INFORME FINAL DE GESTIÓN

Nombre:	René Cubillo Rivera
Dependencia:	Área Seguridad Informática
Periodo de Gestión:	2020-2025
Destinatarios:	Mba.Silvia Goyez Rojas,Directora DIRCCH Lic. Zarina Arquedas Porras, Jefatura SECOPS Jefatura ASINF
Firma:	MARTIN RENE CUBILLO RIVERA (FIRMA) Fecha: 2025.08.12 15:54:43 -06'00'
Fecha:	08/08/2025

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 el Área de Seguridad Informatica por el suscrito, René M. Cubillo Rivera, como Informe final de gestión, Puesto 3035.01, Jefe de Área 2, T.I., labores realizadas como parte de las competencias y facultades, periodo abarca entre el 05/10/2010 al 11/08/2025.

Por lo anterior, mediante el presente informe se pretende, de manera concisa y ejecutiva, presentar los resultados de la gestión desarrollada, destacando los principales logros y limitaciones, así como brindar una perspectiva clara de los retos de gestión que se enfrentan. Asimismo, se exponen los proyectos e iniciativas en curso que deben ser avalados y aceptados por quien asuma la responsabilidad del Área, considerando las limitaciones actuales que esta enfrenta.

Cabe mencionar la circunstancia por la cual dicho informe se presenta en esta fecha, debido a la participación en un concurso para un puesto, en el cual se obtuvieron resultados satisfactorios siguiendo todo el proceso reglamentario, de forma transparente y cumpliendo con los requisitos establecidos.

Resultados de la gestión

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 de amenazas y protección tecnológica
- Supervisar la infraestructura para detectar eventos relacionados con la seguridad

Cambios en el entorno

El Área de Seguridad Informática surge ante la necesidad estratégica de establecer y mantener un nivel de seguridad altamente aceptable, que proteja de manera integral los activos de información y los recursos tecnológicos del Banco. Para ello, aplica normativas, políticas, procedimientos y controles alineados con las buenas prácticas internacionales en gestión de la seguridad de la información, en particular la ISO/IEC 27001:2022.

En concordancia con la ISO/IEC 27002:2022, se implementan controles técnicos, físicos y organizativos que cubren el ciclo completo de protección, desde el acceso y autenticación hasta el cifrado de la información en tránsito y en reposo, la gestión de vulnerabilidades y la respuesta a incidentes.

El área también da cumplimiento al Reglamento sobre la Gestión de la Tecnología de Información (SUGEF 14-09 / CONASSIF 5-24), asegurando que la gestión de TI cumpla con los criterios de evaluación establecidos en materia de seguridad operativa, así como con los requerimientos regulatorios específicos para entidades financieras supervisadas.

Para optimizar la administración de los recursos informáticos, el área integra técnicas y herramientas especializadas, incluyendo:

- Plataformas de detección y respuesta ante amenazas (EDR/NDR/XDR).
- Sistemas de Gestión de Eventos e Información de Seguridad (SIEM) para la correlación y monitoreo continuo.
- Firewalls de nueva generación (NGFW) y sistemas de prevención de intrusiones (IPS).
- Políticas de control de acceso basado en el principio de privilegio mínimo y autenticación multifactor (MFA).

Su labor se orienta a garantizar, mediante la aplicación de estándares y metodologías reconocidas, la confidencialidad, integridad y disponibilidad de la información, complementada con controles que regulen los aspectos físicos (acceso a centros de datos, seguridad perimetral) y lógicos (segmentación de red, hardening de sistemas), minimizando así los riesgos inherentes al uso de las tecnologías de información.

Finalmente, el Área de Seguridad Informática fomenta la mejora continua a través de revisiones periódicas, auditorías internas, pruebas de intrusión y ejercicios de simulación de incidentes, asegurando que las medidas de seguridad evolucionen al ritmo de las amenazas emergentes y los cambios regulatorios, manteniendo así un entorno tecnológico seguro, resiliente y conforme a las exigencias del sector financiero.

El Área de Seguridad Informática ha desempeñado un papel esencial en la ejecución del proceso DSS05 de COBIT 5 en la versión actual y en sus versiones anteriores, cuyo objetivo es proteger la información y los activos tecnológicos de la organización frente a amenazas internas y externas, garantizando que los servicios de TI se brinden de forma segura, confiable y conforme a la normativa vigente.

Este proceso es crítico en el sector financiero, donde la confidencialidad, integridad y disponibilidad de la información no solo representan un valor estratégico, sino también un requisito regulatorio impuesto por marcos como ISO/IEC 27001:2022, el Reglamento sobre la Gestión de la Tecnología de Información, y las mejores prácticas.

El Área de Seguridad Informática, en su rol de responsable de la implementación de las políticas y controles de seguridad, asegura que el DSS05 se cumpla mediante:

- Definición y aplicación de controles de acceso, autenticación y segregación de funciones para minimizar riesgos de uso indebido o acceso no autorizado.
- Monitoreo continuo de eventos de seguridad, detección de incidentes y respuesta oportuna, en coordinación con las áreas operativas y de negocio.
- Protección de la infraestructura tecnológica, incluyendo redes, servidores, aplicaciones y dispositivos de usuario final, mediante medidas de ciberseguridad avanzadas.

Cumplir con el DSS05 no solo mitiga la probabilidad e impacto de incidentes, sino que también fortalece la confianza de clientes, entes reguladores y partes interesadas, asegurando la resiliencia de la organización frente a un entorno de amenazas en constante evolución. De esta manera, el Área de Seguridad Informática se consolida como un pilar estratégico para la gobernanza tecnológica, la protección de los servicios y la sostenibilidad del negocio.

En el año 2021, el país enfrentó una ola sin precedentes de ciberamenazas, registrando aproximadamente 2.500 millones de intentos de ciberataques dirigidos contra infraestructuras críticas y organizaciones tanto del sector público como privado. Este contexto evidenció la necesidad de reforzar la capacidad defensiva y la resiliencia institucional, motivando la ejecución de diagnósticos exhaustivos para determinar la postura real de seguridad y la efectividad de los controles existentes.

Como parte de la respuesta, se fortalecieron las iniciativas y actividades operativas contempladas en el Plan de Gestión de Seguridad de la Información y Ciberseguridad (PGSIC), liderado por la División de Seguridad Corporativa, incluyendo la atención de recomendaciones de auditoría, la gestión de riesgos operativos, la ejecución de autoevaluaciones de seguridad y la verificación de cumplimiento normativo. En este proceso, el Área de Seguridad Informática asumió un papel central, liderando la implementación de controles preventivos, detectivos y correctivos para mitigar la probabilidad de ser víctimas de ataques cibernéticos como los que han afectado a numerosas instituciones a nivel nacional.

Los incidentes de ciberseguridad registrados no solo impulsaron la aprobación, por parte de la Gerencia General Corporativa (GGC), de nuevas plazas para reclutar profesionales especializados en ciberseguridad, sino que también marcaron un cambio estratégico en la forma en que la organización aborda la gestión de riesgos digitales.

Actualmente, los nuevos retos que enfrenta el Área de Seguridad Informática incluyen:

- Aumento y sofisticación de ataques basados en ransomware, phishing avanzado y amenazas persistentes avanzadas (APT).

- Protección de infraestructuras híbridas y entornos en la nube, garantizando la seguridad de datos y servicios críticos bajo modelos multi-nube y de terceros.
- Cumplimiento regulatorio más exigente, con mayores requerimientos de auditoría, trazabilidad y reporte a entes supervisores.
- Gestión de amenazas internas (intencionales o accidentales) que requieren políticas más estrictas de control de acceso, monitoreo.
- Respuesta a incidentes en tiempo real, con capacidades de análisis forense digital.
- Integración de inteligencia de amenazas para anticipar y neutralizar riesgos antes de que impacten a la organización.

Estas acciones y desafíos reflejan un cambio cultural y operativo, orientado a garantizar la confidencialidad, integridad y disponibilidad de la información, así como la continuidad de las operaciones en un entorno de amenazas en constante evolución.

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 Informática, esto según registros obtenidos de la Unidad Técnica de Evaluación de Gestión:

Área Seguridad Informática

Autoevaluaciones Control Interno y Riesgo Operativo 2020-2025

Año	Control Interno	Nivel	Riesgo Operativo	Nivel	Referencia
2020	0%	Excelente	0%	Excelente	UTEG-0142-2020
2021	0%	Excelente	0%	Excelente	Nota de la UTEG del 05/01/2022
2022	0%	Excelente	0%	Excelente	Correo de la UTEG del 04/01/2023
2023	0%	Excelente	0%	Excelente	Correo de la UTEG del 02/01/2024
2024	0%	Excelente	0%	Excelente	Correo de la UTEG del 08/01/2025

Acciones sobre el Control Interno

Como se evidencia en los resultados de las evaluaciones de Control Interno y Riesgo Operativo aplicadas al Área de Seguridad Informática, el desempeño ha sido satisfactorio, manteniéndose en el nivel más alto de la escala de calificación, lo que refleja el compromiso y esfuerzo del equipo de trabajo. A ello se suma la ejecución de fiscalizaciones por parte de la Auditoría Interna y Externa

Estas evaluaciones han concluido con resultados excelentes en cuanto a la fortaleza, eficacia y completitud de las estructuras de control implementadas, evidenciando una gestión sólida y alineada con los estándares regulatorios y mejores prácticas internacionales.

No obstante, dada la naturaleza crítica del Área y el entorno de amenazas en constante evolución actualmente, se ejecutan planes y proyectos para fortalecer y robustecer las estructuras de control existentes, incorporando controles más avanzados, procesos de monitoreo continuo, mecanismos de respuesta a incidentes de última generación e iniciativas de mejora continua que aseguren la resiliencia y el cumplimiento normativo frente a los retos actuales y futuros.

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 Dirección 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 Informática

Plan Anual Operativo 2020-2024

Año	Avance logrado	Referencia
2020	100%	ASOI-0007-2021 (APRE-831-2020)
2021	100%	ASOI-0010-2022 (APRE-607-2021)
2022	100%	ASOI-0017-2023 (APRE-604-2022)
2023	100%	ASOI-0002-2024 (APRE-664-2023)
2024	100%	ASINF-0004-2025 (APRE-638-2024)

Por lo tanto, considerando la naturaleza crítica del Área de Seguridad Informática, se han establecido metas y objetivos anuales claramente definidos para garantizar el cumplimiento de los objetivos estratégicos institucionales en materia de protección de la información. Estas metas contemplan acciones específicas emprendidas por el equipo de trabajo para mantener, perfeccionar y evaluar de forma continua los controles, asegurando que esté alineado con las normativas vigentes, las políticas internas y las mejores prácticas internacionales (ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 y marcos como COBIT DSS05).

Dichas acciones han sido objeto de procesos de auditoría interna y revisiones independientes, obteniendo resultados satisfactorios en términos de eficacia, alcance y pertinencia de los controles implementados. La definición y ejecución de estos objetivos han sido reconocidas positivamente por su claridad, amplitud y capacidad de respuesta frente a un entorno de ciberamenazas en constante evolución.

Como parte del fortalecimiento del Área de Seguridad Informática, y en respuesta a los relevantes incidentes ocasionados por ciberataques a nivel nacional e internacional, se identificó la necesidad de contar con el talento humano especializado para ejecutar los planes estratégicos y operativos, así como para definir e implementar estrategias de mejora continua en materia de ciberseguridad.

En este contexto, se logró incorporar nueve profesionales con experiencia y certificaciones en ciberseguridad, especializados en diversas áreas.

Esta incorporación de recurso humano altamente calificado ha permitido:

- Mantener y elevar los niveles de seguridad institucional, fortaleciendo la capacidad de prevención, detección y respuesta ante amenazas.
- Optimizar la ejecución del Plan de Gestión de Seguridad de la Información y Ciberseguridad (PGSIC), asegurando el cumplimiento de los objetivos estratégicos y regulatorios.
- Implementar controles más avanzados y adaptativos frente a amenazas emergentes, incluyendo técnicas de Threat Hunting e inteligencia de amenazas (Threat Intelligence).

- Reducir los tiempos de respuesta ante incidentes y mejorar la resiliencia operacional.
- Fomentar la mejora continua mediante revisiones periódicas de la postura de seguridad, auditorías internas y ejercicios de simulación de ataques (Red Team/Blue Team).

En cuanto al resultado obtenido en el Índice de Liderazgo de junio de 2025, el cual constituye un componente esencial del indicador estratégico de Ambiente Laboral y tiene como propósito fortalecer las prácticas de liderazgo dentro de la organización, se indica que la calificación alcanzada se ubica en el rango de **Clara Fortaleza**, de acuerdo con el mapa de calor adjunto. Este resultado refleja un desempeño sobresaliente y consolidado, así como un impacto positivo en el ambiente laboral del equipo de trabajo.

LÍDER: Cubillo Rivera Martín Rene

CALIFICACIÓN ÍNDICE DE LIDERAZGO: 92.31% CLARA FORTALEZA

Jefatura:	CUBILLO RIVERA MARTIN RENE
Dependencia Designada:	AREA SEGURIDAD INFORMATICA
Objetivo encuesta Índice de Liderazgo	Proporcionar una visión clara y objetiva del desempeño de los líderes en relación con su capacidad para desarrollar equipos, comunicar eficazmente, promover los valores organizacionales y fomentar una cultura de alto rendimiento.

MAPA DE CALOR	
CLARA FORTALEZA	≥80% a 100%
MODERADA FORTALEZA	≥66% a 79%
OPORTUNIDAD DE MEJORA	≥56% a 65%
ALERTA-CRÍTICO	≤55%

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 2020-2025. 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-PLA-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. Dichas iniciativas son:

Código A/I/P*	Descripción
ACT19	Fortalecer seguridad
ACT26	Gestionar análisis de vulnerabilidades

ACT31	Fortalecer seguridad
ACT33	Proteger los sistemas en línea
ACT34	Aseguramiento de ambientes Microsoft
ACT36	Monitorear Integridad
INI10	Centro de Operaciones de Seguridad
INI20	Mecanismos técnicos para la eliminación segura
INI21	Mecanismos que aseguren el uso de bitácoras
INI24	Microsegmentación.
PLA04	Contar con servicios respuesta de incidentes.
PLA11	Mecanismos de control.
PLA30	Mecanismos y procedimientos para la recolección de evidencia.
PLA31	Microsegmentación
PLA35	Mecanismos para auditar las reglas
PLA49	Mecanismos de cuarentena.
PLA50	Controles automatizados

*ACT: Actividad, INI: Iniciativa, PLA: Plan de Acción

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-PLA-ACT, se

encuentra en desarrollo o bien en su normalización:

ÁREA SEGURIDAD INFORMÁTICA
AVANCE DE INICIATIVAS 2025

Código A/I/P	% Avance Real	% Avance Planeado	Etapa
ACT19	100%	100%	Finalizado
ACT26	100%	100%	Finalizado
ACT31	0%	0%	No iniciada
ACT33	100%	100%	Finalizado
ACT34	100%	100%	Finalizado
INI10	100%	100%	Finalizado
ACT36 (INI17)	85%	60%	Ejecución Plan de Trabajo
PLA04	100%	100%	Finalizado
PLA11	100%	100%	Finalizado
INI20	46%	41%	Ejecución Plan de Trabajo
INI21	93%	92%	Ejecución Plan de Trabajo
INI24	68%	66%	Ejecución Plan de Trabajo
PLA30	49%	35%	Ejecución Plan de Trabajo
PLA31	100%	100%	Finalizado
PLA35	100%	100%	Finalizado

PLA49	100%	100%	Finalizado
PLA50	100%	100%	Finalizado

Se tiene participación en diferentes foros del Conglomerado:

- Análisis de incidentes (según sea requerido por División de Seguridad Bancaria y Auditoria)
- Comité Corporativo de Seguridad de la 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 2025 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:

Formulación Presupuestaria 2025

Dirección	Presupuesto Aprobado 2025	Justificación
Dirección Tecnología de Información	₡116 262 195,32	Dar continuidad al objeto de infraestructura
Dirección Tecnología de Información	₡6 821 678,64	Dar continuidad a renovación de infraestructura
Dirección Tecnología de Información	₡140 970 012,60	Dar continuidad al objeto del servicio
Dirección Tecnología de Información	₡13 468 269,24	Dar continuidad al objeto del servicio
Dirección Tecnología de Información	₡14 552 883,54	Dar continuidad al objeto del servicio
Dirección Tecnología de Información	₡233 606 188,68	Dar continuidad a renovación de infraestructura

Dirección Tecnología de Información	₡159 983 117,64	Dar continuidad al objeto de renovación
Dirección Tecnología de Información	₡152 015 940,84	Dar continuidad al objeto del servicio
Dirección Tecnología de Información	₡9 290 535,12	Dar continuidad al objeto del servicio
Dirección Tecnología de Información	₡211 609 445,00	Ampliación de la cobertura de la solución
Dirección Tecnología de Información	₡48 102 933,85	Ampliación de la cobertura de la solución
Dirección Tecnología de Información	₡2 750 985,00	Ampliación de la cobertura de la solución
Dirección Tecnología de Información	₡177 448 000,00	Dar continuidad al objeto de renovación
Dirección Tecnología de Información	₡15 311 500,00	Ampliación del licenciamiento y soporte
Dirección Tecnología de Información	₡6 000 000,00	Especies fiscales
Dirección Tecnología de Información	₡3 795 505,68	Renovación del licenciamiento y soporte
Dirección Tecnología de Información	₡169 217 500,00	Renovación del licenciamiento y soporte
Dirección Tecnología de Información	₡3 441 528,00	Renovación del licenciamiento y soporte
Dirección Tecnología de Información	₡30 621 758,40	Servicio de soporte
Dirección Tecnología de Información	₡90 384 801,36	Renovación del licenciamiento y soporte
Dirección Tecnología de Información	₡5 961 480,00	Renovación del licenciamiento y soporte
Dirección Tecnología de Información	₡12 000 000,00	Servicios de soporte
Dirección Tecnología de Información	₡123 974 532,00	Servicio Monitoreo
Dirección Tecnología de Información	₡13 888 477,44	Certificados digitales
Dirección Tecnología de Información	₡80 569 000,00	Renovación del licenciamiento y soporte
Dirección Tecnología de Información	₡81 360 000,00	Renovación del licenciamiento y soporte
Dirección Tecnología de Información	₡36 381 384,00	Renovación del licenciamiento y soporte
Dirección Tecnología de Información	₡18 737 433,60	Renovación del licenciamiento y soporte
	₡1 978 527 085,95	

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

- Adquisición de solución de borrado seguro.
- Renovación de licenciamiento de filtrado de contenido

- Monitoreo de la marca Banco Popular en internet (antiphishing)
- Renovación de licenciamiento y soporte de herramientas de seguridad informática
- Suscripción De Licenciamiento Y Soporte De La Plataforma Symantec

Sugerencias

Como se expone a lo largo del presente informe, y dada la relevancia del Área dentro de la Organización, así como la naturaleza de sus tareas diarias y la cantidad de iniciativas asignadas, surge la necesidad de recuperar dos plazas de funcionarios que, en noviembre de 2024, presentaron su renuncia. La reincorporación de estos recursos resulta fundamental para dar continuidad a las acciones previstas, las cuales son elementos clave para la gestión y mitigación de riesgos derivados de posibles brechas de seguridad, conforme a lo establecido en el Plan de Seguridad de la Información y en las funciones definidas para el Área.

Dar seguimiento a los planes de pruebas y a los planes de mejora del SIEM. En este último, es relevante que se complete su implementación para poder abarcar las demás áreas de la DIRTI y evaluar su extensión a las sociedades anónimas.

Adicionalmente, se reconoce que existen otras funciones que el Área actualmente no ha podido asumir, así como ciertas labores que no corresponden a su naturaleza y que deben ser reasignadas a otras dependencias para optimizar la eficiencia operativa y asegurar el cumplimiento de los objetivos estratégicos en materia de ciberseguridad.

Observaciones

Es fundamental valorar las sugerencias recibidas, ya que el Área se encuentra en una etapa clave para consolidar y dar continuidad al desarrollo de las iniciativas en curso dentro del Proyecto del Programa de Gestión de Seguridad de la Información. El compromiso y la dedicación del equipo permitirán no solo atender de manera efectiva las brechas identificadas, sino también fortalecer nuestra postura de seguridad y habilitar la ejecución de nuevos proyectos estratégicos. Con este enfoque, aseguramos un avance sostenido hacia nuestros objetivos, potenciando la resiliencia y la innovación en la gestión de la seguridad de la información.

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 Informática

Recomendaciones en Proceso

Informe	Recomendación	Fecha vencimiento
AIRI-06-2025	8	30/11/2025
AIRI-06-2025	10	30/9/2025
AIRI-06-2025	12	31/8/2025
ATI-11-2025	9	30/11/2025
ATI-11-2025	11	31/1/2026
ATI-11-2025	13	30/9/2025
ATI-11-2025	17	31/1/2026
ATI-11-2025	20	31/1/2026
ATI-11-2025	21	31/1/2026
ATI-11-2025	22	31/1/2026
ATI-11-2025	24	31/1/2026
ATI-11-2025	27	31/1/2026
AIRI-18-2025	2	30/6/2026
AIRI-18-2025	4	31/3/2026

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

A continuación, se detalla los contratos en ejecución, así como información importante para su seguimiento y control.

Es importante indicar que los contratos se les genera los informes de desempeño y el periodo, según lo normado por la División de Contratación Administrativa y que para la gestión de pagos se realiza de previo una evaluación de servicios para determinar el cumplimiento del proveedor y para aplicación de multas en caso de que estas procedan.

Toda la documentación se carga en expediente electrónico del SICOP

ÁREA SEGURIDAD INFORMÁTICA
CONTRATOS VIGENTES

Licitación	Descripción	Vencimiento
2023LE-000002-0020600001	Adquisición y renovación de licencias de seguridad	29/6/2027
2021LA-000005-0020600001	Adquisición de licenciamiento	13/2/2026
2022LN-000005-0020600001	Adquisición y renovación de licencias y soporte	5/9/2026
2022CD-000068-0020600001	Adquisición de Infraestructura	21/6/2027
2022CD-000052-0020600001	Adquisición de Herramientas y Licenciamiento	30/1/2027
2023LE-000012-0020600001	CERTIFICADOS DIGITALES	8/3/2028
2023LY-000006-0020600001	Servicio De Monitoreo	5/4/2028
2023LY-000028-0020600001	Adquisición y renovación de licenciamiento y soporte	14/5/2028
2023LY-000033-0020600001	Renovación de licenciamiento y soporte	17/5/2028
2024LE-000001-0020600001	Renovación de licenciamiento y soporte	10/5/2028
2024XE-000004-0020600001	Renovación de licenciamiento y soporte	20/9/2025
2024LE-000003-0020600001	Renovación de licenciamiento y soporte	1/12/2028
2024XE-000005-0020600001	Servicio De Monitoreo	2/12/2025
2023LY-000025-0020600001	Adquisición y renovación de licenciamiento y soporte	26/1/2029
2024LY-000013-0020600001	Renovación de licenciamiento y soporte	13/3/2029
2025LD-000007-0020600001	Renovación de licenciamiento y soporte	14/2/2030
2025LY-000007-0020600001	Suscripción de Licencias, soporte y mantenimiento	5/8/2029
Total		**17**

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.