DANIELS HIDALGO JIMENEZ (FIRMA)

Firmado digitalmente por DANIELS HIDALGO JIMENEZ (FIRMA)
Fecha: 2020.08.06 14:48:08 -06'00'

INFORME FINAL DE GESTIÓN

Nombre:	Daniels Hidalgo Jimenez
Dependencia:	Área Seguridad Operativa Informatica
Periodo de Gestión:	05/2019-08/2020
Fecha:	06/08/2020

INDICE

Contenido

Presentación 2

Resultados de la gestión 2

A. Labor Sustantiva Institucional 2

B. Cambios en el entorno 2

Estado de la autoevaluación y Riesgo Operativo 2

Acciones sobre el Control Interno 3

Principales Logros 3

Proyectos más relevantes 4

Administración de Recursos Financieros 5

Sugerencias 6

Observaciones 6

Cumplimiento de las disposiciones giradas por la Contraloría General de la República 6

Cumplimiento de las disposiciones giradas por órgano de control externo 6

Cumplimiento de las disposiciones giradas por la Auditoría Interna 6

Cumplimiento de las disposiciones de la Información de Uso Público 8

Presentación

Este documento tiene objetivo presentar el resumen de las principales actividades y resultados de la gestión ejecutada en el Área de Seguridad Operativa Informática por el suscrito, como Informe final de gestión, Jefe de Área 2, T.I., labores realizadas como parte de las competencias y facultades, periodo abarca entre el 01/05/2019 al 05/8/2020.

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, limitaciones y, ante todo, dejar clara perspectiva de los principales retos de gestión que se enfrentan y los proyectos e iniciativas en curso que deben ser de avalados y de aceptación de quien asume la responsabilidad del Área, esto en el entendido de las limitaciones que se enfrenta el Área.

Resultados de la gestión

A. Labor Sustantiva Institucional

Proteger la información de la Organización, manteniendo en niveles aceptables los riesgos de seguridad operativa informática de acuerdo con la normativa de Seguridad de la Información, estableciendo controles técnicos y roles de seguridad, así como gestión de accesos de la información, a su vez, realizar la supervisión de la seguridad, minimizando los posibles impactos por vulnerabilidad e incidentes de seguridad.

Funciones propias del Área:

- Proteger contra software malicioso
- Gestionar la seguridad de la red y las conexiones
- Gestionar la seguridad de los puestos de usuario finales
- Gestionar la identidad del usuario y el acceso lógico
- Gestionar el acceso físico a los activos de TI
- Gestionar documentos sensibles y dispositivos de salida
- Supervisar la infraestructura para detectar eventos relacionados con la seguridad

B. Cambios en el entorno

El Área de Seguridad Operativa Informática surge bajo la necesidad de constituir un nivel de seguridad, aceptable, mediante la atención de la normativa y políticas de seguridad de conformidad junto con las buenas prácticas para el manejo de seguridad de la información, específicamente la normativa ISO 27001, a su vez, estableciendo técnicas y herramientas que contribuyan a optimizar la administración de los recursos informáticos del Banco, de ahí que, se ha enfocado en garantizar a través del uso de técnicas o estándares la confidencialidad, integridad y disponibilidad de la información almacenada en un sistema informático, además de la implementación de los elementos de control que regulen los aspectos físicos, lógicos, minimizando los riesgos en el uso de las tecnologías de información.

Estado de la autoevaluación y Riesgo Operativo

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

ÁREA SEGURIDAD OPERATIVA INFORMÁTICA AUTOEVALUACIONES CONTROL INTERNO / RIESGO OPERATIVO 2019					
Año	Control Interno	Nivel	Riesgo Operativo	Nivel	Referencia
2019	0%	Excelente	0%	Excelente	UTEG-234-2019

Fuente: Unidad Técnica de Evaluación de Gestión.

Acciones sobre el Control Interno

El área mantiene procedimientos internos, que se revisan y actualizan periódicamente con el fin de mantener una adecuada gestión del control interno asociada a la operativa del área, adicionalmente se da mantenimiento a todas las plataformas de seguridad informática administrada a lo interno, con el fin generar un equilibrio entre la seguridad y la operación de servicios del Banco.

Adicionalmente, se detallan las acciones que se atienden en el área como parte de la mejora continua:

1. Atención de las iniciativas y actividades 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.
4. Atención de reportes e incidentes asignados a través de la mesa de servicios.
5. Cumplimiento de los Acuerdos de niveles de servicios pactados entre el Área y Sociedades Anónimas
6. Programación y cumplimiento del cuadro de vacacionales del personal del Área.

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 materializado una serie de logros, mismos que apoyan la consecución de los planes estratégicos de la organización, de ahí que, dada la relevancia de este Plan y por cuestiones de confidencialidad, se estima necesario dar un breve resumen acerca de los logros, es decir, sin entrar a detalle en temas de brechas de seguridad o incidentes, por lo que, en caso de ser necesario ampliar al respecto, en sitio de forma presencial se pueden ahondar en estos.

Planes Estratégicos:

A continuación, se resume las calificaciones obtenidas durante los últimos años de gestión del PAO:

ÁREA SEGURIDAD OPERATIVA INFORMÁTICA PLAN ANUAL OPERATIVO 2019-2020		
Año	Avance logrado	Referencia
2019	99,52%	APRE-1255-2019
2020 (I S)	100%	APRE-0399-2020

Fuente: SIPRE – ÁREA DE PRESUPUESTO

Por lo tanto, considerando la naturaleza del Área, año a año se han establecido metas definidas para garantizar el cumplimiento a los objetivos estratégicos, acciones que han sido emprendidas por el equipo de trabajo del Área de Seguridad Operativa Informática para mantener, perfeccionar y evaluar el sistema de control interno institucional, acciones que han sido auditadas a lo interno de la organización, de igual forma, de aceptación en su definición, alcance y resultados obtenidos.

1. En cuanto a la normativa que se define en el Área, en relación con el proceso Cobit DSS05, Gestionar los servicios de seguridad, se actualiza de conformidad con el acuerdo SUGEG 14-17.
2. Sobre las herramientas administradas por el Área, se logra dar cobertura al 100% con las licencias consumidas, evitando inconvenientes por asuntos de auditoria e incumplimientos legales.
3. Sobre las herramientas administradas por el Área, se logra mantener al día los derechos de uso de licencias, soporte e implementación de las últimas versiones del software liberado por los fabricantes.
4. Se apoya e impulsa el cumplimiento de lo estipulado en el DECRETO N°39225-MP-MTSS-MICITT, referente a la implementación de la modalidad del teletrabajo a través de accesos seguros y controlado (acceso remoto).
5. Se brinda apoyo en diferentes proyectos institucionales, entre algunos:

   - Acceso remoto (teletrabajo)
   - Actualización plataforma T24 r09 y r17 (ActivID, TCBIB, T24),
   - ATM's
   - Banca Móvil
   - Microsoft Azure
   - Office 365
   - Página presencial
   - Página transaccional

Proyectos más relevantes

Se brinda apoyo en la definición y revisión del Plan de Gestión de Seguridad de la Información (PGSI), proyecto institucional que comprende el periodo 2017-2020. Este Plan define el propósito y los objetivos que se apremia 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.

De dicho plan se derivan una serie de iniciativas (identificadas como el sufijo INI) y actividades (ACT) que hoy en día se encuentran asignadas al Área, cuya atención debe ser de conformidad con la normativa interna en materia de administración de proyectos del Conglomerado en el caso de iniciativas y bajo un plan de trabajo para el caso de actividades. A continuación, se lista las iniciativas y actividades asignadas al área:

1. INI01 - Controlar el acceso a la red
2. INI14 - Proteger los sistemas en línea ante ataques de denegación de servicio (DDoS)
3. INI20 - Adquirir herramientas y/o servicio para la prevención de fraude electrónico

4. ACT19 Fortalecer seguridad en computadoras de usuario final (Endpoints) y ATM´s.
5. ACT24 Protección y acceso de información en ambientes híbridos (On premise – Cloud).
6. ACT25 Gestionar la administración de identidades y accesos de cuentas privilegiadas a nivel de Nube
7. ACT26 Gestionar el análisis de vulnerabilidades en sistemas de información

Por lo tanto, además de la operativa diaria, el Área se encuentra de lleno en todo lo que involucra la atención de dichas iniciativas, tales como estudios de mercado, definición y creación del FURP, gestión de compra, implementación, administración y soporte. De estas INI, se encuentra en desarrollo o bien en su normalización:

ÁREA SEGURIDAD OPERATIVA INFORMÁTICA
AVANCE DE INICIATIVAS 2019

Nombre Actividad	Real	Esperado	Dif.	Etapa
INI01 - Controlar el acceso a la red	100%	100%	0%	Finalizada
INI14 - Proteger los sistemas en línea ante ataques de denegación de servicio (DDoS)	25%	25%	0%	Contratación
INI20 - Adquirir herramientas y/o servicio para la prevención de fraude electrónico	33%	33%	0%	Suspendida
ACT19 Fortalecer seguridad en computadoras de usuario final (Endpoints) y ATM´s.	69%	73%	-4%	Ejecución Plan de Trabajo
ACT24 Protección y acceso de información en ambientes híbridos (On premise – Cloud).	89%	89%	0%	Ejecución Plan de Trabajo
ACT25 Gestionar la administración de identidades y accesos de cuentas privilegiadas a nivel de Nube	55%	55%	0%	Ejecución Plan de Trabajo
ACT26 Gestionar el análisis de vulnerabilidades en sistemas de información	76%	76%	0%	Ejecución Plan de Trabajo

Fuente: División Seguridad de la Información. Informe de avance de programa 01-m-02-19. Plan de Gestión de Seguridad de la Información

Administración de Recursos Financieros

En el Plan Anual Operativo del Área correspondiente al año 2019 se estableció presupuesto, el cual se relaciona principalmente con la renovación de licenciamiento de herramientas de seguridad informática y estimación de recursos para la implementación de las iniciativas del Programa de Seguridad de la Información.

Sugerencias

Todo esto considerando a su vez que existen otras funciones que actualmente no ha logrado asumir el Área, principalmente por asuntos de capacidad instalada, a su vez, existen otras labores que no son concernientes a la naturaleza del Área y que reasignarse a otras dependencias, siendo que continua pendiente la atención de lo indicado en el oficio GGC-1639-2018.

Observaciones

Es sumamente importante considerar lo indicado en las sugerencias porque el Área está en punto donde debe considerarse si se da seguimiento o no al desarrollo y atención de iniciativas que se cursan en este momento, contenidas en el proyecto del Programa de Gestión de Seguridad de la Información. Sumado a esto, el imposible impacto que pudiera darse en caso de que alguna brecha no lograra atenderse, brechas contenidas en dicho programa.

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

No se tiene disposiciones emitidas la Contraloría General de la República u otro órgano de control externo.

Cumplimiento de las disposiciones giradas por órgano de control externo

No se tiene disposiciones emitidas la Contraloría General de la República u otro órgano de control externo.

Cumplimiento de las disposiciones giradas por la Auditoría Interna

A continuación, se detallan las recomendaciones de auditoría interna atendidas durante mi gestión:

Oficio	Número	Unidad Responsable	Fecha Cumplimiento	Estado
ATI-0022-2017	6	Area Seguridad Informática	9/11/2019	Cumplida
ATI-0100-2018	6	Area Seguridad Informática	30/11/2019	Cumplida
ATI-0020-2019	2	Area Seguridad Informática	15/1/2020	Cumplida
ATI-0020-2019	3	Area Seguridad Informática	30/9/2019	Cumplida
ATI-0020-2019	4	Area Seguridad Informática	28/2/2020	Cumplida
ATI-0020-2019	8	Area Seguridad Informática	20/1/2020	Cumplida
ATI-0020-2019	9	Area Seguridad Informática	20/1/2020	Cumplida
ATI-0050-2019	6	Area Seguridad Informática	26/7/2019	Cumplida
ATI-0050-2019	8	Area Seguridad Informática	30/11/2019	Cumplida
ATI-0065-2019	7	Area Seguridad Informática	30/4/2020	Cumplida
ATI-0065-2019	12	Area Seguridad Informática	30/9/2019	Cumplida
ATI-0124-2019	9	Area Seguridad Informática	31/7/2020	Cumplida
ATI-0020-2020	1	Area Seguridad Informática	31/7/2020	Cumplida

A continuación, se detalla las recomendaciones emitidas por la Auditoria interna que se encuentra en procesos por parte del Área:

Oficio	Numero	Unidad Responsable	Fecha Cumplimiento	Estado
ATI-0020-2020	2	Area Seguridad Informática	30/9/2020	En Proceso
ATI-0023-2020	1	Area Seguridad Informática	18/12/2020	En Proceso
ATI-0091-2020	1	Area Seguridad Informática	31/1/2021	En Proceso

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.