INFORME FINAL DE GESTIÓN

Nombre:	Freddy Roca Abarca
Dependencia:	División de Seguridad de la Información
Periodo de Gestión:	Mayo 2017-Dicimbre 2019
Fecha:	08/05/2020

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 objetivo presentar el resumen de las principales actividades y resultados de la gestión ejecutada en la División de Seguridad de Seguridad de la Información (DSI) por el suscrito, Freddy Roca Abarca, como Informe final de gestión, Puesto 3016.10, Jefe de División 1, labores realizadas como parte de las competencias y facultades, esto según oficio **APM.2017-04415**, periodo abarca entre el 15/05/2017 al 25/12/2019.

Por lo anterior, a través del presente informe se pretende de manera compendiosa y ejecutiva, dar cuenta de los resultados de la gestión desarrollada; acentuando en los principales logros, y dejando clara perspectiva de los principales retos de gestión que se enfrentan y las actividades e iniciativas en curso que deben ser de avalados y de aceptación por quien asume la responsabilidad de la División, asimismo, tomando en consideración resguardar el **PRINCIPIO DE CONFIDENCIALIDAD** en su confección, sobre toda aquella información que posea esta condición especial en relación con la ejecución propia de la función de seguridad de la información.

Cabe mencionar la circunstancia por la que dicho informe se presenta hasta este día, en razón que, según la normativa aplicable **URP-DIR-01 Informes Finales de Gestión**, en su apartado **Responsabilidades de Jerarcas y titulares subordinados**, cita:

> a. Debe confeccionar su informe final de gestión **una vez que deje su cargo de manera permanente**; esto en cumplimiento de lo dispuesto en la Directriz de la Contraloría General de la República número D-1-2005-CO-DFOE, denominada “Directrices que deben observar los funcionarios obligados a presentar el informe final de su gestión, según lo dispuesto en el inciso e) del artículo 12 de la Ley General de Control Interno”.
>
> **Nota**: Lo subrayado y negrita no forma parte del original.

Aunado con lo anterior, siendo que mi promoción y traslado hacia a la División Operación de Servicios es de forma temporal e interina según consta en el oficio GGC-1886-2019 y acciones de personal APM.2020-01807 y APM.2020-03070, lo cual hace que no se considere de manera permanente, sin embargo, en atención del oficio DIRCH-0509-2020 donde solicita la elaboración de este se procede con su confección.

Resultados de la gestión

Labor Sustantiva Institucional

Administrar el Sistema de Gestión de Seguridad de la Información del Conglomerado Financiero Banco Popular y Desarrollo Comunal con base en un ciclo de mejora continua que permita la evolución de la Gestión de Seguridad de la Información de una manera más eficaz y eficiente, con el fin de salvaguardar la confidencialidad, disponibilidad e integridad de la información de clientes y del Conglomerado, asimismo brindar asesoría en cumplimiento de las leyes y regulaciones aplicables al Conglomerado.

Funciones propias de la División:

- Establecer el Sistema de Gestión de Seguridad de la Información.
- Impulsar el plan de gestión de seguridad de la información.
- Liderar el programa de proyectos de seguridad de la información.
- Promover la clasificación de activos de información.
- Gestionar riesgos de seguridad de la información.
- Establecer y evaluar la normativa interna de seguridad de la información.
- Promover la cultura de seguridad de la información.
- Establecer el programa de concientización y capacitación de seguridad de la información.

Cambios en el entorno

La División de Seguridad de la Información surge bajo la necesidad de constituir un nivel de seguridad, altamente aceptable, en atención de la normativa interna y externa aplicable, de conformidad con las buenas prácticas y estándares para el manejo de seguridad de la información, específicamente la normativa ISO/IEC 27001, a su vez, estableciendo las acciones pertinentes que contribuyan en asegurar los activos de información del Conglomerado de las amenazas y riesgos de seguridad, de ahí que, se ha enfocado en garantizar a través del plan de gestión de seguridad de la información, las actividades e iniciativas que permitan asegurar uso de técnicas o estándares la confidencialidad, integridad y disponibilidad de la información del Conglomerado, asegurando los sistemas de información, además de la implementación de los elementos de control que regulen los aspectos físicos y lógicos, gestionando la superficie del riesgo de seguridad.

Aunado con lo anterior, a partir del 2017, se actualizó el acuerdo SUGEF 14-09 el "Reglamento sobre la Gestión de la Tecnología de Información" que aplica a las entidades supervisadas por la Superintendencia General de Entidades Financieras, generando la actualización con el nombre acuerdo **SUGEF 14-17** Reglamento sobre la Gestión de la Tecnología de Información, cuyo propósito es establecer los requerimientos mínimos para la gestión de la tecnología de información que deben acatar las entidades supervisadas y reguladas del sistema financiero costarricense, el cual, en esta ocasión aplica para entidades supervisadas por la Superintendencia General de Valores (SUGEVAL), la Superintendencia de Pensiones (SUPEN), la Superintendencia General de Seguros (SUGESE) y la Superintendencia General de Entidades Financieras (SUGEF), lo que implica un reordenamiento, ajuste y definición en los planes y normativa de seguridad de la información.

Todo esto encauzó la ejecución de diversas iniciativas y actividades, de forma alineada con el proceso APO13 Gestionar la Seguridad del COBIT[1] 5, surgiendo la necesidad de actualizar el Plan de Gestión de Seguridad de la Información que se disponía producto de ejecución del contrato 013-2012, donde se efectuó la contratación de una consultoría externa para desarrollar la base y primeras acciones para impulsar el Sistema de Gestión de Seguridad de la Información en el Banco, como herramienta que considere aspectos de riesgos, amenazas y vulnerabilidades

[1] COBIT : Control Objectives for Information and related Technology

que atenten contra la confidencialidad, integridad y disponibilidad de la información durante su ciclo de vida; lo anterior con el fin de asegurar la protección de los activos información, así como el cumplimiento regulatorio en materia de Seguridad de la Información.

De esta manera se formaliza la División de Seguridad de la Información adscrita a la Dirección de Gestión, según lo establecido en la estructura organizacional y manual de la organización:

Detalle de cargos del personal de la División de Seguridad de la Información:

Código de Cargo	Nombre del Cargo	Cantidad
3016.10	Jefe División Seguridad de la Información	1
3011.10	Profesional Seguridad de la Información	4
2009.02	Técnico Seguridad de la Información	2

Fuente: Elaboración propia datos DSI.

Estado de la autoevaluación y Riesgo Operativo

Se listan los resultados obtenidos de las autoevaluaciones de Control Interno y de Riesgo Operativo aplicadas a la División de Seguridad de la Información, esto según registros obtenidos de la Unidad Técnica de Evaluación de Gestión:

AUTOEVALUACIONES CONTROL INTERNO / RIESGO OPERATIVO 2017-2019					
Año	**Control Interno**	**Nivel**	**Riesgo Operativo**	**Nivel**	**Referencia**
2017	0%	Excelente	0%	Excelente	NA*
2018	0%	Excelente	0%	Excelente	UTEG-279-2018
2019	0%	Excelente	0%	Excelente	UTEG-276-2019

Fuente: Unidad Técnica de Evaluación de Gestión.
*Nota: Para el periodo comprendido entre los años 2017 se envía resultado por medio de correo electrónico.

Acciones sobre el Control Interno

Según los resultados obtenidos sobre estas evaluaciones Control Interno y de Riesgo Operativo aplicadas a la División de Seguridad de la Información han sido excelentes logrando el nivel más alto de la escala, siendo claros los esfuerzos del equipo de trabajo; aunado a esto, se han

realizado una cantidad significativa de evaluaciones por parte de la Auditoría Interna de Tecnologías de Información, así como autoevaluaciones de cumplimiento normativo del acuerdo SUGEF 14-17, concluyendo resultados satisfactorios en cuanto a la fortaleza y completez de las estructuras de control dispuestas; sin embargo, a pesar de estas, por naturaleza de la División y por nuestro entorno, se presentan algunas oportunidades de mejora sobre las cuales se siguen ejecutando para dar mayor robustez a las estructuras dispuestas.

De igual forma se lista algunas acciones que han permitido mantener en el tiempo estas calificaciones:

1. Atención de las iniciativas derivadas del Plan de Gestión de Seguridad de la Información.
2. Atención de las recomendaciones de conformidad con los plazos acordados.
3. Atención de los planes de acción de Riesgo Operativo y Control Interno.
4. Atención de acuerdos de Comités internos y Junta Directiva Nacional.
5. Programación y cumplimiento de programas vacacionales de los funcionarios.

Aspectos que coadyuvan en las mejoras de los parámetros que se han definidos para los procesos de evaluación, los cuales de igual forma apoyan temas de cumplimiento regulatorio.

Principales Logros

De conformidad con la planificación institucional, a través del periodo que comprende este informe se ha logrado materializar una serie de logros, mismos que apoyan la consecución de los planes estratégicos de la organización, de ahí que, dada la relevancia del Plan de Gestión de Seguridad de la Información y por cuestiones de confidencialidad, se estima necesario dar un breve resumen acerca de los logros, sin entrar a detalles que puedan comprometer aspectos de seguridad del Conglomerado, por lo que, en caso de ser necesario ampliar al respecto, se puede realizar en sitio de forma presencial para ahondar en estos:

1. Actualización del Plan de Gestión de Seguridad de la Información, en alineación con la estrategia y riesgos de Conglomerado.
2. Gestionar la contratación de las posiciones que se dotaron a la División de Seguridad de la Información, además, coordinar el acondicionamiento del espacio físico y equipamiento informático.
3. Formalizar la gestión del Comité Corporativo de Seguridad de la Información.
4. Actualizar del marco normativo de seguridad de la información (reglamento, política y directrices de seguridad de la información).
5. Establecer el proceso de clasificación de activos de información.
6. Establecer el modelo de gestión de riesgos de seguridad de la información y alineamiento con la gestión de Riesgos Operativos.
7. Instaurar el programa de concientización en seguridad.
8. Impulsar clausulas de seguridad en para procesos de contratación y acciones para evaluar de seguridad en proveedores.

Proyectos más relevantes

Estar a cargo de la Dirección del Programa del Plan de Gestión de Seguridad de la Información, logrando brindar apoyo en la definición y atención de la actividades e iniciativas del Plan de Gestión de Seguridad de la Información (PGSI), dentro de la cartera de proyectos institucional. Este programa define el propósito y los objetivos que se apremian en el Conglomerado en esta materia, los cuales están alineados con la estrategia corporativa, asegurando que las inversiones apoyarán los objetivos estratégicos institucionales y agregará valor a las operaciones del negocio, plan documentado según el estándar internacional ISO/IEC 27001 e ISO/IEC 27002, además de buenas prácticas y normas de seguridad relacionadas.

Dicho programa se gestiona en coordinación con la División Oficina Corporativa de Administración de Proyectos, donde se conserva toda la documentación correspondiente al estado, avances y logros de este, no se detalla la información de las iniciativas y proyectos que conforman el programa por motivos de confidencialidad, por lo cual, en caso de ser necesario ampliar al respecto, se puede realizar una revisión en sitio de forma presencial para ahondar en detalles.

Administración de Recursos Financieros

Año 2017
La División de Seguridad de la Información inicia operaciones en el mes mayo del 2017, por lo cual no dispone con centro de costos asignado, para lo que resta de ese año, se mantiene con el apoyo a nivel de presupuesto de la Dirección de Gestión, asimismo, se realizan los trámites correspondientes para la creación del centro de costos, el cual se empieza a utilizar a partir del 2018.

Año 2018
Para el año 2018 se formularon y cumplieron los siguientes objetivos y metas:

Objetivo	Cumplimiento
03 Cumplir con las actividades del Sistema Gestión Seguridad de Información en las cuales la División de Seguridad de la información es responsable.	**Se cumple a cabalidad con los objetivos y metas propuestas.**
04 Alcanzar el nivel de capacidad de madurez 1 del el Sistema Gestión Seguridad de Información conforme a la norma ISO 27001, utilizando el Modelo de Evaluación de Procesos (PAM), para evaluar el proceso APO13 "Gestionar Seguridad" del COBIT 5 de conformidad con el acuerdo SUGEF 14-17)	
05 Cumplir con los requerimientos pactados para atender los convenios de servicios con las áreas pactadas y las sociedades	

Fuente: Elaboración propia datos DSI.

Además, con respecto a los recursos presupuestarios del 2018 se solicitaron los siguientes rubros:

Partida	Observaciones
Servicios Generales	**Se gestionó su uso y devolución de sobrantes de manera apropiada en cumplimiento de la normativa aplicable.**
Transporte dentro del País	
Viáticos dentro del País	

Fuente: Elaboración propia datos DSI.

Año 2019

Para el año 2019 se formularon y cumplieron los siguientes objetivos y metas:

Objetivo	Cumplimiento
03 Ejecutar las actividades del Plan de Gestión de Seguridad de la Información (PGSI), donde la División de Seguridad de la información es responsable.	**Se cumple a cabalidad con los objetivos y metas propuestas.**
04 Alcanzar el nivel de capacidad de madurez 2 del Sistema Gestión Seguridad de Información (SGSI) conforme a la norma ISO 27001, utilizando el Modelo de Evaluación de Procesos (PAM), para evaluar el proceso APO13 "Gestionar la Seguridad" del COBIT 5 de conformidad con el acuerdo SUGEF 14-17.	

Fuente: Elaboración propia datos DSI.

Además, con respecto a los recursos presupuestarios del 2019 se solicitaron los siguientes montos:

Partida	Observaciones
Servicios Generales	**Se gestionó su uso y devolución de sobrantes de manera apropiada en cumplimiento de la normativa aplicable.**
Transporte dentro del País	
Viáticos dentro del País	

Fuente: Elaboración propia datos DSI.

Sugerencias

Como bien se denota en el desarrollo del presente informe, debido a la relevancia de la División de Seguridad de la información dentro del Conglomerado, considerando las acciones que debe emprender diariamente, sumado a esto la aparición constante de nuevas amenazas, vulnerabilidades y riesgos de seguridad que se presentan de forma permanente, es importante asegurar la evolución de la gestión del modelo seguridad de la información del Conglomerado, para disponer de capacidades de defensa de resiliencia de ciberseguridad.

Mantener la formación y capacitación constante del personal de la División sobre los sistemas de información de Conglomerado respecto a infraestructuras, sistemas, servicios, entre otros.

Observaciones

Es sumamente importante considerar lo indicado en las sugerencias, dado que la División debe mantener el desarrollo, atención y ejecución del Programa Plan de Gestión de Seguridad de la Información del Conglomerado de forma exitosa.

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

No se tiene disposiciones emitidas la Contraloría General de la República.

Cumplimiento de las disposiciones giradas por órgano de control externo

No se tiene disposiciones emitidas por órgano de control externo.

Cumplimiento de las disposiciones giradas por la Auditoría Interna

A continuación, se detalla la única recomendación emitidas por la Auditoria interna que se encuentra en proceso de atención por parte de la División:

INFORME	RECOMENDACIÓN	VENCIMIENTO
Informe de Auditoria ATI-119-2019	**Recomendación 9***	28/2/2020

Fuente: Elaboración propia datos DSI.
*__Nota__: El detalle de la recomendación 9 está en el ATI-119-2019

Estado actual de los expedientes de fiscalización contractual que pueda tener a cargo.

No se tiene fiscalización de contratos.

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.