología de valoración de la 14-17, esta es aplicable al Banco únicamente no a las sociedades, no obstante, se ha comunicado que la 24-00 ha sido derogada, por lo que queda sin vigencia a partir de enero del 2023, según se indica:

Disposiciones Derogatorias

Disposición derogatoria única.

Derogación de reglamentos.

Los siguientes reglamentos quedan derogados expresamente:

1) *Reglamento para Juzgar la Situación Económica-Financiera de las Entidades Fiscalizadas*, Acuerdo SUGEF 24-00.

2) *Reglamento para Juzgar la Situación Económica-Financiera de las Asociaciones Mutualistas de Ahorro y Préstamo para la Vivienda,* Acuerdo SUGEF 27-00.

Además, se derogan todas las disposiciones de igual o inferior rango que contravengan lo establecido en este reglamento.

Rige a partir del 1° de enero de 2023.

A pesar de lo indicado se considera necesario que exista un mecanismo de medición interna, dado que la única forma de medir el nivel de cumplimiento de los procesos sería mediante auditoría externa. Razón por la cual se debería proponer proseguir con las autoevaluaciones, con una periodicidad anual o de cada dos años, según se considere conveniente, los resultados serían presentados a los niveles superiores. Previo a cualquier propuesta que deberá elevarse a Gerencia y CCTI, este aspecto sería apropiado valorarlo con la Dirección Corporativa de Riesgo y Auditoría de TI.

- Auditoría externa: Según la 14-17 ésta es solicitada por la SUGEF a la Gerencia General, quienes inmediatamente a TI, a partir de la fecha de recepción se contará con 9 meses para convocar a la SUGEF para presentar el informe de salida y remitir los

resultados por parte de la SUGEF. La DCO será la contraparte entre el Banco y la auditoría externa, de manera que deberá revisar y presentar a los niveles superiores, los atestados y cumplimiento de los requisitos de los auditores, los planes, el cumplimiento del alcance que sea solicitado por la SUGEF, así como los resultados.

En este punto es de mucha importancia considerar que la contratación del despacho de autoría externa debe cumplir una serie de requisitos, tanto el despacho como de manera específica los auditores designados, los cuales debe estar autorizados y listados en el sitio de la SUGEVAL.

Con el objetivo de facilitar este proceso de contratación, se llegó al acuerdo con la División de Contabilidad Analítica, quienes fiscalizan el contrato de auditoría externa que debe ejecutarse anualmente a los estados financieros del Banco, por lo que se amplió para incluir este tipo de auditorías especiales, para lo cual se les remitió los requisitos que se deben cumplir. Se debe mantener un presupuesto suficiente para dar cobertura en caso de que se requiera. Cabe indicar que la última auditoría fue llevada a cabo a finales del 2019 y los resultados se remitieron a inicios del 2020, razón por la cual se estima que como probable que esté próxima la solicitud de la SUGEF para la realización de la auditoría.

Una vez que se remite el informe, la SUGEF puede solicitar correcciones o dar por aprobado, en este último caso se deberá remitir aprobado por Junta Directiva el plan de acción para la atención de las recomendaciones. Dado que esta remisión se debe realizar en un plazo no mayor de 20 días hábiles, lo que procede es que con el informe de auditoría se emitan y validen los planes de acción, de manera que se presenten juntos para aprobación.

El registro, seguimiento e informe de cumplimiento de los planes de acción corresponde a la UTEG.

- Carta de Gerencia de TI: Anualmente, los estados financieros del Banco son auditados, razón por la cual dentro del alcance de Auditoría Externa se incluye el componente tecnológico, razón por la cual la DCO es contraparte de dicha evaluación, requiriéndose que:
    - Se coordine con los auditores externos encargados, las entrevistas y labor de campo a ejecutar, así como la consecución y entrega de la documentación requerida.
    - Revisión del informe borrador
    - Distribución de los hallazgos y recomendaciones a las áreas correspondientes para su revisión, aceptación, así como para la emisión del plan de trabajo para la atención de cada recomendación por parte de los responsables.

- Se presenta el informe de Carta de Gerencia de TI por parte de los auditores en el CETI y al Comité de Auditoría, eventualmente puede ser de interés en el CCTI.
- En conjunto con la presentación del informe de salida por parte de la Auditoría Externa, la DCO presenta los planes de acción emitidos por las áreas responsables designadas.
- El seguimiento de las recomendaciones es responsabilidad de la UTEG.

Procesos 14-17 asociados a la División:

En ejecución del cumplimiento, la División está como responsable de la operativización de tres procesos de Gobierno más cuatro procesos de gestión de TI, según se indica a continuación:

ID SUGEF	Proceso COBIT 2019	Proceso BP	Responsable
1.1	EDM01—Asegurar el establecimiento y el mantenimiento del marco de gobierno	Gestión del marco de gobierno y partes interesadas	Junta Directiva / Dirección de Gestión / División Control Operativo
1.5	EDM05—Asegurar el compromiso de las partes interesadas		
1.2	EDM02—Asegurar la entrega de beneficios	Obtención de beneficios y optimización de recursos	Junta Directiva / División Control Operativo
1.4	EDM04—Asegurar la optimización de recursos		
2.1	APO01—Gestionar el marco de gestión de I&T	Gestión por procesos e ingeniería organizacional	Dirección de Gestión / División de Control Operativo
2.4	APO05—Gestionar el portafolio	Gestión del portafolio de TI	Dirección de TI / División Control Operativo
5.1	MEA01—Gestionar la monitorización del rendimiento y la conformidad		División de Control Operativo
5.2	MEA02—Gestionar el sistema de control interno	Gestión de control interno	Unidad Técnica de Gestión / División Control Operativo

Importante recalcar que los procesos de gobierno de TI, fueron incluidos en la justificación para la contratación del SubDirector de TI, razón por la cual se debe plantear la transición de dichos procesos que están documentados pero pendientes de presentación a Gerencia General y

Junta Directiva, por falta de personal para su ejecución, razón por la cual se convierte en una necesidad que se cambie la responsabilidad y ejecución de estos procesos.

Totalidad de Procesos División y áreas adscritas:

Área	Q Procesos
Aseguramiento de la Calidad	**4**
Administración del Sourcing	**2**
Seguridad Operativa Informática	**1**
División Control Operativo	**7**

ID SUGEF	Proceso COBIT 2019	Proceso BP	Responsable
1.1	EDM01—Asegurar el establecimiento y el mantenimiento del marco de gobierno	Gestión del marco de gobierno y partes interesadas	Junta Directiva / Dirección de Gestión / División Control Operativo
1.5	EDM05—Asegurar el compromiso de las partes interesadas		
1.2	EDM02—Asegurar la entrega de beneficios	Obtención de beneficios y optimización de recursos	Junta Directiva / División Control Operativo
1.4	EDM04—Asegurar la optimización de recursos		
2.1	APO01—Gestionar el marco de gestión de I&T	Gestión por procesos e ingeniería organizacional	División de Control Operativo
2.4	APO05—Gestionar el portafolio	Gestión del portafolio de TI	Dirección de TI / División Control Operativo
2.5	APO06—Gestionar el presupuesto y los costos	Gestión financiera y regulatoria	División de Contabilidad Analítica / División de Control Operativo - Área de Administración del Sourcing
2.9	APO10—Gestionar los proveedores	Gestión de las adquisiciones	División Contratación Administrativa / División de Control Operativo - Área de Administración del Sourcing
2.10	APO11—Gestionar la calidad	Gestión de calidad	División Gestión de Calidad / División de Control Operativo
4.5	DSS05—Gestionar los servicios de seguridad	Gestión de control interno	División de Control Operativo - Área Seguridad Operativa Informática
5.2	MEA02—Gestionar el sistema de control interno		Unidad Monitoreo Control / División Control Operativo

ID SUGEF	Proceso COBIT 2019	Proceso BP	Responsable
3.5	BAI06—Gestionar los cambios de TI	Gestión cambios y configuración de TI	División de Control Operativo - Área de Aseguramiento de la Calidad
3.8	BAI10—Gestionar la configuración		
3.8	BAI09—Gestionar los activos	Gestión de la infraestructura	División de Control Operativo - Área de Aseguramiento de la Calidad
5.1	MEA01—Gestionar la monitorización del rendimiento y la conformidad	Gestión por procesos e ingeniería organizacional	División de Control Operativo
5.2	MEA02—Gestionar el sistema de control interno	Gestión de control interno	Unidad Monitoreo Control / División Control Operativo

Plan de Recuperación de TI

La División Control Operativo tiene como responsabilidad de la coordinación para la documentación y emisión de los productos indicados en la siguiente tabla, la cual incluye el estado actual:

PRODUCTO	INICIO	FIN	Estado	Comentario Pendiente
Análisis de Impacto Tecnológico	Enero 2022	Marzo 2022	Listo	La persona para el puesto de gestor de continuidad de TI, se estima quedará cubierto a inicios de octubre del 2022, a partir de lo cual se debe establecer un proceso de curva de aprendizaje para el entendimiento tanto de la documentación vigente como de la infraestructura, con el objetivo que emita las versiones actualizadas a marzo 2023. En este punto es urgente coordinar y realizar una prueba de recuperación, dado que la última que se realizó fue en mayo 2021. Para lo cual se requiere, sea revisado el plan de capacitación para el alineamiento con las pruebas a ejecutar, dado que estas capacitaciones deben ejecutarse previo a las pruebas.
Plan de Continuidad de TI	Marzo 2022	Julio 2022	Listo	
Plan de Pruebas	Enero 2022	Febrero 2022	Listo, sin embargo, durante el 2022 no se ha podido realizar pruebas debido a los ataques de ransomware y que no se dispone del gestor de continuidad de TI	
Plan de Capacitación	Enero 2022	Febrero 2022	Listo	

Toda la documentación actual e histórica de Recuperación de TI será compartida para su respectiva copia.

Contrataciones:

Además del proceso de contratación de la auditoría externa, indicada anteriormente, la DCO fiscaliza el siguiente contrato:

- Asesoría 14-17 Conglomerado – falencias en evaluaciones de cumplimiento de procesos, control interno

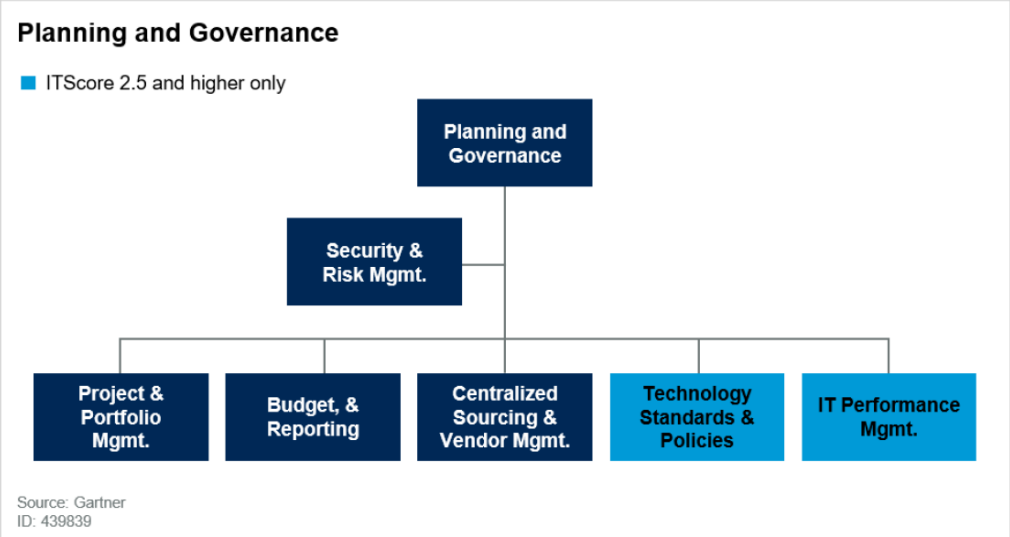
Actividades tercerizadas	Proveedor / Fecha Finalización	Observaciones
Mejora y adaptación de procesos del marco de gestión de TI en cumplimiento SUGEF 14-17.	Proveedor finaliza julio 2024	No corresponde con una tercerización sino una asesoría, sin embargo, sería conveniente disponer de personal capacitado en el Área de Calidad para tener esta actividad de forma permanente. Tiene alcance conglomeral, por lo que cada sociedad debe disponer de su propio presupuesto para su planificación y ejecución.

Se indica que se ha asignado a funcionaria de la DCO el control del presupuesto, tramitación de facturas y control del estado de las solicitudes realizadas.

Estructura de la DCO

Con el objetivo de proponer una readecuación de la División de Control Operativo, se indica que se ha analizado el documento denominado “How to Organize IT for Efficiency” en que establece una propuesta genérica de estructura de TI como sigue:

En el caso particular de la DCO, se alinea con “Planning & Governance”, la cual se estructura de la siguiente manera:



Según la estructura que recomienda el asesor especializado, se estima necesario considerar esta documentación emitida y publicada por el especialista, de forma que se complementen los aspectos que actualmente son cubiertos por la División con los siguientes indicados por la práctica:

Área Organizacional	Observaciones
Seguridad y Gestión de Riesgos	Se asocia con ASOI y la nueva estructura para fortalecer la ciberseguridad
Gestión de cartera y demanda	Este aspecto se vincula con el alcance del proceso APO05—Gestionar el portafolio, asignado a esta División.
Gestión del presupuesto y el rendimiento	Se asocia con Administración del Sourcing
Normas y políticas tecnológicas	Se asocia con el Área de Aseguramiento de la Calidad
Gestión de riesgos de recuperación ante desastres y continuidad del negocio	Gestor de Recuperación de TI
Gestión centralizada de abastecimiento y proveedores	Se asocia con Administración del Sourcing

Estado recomendaciones de Auditoría Interna:

Recomendaciones pendientes de la División y áreas adscritas, incluidas en el sistema SIAR:

N° de Recomendación	N° de Oficio	Unidad Responsable	Fecha Cumplimiento	Nivel Riesgo	Estado	Grado Avance
6	ATI-0017-2021	Área Aseguramiento de la Calidad	30/9/2022	Medio	Proceso	75
8	ATI-0017-2021	Área Aseguramiento de la Calidad	31/10/2022	Medio	Proceso	50
3	AIRI-0015-2021	Área Seguridad Informática	31/10/2022	Alto	Pendiente	0
1	AIRI-0002-2022	División Control Operativo	31/12/2022	Medio	Proceso	50
3	AIRI-0002-2022	Área Seguridad Informática	31/12/2022	Medio	Pendiente	0
3	AIRI-0003-2022	Área Aseguramiento de la Calidad	31/10/2022	Medio	Proceso	50
4	AIRI-0007-2022	División Control Operativo	31/8/2022	Alto	Proceso	50
9	AIRI-0007-2022	División Control Operativo	30/11/2022	Alto	Proceso	25
11	AIRI-0007-2022	División Control Operativo	31/7/2022	Alto	Proceso	25
16	AIRI-0007-2022	División Control Operativo	28/2/2023	Medio	Proceso	25
1	ATI-0031-2022	Área Seguridad Informática	30/6/2022	Alto	Pendiente	0
2	ATI-0031-2022	Área Seguridad Informática	30/6/2022	Alto	Pendiente	0
5	ATI-0031-2022	Área Seguridad Informática	30/6/2022	Medio	Pendiente	0
8	ATI-0031-2022	Área Seguridad Informática	30/6/2022	Alto	Pendiente	0
9	ATI-0031-2022	Área Seguridad Informática	30/6/2022	Medio	Pendiente	0
10	ATI-0031-2022	Área Seguridad Informática	30/6/2022	Medio	Pendiente	0
11	ATI-0031-2022	Área Seguridad Informática	30/6/2022	Bajo	Pendiente	0
4	AE-1121-2022	Área Seguridad Informática	31/12/2023	Alto	Pendiente	0
7	AE-1121-2022	División Control Operativo	1/11/2022	Alto	Proceso	25
8	AE-1121-2022	División Control Operativo	31/10/2022	Alto	Proceso	25

Logros generales del último periodo anual

- Durante el último año de la gestión en la División de Control Operativo, se trabajó con el acompañamiento de una asesoría externa, en la Mejora y Adaptación de Procesos del Marco de Gestión de TI en cumplimiento con SUGEF 14-17, incluyendo las Sociedades del conglomerado

Banco Popular, impulsando al nivel conglomeral el cumplimiento y buenas prácticas de gobierno y gestión de TI.

- En cuanto a normativa de Tecnología de Información, se actualizó la Política de Tecnología de Información y se realizó un trabajo especial en cuanto a la relación con procesos, guías, manuales y responsables, así mismo se actualizó el capítulo #27 del manual de Políticas Institucionales cuya norma es interna a nivel institucional.
- Se implementó el uso de una APP, llamada "Evaluaciones" mediante las herramientas y licencias de office 365 (PowerApp, PowerBI, SharePoint) como una mejora y piloto, con el fin de realizar las evaluaciones tanto de capacitaciones como evaluaciones técnicas y usuario al final de los proyectos. Esta mejora queda para los siguientes proyectos y/o iniciativas o cualquier otra actividad de Tecnología de Información que requiera evaluar una capacitación o salida de un producto a producción.
- Se da atención a las tareas o actividades producto a la ejecución de los planes de trabajo y cronogramas de las actividades del Programa de Gestión de Seguridad de la Información, correspondientes al aseguramiento de equipos de usuario final, gestión de análisis de vulnerabilidades y protección contra la denegación de servicios.
- Se apoyó y lideró las diferentes actividades de cronogramas de proyectos con aspectos Tecnológicos e estratégicos a nivel institucional.
- Se realizó un replanteamiento y mejor de la infraestructura de ciberseguridad institucional.
- Se dio seguimiento y cumplimiento a los requisitos de cumplimiento asociados al Reglamento General de Gestión de TI SUGEF 14-17.

Estado de la autoevaluación y Riesgo Operativo

Durante la gestión se aplicó el Cuestionario de Control Interno y autoevaluación de Riesgo Operativo tanto para la División de Control Operativo como para las Áreas Adscritas obteniendo una calificación remitida por la Unidad Técnica de Evaluación de la Gestión de 0% de Riesgo Operativo con nivel excelente, dicho resultado se ha mantenido durante los últimos 3 años.

Acciones sobre el Control Interno

Dentro de las acciones sobre el control interno realizadas durante esta gestión, se trabajó en las siguientes acciones:

a) Implementación de planes de trabajo para la atención de las Recomendaciones de Auditoria

b) Implementación de Planes de trabajo para la mitigación de los riesgos que se identificaron con los dueños de procesos de mejora de la normativa 14-17

c) Se coordinaron planes de vacaciones con el fin de cumplir con la normativa y el disfrute de los funcionarios.

D) Mensualmente se compartió y repasó temas de interés como Código conducta , y material compartido por comunicación Corporativa Informa, relacionado con los temas de Construimos Bienestar.

Recomendaciones de Auditoría Externa:

Asignada a: **División Control Operativo**

Relacionada con mejoras en las pruebas de recuperación y capacitación en temas de continuidad.

Respuesta emitida mediante oficio: DCO-016-2022 del 21 de febrero del 2022

Estado Planes de Acción Riesgo:

A continuación, el estado de los planes de acción registrados en la herramienta de Riesgo Operativo denominada OpRisk y asignadas a la DCO razón por la cual mensualmente se debe registrar el avance, a la fecha de este informe:

No. Plan	Fecha de Cumplimiento	% Avance
2555	15/12/2022	90
2576	15/12/2022	90
2563	15/12/2022	90
2554	15/12/2022	90
2952	31/12/2023	1
2783	31/12/2022	80

En relación con el plan número 2952*:* se indica que se asignó a la División Control Operativo liderar la iniciativa de ITSM, para lo cual se solicitó a Investigación Tecnológica que retome la investigación.

Cambios en el entorno

Durante el 2017 la CONASIF emitió una actualización del Reglamento General de Gestión de TI, pasando a denominarse SUGEF 14-17, la cual está basada en COBIT 5.0

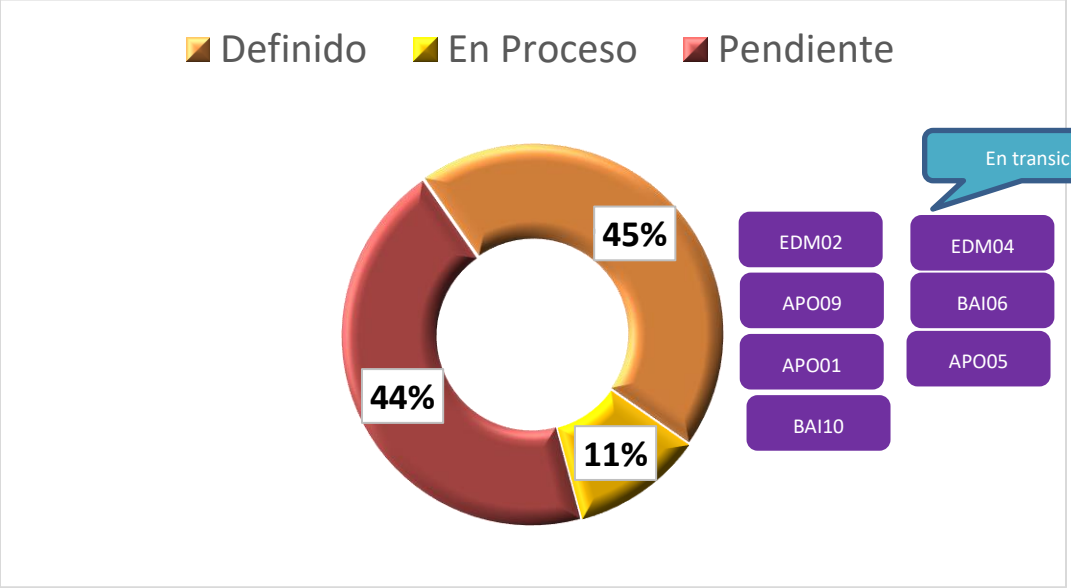
Asimismo, para el marco de referencia COBIT, se emitió una actualización a COBIT 2019, razón por la cual se impulsa la migración de los procesos hacia esta nueva versión.

Proyectos más relevantes

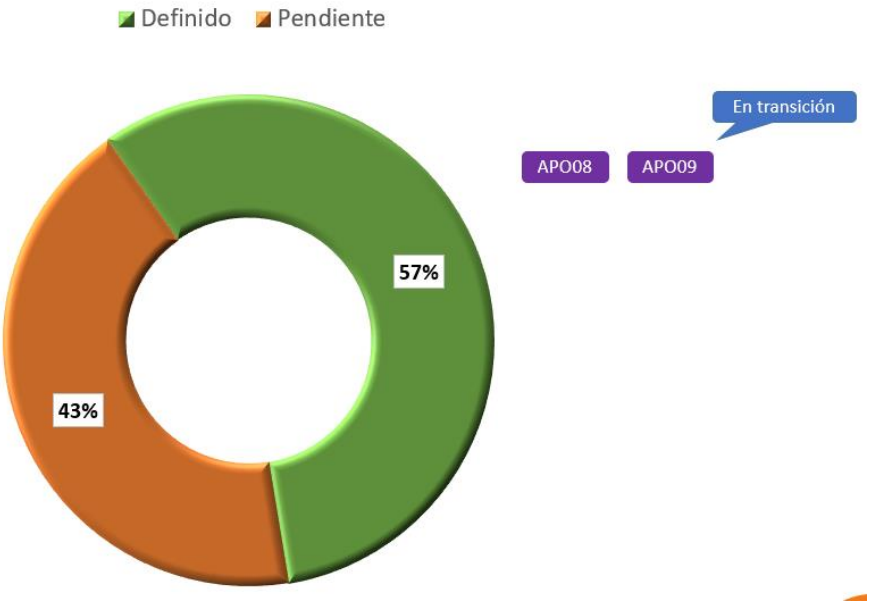
Las mejoras en los procesos del marco de gestión de TI se han definido una estructura de trabajo por bloques priorizados con la herramienta para el diseño de un Sistema de gobierno de COBIT® 2019, en una prueba que fue conocida y aprobada por el CITI en el mes de mayo, donde se propusieron niveles de capacidad objetivo de los procesos.

La metodología de trabajo se dirige hacia el abordaje por bloques cada uno de los cuales agrupa una serie de procesos lo cual significa que se trabajará por proceso organizacional.

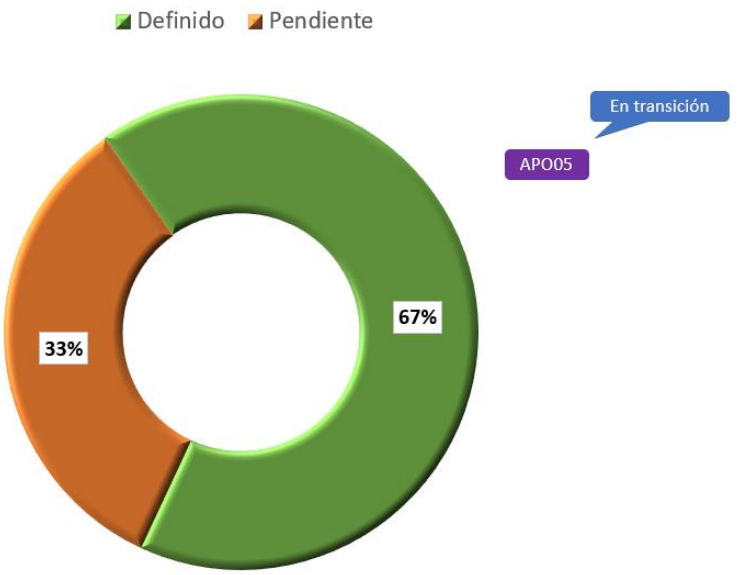
En la siguiente imagen se resume el estado de los procesos del marco de gestión de TI, según el abordaje:



Popular Pensiones



Popular Popular Seguros



Las demás UEN disponen de sus propios planes para la implementación de los procesos de los particulares marcos de gestión.

Administración de Recursos Financieros

Los recursos financieros de la División se encuentran asociados con el presupuesto anual y los planes operativos, los cuales son definidos en coordinación con el Área de Administración del Sourcing, asimismo, en dicha área se controla la ejecución y saldos.

Razón por la cual se indica que el presupuesto para el periodo 2022 se encuentra con una ejecución presupuestaria que garantizará el cumplimiento del plan aprobado.

Sugerencias

Como se ha indicado, al actualizarse la normativa 14-17 con COBIT 5.0, asimismo, considerando que el marco de gestión constituye 34 procesos lo que implica que 3 procesos de COBIT 5.0 no son obligatorios.

Adicionalmente, para la actualización a COBIT 2019, son incorporados nuevos procesos hasta alcanzar la cantidad de 40 procesos, razón por la cual se debe analizar la conveniencia de la implementación de 7 procesos que no están definidos como obligatorios, sin embargo, al estimar que COBIT es un marco con procesos integrados, la ausencia de un proceso podría afectar el modelo completo.

Observaciones

No se tienen observaciones adicionales, dado que todos los aspectos fueron incluidos en los diferentes apartados de este informe.

Cumplimiento de las disposiciones giradas por la Contraloría General de la República

A la División Control Operativo no le ha sido girada disposiciones por parte de la Contraloría General de la República.

- **Cumplimiento de las disposiciones de la Información de Uso Público**

El suscrito conoce que la información contenida en este documento es de Uso Público y puede darse a conocer al público en general a través de los canales aprobados por el Conglomerado Financiero Banco Popular.

Situación de las áreas adscritas:

Área Aseguramiento de la Calidad

En cuanto a la Gestión de la Calidad de TI, actualmente se cuenta con un Gestor de Calidad, cubriendo insuficientemente elementos prioritarios del Plan de Calidad de TI, el cual fue planteado y se venía ejecutando desde 2021 por tres gestores de calidad. Sin embargo, por prioridades de la Dirección de TI (Olivo Blanco) fue necesario reasignar a dos gestores de calidad para reforzar temas de Ciberseguridad que está a cargo del Área Seguridad Operativa Informática, por un periodo mínimo de 6 meses

Ante la jubilación de dos funcionarios vinculados con la Gestión de Cambios, únicamente se dispone de un profesional y un técnico administrativo para cubrir los trámites de pases a producción, los cuales son totalmente insuficientes para dar cobertura a los controles, razón por la cual resulta imposible ejercer controles de cambios adecuados, dado que no se gestionan los códigos fuentes y su versionamiento, como tampoco es factible realizar revisiones de los códigos fuentes y componentes modificados que se pasan a producción, lo cual requiere de conocimiento técnicos y especializados sobre los distintos lenguajes de programación, rutinas, Bcon, como es el caso de la plataforma T24.

En relación con la gestión de configuración, es requerido mejorar la herramienta de trabajo, así como incrementar los técnicos designados a esta función dado la complejidad de plataformas que se disponen.

Mediante oficio DCO-202-2021, del 01 de diciembre del 2021, se presentó a la Dirección de TI el requerimiento de recursos para la División Control Operativo y las áreas adscritas, en que se previó como nueva actividad la “Gestión y Control de Ambientes”, según se transcribe del indicado oficio:

En el siguiente cuadro se resume los requerimientos de personal antes indicados:

Área	Rol	Cantidad Requerida
Área de Aseguramiento de la Calidad	Gestor de Calidad	1 profesional informático
	Gestión de Cambios	2 profesional informático
	Gestión de la configuración	1 profesional informático
	Gestión y control de ambientes	1 Nueva actividad
	Gestión de los activos de software	**Opción** 1: 1 profesional informático **Opción** 2: 2 nivel técnico

Dado que los requerimientos de personal, comunicados en el oficio DCO-0202-2021, no han sido factibles de satisfacer, más bien por el contrario, como se indicó, ya no se cuenta con dos gestores de calidad, que al corto plazo o retornan los funcionarios cedidos a temas de seguridad informática o se tramitan concursos para recuperar ambas plazas. Adicionalmente, en la tabla antes indicada, tampoco se

había previsto el impacto del control de vencimiento de certificados lo que también ha mermado nuestra capacidad de ejercer los controles de configuración requeridos.

Por otra parte, se remitió a la Gerencia General, mediante oficio DIRTI-0353-2022 del 06 de junio del 2022, firmado por la Dirección de TI, la Jefatura de Aseguramiento de la Calidad y esta División, el cual tenía por objetivo solicitar la recuperación de las siguientes plazas:

1. **NÚMERO DE PLAZA 2206 - PROFESIONAL DE PROCESAMIENTO DE DATOS 1** – ADMINISTRADOR DE CAMBIOS, CATEGORÍA 20 DEL ÁREA ASEGURAMIENTO DE LA CALIDAD, ADSCRITA A LA DIVISIÓN CONTROL OPERATIVO

2. **NÚMERO DE PLAZA 0779 - EJECUTIVO BANCARIO ADMINISTRATIVO 1** CATEGORÍA 20– GESTOR DE CAMBIOS, CATEGORÍA 20 DEL ÁREA ASEGURAMIENTO DE LA CALIDAD, ADSCRITA A LA DIVISIÓN CONTROL OPERATIVO

Sin renunciar al requerimiento integral de personal emitido mediante el oficio DCO-0202-2021, una estrategia que eventualmente podría aplicarse, para hacer viable esta designación, es continuar con el esfuerzo iniciado para recuperar las dos plazas indicadas, de manera que se pueda emitir los respectivos concursos para cubrir con dichas plazas, uno para control de cambios y otro para control de configuración, asignándose el recargo de la gestión de ambientas a ambos funcionarios, en tanto la Dirección asigna un funcionario específico para esta función.

Gestión de ambientes

Se recibió recomendación de Auditoría, la cual se ha elevado a la Dirección de TI, por la imposibilidad de atención. Esta se refiere a la asignación de un gestor de ambientes, no obstante, no se dispone de recursos para implementar las actividades requeridas, asimismo, se debe considerar que se debe estandarizar los ambientes, los cuales podrían incluir: Desarrollo, QA, Pruebas, Capacitación, Preproducción. Asimismo, para un adecuado control de ambientes este debe enfocarse hacia el control de la configuración y cambios y no en coordinar la instalación, actualización, modificación, utilización, etc. de dichos ambientes, esto en aras de mantener separadas las funciones de control de las de ejecución.

Área Administración del Sourcing

Descripción General de Principales Actividades del Área: considerar las indicadas en el gráfico anterior y además:

- Control Presupuestario de las partidas de TI:
    - Establecer un marco financiero para la DIRTI que permita monitorear el costo/beneficio, basados en las inversiones de bienes, servicios y proyectos.
    - Mantener un programa de inversiones del portafolio de activos y servicios de TI, los cuales forman la base de las compras actuales de TI. Proveer entradas a casos de negocio para nuevas inversiones, tomando en cuenta los activos actuales de TI y el portafolio de activos. Comunicar aspectos de costo/beneficio del portafolio, compras prioritarias, administración del costo y el proceso de administración de los beneficios.
    - Priorizar la asignación de los recursos de TI para operaciones, proyectos y mantenimiento, maximizando la contribución de TI y la optimización del portafolio de la inversión programada y otros servicios de TI.
    - Coordinar la generación del presupuesto anual de la DIRTI, la cual inicia en el mes de mayo y finaliza en septiembre;
    - Preparar las órdenes de pago para cancelar los servicios y bienes recibidos según el procedimiento establecido para tales efectos. Verificar los cálculos de retención del impuesto sobre la renta y de multas en los casos que aplique. Llevar un control de las principales fechas en que deben realizarse trámites relacionados con asuntos presupuestarios.
    - Mensualmente se generan los informes de control y resultados del presupuesto y aquellos que eventualmente sean requeridos por los niveles superiores. Se realiza un reporte mensual de la evolución del presupuesto al CITI

- Procesos Contratación Administrativa
    - Se establece un proceso para preparar y administrar las compras de TI, reflejando las prioridades establecidas en el portafolio de las inversiones. El proceso es congruente con el desarrollo de las políticas de adquisición del Banco relacionadas con la Ley de Contratación Administrativa.
    - Monitorear el proceso de abastecimiento de recursos tecnológicos, brindando un estricto seguimiento a todas las gestiones desde la presentación y el análisis de los insumos necesarios (Formulario Único Requisitos Previos FURP e información de soporte), confección de la solicitud de compra hasta la adjudicación (confección cartel, coordinar la emisión de los criterios, aclaraciones, respuesta de recursos, vistos buenos jurídicos, etc.). Llevar un control sistemático de las diferentes gestiones de compra, de manera que fácilmente se pueda conocer el estado en que se encuentran y mejorar los tiempos de respuesta para adjudicar. Realizar el análisis de actividades críticas y proponer medidas correctivas.

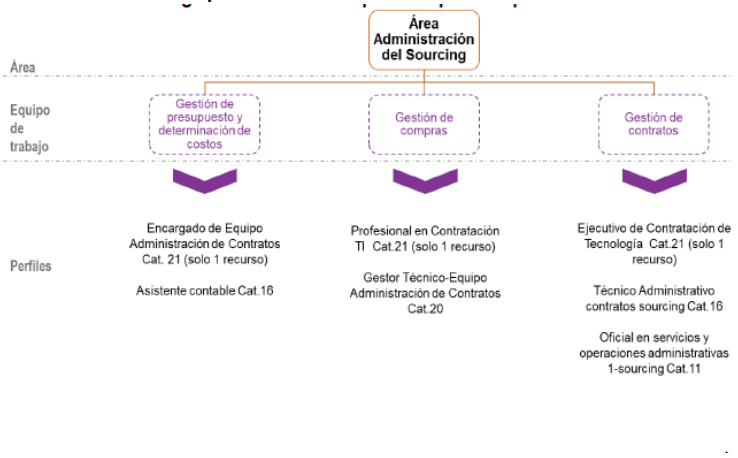
- Costeo Servicios de TI
    - Se establece y utiliza un modelo de costos basado en la definición del servicio, asegurando que la asignación de costos de los servicios es identificable, medible

y predecible, para fomentar el uso responsable de los recursos, incluyendo aquellos proporcionados por proveedores de servicio.

- Se establece una frecuencia trimestral para revisar y comparar la idoneidad del modelo de costes/prorrateo de costes para mantener su pertinencia y adecuación al negocio en evolución y las actividades de TI que le dan soporte.

- Gestión de Contratos – Apoyo Administrativo a Contratos de la Dirección de TI:

  - Se desarrollo un estudio por parte de la División Gestión de la Calidad para el traslado de las actividades administrativas de la fiscalización de contratos de TI hacia una nueva unidad en el Sourcing, definiéndose una nueva estructura del Área, la cual se presenta a continuación:



  - Con base en los avances en las contrataciones de personal, está en marcha la ejecución del plan aprobado y comunicado por la Dirección de TI, del cual se muestra el siguiente cronograma de alto nivel y su seguimiento a la fecha de este informe:

	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	% compl
		Plan de transición y migración contratos	134 días?	lun 25/7/22	mar 31/1/23	20%
✓		Inicio	13 días?	lun 25/7/22	mié 10/8/22	100%
✓		Fase I Contratos Ago 11 Contratos Criticos / Facturación DDS	12 días?	mar 16/8/22	mié 31/8/22	100%
		Fase II Contratos Sep 10 Contratos	21 días?	jue 1/9/22	vie 30/9/22	0%
		Fase III Contratos Oct 10 Contratos ASOI	21 días?	lun 3/10/22	lun 31/10/22	0%
		Fase IV Contratos Nov 10 Contratos	22 días?	mar 1/11/22	mié 30/11/2	0%
		Fase V Contratos Dic 4 Contratos	14 días	jue 1/12/22	mié 21/12/2	0%
		Fase VI Contratos Ene Contratos y Adendas DDS ***	22 días?	lun 2/1/23	mar 31/1/23	0%
		Fin	0 días	mar 31/1/23	mar 31/1/23	0%

Procesos 14-17 asociados al Área:

ID SUGEF	Proceso COBIT 2019	Proceso BP	Responsable
2.5	APO06—Gestionar el presupuesto y los costos	Gestión financiera y regulatoria	División de Control Operativo - Área de Administración del Sourcing
2.9	APO10—Gestionar los proveedores	Gestión de las adquisiciones	División de Control Operativo - Área de Administración del Sourcing

Área Seguridad Operativa Informática

Descripción General de Principales Actividades del Área:

Importante indicar que se incluirá aspectos generales, dado que no es factible incluir detalles técnicos de herramientas, diseños, e iniciativas en progreso, para mantener la confidencialidad correspondiente.

Herramientas de Seguridad:

Antes de iniciar con los temas de Hotel Bass y la atención de las actividades clasificadas con prioridad Olivo Blanco, en el ASOI se gestionaba un total de 48 herramientas de seguridad, las cuales son fundamentales para la operación segura de los servicios del Banco.

Infraestructuras y ambientes

Actualmente TI dispone de diferentes ambientes para la operación del Banco, tales como servicios en nube, on-premise, productivos y desarrollo, los cuales, como buena práctica, requieren de elementos o controles de seguridad para su operación, siendo necesario dedicar el recurso humano del Área para la implementación y gestión de herramientas de seguridad, dependencia que a hoy se ha incrementado y limita en alguna medida la gestión de todos estos ambientes.

Estándares de Seguridad de la Información

Como parte de las labores de la División de Seguridad de la Información, apoyados en las buenas prácticas, se emiten estándares los cuales deben ser implementados sobre las plataformas tecnológicas, no obstante, esto es un reto importante que requiere planificación y coordinación de manera que al aplicar los estándares se logre sin afectación a los servicios tecnológicos, así será factible cumplir con la atención de los compromisos plasmados en el plan de gestión de seguridad de la información y ciberseguridad,

Capacitación técnica

Se ha iniciado con un ciclo de capacitaciones dirigidas hacia ComTia+, para la cual se tiene compromiso de tres funcionarios de alcanzar la certificación, fue necesario retirar una funcionaria de esta capacitación debido a importantes problemas personales.

Funciones que no son de seguridad

Una parte importante de la función de ASOI se asocia a temas de soporte y no a las funciones propias del Área, debido que existen muchas tareas que históricamente se han gestionado en ASOI, a pesar que no son funciones propias de seguridad, lo que suma a que los temas de seguridad sean relegados en aras de atender la operativa de estas otras plataformas necesarias para el soporte de los servicios que brinda el banco, razón por la cual se debe coordinar una estrategia con la División de Operación de Servicios para trasladar herramientas tales como las que se listan de seguido, sin que esto represente una saturación para la DOS ni tampoco una pérdida de personal para ASOI:

- Administración y soporte del Active Directory
- Administración y soporte del Azure Active Directory
- Administración y soporte del DNS (Interno)
- Administración y soporte del DNS (Externo)
- Administración y soporte del Servicio AADC (Azure AD Connect)
- Administración y soporte del Servicio de Correo electrónico
- Administración y soporte del Servicio de envío de Correo Masivo (SMTP)
- Administración y soporte del Filtrado de Correo Entrante
- Administración y soporte del Servicio Pass Through Authentication (PTA)

Procesos de contratación y fiscalización de contratos:

Los procesos de contratación sobre las tecnologías o servicios que administra el Área, forma impactan en la debida gestión de la seguridad operativa, dado que, por imposibilidad que exclusivamente la jefatura gestione los contratos, cada uno de los técnicos a cargo de los servicios y herramientas administradas, debe asegurar la atención oportuna de cada uno de los contratos para el soporte de estas tecnologías, garantizando la continuidad del licenciamiento, soporte de soluciones y servicios adquiridos de seguridad informática, esto mediante las gestiones de renovación y actualización de las

plataformas administradas, lo cual consecuentemente genera un mayor volumen de contratos bajos nuestra fiscalización, así como de las gestiones administrativas asociados que esto conlleva, tales como ordenes de inicio, actas de recepción, evaluación de niveles de servicio, pagos, prórrogas, expedientes (AAS y SICOP), velar por el cumplimiento de la política conozca su proveedor, pago de especies fiscales, informes de calidad y desempeño, informes de periodo, entre otros. Actualmente nuestra Área fiscaliza un total de 13 contratos.

Recientemente fueron adjudicados y se encuentran en firma del contrato, para dar continuidad a herramientas importantes ya implementadas. Asimismo, se tramitan el FURP de una herramienta que prevenga que un atacante realice movimientos laterales en el ambiente virtualizado. Asimismo, se encuentran en procesos de definición del FURP para el servicio SOC y la herramienta para supervisar labores de terceros, todo esto se encuentra dando seguimiento semanal con la administradora de Proyectos asignada por la DIRTI.

Procesos 14-17 asociados al Área:

ID SUGEF	Proceso COBIT 2019	Responsable
4.5	DSS05— Gestionar los servicios de seguridad	División de Control Operativo - Área Seguridad Operativa Informática