INFORME FINAL DE GESTIÓN

Nombre:	Ing. Noé Javier Castro Rueda
Dependencia:	Área Seguridad Operativa Informatica
Periodo de Gestión:	2010-2019
Fecha:	05/01/2019

INDICE

Contenido

Presentación

Este documento tiene objetivo presentar el resumen de las principales actividades y resultados de la gestión ejecutada en el Área de Seguridad Operativa Informatica por el suscrito, Noé J. Castro Rueda, como Informe final de gestión, Puesto 3035.01, Jefe de Área 2, T.I., labores realizadas como parte de las competencias y facultades, esto según oficio DTDI-375-2010, periodo abarca entre el 03/08/2010 al 30/04/2019.

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, 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.

Cabe mencionar la circunstancia por la que el dicho informe se presenta a este día, en razón que no ha existido un acaecimiento de índole técnico o laboral para el cese o interrupción del puesto, de ahí que a la fecha no he sido notificado formalmente del cambio por las Área competentes en temas de recurso humano y/o reclutamiento.

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 Informatica surge bajo la necesidad de constituir un nivel de seguridad, altamente aceptable, mediante la definición de la normativa y políticas de seguridad de conformidad con las buenas prácticas para el manejo de seguridad de la información, específicamente la normativa ISO/IEC 17799, 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.

No obstante, en consideración del aumento de la dependencia tecnológica que caracteriza el desarrollo de las actividades financieras, la escala y los costos de las inversiones en sistemas de información, la proliferación de amenazas y eventos no deseados; y el potencial que poseen las tecnologías para cambiar drásticamente los procesos de negocio de las organizaciones, a través del Consejo Nacional de Supervisión del Sistema Financiero se resuelve mediante 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, reglamento tiene por objeto la definición de los criterios y metodología para la evaluación y calificación de la gestión de la tecnología de información (TI).

Ahora bien, el contexto del marco dispuesto en el artículo 13 del Reglamento, se dicta la obligatoriedad de aplicar auditoría externa de TI, la cual debe ejecutarse utilizando los "Estándares de TI, guías, herramientas y técnicas para auditoría, aseguramiento y control profesional" emitido por ISACA, con el objetivo de obtener una conclusión sobre el cumplimiento de los objetivos de control y nivel de madurez asociados a cada proceso evaluado a partir de los requisitos establecidos por la versión 4.0 de CobiT, de ahí que, apoyados en el Contrato Servicios de Consultoría, Guía y/o Acompañamiento en la Implementación del modelo COBIT. (Control Objectives for Information and related Technology), es que la firma Deloitte & Touche Tohmatsu, razón por la cual finales del año 2010 da inicio con el reordenamiento, ajuste y definición de políticas, procedimientos y estándares de seguridad de TI y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad, específicamente el desarrollo del proceso DS05 que permite Gestionar los servicios de seguridad proporcionan una guía básica acerca de cómo definir, operar y monitorizar un sistema para la gestión general de seguridad, de igual forma, apoyar en la consecución de la implementación de demás procesos COBIT para el Banco Popular. [Consejo Nacional de Supervisión del Sistema Financiero, mediante Artículo 6, del acta de la sesión 773-2009. Celebrada el 20 de febrero del 2009. Publicado en el diario oficial La Gaceta N°50 del jueves 12 de marzo del 2009]

Sobre esta misma línea, a partir del 2017, surge una actualización de la cual se derive el 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 de políticas, procedimientos y estándares de seguridad de TI.

Todo esto encauzó la ejecución de diversas actividades, tales como la realización del análisis del contexto del Área, incluyendo las principales disposiciones legales que los rigen, análisis de la normativa existentes y determinar cuáles son los más apropiados para la creación del modelo a implementar, dar apoyo en la ejecución de la autoevaluación de nivel de madurez de Gobierno de TI, específicamente proceso DS05, a su vez, apoyo en el desarrollo de un modelo de Gobierno de TI, basado en dicho acuerdo.

Otro aspecto esencial durante este periodo, fue la creación de la División de Seguridad de la

Información, como Área análoga a la gestionada, siendo que, a partir del año 2013 surge la necesidad de contar con un Plan de Gestión de Seguridad de la Información, por lo cual, mediante la ejecución del contrato 013-2012, se efectuó la contratación de una consultoría a la empresa Deloitte & Touche Tohmatsu 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 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. [Licitación Abreviada No. 2011LA-000059-PCAD "Contrato de Servicios Profesionales en la Elaboración de un Plan de Gestión de Seguridad de la información para el Banco Popular y de Desarrollo Comunal"]

Es por lo tanto que al definirse este plan, las tareas que asumía el Área de Seguridad Operativa Informatica en materia de normativa, su evaluación, así como el dictar planes de acción para la atención de las iniciativas que se derivan de dicho plan, se asignan a la División de Seguridad de la Información, siendo que, a través de dicho plan, se establece el alineamiento con la estrategia corporativa de conformidad con el estándar internacional ISO/IEC 27001 e ISO/IEC 27002, el cual separa la adquisición, implementación y administración de controles como tareas propias de la actividad del Área, todo esto en apoyo al cumplimiento normativo que en su momento se gestionaba en al Banco, sumando a su vez, nuevos cumplimientos, tal como se define en el Plan. [Acuerdo según oficio DIRG-359-2016, Acta DGCA-ACT-06, 2016, Circular DGCA-C-06-2017, 01/02/2017]

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 2010-2018

Año	Control Interno	Nivel	Riesgo Operativo	Nivel	Referencia
2015	1%	Excelente	1%	Excelente	UTEG-205-2015
2016	0%	Excelente	0%	Excelente	UTEG-179-2016
2017	0%	Excelente	0%	Excelente	- -
2018	0%	Excelente	0%	Excelente	UTEG-0281-2018

Fuente: Unidad Técnica de Evaluación de Gestión. Nota: Para el periodo comprendido entre los años 2010-2014 no se obtienen registros.

Acciones sobre el Control Interno

Como se puede notar, los resultados obtenidos sobre estas evaluaciones Control Interno y de Riesgo Operativo aplicadas al Área de Seguridad Operativa han sido satisfactorios en razón de que se mantienen en el más alto nivel de la escala, siendo claros los esfuerzos del equipo de trabajo; aunado a esto, se han realizado una cantidad significativa de fiscalizaciones por parte de la Auditoria Interna de Tecnologías de Información, así como autoevaluaciones de cumplimiento normativo de los acuerdos SUGEF 14-09 y 14-17, concluyendo en excelentes resultados en cuanto a la fortaleza y

completez de las estructuras de control dispuestas; sin embargo, a pesar de estas, por naturaleza del Área y por nuestro entorno, se presentan varias 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 reportes e incidentes asignados a través de la mesa de servicios.
5. Cumplimiento de los niveles de servicios pactados entre el Área y Sociedades Anónimas
6. Programación y cumplimiento de programas vacacionales de los funcionarios 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 logrado materializar 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:

Debido a la relevancia del carácter operativo que comprende el Plan Anual Operativo (PAO), como instrumento de gestión y planificación, al igual que demás dependencias de la Direccion de Tecnologías de Información, se ha participado en la formulación del Plan Táctico de TI, alineado con los objetivos, metas e indicadores del Plan Estratégico del Conglomerado Financiero Banco Popular para dar cumplimiento con los objetivos estratégicos, visión y misión del Conglomerado, de ahí que, se resume las calificaciones obtenidas durante los últimos años de gestión en la atención del PAO:

ÁREA SEGURIDAD OPERATIVA INFORMÁTICA
PLAN ANUAL OPERATIVO 2010-2018

Año	Avance logrado	Referencia
2015	99,28%	APRE-1325-2015
2016	98,60%	APRE-1479-2016
2017	99,98%	APRE-1230-2017
2018	100,00%	APRE-1327-2018
2019	100,00%	APRE-226-2019 *(1)*

Fuente: SIPRE – ÁREA DE PRESUPUESTO. Para el periodo comprendido entre los años 2010-2014 no se obtienen registros.
(1) Corresponde al resultado obtenida sobre la Orientación Estratégica 2019 al final del 1er. trimestre.

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 importancia de las cosas, dentro de los principales alcances, el recurso humano del Área:

   Se da en concurso las plazas pendientes y el nombramiento en propiedad de los miembros del equipo de trabajo del Área de Seguridad Operativa Informática de conformidad con lineamientos generales de Equidad e Igualdad de Género:

ÁREA SEGURIDAD OPERATIVA INFORMÁTICA PERSONAL ASIGNADO 2010-2019		
NOMBRE	GÉNERO	CATEGORIA
CARRILLO NAVARRO EVELYN MARIA	FEMENINO	20
CUBILLO RIVERA MARTIN RENE	MASCULINO	21
MONGE RODRIGUEZ ALEJANDRA	FEMENINO	21
NUÑEZ MORALES DAVID ANTONIO	MASCULINO	21
PICADO SANABRIA GABRIEL BERNARDO	MASCULINO	21
RODRIGUEZ TREJOS MELISSA	FEMENINO	21
VIQUEZ CHAVES YOHOJAN	MASCULINO	21

*Fuente: Dirección de Desarrollo Humano. Sistema STAR*H. Personal con nombramiento en propiedad*

Asimismo, como parte de los planes de capacitación de la Direccion de Tecnología de Información, y según se hace constar en el portal de la Direccion de Capital Humano, cada año se capacita al personal temas referentes a seguridad de la información y seguridad operativa.

Sobre esta misma línea, a la fecha de cierre de calificaciones aplicadas cada año, así como al de este informe, el personal cumple a cabalidad con lo establecido para el goce de días de vacaciones.

En cuanto al ambiente de trabajo, se detalla acerca de los logros obtenidos, según factores evaluados por el equipo de trabajo:

ÁREA SEGURIDAD OPERATIVA INFORMÁTICA EVALUACION DE AMBIENTE LABORAL – A SETIEMBRE 2018	
ASPECTO QUE SE EVALÚA	%
Adecuación al Cargo	
1. Mi trabajo me permite realizar tareas interesantes y desafiantes	100
2. Mis aptitudes y habilidades son aprovechadas en el cargo que ocupo	
Ambiente Facilitador	
3. Las condiciones de infraestructura en mi área de trabajo me permiten ser lo más productivo que puedo ser	97
4. Puedo realizar mi trabajo efectivamente sin obstáculos que lo impidan	
5. En mi área de trabajo, existe un ambiente interpersonal estimulante que me invita a ser productivo	
6. En mi área de trabajo predominan las relaciones armónicas que favorecen la productividad.	

Autonomía y Empowerment 7. Mi Jefatura o Supervisores brindan oportunidades para que mis ideas sean aceptadas e implementadas 8. Tengo la autonomía que requiere el puesto para realizar mi trabajo de manera efectiva 9. Mi Jefatura o Supervisores me incentivan para proponer nuevas y mejores ideas para hacer las cosas	*100*
Calidad y Orientación al Cliente 10. En mi área de trabajo la atención al cliente interno y/o externo es adecuada (Flexibilidad, Capacidad de respuesta, entre otras) 11. En mi área de trabajo se ofrecen los productos y/o servicios al cliente interno y/o externo 12. En mi área de trabajo se esmeran por conocer las necesidades y exigencias del cliente interno y/o externo 13. En mi área de trabajo el personal está comprometido a entregar un servicio de alta calidad sea con otras áreas de la organización o bien con clientes externos.	*100*
Colaboración 18. Existe trabajo en equipo y buena cooperación dentro de mi área de trabajo 19. En mi área de trabajo se promueve el intercambio de ideas para el enriquecimiento del equipo. 20. En mi área de trabajo se promueve la cooperación y comunicación con otras áreas.	*100*
Compromiso 21. Siento gran agradecimiento por pertenecer a esta organización 22. Siento orgullo de trabajar en mi organización	*100*
Comunicación 23. Mi Jefatura o Supervisores permiten que el personal pueda decir abiertamente lo que piensa, aunque esté en desacuerdo con los jefes o supervisores 24. Mi Jefatura o Supervisores comunican el avance de las tareas y proyectos del área de trabajo	*92*
Confianza en los líderes 25. Mi Jefatura o Supervisores predican con el ejemplo 26. Mi Jefatura o Supervisores se preocupan de apoyar y respaldar a su equipo ante el resto de la organización 27. Mi Jefatura o Supervisores se comunican de forma abierta y honesta con los empleados 28. Tengo confianza en mi Jefatura o Supervisores. 29. Mi Jefatura o Supervisor es un buen líder del equipo a su cargo 30. Mi Jefatura o Supervisor demuestra competencia técnica para hacer el trabajo	*100*
Entrenamiento 31. Mi Jefatura o Supervisor promueve una adecuada organización de los procesos de entrenamiento y/o capacitaciones con recursos internos. 32. Los nuevos empleados reciben el soporte y entrenamiento necesario para realizar su trabajo. 33. Mi Jefatura o Supervisor promueve igualdad de oportunidades para asistir a entrenamientos y/o capacitaciones.	*100*
Equidad e Igualdad de Género 34. En mi área de trabajo, se brinda igualdad de oportunidades para hombres y mujeres en cuanto al trato, la asignación de funciones, la promoción y el desarrollo de carrera 35. En mi área de trabajo, se promueve el respeto y una política clara de no al hostigamiento laboral y sexual	*100*
Esfuerzo Discrecional 36. Me siento motivado por hacer más de lo que mi puesto me exige 37. Mi organización me motiva a contribuir más allá de lo que mi puesto requiere	*100*
Estructura y Procesos 38. En mi área de trabajo, las labores están bien distribuidas 39. Mi área de trabajo tiene una estructura funcional adecuada 40. Mi área de trabajo innova y mejora los procesos internos regularmente.	*100*

Gestión del Desempeño 41. En mi área de trabajo se valora de forma clara y objetiva la productividad. 42. En mi área de trabajo se establece un estándar de alto desempeño. 43. Tengo una clara idea de los resultados que se esperan de mi trabajo 44. Recibo frecuente retroalimentación sobre cómo realizo mi trabajo	*100*
Resolución de conflictos 54. Cuando se comete un error en mi área de trabajo, mi jefatura o Supervisor busca solucionar el problema más que señalar a los culpables de este 55. Mi Jefatura o Supervisor estimula y facilita que los conflictos entre los miembros del equipo se conversen y se resuelvan.	*100*
Respeto y Reconocimiento 56. Mi Jefatura o Supervisor promueve el equilibrio entre mi vida profesional y personal 57. Mi Jefatura o Supervisor se interesa por el bienestar de sus colaboradores 58. Recibo reconocimiento de parte de mi Jefatura o Supervisor cuando realizo un buen trabajo 59. Mi Jefatura o Supervisor promueve una cultura de respeto en mi área de trabajo.	*100*
Compromiso Social 60. El Conglomerado Financiero divulga con claridad los objetivos y alcances de su compromiso social (por ejemplo, informar sobre productos y servicios diferenciados; financiamiento para organizaciones sociales como asociaciones comunales, solidaristas y acueductos rurales; creación de canales con cobertura en los diferentes territorios, alianzas estratégicas con organizaciones que comparten los mismos objetivos, entre otros). 61. El Conglomerado Financiero posee espacios o mecanismos para que las personas planteen o canalicen propuestas para fortalecer el rubro del compromiso social. 62. En mi área de trabajo se realizan actividades o iniciativas para sensibilizar a las personas acerca del origen del compromiso social del Conglomerado Financiero (por ejemplo, conocimiento de la Ley orgánica del BPDC, Pautas y Orientaciones Generales establecidas por la Asamblea de Trabajadores y Trabajadoras, Plan Estratégico del Conglomerado). 63. En mi área de trabajo se realizan actividades o iniciativas que impulsen el compromiso social del Conglomerado Financiero. 64. En mi área de trabajo se realizan actividades o iniciativas que impulsen la corresponsabilidad familiar (equilibrio entre el trabajo y la familia) del personal. 65. En mi área de trabajo se realizan actividades o iniciativas que impulsen el cumplimiento de los principios éticos del personal.	*97*
Claridad y Direccionamiento 14. Conozco la proyección de mi organización para los próximos 3 años 15. Tengo claro los planes definidos por mi organización para lograr los objetivos y metas. 16. Comprendo cómo el direccionamiento estratégico de mi organización nos permite ser más competitivos. 17. Entiendo cómo mi trabajo contribuye con las metas y objetivos de mi organización.	*92*
Oportunidades de Desarrollo 45. En mi organización existen oportunidades para lograr mis objetivos profesionales 46. En mi organización existen otras oportunidades de desarrollo profesional además de las promociones (Ej.: rotaciones, asignaciones especiales) 47. En mi organización existen mecanismos técnicos para facilitar el desarrollo de los colaboradores.	*94*
Recursos 48. La cantidad de personas que integran mi área de trabajo es adecuada en relación con el volumen de trabajo existente 49. En mi área de trabajo, las condiciones físico-ambientales de trabajo son las adecuadas 50. La organización me brinda la información necesaria para hacer bien mi trabajo ej. Cambio de procedimientos, nuevos productos y/o servicios, cambios en políticas y otros insumos de trabajo 51. La organización me brinda las herramientas y recursos necesarios para hacer mi trabajo de manera efectiva ej. Software, equipos, papelería, entre otros.	*90*

Remuneración y Beneficios	
52. Considerando el puesto que ocupo, creo que mi remuneración es adecuada con relación al mercado	100
53. Los beneficios otorgados por mi organización satisfacen mis necesidades	

Fuente: Dirección de Desarrollo Humano.

2. En cuanto a la normativa que se define en el Área, en relación con el proceso Cobit DS05, Gestionar los servicios de seguridad, se actualiza de conformidad con el acuerdo SUGEG 14-17.
3. 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.
4. 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.
5. 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).
6. Se brinda apoyo en diferentes proyectos institucionales, entre algunos:

- Accesos inalámbricos
- Acceso remoto (teletrabajo)
- Actualización plataforma T24 r09 y r17 (ActivID, TCBIB, T24),
- Acuerdo SUGEF 18-16 (Uso de firma digital)
- ATM's
- Autoriza7
- BACOSI
- Banca Móvil
- Bóveda digital
- Cámaras de seguridad y vigilancia bancaria,
- CARSI
- COBA
- Cobros, crédito
- FATCA-CRS
- Implementación
- INVENIO
- Microsoft Azure
- MORPHO
- Office 365
- Página presencial
- Página transaccional
- Quick Pass
- Servicio de chat
- SINPE (entrante y saliente)
- Tarjeta Chip
- Venta de bienes
- Web Popular Pensiones, entre otros.

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) 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. Dichas iniciativas son:

1. INI01 - Controlar el acceso a la red
2. INI02 - Gestionar dispositivos móviles
3. INI03 - Doble factor de autenticación en plataformas Core y VPN
4. INI04 - Fortalecer el proceso de manejo de vulnerabilidades y parchado
5. INI05 - Proteger y asegurar la información en soluciones en la nube
6. INI06 - Gestionar la administración de identidades y accesos de los usuarios
7. INI07 - Fortalecer seguridad en computadoras de usuario final (Endpoints)
8. INI08 - Respaldos de usuarios finales
9. INI09 - Fortalecer seguridad en ATM's
10. INI10 - Implementar Centro de Operaciones de Seguridad (SOC)
11. INI13 - Controlar el uso de carpetas compartidas en servidores
12. INI14 - Proteger los sistemas en línea ante ataques de denegación de servicio (DDoS)
13. INI15 - Adquirir herramienta de seguridad para analizar vulnerabilidades en el código de programación
14. INI16 - Proteger la información almacenada en las Bases de Datos
15. INI17 - Monitorear la integridad de archivos de configuración (FIM, File Integrity Monitoring)
16. INI18 - Automatizar el etiquetado de activos de información
17. INI20 - Adquirir herramientas y/o servicio para la prevención de fraude electrónico

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
ACT19: Fortalecer seguridad en computadoras de usuario final Endpoints – ATM's.	39%	42%	-3%	Ejecución Plan trabajo
GP01: Protección de información y acceso en ambientes híbridos INI03: Doble factor de autenticación en plataformas Core y VPN INI05: Proteger y asegurar la información en soluciones en la nube INI18: Automatizar el etiquetado de activos de información	75%	83%	-8%	II Parte CN

GP02: Aseguramiento, monitoreo de seguridad informática y gestión de identidades INI06: Gestionar la administración de identidades y accesos de los usuarios INI10: Implementar Centro de Operaciones de Seguridad (SOC) INI16: Proteger la información almacenada en las Bases de Datos	80%	92%	-12%	II Parte CN
GP03: Gestión de análisis de vulnerabilidades en sistemas de información. INI04: Vulnerabilidades y parchado INI15: Seguridad código programación INI17: FIM	6%	5%	1%	I Parte CN
INI01: Controlar el acceso a la red.	0%	0%	0%	Proyecto
INI14: Proteger los sistemas en línea ante ataques de denegación de servicio (DDoS)	6%	6%	0%	I Parte CN
INI20: Adquirir herramientas y/o servicio para la prevención de fraude electrónico	79%	89%	-10%	II Parte CN

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

En cuanto al estado de los proyectos más relevantes en el ámbito institucional que actualmente se encuentran en ejecución:

- INI01 - Controlar el acceso a la red, cuyo objetivo según PGSI es monitorear y controlar en tiempo real los dispositivos conectados a la red del Banco, así como proteger la segmentación de la red.

  De esta iniciativa se desprenden 2 actividades:

  1. Implementación de Firewalls físicos y virtuales en el Datacenter CODISA y Datacenter Monte Piedad, proceso que supero lo contractualmente acordado entre las partes y que actualmente se encuentra en etapa de normalización, de ahí que se encuentra en sitio un técnico de la Empresa Adjudicada como apoyo en la normalización, esto es, definición de reglas de conexión del tráfico entrante y saliente de la red (direcciones IP fuente y destino, puertos, protocolos, usuarios de conexión).

     Entre las actividades a realizar se encuentran:

     - **Grupo 1 (Servicios DHCP, DNS, Active Directory, Exchange, SINPE)**
       Fecha de Implementación 08 Abril – 31 Mayo 2019

       Para DNS (8 Abril – 26 Abril)
       1. *Levantamiento de Información (Revisión de entorno Virtualizado, Reuniones de Interesados – Dueños de Aplicaciones)*
       2. *Análisis de información recolectada*
       3. *Implementación de Firewalls Virtuales en modo monitoreo*
       4. *Análisis de Trafico en Firewalls Físicos y Virtuales*
       5. *Propuesta de Políticas de Seguridad Norte-Sur y Este-Oeste*
       6. *Implementación de Políticas de Seguridad Norte-Sur y Este-Oeste*
       7. *Ejecución de Protocolo de Pruebas*
       8. *Documentación*

     - DHCP (8 Abril – 26 Abril)
       1. *Levantamiento de Información (Revisión de entorno Virtualizado, Reuniones de Interesados –*

Dueños de Aplicaciones)
2. *Análisis de información recolectada*
3. *Implementación de Firewalls Virtuales en modo monitoreo*
4. *Análisis de Trafico en Firewalls Físicos y Virtuales*
5. *Propuesta de Políticas de Seguridad Norte-Sur y Este-Oeste*
6. *Implementación de Políticas de Seguridad Norte-Sur y Este-Oeste*
7. *Ejecución de Protocolo de Pruebas*
8. *Documentación*

- Active Directory (8 Abril – 26 Abril)
  1. *Levantamiento de información (Revisión de entorno Virtualizado, Reuniones de Interesados – Dueños de Aplicaciones)*
  2. *Análisis de información recolectada*
  3. *Implementación de Firewalls Virtuales en modo monitoreo*
  4. *Análisis de Trafico en Firewalls Físicos y Virtuales*
  5. *Propuesta de Políticas de Seguridad Norte-Sur y Este-Oeste*
  6. *Implementación de Políticas de Seguridad Norte-Sur y Este-Oeste*
  7. *Ejecución de Protocolo de Pruebas*
  8. *Documentación*

- Exchange (29 Abril – 10 Mayo)
  1. *Levantamiento de información (Revisión de entorno Virtualizado, Reuniones de Interesados – Dueños de Aplicaciones)*
  2. *Análisis de información recolectada*
  3. *Implementación de Firewalls Virtuales en modo monitoreo*
  4. *Análisis de Trafico en Firewalls Físicos y Virtuales*
  5. *Propuesta de Políticas de Seguridad Norte-Sur y Este-Oeste*
  6. *Implementación de Políticas de Seguridad Norte-Sur y Este-Oeste*
  7. *Ejecución de Protocolo de Pruebas*
  8. *Documentación*

- SINPE (4 Abril – 31 Mayo)
  1. *Levantamiento de información (Revisión de entorno Virtualizado, Reuniones de Interesados – Dueños de Aplicaciones)*
  2. *Análisis de información recolectada*
  3. *Implementación de Firewalls Virtuales en modo monitoreo*
  4. *Análisis de Trafico en Firewalls Físicos y Virtuales*
  5. *Propuesta de Políticas de Seguridad Norte-Sur y Este-Oeste*
  6. *Implementación de Políticas de Seguridad Norte-Sur y Este-Oeste*
  7. *Ejecución de Protocolo de Pruebas*
  8. *Documentación*

- **Grupo 2 (Servicios de Datos de Tarjetas, BP proveerá lista especifica de Servicios)**
  Fecha de Implementación 3 Junio – 1 Agosto 2019

- *Para cada aplicación:*
  1. *Levantamiento de información (Revisión de entorno Virtualizado, Reuniones de Interesados – Dueños de Aplicaciones)*
  2. *Análisis de información recolectada*
  3. *Implementación de Firewalls Virtuales en modo monitoreo*
  4. *Análisis de Trafico en Firewalls Físicos y Virtuales*

5. *Propuesta de Políticas de Seguridad Norte-Sur y Este-Oeste*
6. *Implementación de Políticas de Seguridad Norte-Sur y Este-Oeste*
7. *Ejecución de Protocolo de Pruebas*
8. *Documentación*

- **Grupo 3 (Servicios de Datos de Clientes, BP proveerá lista especifica de Servicios)**
  Fecha de Implementación 5 Agosto – 27 Septiembre 2019

- *Para cada aplicación:*
  1. *Levantamiento de información (Revisión de entorno Virtualizado, Reuniones de Interesados – Dueños de Aplicaciones)*
  2. *Análisis de información recolectada*
  3. *Implementación de Firewalls Virtuales en modo monitoreo*
  4. *Análisis de Trafico en Firewalls Físicos y Virtuales*
  5. *Propuesta de Políticas de Seguridad Norte-Sur y Este-Oeste*
  6. *Implementación de Políticas de Seguridad Norte-Sur y Este-Oeste*
  7. *Ejecución de Protocolo de Pruebas*
  8. *Documentación*

- **Grupo 4 (Servicios Restantes según lista de Análisis de Impacto de TI, BP proveerá lista de Servicios)**
  Fecha de Implementación 30 Septiembre – 1 Noviembre 2019

  Para cada aplicación:
  1. *Levantamiento de información (Revisión de entorno Virtualizado, Reuniones de Interesados – Dueños de Aplicaciones)*
  2. *Análisis de información recolectada*
  3. *Implementación de Firewalls Virtuales en modo monitoreo*
  4. *Análisis de Trafico en Firewalls Físicos y Virtuales*
  5. *Propuesta de Políticas de Seguridad Norte-Sur y Este-Oeste*
  6. *Implementación de Políticas de Seguridad Norte-Sur y Este-Oeste*
  7. *Ejecución de Protocolo de Pruebas*
  8. *Documentación*

2. Implementación de Tecnología de Control de Acceso a la Red (NAC), proceso que se encuentra en proceso de implementación de conformidad con lo contractualmente establecido.

Este proyecto está sustentado en la LICITACIÓN ABREVIADA No. 2018LA-000004-DCADM (DOCUMENTO CONTRACTUAL No.198-2018), por lo que, para mayor referencia debe consultar el documento "PLAN DE EJECUCIÓN DEL PROYECTO".

Para la implementación del producto, se acordó entre las partes el cronograma siguiente de actividades:

Nombre de tarea	% completado	%Planificado(%)	%Diferencia(%)
ISE - Control de Acceso a la Red PCAR-NAC	53%	36%	17%
Inicio	100%	100%	0%
Actividades previas a la ejecución contractual	91%	80%	11%
Entrega de equipo almacén / retiro de equipos	99%	100%	-1%
Planificación de la ejecución del proyecto	87%	81%	6%

Conformación de Equipo de Trabajo	100%	100%	0%
Plan de Calidad	100%	100%	0%
Matriz de Comunicación	40%	100%	-60%
Matriz de roles y responsabilidades	55%	100%	-45%
Cronograma y Plan de Proyecto	94%	94%	0%
Capacitación	99%	100%	-1%
Actividades Contractuales	41%	28%	13%
Ejecución	44%	29%	15%
Pase a producción (despliegue)	0%	0%	0%
Cierre del Proyecto	0%	0%	0%

Fuente: División Oficina Corporativa Administración Proyectos. Implementación tecnología NAC

El objetivo general del proyecto es proveer a la plataforma de TI del Banco Popular del hardware y software especializado para la solución de Control de Acceso a la Red para prevenir problemas de seguridad informática generados en el tráfico de la información provenientes de fuentes externas e internas; este por este motivo que dicha solución se debe integrar con la plataforma de red existente en la institución.

Como principales objetivos específicos (el detalle completo se encuentra en el cartel sección 2.1):

- Implementación de dos appliance físicos marca CISCO (SNS-3595) en el Data Center Principal y en el Alterno (uno por sitio en una configuración de HA).
- Realizar la capacitación específica para esta solución con un curso certificado de fabrica para cinco (5) funcionarios del Banco Popular.
- Realizar control y políticas de acceso por medio de una plataforma tipo NAC, la cual corresponde a una nueva implementación.
- Registrar inicialmente al menos la licencia de suscripción por un año para 10.000 dispositivos. Además, incluir el licenciamiento necesario para estos dispositivos, tomando en consideración que se incluyan usuarios internos e invitados con dispositivos en la red alámbrica y dispositivos en la red inalámbrica.
- Registrar el licenciamiento por suscripción por 1 año necesario para funciones avanzadas, como el análisis de postura y remediación, identificación de dispositivos y control de acceso de dispositivos de usuarios por medio de autenticación y autorización.
- Mantener los datos en tiempo real sobre los roles de usuarios, tipos de dispositivo, el uso de aplicaciones, la ubicación y la hora del día para darle visibilidad a la red, la automatización del flujo de trabajo, y la seguridad de los dispositivos personales y de propiedad del banco.
- Implementar la consola web integrada para monitoreo, reporte y solución de problemas para ayudar a los operadores de redes en la identificación y resolución de problemas de manera rápida.

Se tiene participación en diferentes foros del Conglomerado:

- Análisis de incidentes (según sea requerido por División de Seguridad Bancaria y Auditoria Forense)
- Comité Corporativo de Seguridad de la Información
- Comité Corporativo de Tecnología de Información
- Comité de Prevención de Fraude
- Comité Ejecutivo de Tecnología de Información
- Equipo Técnico Corporativo Seguridad de la Información
- Grupo de Arquitectura de Tecnología de Información

Administración de Recursos Financieros

En el Plan Anual Operativo del Área correspondiente al año 2019 se estableció el siguiente 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 en procesos:

ÁREA SEGURIDAD OPERATIVA INFORMÁTICA
PRESUPUESTO 2019 – EN COLONES

Objetivo	Meta	Presupuesto	Justificación
3 Cumplir con la disponibilidad de los servicios acordados con el negocio	Cumplir trimestralmente con el 95% de la evaluación de los SLAs (Acuerdos de niveles de servicio) vigentes	64,260,000.00	Inicio proceso de contratación de servicios de realización de pruebas de seguridad externa, así como aplicaciones como App SINPE Móvil, web transaccional, entre otras.
4 Identificar las brechas de seguridad de la infraestructura tecnológica crítica del negocio	Realizar trimestralmente un análisis de vulnerabilidades sobre la infraestructura tecnológica que soporta los servicios críticos del negocio.	1,575,738,500.00	Renovación del licenciamiento y soporte de las plataformas de seguridad informática, las cuales permiten asegurar los servicios del negocio.
5 Medir la efectividad de los controles de seguridad informática implementados	Realizar trimestralmente un informe estadístico de los eventos registrados por las herramientas de seguridad a la División de Control Operativo.	2,147,950,000.00	Atención de las iniciativas del Programa de Gestión de Seguridad de la Información.
6 Resolver en los tiempos establecidos los incidentes que afecten los servicios	Atender trimestralmente el 90% de los incidentes de seguridad asignados al área, en los tiempos establecidos en la mesa de servicios	955,531.25	Reemplazo de las sillas actuales.

En cuanto a los procesos de contratación referente pendiente de iniciar se encuentran los siguientes:

- Adquisición de certificados públicos digitales, los cuales permiten dar autenticidad a los sitios expuestos en Internet en lo que referencia la marca comercial del Banco.
- Firewalls (renovación de uso de licencia y soporte)
- Monitoreo de la marca Banco Popular en internet (*antiphishing*)
- Renovación del licenciamiento de usuario de la plataforma de autenticación y autorización de la web transaccional y el App Banca Móvil (ActivID)
- Servicio de análisis de vulnerabilidades, para la ejecución de pruebas de intrusión externas y el análisis de nuevas versiones del App Banca Móvil y el sitio web transaccional.

Sugerencias

Como bien se puede observar en el desarrollo del presente informe, debido a la relevancia del Área dentro de la Organización, sus tareas del día a día, sumado a esto la cantidad de

iniciativas asignadas al Área, así como los procesos de marcha y a su vez, tal como se desprende de la evaluación de ambiente laboral aplicada al mes de setiembre 2018, surge la necesidad de dotar de recurso humano al Área para para la buena marcha del Área dentro de la Organización, a fin de poder dar tono en todo lo que se pretende desarrollar, como elementos importantes para la gestión y mitigación de riesgos que podrían derivarse de las brechas de seguridad según pretende a través del Plan de Seguridad de la Información y la definición del Área (su naturaleza). Los argumentos de necesidad de dotar recursos al Área de igual forma se sustentan en lo gestionado a través de los oficios DGT-1961-2018, GGC-2019-2018, GGC-1639-2018.

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.

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

ÁREA SEGURIDAD OPERATIVA INFORMÁTICA DISPOSICIONES GIRADAS POR LA AUDITORÍA INTERNA		
INFORME	**RECOMENDACIÓN**	**VENCIMIENTO**
Informe de Auditoria #ATI-0022-2017 - Recomendación #6	Gestionar la formalización de los servicios de hardening para la infraestructura y aplicaciones del canal de banca móvil, considerando que para cada publicación de nuevas versiones se requiere la ejecución previa de pruebas de vulnerabilidades.	31-05-19
Informe de Auditoria #ATI-0100-2018 - Recomendación #6: La infraestructura base de seguridad presenta limitaciones en sus esquemas de resiliencia.	Realizarlas gestiones que correspondan para implementar esquemas redundantes en ambos centros de procesamiento de datos, de la infraestructura de seguridad perimetral y plataformas de autenticación administradas por su dependencia, según los resultados obtenidos de un análisis de riesgos, factibilidad técnica y costo-beneficio.	15-03-19
Informe de Auditoria #ATI-0020-2019 - Recomendación #2: La identidad del usuario y su acceso lógico a nivel del IBM i y Autoriza7, no se gestionan de forma adecuada.	En coordinación con la División de Desarrollo de Servicios, realizar una depuración de los usuarios agrupados en el Perfil General de Autoriza 7, de manera que se mantengan con ese perfil únicamente aquellos que por su naturaleza lo requieran.	31-05-19
Informe de Auditoria #ATI-0020-2019 - Recomendación #3: La identidad del usuario y su acceso lógico a nivel del IBM i y Autoriza7, no se gestionan de forma adecuada.	En coordinación con la División de Desarrollo de Servicios, establecer los procedimientos necesarios para delimitar la asignación de usuarios al Perfil General, asegurándose que se agreguen a ese perfil únicamente los usuarios que por sus funciones lo requieran.	31-05-19
Informe de Auditoria #ATI-0020-2019 - Recomendación #4: La identidad del usuario y su acceso lógico a nivel del IBM i y Autoriza7, no se gestionan de forma adecuada.	En coordinación con la División de Desarrollo de Servicios, definir e implementar los mecanismos automatizados para realizar el seguimiento del historial de cambios de perfil a que son sujetos los usuarios de Autoriza7.	31-05-19
Informe de Auditoria #ATI-0020-2019 - Recomendación #8: Manejo insuficiente de las potenciales vulnerabilidades en la infraestructura del IBM i	Analizar las potenciales vulnerabilidades asociadas a la versión 2.4.20 de Apache, sin limitarse a las indicadas en este informe, a partir de dicho análisis realizar las acciones que procedan para su mitigación al máximo posible, coordinando lo correspondiente con el Área de Soporte Técnico.	30-04-19
Informe de Auditoria #ATI-0020-2019 - Recomendación #9: Manejo insuficiente de las potenciales vulnerabilidades en la infraestructura del IBM i	Normar la revisión periódica de vulnerabilidades en la infraestructura del IBM i y Switch Transaccional como parte de las actividades operativas del Área.	31-05-19
Informe de Auditoria #ATI-0050-2019 - Recomendación #6: Escaso aprovechamiento de los servicios disponibles en la Nube debido a la ausencia de un adecuado esquema de seguridad lógica	En coordinación con la División de Seguridad de la Información, realizar las gestiones necesarias para habilitar los mecanismos de seguridad provistos por Microsoft para sus servicios en la nube, con la finalidad de habilitar el acceso externo a esos servicios a los usuarios que según un adecuado análisis de riesgos y costo beneficio lo requieran.	31-05-19

Informe de Auditoria #ATI-0050-2019 - Recomendación #8: Compra y distribución de equipos de cómputo Apple sin una justificación clara sobre su necesidad de uso	En función de la justificación aprobada para la recomendación 7, del presente informe, definir un plan de mitigación de las vulnerabilidades en seguridad informática y funcionalidad que presenta el uso cotidiano de equipos marca Apple conectados a la red del Banco. Asegurar que se apliquen las medidas para que los equipos cuenten al menos con el mismo nivel de seguridad de las PCs con sistema operativo Windows.	31-07-19
Informe de Auditoria #ATI-0065-2019 – Recomendación #7: Monitoreo de la Infraestructura tecnológica	Establecer un proceso de revisión de accesos fallidos y exitosos para los equipos de comunicaciones del Banco, en donde se establezca al menos: alcance, periodicidad, generación de alertas, áreas a comunicar las situaciones irregulares, responsables por la atención de las situaciones identificadas, seguimiento, escalamiento y cierre.	30-09-19
Informe de Auditoria #ATI-0065-2019 – Recomendación #12: Monitoreo de la Infraestructura tecnológica	12.Realizar los ajustes al procedimiento denominado inclusión, modificación y eliminación de usuarios de red, para que considere el monitoreo periódico de revisión de accesos vigentes o vencidos, la des habilitación y documentación de las excepciones, así como la administración de roles.	Pendiente de definir

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.