INFORME DE AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA SEGURIDAD DE INFORMACIÓN CONTENIDA EN LOS SISTEMAS SUSTANTIVOS DEL INSTITUTO COSTARRICENSE DE ACUEDUCTOS Y ALCANTARILLADOS

12 de octubre 2023

Informe n.° DFOE-SOS-IAD-00006-2023

Contraloría General de la República

División de Fiscalización Operativa y Evaluativa

Área de Fiscalización para el Desarrollo de Sostenible

Auditoría de Carácter Especial - Compromiso de informe directo

CONTENIDO

Resumen Ejecutivo

¿QUÉ EXAMINAMOS?

La auditoría tuvo como objetivo determinar si la seguridad de la información de los sistemas críticos del AyA responden al marco normativo y buenas prácticas aplicables, de forma que respalden la gestión sustantiva institucional. Para ello, se analizó la gobernanza de la seguridad, los controles de ciberseguridad y continuidad del negocio; la operación, gestión y mantenimiento de sistemas, así como los controles para detener, atenuar y responder a posibles incidentes de ciberseguridad, durante el período 2022 y primer semestre 2023.

¿POR QUÉ ES IMPORTANTE?

El AyA tiene a cargo los servicios públicos de abastecimiento de agua potable y de saneamiento de aguas residuales para gran parte de la población. En 2022, la venta de agua de ese Instituto significó un total de ¢127 mil millones y los ingresos por servicios de alcantarillado sanitario y pluvial ¢39 mil millones. En la prestación de estos servicios, se requiere una infraestructura tecnológica que soporte y garantice la seguridad de la información en los sistemas más críticos, del AyA, dado el alto volumen de información que procesan y la relevancia para el país.

¿QUÉ ENCONTRAMOS?

Se determinó que el AyA presenta un muy bajo cumplimiento del marco normativo y buenas prácticas aplicables en materia de seguridad de la información de los sistemas críticos. Al respecto, el AyA cuenta con una política de seguridad de la información, implementación de respaldos de la información y medidas de seguridad física y ambiental para su resguardo; además, atendió oportunamente las vulnerabilidades comunicadas mediante oficio con insumos n.° 6315 (DFOE-SOS-0181) del 18 de mayo de 2023.

Sin embargo, no existe un marco de gobierno para la seguridad de la información, basado en un sistema de gestión en la materia, que se alinee con la estrategia organizacional para brindar garantía razonable de seguridad. Es así como, pese a que existe un Comité de TI, este no ha cumplido con sus funciones y no se han llevado a la práctica los roles y responsabilidades de actores clave como las del Comité de Seguridad y el Oficial de Seguridad. Además, no se ha implementado un programa de sensibilización en cuanto a seguridad, ni se han establecido cláusulas sobre confidencialidad de la información y garantía de continuidad del servicio en los documentos contractuales para servicios de TI que impactan la seguridad de la información.

Además, se encontraron débiles controles en materia de ciberseguridad, ya que producto de diversas pruebas realizadas, se encontró que los sistemas críticos en el AyA presentan vulnerabilidades en cuanto a componentes externos y configuraciones del sitio web. Además, pese a que el acceso a sistemas está restringido y existe una política de contraseñas, no se gestionan las cuentas de usuario ni se evidencia un cumplimiento de la política.

En línea con lo anterior, no se ha implementado una estrategia para la gestión de continuidad del negocio que asegure la provisión de servicios ante eventos que afecten la disponibilidad de sistemas y tampoco se ha implementado un Análisis de Impacto del Negocio (BIA) ni un Plan para la Contingencia Tecnológica, sumado a que la programación de respaldos no contempla las pruebas que garanticen su efectividad.

Por su parte, existen oportunidades de mejora en controles de aplicación y gestión de las operaciones de tecnologías de la información que impactan la seguridad de la información, ya que pese a que el AyA cuenta con controles de autenticación de usuarios y de entrada de datos para los sistemas críticos, estos siguen siendo monofactor, es decir, sin doble autenticación o superior configuración. Tampoco se cuenta con políticas ni procedimientos implementados para normar los procesos de TI que inciden en la seguridad de información como: gestión de cambios, atención de incidentes y problemas, gestión de configuraciones, gestión de versiones, gestión de servicios de TI, mantenimiento preventivo y correctivo, clasificación de información, destrucción segura de medios de almacenamiento e información y uso de dispositivos móviles.

Lo evidenciado obedece al escaso direccionamiento y monitoreo del jerarca y titulares subordinados para conciliar la seguridad de la información como parte esencial del giro de negocio y la falta de seguimiento en la implementación de las políticas y controles de seguridad de la información. Además, la organización no cuenta con un ambiente de control orientado al cumplimiento de buenas prácticas para normar operaciones y sistemas que pueden afectar la seguridad de la información ni ha gestionado oportunamente las actualizaciones en los sistemas.

Las situaciones encontradas exponen a la institución a un riesgo de pérdida de confidencialidad, disponibilidad e integridad de la información que se almacena en sus sistemas de misión crítica, así como a una posible interrupción de servicios y tiempo excesivo de recuperación ante un evento. A su vez, se expone a una pérdida de disponibilidad de sistemas críticos y eventuales contingencias por incumplimiento y exposición a ataques externos.

¿QUÉ SIGUE?

Se emiten disposiciones a la Presidencia Ejecutiva para implementar un Sistema de Gestión de la Seguridad de la Información, así como una estrategia para la gestión de la continuidad del negocio que contenga al menos el análisis de impacto de negocio, el plan de continuidad de negocio, y el plan de contingencia tecnológica. Además, se dispone la implementación de un plan de atención, con las medidas integrales y paliativas, para solventar la obsolescencia tecnológica de aplicaciones y bases de datos que inciden en las operaciones del AyA. También se dispone a la Gerencia General la implementación de un procedimiento para identificar y atender las vulnerabilidades conocidas, así como remediar las vulnerabilidades que le fueron informadas por la Contraloría General, y la implementación de acciones para el establecimiento de controles de ciberseguridad, así como de políticas y procedimientos en materia de seguridad de la información.

INFORME DE AUDITORÍA SOBRE LA SEGURIDAD DE INFORMACIÓN CONTENIDA EN LOS SISTEMAS SUSTANTIVOS DEL INSTITUTO COSTARRICENSE DE ACUEDUCTOS Y ALCANTARILLADOS

1. INTRODUCCIÓN

ORIGEN DE LA AUDITORÍA

1.1. La auditoría se efectuó con fundamento en las competencias que le confieren a la Contraloría General los artículos 183 y 184 de la Constitución Política, así como los artículos 17, 21 y 37 de su Ley Orgánica n.° 7428.

1.2. El AyA tiene a cargo los servicios públicos de abastecimiento de agua potable y de saneamiento de aguas residuales para gran parte de la población. En 2022, la venta de agua de ese Instituto significó un total de ¢127 mil millones y los ingresos por servicios de alcantarillado sanitario y pluvial ¢39 mil millones. En la prestación de estos servicios, se requiere una infraestructura tecnológica que soporte y garantice la seguridad de la información en los sistemas más críticos, del AyA, dado el alto volumen de información que procesan y la relevancia para el país.

OBJETIVO GENERAL

1.3. La auditoría tuvo como objetivo determinar si la seguridad de la información de los sistemas críticos del AyA responden al marco normativo y buenas prácticas aplicables, de forma que respalden la gestión sustantiva institucional. Para ello, se analizó la gobernanza de la seguridad, los controles de ciberseguridad y continuidad del negocio; la operación, gestión y mantenimiento de sistemas, así como los controles para detener, atenuar y responder a posibles incidentes de ciberseguridad.

ALCANCE

1.4. La auditoría comprendió el análisis de la seguridad física y lógica de los sistemas de información sustantivos del AyA que aseguran la confidencialidad, integridad y disponibilidad de la información contenida en estos sistemas. El periodo de análisis comprendió del 01 de enero de 2022 al 30 de junio de 2023, el cual se amplió cuando se consideró necesario.

CRITERIOS DE AUDITORÍA

1.5. Mediante reunión virtual el 28 de junio de 2023 se comunicaron los criterios de auditoría a las siguientes personas funcionarias del AyA: Lic. Alejandro Guillén Guardia, Presidente

Ejecutivo, Licda. María Gabriela Vallejo Astúa, Gerente General; Licda. Sonia Murillo Hurtado, encargada de Control Interno, Lic. Miguel Cordero Leiva, Director de TI; Ing. Luis Fernando Ulate Vargas, encargado de Infraestructura y la Licda. Mauren Alvarado Granados Asesora, Lic. José Castillo Canales, Auditoría Interna. Estos criterios se comunicaron formalmente mediante oficio n.° 9034 (DFOE-SOS-0318-2023) del 07 de julio de 2023.

1.6. Como parte de las fuentes de criterios de auditoría utilizados destacan la Ley General de Control Interno n.° 8292; Marco Normativo de Gobierno y Gestión de las TI, emitido por MICITT en 2021 (Normas Técnicas para Gobierno y Gestión de TI), así como buenas prácticas de la industria y la seguridad, COBIT 5/2019, ISO 27001, además del código de prácticas ISO 27002.

METODOLOGÍA APLICADA

1.7. La auditoría se realizó de conformidad con las Normas Generales de Auditoría para el Sector Público, con el Manual General de Fiscalización Integral de la CGR, el Procedimiento de Auditoría establecido por la DFOE, que está basado en la ISSAI 100: Principios Fundamentales de Auditoría del Sector Público, y los principios de la ISSAI 400: Principios de la Auditoría de Cumplimiento de las Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI por sus siglas en inglés).

1.8. Para el desarrollo de esta auditoría se utilizó la información suministrada en las entrevistas, reuniones, y consultas planteadas por escrito a las personas funcionarias del AyA, así como una visita al Centro de Procesamiento de Datos en oficinas centrales del Instituto. Además, se realizaron pruebas no intrusivas de ciberseguridad sobre la infraestructura y aplicaciones institucionales del AYA, así como pruebas de ciberseguridad sobre componentes externos y configuraciones de direcciones web de la institución.

ASPECTOS POSITIVOS QUE FAVORECIERON LA EJECUCIÓN DE LA AUDITORÍA

1.9. Como parte de los aspectos positivos a resaltar, se encuentra la colaboración prestada por parte de la Auditoría Interna del AyA con un funcionario a tiempo completo como integrante del equipo de auditoría, así como las acciones oportunas emprendidas por el AyA para abordar las vulnerabilidades comunicadas mediante oficio con insumos n.° 6315 (DFOE-SOS-0181) del 18 de mayo de 2023.

GENERALIDADES ACERCA DEL OBJETO AUDITADO

1.10. La gestión de la seguridad de la información es fundamental en la protección de los activos de información, además de ser una herramienta que impulsa la consecución de objetivos estratégicos como la creación de valor, la gestión de riesgos y la optimización de recursos. La seguridad entendida como protección de la información, de la infraestructura, de las personas y de los procesos, abarca el cumplimiento de tres principios o aspiraciones básicas como lo son la confidencialidad, la disponibilidad y la integridad de la información.

1.11. En el caso del AyA, al tratarse de una institución cuya misión es garantizar los servicios de agua potable, alcantarillado sanitario y tratamiento, para contribuir al desarrollo económico y social del país, es fundamental que los procesos de apoyo como recaudación y cobro,

así como la administración del recurso humano, entre otros, aseguren la confidencialidad, disponibilidad y la integridad de la información, especialmente cuando se busca brindar un servicio eficiente, optimizar el uso de recursos y garantizar la entrega de valor.

1.12. Para apoyar estos dos grandes procesos de negocio o macro actividades, el AyA mantiene una infraestructura de tecnologías de información que incluye entre otros: redes, un centro de procesamiento de datos, equipos servidores, equipos de usuario final, dispositivos de conectividad, de almacenamiento y software tanto sistemas operativos como aplicaciones que en conjunto requieren de la aplicación de buenas prácticas de gestión y protección.

1.13. Existen una serie de recursos de misión crítica para el AyA desde el punto de vista de tecnología, aquellos recursos que si estuvieran ausentes impedirían la prestación de servicios, o al menos generaría una dificultad mayor. El suministro eléctrico, las instalaciones de procesamiento en oficinas centrales y las que se han tercerizado, así como el software que se ha desarrollado o adquirido para soportar los procesos sustantivos son componentes relevantes para efectos de este estudio. Se debe aclarar que los sistemas SCADA se consideraron únicamente para la valoración que tiene que ver con el proceso de Continuidad de Negocio y que no se ejecutaron pruebas de funcionalidad a estos componentes.

COMUNICACIÓN PRELIMINAR DE LOS RESULTADOS DE LA AUDITORÍA

1.14. El 25 de setiembre de 2023, mediante oficio n°. DFOE-SOS-0475 (12900) se remitió el Borrador del informe de auditoría al AyA, para que en el plazo concedido formulara las observaciones que estimara pertinentes sobre el contenido del informe.

1.15. La presentación verbal de los resultados se realizó de manera virtual el 2 de octubre de 2023 a Alejandra Mora Segura, Gerente General, Ana Cristina Pereira Meneses, Asesora de Gerencia General, Miguel Cordero Leiva, Director de TI, Luis Fernando Ulate Vargas, Encargado de Infraestructura, así como Roberto Apuy, funcionario Departamento de Control Interno, Karen Espinoza Vindas, Auditora Interna y Jose Castillo Canales, funcionarios de la Auditoría Interna del AyA.

1.16. Finalmente, mediante oficio n°. GG-2023-03152 del 5 de octubre de 2023 el AyA remitió sus observaciones al Borrador de informe, las cuales fueron analizadas e incorporados los ajustes en lo correspondiente al presente informe de auditoría.

2. RESULTADOS

2.1. Se determinó que el AyA cuenta con una política de seguridad de la información, implementación de respaldos de la información y medidas de seguridad física y ambiental para su resguardo; además, atendió oportunamente las vulnerabilidades comunicadas mediante oficio con insumos n.° 6315 (DFOE-SOS-0181) del 18 de mayo de 2023, relacionadas con cifrados de información, exposición de información de infraestructura, políticas de seguridad de contenido de sitio sin configurar, versión vulnerable de Web server, exposición de directorios y librerías de terceros con vulnerabilidades conocidas. No obstante, presenta varias debilidades relacionadas con la gobernanza de la seguridad, la

implementación de controles de ciberseguridad y continuidad de negocio, así como en controles de aplicación y de gestión de operaciones de tecnologías de información.

Gobernanza de la Seguridad

Ausencia de un marco de gobierno para la seguridad de la información

2.2. Se encontró que el AyA no ha desarrollado un sistema de gestión de la seguridad de información que se alinee con la estrategia organizacional para brindar garantía razonable de la seguridad de la información. De esta manera, pese a que existe un Comité de TI, este no ha cumplido con sus funciones y no se han llevado a la práctica los roles y responsabilidades de actores clave como las del Comité de Seguridad y el Oficial de Seguridad. Además, no se ha implementado un programa de sensibilización en materia de seguridad ni se han establecido cláusulas sobre confidencialidad de la información y garantía de continuidad del servicio en los documentos contractuales para servicios de TI que impactan la seguridad de la información.

2.3. Al respecto, el AyA carece de un sistema de gestión de seguridad de información que considere al menos una estrategia de seguridad de información, que esté acorde con los objetivos estratégicos institucionales y que permita conocer el estado actual y el estado deseado en materia de seguridad de información y ciberseguridad, así como los recursos necesarios para implementar, operar y mejorar ese sistema, lo mismo aplica para el programa de seguridad que permite llevar a la práctica la estrategia. Si bien el área técnica ha implementado controles desde el punto de vista de buenas prácticas en ingeniería, esto no está orientado al cumplimiento de objetivos específicos y a la integración del esfuerzo de protección de los activos.

2.4. Esto no es acorde con lo establecido en la Ley General de Control Interno, Ley n.° 8292, la cual establece en sus artículos 7 y 8 la obligatoriedad de disponer de un sistema de control interno, entendido como la serie de acciones ejecutadas por la administración activa, diseñadas para proporcionar seguridad en proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal, exigir confiabilidad y oportunidad de la información, garantizar eficiencia y eficacia de las operaciones y cumplir con el ordenamiento jurídico y técnico.

2.5. También, es contrario a lo que establece el proceso APO 02 del COBIT 5, sobre la necesidad de establecer y formalizar una estrategia de TI que incluye la seguridad y que debe estar en línea con los objetivos y expectativas del negocio. Específicamente destacan los procesos 03, 04, 05 y 06 sobre definir el objetivo de las capacidades de TI, realizar un análisis de diferencias o de brechas, definir el plan estratégico y la hoja de ruta, así como comunicar la estrategia y la dirección de TI.

2.6. Por otra parte, a pesar de que el AyA ha definido roles especializados en materia de seguridad de la información, asignado tareas y responsabilidades que le competen al comité de tecnologías de información como ente colegiado, así como al oficial de seguridad, en la práctica no han sido implementados, ya que el oficial de seguridad no ha sido nombrado y el comité no ha sesionado en años. La implementación de estos roles es la base sobre la cual descansa la estrategia de seguridad, pues son los responsables de

hacer cumplir las políticas y procedimientos así como los demás controles administrativos y técnicos que soportan la seguridad de información.

2.7. En ese sentido, el COBIT 5, en su proceso APO01 señala la necesidad de establecer una estructura organizativa interna que refleje las necesidades del negocio y las prioridades de TI, mediante la implementación de estructuras de gestión requeridas (p. ej., comités) para permitir que la toma de decisiones se lleve a cabo de la forma más eficaz y eficiente posible. A su vez, el APO.02 de ese marco de gestión establece la implementación de prácticas de supervisión adecuadas para garantizar que los roles y las responsabilidades se realicen de forma correcta, para evaluar si todo el personal tiene suficiente autoridad y recursos para llevar a cabo sus roles y responsabilidades y para hacer una revisión general del rendimiento; a su vez, asegurar que la rendición de cuentas queda definida a través de los roles y responsabilidades y estructurar los roles y las responsabilidades para reducir las posibilidades de que un solo rol pueda comprometer un proceso crítico.

2.8. También se encontró que a la fecha el AyA no ha desarrollado e implementado un programa de sensibilización en seguridad de información con alcance institucional, es decir, que cubra la totalidad de sus colaboradores, terceros, y otras partes interesadas, y que atienda a estas diferentes audiencias con material desarrollado específicamente para esos fines. Tampoco se ha desarrollado el seguimiento que se debe brindar al proceso formativo y están ausentes las evaluaciones que prueban el entendimiento de los diferentes temas por parte de la población que participa del programa. Esto, como parte de las primeras etapas para desarrollar un sistema de gestión de la seguridad.

2.9. Esta situación no es acorde con lo señalado en el proceso APO 13 sobre la implementación, monitoreo y gestión de un sistema de gestión de seguridad de la información. Tampoco con lo señalado en la norma ISO 27001, en relación con el soporte de ese sistema, pues establece que las personas que trabajan en la organización deben ser conscientes de la política de la seguridad de la información, su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluyendo los beneficios de una mejora del desempeño en la materia y las implicaciones de no cumplir con los requisitos de ese sistema.

2.10. Por su parte, el código de prácticas ISO 27002 en su apartado 8.2.2 establece que todos los empleados de la organización y, donde sea pertinente, contratistas y usuarios de terceras partes deberían recibir formación adecuada en toma de conciencia y actualizaciones regulares en políticas y procedimientos organizacionales, pertinentes para su función laboral. Además, recalca que la formación continua debería incluir requisitos de seguridad, responsabilidades legales y controles del negocio, así como también formación sobre el uso correcto de recursos de procesamiento de información como por ejemplo procedimiento de autenticación, uso de paquetes de software e información sobre el proceso disciplinario.

2.11. En cuanto a la revisión de contratos con proveedores de servicios de TI que impactan la seguridad de la información, se encontró que de las diez contrataciones con mayor materialidad asignada, ninguna establece cláusulas sobre confidencialidad de la información y garantía de continuidad del servicio en los documentos contractuales. En ese sentido, no hay garantías y penalidades en las contrataciones para dar seguridad de que en caso de ser necesario se pueden presentar los respectivos reclamos al proveedor o la autoridad pertinente. Tampoco existen acuerdos de nivel de servicio, cláusulas de

auditabilidad, procedimientos de salida, ni cláusulas de acceso a información por parte de personal subcontratado. A esto se suma la ausencia de convenios de confidencialidad con terceros, más allá de una cláusula única en las ofertas de servicio, que no indica si la confidencialidad subsiste o no cuando termine la prestación de servicio.

2.12. Se encontró que a la fecha se han implementado algunos controles para verificar que los proveedores cumplen con las especificaciones técnicas de los requerimientos, inclusive, se tienen indicadores y reportes dependiendo del proveedor. Sin embargo, el rol y la responsabilidad de administrar los contratos y de gestionar la relación con el proveedor a nivel de área no ha sido señalada en el AyA al menos para los servicios de TI, la responsabilidad técnica y jurídica no se asume directamente a nivel de TI o a nivel de proveeduría.

2.13. El estado actual de las referidas contrataciones es contraria a lo indicado en las Normas Técnicas para el Gobierno y Control de las TIC (NTGCTI), emitida por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), las cuales indican en relación con la contratación y adquisiciones de bienes y servicios tecnológicos (Apartado VIII), que la Unidad de TI debe disponer y aplicar en forma consistente prácticas para la supervisión y evaluación a través de pruebas de aceptación y valoración del cumplimiento contractual en cuanto al servicio y desempeño en la implementación, configuración y administración de los recursos tecnológicos contratados a terceros.

2.14. Tampoco es acorde a lo que establece el COBIT 5 en su proceso APO10 sobre la gestión con los proveedores, indicando en su práctica 01 que se deberá establecer y mantener criterios relativo al tipo, relevancia y criticidad de los contratos y proveedores, focalizándose en aquellos de mayor importancia, así como establecer y mantener un criterio de evaluación de contratos y proveedores que permita una revisión general del rendimiento de los proveedores de manera consistente. En lo que respecta a las cláusulas, el proceso APO10.03.04 detalla la práctica de incluir en los contratos con los proveedores de servicios clave, disposiciones para revisar los lugares de trabajo y las prácticas y controles de la dirección o de terceras partes.

2.15. Con respecto a la definición de roles y responsabilidades, ese marco de gestión en su proceso APO10 establece la necesidad de incluir y hacer cumplir los derechos y obligaciones de todas las partes en los términos contractuales. Estos pueden incluir la propiedad y el licenciamiento de la propiedad intelectual, el mantenimiento, las garantías, los procesos de arbitraje, las condiciones de actualización y la aptitud para el propósito definido, incluyendo seguridad, depósito de garantía. Respecto a las actividades de control, se establece la asignación de propietarios de las relaciones para cada proveedor y hacerles responsables de la calidad del servicio proporcionado, así como acordar, gestionar, mantener y renovar los contratos con los proveedores. También, asegurar que los contratos son conformes con las normas corporativas y con los requisitos legales y regulatorios y derechos de acceso, además de incluir en los contratos con los proveedores de servicios clave disposiciones para revisar los lugares de trabajo y las prácticas y controles de la dirección o de terceras partes, entre otras.

2.16. A su vez, el estándar ISO 27002 Código de prácticas para la gestión de la seguridad de la información, en su aparte 15.1 sobre seguridad en la relación con los suministradores, plantea a nivel de control que todos los requisitos estatutarios, reguladores, y contractuales pertinentes y el enfoque de la organización para cumplir estos requisitos

deberían ser definidos explícitamente, documentados, y mantenidos al día para cada sistema de información y para la organización, además, que se deberá asegurar la protección y la privacidad de los datos, de acuerdo con la legislación y las regulaciones pertinentes, y si es aplicables, con las cláusulas contractuales.

2.17. Las situaciones evidenciadas sobre la ausencia de un marco de gobierno para la seguridad de la información en el AyA obedecen a un débil direccionamiento y monitoreo del jerarca y titulares subordinados para conciliar la seguridad de la información como parte esencial del giro de negocio, lo que afecta negativamente la estructura organizativa y relaciones de jerarquía que sustentan la seguridad de la información en los sistemas críticos.

2.18. Como consecuencia de ello, se expone a la institución a un riesgo de pérdida de confidencialidad, disponibilidad e integridad de la información que se almacena en sus sistemas de misión crítica. En ese sentido, una de las consecuencias más inmediatas es un mayor riesgo de incidentes de seguridad de la información, como brechas de datos, ataques cibernéticos y fugas de información confidencial, lo que a su vez puede resultar, por ejemplo, en la pérdida o compromiso de datos críticos y daño a la reputación de la organización.

Controles de Ciberseguridad y Continuidad de Negocio

Débiles controles en materia de ciberseguridad y continuidad de negocio

2.19. Se encontró que los sistemas críticos en el AyA presentan vulnerabilidades en materia de componentes externos y configuraciones del sitio web. Además, pese a que el acceso a sistemas está restringido y existe una política de contraseñas, no se gestionan las cuentas de usuario ni se evidencia un cumplimiento de la política, por ejemplo se encuentran más de 40 usuarios sin cambio de contraseña en más de 400 días. Asimismo, no se ha implementado una estrategia para la gestión de continuidad del negocio que asegure la provisión de servicios ante eventos que afecten la disponibilidad de sistemas, tampoco se ha implementado un Análisis de Impacto del Negocio (BIA) ni el Plan para la Contingencia Tecnológica. A su vez, la programación de respaldos no contempla las pruebas que garanticen su efectividad.

2.20. En relación con las vulnerabilidades, la Contraloría General desarrolló una serie de pruebas manuales para inspeccionar componentes externos y configuraciones del sitio web. En virtud de la sensibilidad de los resultados encontrados, se remitió el oficio n.° DFOE-SOS-0434 (11976) el 5 de setiembre de 2023, de carácter confidencial, con el detalle de las vulnerabilidades encontradas, con el propósito de que el AyA valore las situaciones identificadas y defina la procedencia de implementar las medidas y controles de seguridad más adecuados. Con anterioridad, se remitió el oficio n.° DFOE-SOS-0181-2023 (6315)[1], que contenía el detalle de las vulnerabilidades sobre la infraestructura y aplicaciones institucionales del AYA; este oficio fue atendido por el Instituto mediante informe remitido por correo electrónico del 30 de mayo 2023.

2.21. Al respecto, el numeral 12.6 de la norma ISO 27002, sobre gestión de vulnerabilidades técnicas, señala que la gestión de vulnerabilidades técnicas se debería implementar de

[1] En referencia al oficio con insumos DFOE-SOS-OI-00001-2023 del 18 de mayo de 2023

una manera eficaz, sistemática, y repetible con toma de mediciones para confirmar su eficacia, también indica que estas consideraciones deberían incluir los sistemas operativos, y cualquier otra aplicación en uso. En cuanto a los ejercicios de escaneo de vulnerabilidades, estos pueden realizarse de manera automatizada, de manera manual o en una combinación, pueden realizarse internamente o con colaboración de terceros.

2.22. Más específicamente, el numeral 12.6.1 señala que se debería obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso, evaluar la exposición de la organización a tales vulnerabilidades, y tomar medidas apropiadas para gestionar el riesgo asociado.

2.23. Asimismo, la Ley General de Control Interno N.° 8292, en su artículo 12, sobre los deberes del jerarca y de los titulares subordinados en el sistema de control interno, señala el deber de tomar acciones correctivas ante cualquier evidencia de desviaciones o irregularidades. También, el artículo 14 sobre valoración del riesgo, indica que serán deberes del jerarca y los titulares subordinados, analizar el efecto posible de los riesgos identificados, su importancia y la probabilidad de que ocurran, y decidir las acciones que se tomarán para administrarlos.

2.24. Por otra parte, producto de pruebas realizadas en el Administrador de Identidades, el cual es el subsistema que implementa el proveedor de sistemas operativos y de recursos en general para administrar las cuentas de los usuarios que tendrán acceso a recursos de red, sistemas, equipos físicos y otros recursos de TI[2], se determinó que existían un total de 3902 cuentas de usuario entre cuentas de sistema y cuentas de usuario final, de las cuales 3784 se encuentran en estado de “activas”.

2.25. Las cuentas de usuario se dividen en dos categorías, cuentas de sistema y cuentas de usuario final, las primeras son creadas con la finalidad de administrar recursos de otros sistemas y asisten en procesos automatizados, tienen una naturaleza de uso reservado y pueden tener o no altos privilegios. Los usuarios finales o comunes son cuentas que pertenecen a personal que labora para la institución en un rol administrativo desde gerencia general hasta el último nivel operativo. Son cuentas limitadas formalmente en lo que respecta a capacidades y obedecen a las instrucciones de un superior para su definición y alcance.

2.26. Al examinar el detalle de las cuentas de usuario se encontraron un total de 585 cuentas de naturaleza genérica con nombres que no permiten identificar los sistemas, procesos o áreas a las que se les debe relacionar para efectos de rendición de cuentas como por ejemplo: “asesoria técnica”, “Fondo”, “T800”, “info”, “PwC3”.

2.27. En el apartado de cuentas de usuario común se encontraron 168 identidades o cuentas genéricas que no corresponden a personas identificables como “Administracion ABISEAYA”, “Comite Cambio Climatico”, “SILAB Starlims”, las cuales presentan dificultades para la identificación de responsables y de actividades.

2.28. Asimismo, como parte de las pruebas realizadas en el Administrador de Identidades se analizó la frecuencia en el cambio de contraseña y fortaleza, encontrándose que 665 identidades no han cambiado su contraseña en más de 90 días, y además tanto para

[2] Este sistema está centralizado en el área de TI quien es un operador del mismo, el propietario final es el negocio, las gerencias de las diferentes áreas son las que toman decisiones que afectan el estado del Administrador de Identidades.

cuentas de sistema como para usuarios finales se encontraron casos en los que la contraseña no ha cambiado en cientos o miles de días. Además, se encontraron cuentas de sistema cuya contraseña no expira y pruebas adicionales de naturaleza automatizada revelaron que existen contraseñas débiles o fáciles de adivinar. También se identificaron 99 cuentas que no han ingresado a un sistema o a un servidor de autenticación en más de 60 días y usuarios comunes que no han ingresado a un sistema en más de 400 días sin haber sido suspendidos.

2.29. En relación con estas pruebas, el COBIT 5 en el proceso DSS05 sobre gestión de servicios de seguridad establece en la práctica DSS05.04 Gestionar la identidad del usuario y el acceso lógico, que se debe asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio. Para eso, señala dicho marco que se debería mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio, alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer, además de realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.

2.30. Asimismo, cruzando información de las cuentas del Administrador de Identidades con información proporcionada por el departamento de recursos humanos del AyA sobre el detalle del personal que ha dejado la institución en los últimos 2 años y que en definitiva ya no guardan relación laboral con la institución, se encontró un total de 66 cuentas de usuario en estado activo, las cuales podrían tener o no acceso a otros sistemas y recursos de Tecnologías de Información.

2.31. Esto es contrario con lo señalado en el apartado 4.4.1 de las Normas de control interno para el sector público (N-2-2009-CO-DFOE), relativo a la documentación y registro de la gestión institucional, el cual establece que el jerarca y los titulares subordinados, según sus competencias, deben establecer las medidas pertinentes para que los actos de la gestión institucional, sus resultados y otros eventos relevantes, se registren y documenten en el lapso adecuado y conveniente, y se garanticen razonablemente la confidencialidad y el acceso a la información pública, según corresponda.

2.32. Asimismo, no es acorde con lo señalado en el apartado 5.4 de ese cuerpo normativo, el cual señala que el jerarca y los titulares subordinados, según sus competencias, deben asegurar razonablemente que los sistemas de información propicien una debida gestión documental institucional, mediante la que se ejerza control, se almacene y se recupere la información en la organización, de manera oportuna y eficiente, y de conformidad con las necesidades institucionales.

2.33. También es contrario a lo establecido en el proceso DSS05 del COBIT 5, sobre gestión de servicios de seguridad, el cual indica en su actividad DSS05.04.04 que se deben administrar todos los cambios de derechos de acceso como creación, modificación y eliminación, para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.

2.34. También, el código de prácticas ISO 27002 en su apartado 8.3 sobre la finalización de la relación laboral establece que se debe asegurar que los empleados, contratistas o usuarios de terceras partes se desvinculen de una organización o cambien su relación laboral de una forma ordenada, y que además deberían existir responsabilidades para asegurar que la desvinculación de la organización por parte de un empleado, contratista o usuarios de terceras partes sea gestionada, y que sea completada la devolución de todo equipo y la remoción de todos los derechos de acceso. Más específicamente, el apartado 8.3.3 señala que los derechos de acceso de todo empleado, contratista o usuario de terceras partes a información e instalaciones de procesamiento de información deberían ser removidos como consecuencia de la desvinculación de su empleo, contrato o acuerdo, o ajustado cuando cambia.

2.35. En relación con el proceso de gestión de identidades, se determinó al menos un usuario en el Administrador de Identidades que no es conocido por el departamento de Recursos Humanos, tampoco se tiene certeza de las responsabilidades de las partes en la modificación y baja de colaboradores en ese directorio y en los demás sistemas de misión crítica y no se conoce la práctica de suspender usuarios que se ausentan por periodos prolongados, por ejemplo por vacaciones, incapacidades, licencias sin goce. Tampoco se implementan controles para supervisar las actividades que realizan los usuarios tanto finales como con altos privilegios.

2.36. Esto no es acorde con lo establecido en el proceso DSS05 del COBIT 5 sobre la gestión de identidad de usuario y acceso lógico, el cual plantea identificar unívocamente todas las actividades de proceso de la información por roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles están definidos consistentemente, incluyendo roles definidos por el propio negocio en las aplicaciones de procesos de negocio.

2.37. En lo que respecta a supervisión de usuarios, la práctica DSS05.04 en su actividad 7 indica que se debería asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) son identificables unívocamente, además de mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible.

2.38. Por otra parte, en relación con la gestión y continuidad de negocio, se logró evidenciar que el AyA no cuenta con un Plan de Continuidad del Negocio que asegure la provisión de servicios ante eventos que afecten la disponibilidad de sistemas, que cuente con el visto bueno de los gerentes de línea y los líderes de los procesos que integran las actividades críticas del AyA. Si bien, se cuenta con un Análisis de Impacto de Negocio, éste no se ha actualizado desde su emisión en el 2012.

2.39. Tampoco cuenta con un Plan para la Contingencia Tecnológica aprobado y divulgado, por lo que no existe una definición de lo que harán los equipos de negocio en caso de entrar en contingencia. Como parte de la revisión de documentación durante la etapa de examen de la auditoría, se tuvo conocimiento de la existencia de un “Plan de Aseguramiento de Procesos y Contingencia Informática” actualizado al año 2020, pero sin aprobación formal y divulgación en la institución.

2.40. Actualmente, en el AyA estas actividades se encuentran contempladas en el “Plan de acción implementación normas técnicas para la gestión y el control de las tecnologías de información” el cual tiene como objetivo establecer las acciones que son necesarias para lograr el cumplimiento de las Normas Técnicas del MICITT, y tiene plazos de ejecución que se extienden hasta diciembre del 2023; sin embargo, al momento de la verificación, no se contaba con ninguno de estos documentos.

2.41. El artículo 10 de la LGCI, Ley n.° 8292, establece que será responsabilidad del jerarca y del titular subordinado establecer, mantener, perfeccionar y evaluar el sistema de control interno institucional. Asimismo, las Normas de control interno para el Sector Público (N-2-2009-CO-DFOE) en su apartado 5.9 establece que el jerarca y los titulares subordinados, según sus competencias, deben propiciar el aprovechamiento de tecnologías de información que apoyen la gestión institucional mediante el manejo apropiado de la información y la implementación de soluciones ágiles y de amplio alcance; en esa misma línea, indica que el jerarca deberá aprobar el marco de gestión de tecnologías de información y establecer un proceso de implementación gradual de cada uno de sus componentes.

2.42. El hallazgo de referencia se contrapone a la Política de Seguridad de la Información del AyA, la cual establece en su política 8 que la administración de la continuidad de las operaciones es un proceso crítico que debe involucrar a todos los niveles del AyA. Además que el desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las operaciones del AyA puedan restablecerse dentro de los plazos requeridos. Aunado a lo anterior, se indica que dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y gestión. La política 8.1 hace referencia a lo que debe contemplar un plan de continuidad de las actividades del AyA así como la elaboración e implementación, ensayo y mantenimiento de dicho plan.

2.43. También es contrario a lo que establece el proceso DSS04 del COBIT sobre la gestión de la continuidad, cuya primera práctica es definir la política y alcance de continuidad de negocio alineada con los objetivos de negocio y de las partes interesadas, para luego desarrollar y mantener la estrategia de continuidad. Adicionalmente, la práctica de gestión 03 establece que se debe desarrollar un plan de continuidad de negocio basado en la estrategia que documente los procedimientos y la información lista para el uso en un incidente para facilitar que la empresa continúe con sus actividades críticas.

2.44. La práctica 04 de ese mismo proceso señala que se deberían probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera. Esto incluye definir los objetivos para ejercitar y probar los sistemas del plan (de negocio, técnicos, logísticos, administrativos, procedimentales y operacionales) para verificar la completitud del plan de continuidad de negocio, para enfrentarse a los riesgos de negocio, así como definir y acordar ejercicios que sean razonables con las partes interesadas, validar los procedimientos de continuidad, e incluir roles y responsabilidades y acuerdos de retención de datos que ocasionen la mínima disrupción en los procesos de negocio.

2.45. Adicionalmente, el apartado XIII de las Normas técnicas para la gestión y el control de las tecnologías de información emitidas por el MICITT, señalan que la institución debe

establecer prácticas formales para valorar la resiliencia institucional, disponer de una estrategia viable para mantener la continuidad de las operaciones y la recuperación ante un desastre o incidente, que establezca los roles y responsabilidades adecuadas para responder a situaciones adversas.

2.46. En relación con la administración de respaldos de información, se encontró una débil gestión por parte del AyA, referida a la gestión de copias de seguridad de los datos contenidos en sistemas, bases de datos, equipos configurables, como uno de los componentes más importantes de la continuidad de negocio[3].

2.47. Al respecto, se encontró que como no se ha actualizado en el plan de continuidad de negocio los cálculos relacionados con continuidad de negocio, la programación de respaldos no está necesariamente alineada con las expectativas del negocio, respondiendo al criterio de los equipos de ingeniería que lo realizan. Se encuentran respaldos implementados para bases de datos de sistemas críticos, sin embargo, la responsabilidad de respaldar la información de usuario final ha sido trasladada al usuario. Si bien se entiende que esto es viable, no se garantiza que el usuario disponga de los medios físicos y lógicos y del conocimiento necesario para realizar esos respaldos. Además en ningún caso, tratándose de bases de datos o de información de usuario final se realizan pruebas a los respaldos para garantizar razonablemente su utilizabilidad.

2.48. Al respecto, la Política de Seguridad de la Información del AyA, en su política 9.1 hace referencia a la protección de los respaldos y software, indicando que los respaldos y software críticos del AyA se protegerán contra pérdida, destrucción y falsificación.

2.49. A su vez, la norma ISO 27002 establece en su apartado 10.5 sobre respaldos, que se deberían establecer procedimientos de rutina para implementar una política y estrategia acordada de respaldo (…) haciendo copias de respaldo de datos y ensayando su oportuna restauración. Además, señala que se debería producir procedimientos documentados de restauración y registros exactos y completos de las copias de respaldo, y en el inciso f) de la guía de implementación se establece que los medios de respaldo se deberían probar regularmente para asegurarse que pueden ser confiables para el uso cuando sean necesarios.

2.50. Se determinaron debilidades en la implementación de controles preventivos, detectivos y correctivos en materia de seguridad de la información en el AyA. Si bien la ciberseguridad trata sobre un conjunto de controles técnicos muy amplio, existen controles de naturaleza preventiva, detectiva y correctiva que facultan la protección de la información en sus diferentes estados y facilitan la rendición de cuentas y el ejercicio de la auditoría y la investigación cuando suceden eventos adversos. Estos controles si bien pueden clasificarse en términos de criticidad van a depender para efectos de implementación de la estrategia de negocio y su impacto en la estrategia de seguridad.

[3] Esta tarea depende de una serie de indicadores que se plantean como parte de la continuidad de negocio entre ellos el RPO y el RTO. Estos valores afectan la forma como se estructura la estrategia de respaldo y recuperación de datos, entre más bajos esos valores más frecuente será el respaldo de información. El RPO (Objetivo de punto de recuperación) es un indicador que establece el umbral de pérdida de datos en función del tiempo, es decir cuántos datos puede la institución perder en caso de presentarse un evento disruptivo y es clave para la definición de la estrategia de respaldos. Por su parte el RTO (Objetivo de tiempo de recuperación) marca el umbral de tiempo en el cual un sistema debería recuperarse ante la ocurrencia de un evento disruptivo, por ejemplo 30 minutos o 60 minutos o 4 horas después de la ocurrencia del evento. Este indicador afecta el plan de recuperación en caso de desastre.

2.51. Al respecto, se determinó que el AyA no ha implementado controles automatizados y herramientas para cifrar datos en reposo, es decir, una protección que hace que los datos en reposo no sean legibles a menos que se cuente con una llave o código de acceso que le permite al usuario autorizado descifrar la información. Esto se aplica a nivel de bases de datos y de equipo de usuario final.

2.52. Por otro lado, carece de fortalecimiento o "hardening" de servidores, las cuales son un conjunto técnicas y tareas que se desarrollan para asegurar que los equipos son configurados en atención a las reglas de negocio y a lo establecido en las políticas, esto evita que los equipos que se adquieren de terceros conserven configuraciones por defecto (configuraciones conocidas por el proveedor). Ejemplo de estas configuraciones se encuentran en usuarios genéricos como "admin" o contraseñas como "1234" que suelen ser instaladas en equipos nuevos y que deben ser modificadas.

2.53. Tampoco se ha implementado la práctica en el AyA de establecer un control relacionado con la rendición de cuentas, como es el uso y revisión periódica de bitácoras transaccionales, esto es particularmente importante cuando se cuenta con usuarios con altos privilegios. Las bitácoras permiten conservar un registro de base de datos de todas y cada una de las actividades llevadas a cabo por un usuario o conjunto de usuarios y se debe combinar con una supervisión de las actividades operativas que realizan los colaboradores, en particular los de TI.

2.54. Al respecto, el artículo 13 de la Ley General de Control Interno, Ley n.° 8292, establece entre otros que el jerarca es responsable de mantener un ambiente de control adecuado considerando desarrollar y mantener una filosofía y un estilo de gestión que permitan administrar un nivel de riesgo determinado, orientados al logro de resultados y a la medición del desempeño, y que promuevan una actitud abierta hacia mecanismos y procesos que mejoren el sistema de control interno.

2.55. El marco de gestión del COBIT 5, en su proceso DSS05 sobre gestión de servicios de seguridad, establece como parte de las prácticas el cifrar la información en tránsito de acuerdo con su clasificación, así como cifrar la información almacenada de acuerdo a su clasificación. A su vez, el código de prácticas ISO 27002 indica en el apartado 10.5.1 sobre respaldos, en su inciso h) que ante situaciones donde la confidencialidad es de importancia, los respaldos deberían ser protegidos por medio del cifrado, mientras en el apartado 10.9.2 sobre transacciones en línea, el inciso c) plantea el canal de comunicación entre todas las partes implicadas es cifrado.

2.56. En lo que respecta al fortalecimiento de servidores, el código de prácticas ISO 27002 en su aparte 11.4.4 establece que el acceso lógico y físico a los puertos de configuración y de diagnóstico debería de estar controlado. Asimismo, en el numeral 10.10.6 se establece que la configuración correcta de relojes de los equipos de cómputo es importante para asegurar la exactitud de las bitácoras de auditoría, que pueden requerirse para investigaciones o como pruebas en casos legales o disciplinarios. Por su parte COBIT 5 en su práctica DSS05.03 indica que se debe asegurar que los puestos de usuario final (es decir, portátil, equipo sobremesa, servidor y otros dispositivos y software móviles y de red) están asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida.}

2.57. Las bitácoras son necesarias para garantizar la rendición de cuentas, por ello el código de prácticas ISO 27002 en su aparte 10.10.1 sobre bitácoras de auditoría indica que se deberían elaborar bitácoras de auditoría que registren las actividades de los usuarios, excepciones y eventos de seguridad de la información, y se deben mantener durante un período acordado para ayudar a futuras investigaciones y en la supervisión del control de acceso. Estas bitácoras deberían incluir, entre otras, la identificación (ID) de usuario, fechas, horas, y los detalles de acontecimientos claves, por ejemplo inicio y fin de una sesión, la identidad de la terminal y ubicación, así como los registros de los intentos aceptados y rechazados de acceso al sistema.

2.58. Las debilidades expuestas obedecen a la ausencia de un procedimiento con roles y responsables para identificar vulnerabilidades conocidas en los sistemas críticos. Asimismo, a la falta de seguimiento del jerarca y titulares subordinados, de la implementación de las políticas y controles de seguridad de la información, los cuales deben velar por el cumplimiento de los objetivos de negocio soportados por TI, y orientar a los equipos en la implementación de controles para garantizar que se satisfacen las necesidades de las diferentes partes interesadas; así como la ausencia de acciones para la gestión de la continuidad del negocio.

2.59. Las deficiencias en materia de seguridad lógica pueden tener un impacto sobre la confidencialidad y la disponibilidad de la información y los sistemas; suelen asociarse con la posibilidad de dejar abiertos portillos que pueden ser explotados por un atacante. Por ejemplo, el uso de usuarios genéricos no controlados podría facilitar la escalación de privilegios en la red o el acceso no autorizado si se combina con otras vulnerabilidades en el entorno web. A su vez, las debilidades en la gestión de identidades exponen a la organización a una pérdida de confidencialidad e integridad de información, cada cuenta de usuario mal gestionada es una puerta de entrada para ciber atacantes y por ende un riesgo latente para la institución.

2.60. También, contar con identidades activas en el Administrador de Identidades o en cualquier sistema de misión crítica sin que sea necesario que esa identidad exista y por ende sin tener control directo sobre esa cuenta, expone a la organización a un riesgo de pérdida de confidencialidad y de integridad y posiblemente además de disponibilidad de la información.

2.61. Además, la ausencia de planes de continuidad de negocio tiene un impacto directo sobre la disponibilidad de los sistemas de misión crítica. Cuando no se determinan los umbrales de recuperación adecuadamente, se expone la infraestructura a pérdidas de datos. Como resultado de esto, se puede generar un impacto adverso a la infraestructura de tecnologías de información existente de manera que se comprometa la confidencialidad, integridad y disponibilidad de los activos de información, exponiéndose a pérdida, destrucción o falsificación, así como en la capacidad operativa de la institución.

Operación, gestión y mantenimiento de sistemas

Oportunidades de mejora en controles de aplicación y de gestión de operaciones de TI

2.62. Pese a que el AyA cuenta con controles de autenticación de usuarios y de entrada de datos para los sistemas críticos, estos son monofactor (sin doble autenticación o superior). Además, las aplicaciones web no cuentan con controles para prevenir ataques de denegación de servicio. Tampoco se cuenta con políticas ni procedimientos implementados para normar los procesos de TI que inciden en la seguridad de información como: gestión de cambios, atención de incidentes y problemas, gestión de configuraciones, gestión de versiones, gestión de servicios de TI, mantenimiento preventivo y correctivo, clasificación de información, destrucción segura de medios de almacenamiento e información y uso de dispositivos móviles.

2.63. Se realizaron pruebas de autenticación y controles de ingreso a 3 de los sistemas críticos del AyA a saber: en el sistema financiero y estratégico, en el sistema de gestión de recursos humanos y en el sistema comercial integrado; donde se gestionan los consumos y servicios de Agua, sistema estratégico de alta prioridad para verificar las medidas y configuraciones de seguridad que tienen estos sistemas.

2.64. Se determinó que pese a que el AyA cuenta con controles de autenticación de usuarios y de entrada de datos para los sistemas críticos evaluados, dichos controles presentan algunas debilidades como el hecho de que el modelo de autenticación es de un solo factor, usuario y contraseña, es decir, sin doble autenticación o superior. Asimismo, se permite el uso de caracteres o números consecutivos, lo que se clasifica como de baja complejidad; y se permite el uso de palabras reservadas[4] en las contraseñas.

2.65. Por su parte, los parámetros de longitud mínima de contraseña son insuficientes, es decir, de únicamente 8 caracteres; el control de suspensión por inactividad del sistema no es efectivo ya que se observaron casos en los que el bloqueo por inactividad del usuario se daba en lapsos muy extensos de hasta de 40 minutos; y además, se permite el uso de sesiones concurrentes, es decir, una misma sesión en funcionamiento, con un mismo usuario en diferentes ordenadores. Asimismo, las aplicaciones web no cuentan con controles para prevenir ataques de denegación de servicio.

2.66. Se realizaron pruebas de automatizadas en la intranet de verificación de contraseñas, encontrándose que existen contraseñas inseguras (113), contraseñas que no son únicas, es decir, que pueden estar repetidas en la red (413), también se identificaron cuentas cuya contraseña no expira (624) y cuentas que no requieren el uso de contraseña (5). Estas debilidades, aunado al hecho de contar una gestión deficitaria del Administrador de Identidades supone un riesgo adicional.

2.67. Al respecto, la Política de Seguridad de la Información del AyA, en su política 6 sobre control de accesos, en relación con la administración de contraseñas de usuario indica que

[4] Una palabra reservada es aquella que es reconocida como una instrucción o comando específico en el lenguaje de programación.

las contraseñas deben de tener 10 caracteres, además, que se debe suspender o bloquear permanentemente al usuario luego de 3 intentos de entrar con una contraseña incorrecta, asimismo, que se debe solicitar el cambio de la contraseña cada 90 días, se debe impedir que las últimas 12 contraseñas sean reutilizadas, y se debe establecer un tiempo de gracia mínimo de 3 días para las contraseñas vencidas.

2.68. Sobre el particular, conviene indicar que la Norma ISO 27001:2014 indica en su aparte A.9.4 sobre el control de acceso a sistemas y aplicaciones, para prevenir el acceso no autorizado a los sistemas y aplicaciones específicamente en el control, que se deberá restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.

2.69. Asimismo, la Norma ISO 27002 en su apartado 11 sobre el control de acceso, hace referencia a que se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos de acceso del negocio y de seguridad, y que debe considerar entre otros aspectos, la consistencia entre los controles de acceso, la gestión de derechos de acceso en un ambiente distribuido y de redes, la separación de roles de control de acceso, los requisitos para autorizaciones formales de pedidos de acceso y para revisión periódica de controles de acceso así como la revocación de derechos de acceso.

2.70. Por otra parte, se determinó que si bien el AyA cuenta con un catálogo de servicios tecnológicos actualizado al mes de agosto de 2021, no existen políticas ni procedimientos relacionados con la gestión de cambios en los sistemas, gestión de configuraciones, gestión de versiones, gestión de incidentes y problemas, así como para el mantenimiento preventivo y correctivo, los cuales si son sistemas institucionales implementados por TI se realizan a solicitud de cada unidad. En la Política de Seguridad del AyA se hace mención a algunos de estos procedimientos pero de manera muy general, por lo que no puede considerarse que en ese documento se aborden de manera específica y detallada, con una secuencia lógica procedimental ni con roles y responsabilidades asignadas para una gestión ordenada.

2.71. Asimismo, se encontró que el AyA tampoco cuenta con políticas y procedimientos para clasificación de información, destrucción segura de medios de almacenamiento e información y uso de dispositivos móviles.

2.72. Al respecto, el artículo 15 de la Ley General de Control Interno, ley 8292, indica el deber de divulgar las políticas, normas y procedimientos que definan, entre otros aspectos,la protección y conservación de activos, así como los controles generales comunes a todos los sistemas de información.

2.73. Conviene destacar, que en cuanto al proceso de gestión de cambios, el proceso BAI06 de base de datos COBIT 5, establece la necesidad de gestionar todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura.

2.74. Por su parte, en el proceso BAI09 de ese mismo marco de gestión se indica que se debe mantener la resiliencia de los activos críticos mediante la aplicación de un mantenimiento preventivo regular, de supervisión del rendimiento y, si fuera necesario, proporcionando alternativas o activos adicionales para reducir la probabilidad de fallo. Adicionalmente, refiere al establecimiento de un plan de mantenimiento preventivo para todo el hardware,

considerando un análisis costo-beneficio, recomendaciones del proveedor, el riesgo de interrupción del servicio, personal cualificado y otros factores relevantes.

2.75. En cuanto a la gestión de configuraciones, el proceso BAI010 de COBIT 5 establece la importancia de definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarios para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información asociada con la configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración.

2.76. Asimismo, en relación con la Gestión de incidentes y problemas COBIT 5 en el proceso DSS02, se define la necesidad de proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes; lo cual implica recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.

2.77. Las situaciones descritas obedecen a que el AyA no ha gestionado oportunamente las actualizaciones en los sistemas, en ese sentido, los sistemas con que cuenta el AyA tienen un prolongado tiempo en operación y los proveedores de dichos sistemas ya no pueden brindar el mantenimiento necesario para proceder con las actualizaciones que corresponden. Además, la organización no cuenta con un ambiente de control orientado al cumplimiento de buenas prácticas para normar operaciones y sistemas que pueden afectar la seguridad de la información.

2.78. La consecuencia de contar con sistemas obsoletos y sin respaldo de proveedores externos, conlleva el riesgo de exponer a la institución a una pérdida de disponibilidad de sistemas de misión crítica, así como riesgos de pérdida de confidencialidad e integridad de información. Lo anterior, expone a la institución a un riesgo de afectación por ocurrencia de incidencias, o a un impacto adverso a la infraestructura de tecnologías de información existente y con ello se comprometa la confidencialidad, integridad y disponibilidad de los activos de información. Estos procesos coadyuvan al funcionamiento eficiente de la infraestructura tecnológica de manera que esta sea más robusta y confiable y contribuyen a mejorar la satisfacción de los usuarios, minimizando riesgos y evitando interrupciones no planificadas.

3. CONCLUSIÓN

3.1. Se determinó que el AyA presenta un muy bajo cumplimiento del marco normativo y buenas prácticas aplicables en materia de seguridad de la información de los sistemas críticos. Al respecto, el AyA cuenta con una política de seguridad de la información, implementación de respaldos de la información y medidas de seguridad física y ambiental para su resguardo, además, salvo un tipo de vulnerabilidad, atendió oportunamente las vulnerabilidades comunicadas mediante oficio con insumos n.° 6315 (DFOE-SOS-0181) del 18 de mayo de 2023.

3.2. No obstante, en cuanto a la protección de sus sistemas críticos no cumple razonablemente con lo establecido en la normativa y las buenas prácticas relativas a gobierno y gestión de seguridad de información. Asimismo, los procesos de gobierno y gestión que se vinculan a sistemas críticos no cumplen razonablemente con los principios

de confidencialidad, disponibilidad e integridad de información. Además, existen vulnerabilidades conocidas en componentes externos y configuraciones de direcciones web de la institución que ponen en riesgo la infraestructura de TI y por ende la disponibilidad de los servicios soportados por TI.

4. DISPOSICIONES

4.1. De conformidad con las competencias asignadas en los artículos 183 y 184 de la Constitución Política, los artículos 12 y 21 de la Ley Orgánica de la Contraloría General de la República, Nro. 7428, y el artículo 12 inciso c) de la Ley General de Control Interno, se emiten las siguientes disposiciones, las cuales son de acatamiento obligatorio y deberán ser cumplidas dentro del plazo (o en el término) conferido para ello, por lo que su incumplimiento no justificado constituye causal de responsabilidad.

4.2. Para la atención de las disposiciones incorporadas en este informe deberán observarse los "Lineamientos generales para el cumplimiento de las disposiciones y recomendaciones emitidas por la Contraloría General de la República en sus informes de auditoría", emitidos mediante resolución Nro. R-DC-144-2015, publicados en La Gaceta Nro. 242 del 14 de diciembre del 2015, los cuales entraron en vigencia desde el 4 de enero de 2016

4.3. Este Órgano Contralor se reserva la posibilidad de verificar, por los medios que considere pertinentes, la efectiva implementación de las disposiciones emitidas, así como de valorar el establecimiento de las responsabilidades que correspondan, en caso de incumplimiento injustificado de tales disposiciones.

A ALEJANDRO GUILLÉN GUARDIA, PRESIDENTE EJECUTIVO DEL AYA Y MIEMBRO DEL COMITÉ DE TI O A QUIEN EN SU LUGAR OCUPE EL CARGO.

4.4. Elaborar, divulgar e implementar una política para la gestión de la continuidad del negocio, que contenga al menos: i) el análisis de impacto de negocio, ii) el plan de continuidad de negocio, iii) plan de contingencia tecnológica; para cada componente deben incluirse indicadores de continuidad. Remitir a la Contraloría General una certificación sobre la elaboración y divulgación de la mencionada política a más tardar el 29 de marzo de 2024, además, un primer informe de avance de su implementación a más tardar el 30 de setiembre de 2024 y un segundo informe de avance a más tardar el 30 de abril de 2025. (ver párrafos del 2.19 al 2.61).

A ALEJANDRO GUILLÉN GUARDIA EN SU CALIDAD DE PRESIDENTE EJECUTIVO DEL AYA O A QUIEN EN SU LUGAR OCUPE EL CARGO.

4.5. Elaborar, oficializar, divulgar e implementar un Sistema de Gestión de la Seguridad de la Información (SGSI), que incluya al menos: i) la valoración de brechas en seguridad de la información; ii) el alcance, los objetivos y los límites del SGSI; iii) definición e implementación de roles y responsabilidades para al menos el Comité de TI, Comité de Seguridad, Oficial de Seguridad, Gestores de seguridad; iv) actividades de sensibilización en seguridad de información; v) las medidas de atención de los vacíos contractuales

sobre confidencialidad de la información y garantía de continuidad del servicio para contrataciones de servicios de tecnologías de información que impactan la seguridad de la información. Remitir a la Contraloría General una certificación sobre la elaboración, oficialización y divulgación del SGSI a más tardar el 29 de marzo de 2024, además, un primer informe de avance de su implementación a más tardar el 30 de setiembre de 2024 y un segundo informe de avance a más tardar el 28 de marzo de 2025. (ver párrafos del 2.2 al 2.18).

4.6. Elaborar, divulgar e implementar un plan de atención, con las medidas integrales y paliativas, para solventar la obsolescencia tecnológica de aplicaciones y bases de datos que inciden en las operaciones de misión crítica del AyA, el cual debe contener al menos: actividades, fechas, responsables y recursos asignados. Remitir a la Contraloría General una certificación sobre la elaboración y divulgación del plan para solventar la obsolescencia tecnológica a más tardar el 28 de febrero de 2024, además un primer informe de avance con respecto a la implementación de medidas a más tardar el 30 de agosto de 2024 y un segundo informe de avance a más tardar el 28 de febrero 2025. (ver párrafos del 2.62 al 2.78).

A MARIA ALEJANDRA MORA SEGURA EN SU CALIDAD DE GERENTE GENERAL DEL AYA O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.7. Elaborar, divulgar e implementar un procedimiento para identificación y atención de las vulnerabilidades conocidas, que contenga al menos: identificación periódica, priorización y estrategia de atención, con sus respectivos roles y responsables. Remitir a la Contraloría General una certificación sobre la elaboración y divulgación del mencionado procedimiento a más tardar el 15 de diciembre de 2023, además, un primer informe de avance de su implementación a más tardar el 28 de junio de 2024 y un segundo informe de avance a más tardar el 16 de diciembre de 2024. (ver párrafos del 2.19 al 2.61).

4.8. Elaborar e implementar un plan de remediación de las vulnerabilidades encontradas en los sistemas críticos, comunicados complementariamente mediante oficio DFOE-SOS-0434(11976) que incluya al menos las acciones requeridas, los responsables y plazos de ejecución para solventar las vulnerabilidades. Remitir a la Contraloría General una certificación sobre la elaboración del plan de remediación de vulnerabilidades incluyendo acciones, responsables y plazos de ejecución a más tardar el 15 de diciembre de 2023, además, un primer informe de avance de su implementación a más tardar el 15 de marzo de 2024.(ver párrafos del 2.19 al 2.61).

4.9. Actualizar e implementar el proceso de gestión de identidades, para que contenga al menos la conciliación periódica de las cuentas del Administrador de Identidades y de los sistemas críticos, análisis de las cuentas, su estado y configuración, además de la coordinación con las diferentes unidades internas. Remitir a la Contraloría General un avance sobre la conciliación de cuentas del Administrador de Identidades a más tardar el 15 de enero de 2024, además, una certificación que haga constar que se actualizó e implementó el proceso de gestión de identidades a más tardar el 15 de marzo de 2024. (ver párrafos del 2.19 al 2.61).

4.10. Elaborar, divulgar e implementar los mecanismos de control de ciberseguridad para atender las debilidades señaladas en materia de: a) cifrado de datos, b) bloqueo de sesión por inactividad, c) concurrencia de sesiones en los sistemas críticos, d) configuración de contraseñas, e) modelos de autenticación, f) controles de entrada en aplicaciones, g) bitácoras transaccionales, h) supervisión de usuarios privilegiados / usuarios finales, que se basen en un análisis preliminar de factibilidad de implementación. Remitir a la Contraloría General una certificación sobre la elaboración y divulgación de los mecanismos de control a más tardar el 15 de abril de 2024, además, un primer informe de avance de la implementación de los controles a más tardar el 15 de octubre de 2024 y un segundo informe de avance de la implementación a más tardar el 28 de febrero de 2025. (ver párrafos del 2.19 al 2.61).

4.11. Elaborar, divulgar e implementar las políticas y los procedimientos en materia de seguridad de la información, con los respectivos roles y responsables, que contemplen los procesos de: i) la gestión de cambios, ii) gestión de incidentes y problemas, iii) gestión de configuración, iv) gestión de versiones, v) gestión de servicios de TI, vi) mantenimiento preventivo y correctivo, vii) clasificación de información, viii) destrucción segura de medios de almacenamientos e información y ix) uso de dispositivos móviles. Remitir a la Contraloría General una certificación sobre la elaboración y divulgación de las políticas y procedimiento, a más tardar el 15 de marzo de 2024, además, un primer informe de avance de la implementación a más tardar el 30 de agosto de 2024 y un segundo informe de avance a más tardar el 16 de diciembre de 2024. (ver párrafos del 2.62 al 2.78).

Licda. Lía Barrantes León
Gerente de Área a.i

Lic. Erick Alvarado Muñoz
Asistente Técnico

MATI. Alejandro Zúñiga Gómez
Coordinador

MSc. Vanessa Pacheco Acuña
Colaboradora

MAFF. Jennifer Priscilla Villarreal Sequeira
Colaboradora

CGR Firmado digitalmente
Valide las firmas digitales

CRV/pmt
G: 2022000028-1