CGR
COSTA RICA

SEGURIDAD DE LA INFORMACIÓN EN LA REFINADORA COSTARRICENSE DE PETRÓLEO S.A.

Dirigido a la Refinadora Costarricense de Petróleo S.A.

DFOE-SOS-IAD-00006-2025
05 de setiembre de 2025

Resumen Ejecutivo

¿Qué auditamos?

Los controles establecidos por la Refinadora Costarricense de Petróleo S.A. (RECOPE S.A) para implementar la seguridad de la información, con el fin de determinar si se ajustan al marco regulatorio y buenas prácticas aplicables, a efectos de prevenir afectaciones en la prestación de los servicios. El período de análisis comprendió del 1° de enero de 2023 al 31 de diciembre de 2024.

¿Por qué es importante?

La seguridad de la información se orienta a garantizar la continuidad y la eficacia de los servicios públicos esenciales, pues las instituciones públicas dependen en muchos casos de sus sistemas informáticos para la recopilación, procesamiento, almacenamiento y comunicación de datos críticos. La protección de esta información es clave ante amenazas como el uso fraudulento, accesos no autorizados, pérdida, alteración o difusión indebida.

RECOPE S.A. es una entidad estratégica para satisfacer la demanda de combustibles y para asegurar el abastecimiento energético del país, por lo que eventos adversos en materia de seguridad de la información pueden menoscabar la seguridad nacional, la resiliencia energética y la operatividad de los sectores productivos.

¿Qué concluimos?

Los controles de seguridad de la información implementados por RECOPE S.A. no cumplen en aspectos significativos con los criterios del marco normativo y técnico aplicable, lo que implica una limitada capacidad de respuesta y recuperación ante incidentes, y aumenta la vulnerabilidad de los sistemas críticos a ataques y accesos no autorizados, comprometiendo la integridad, disponibilidad y confidencialidad de la información.

Resultados

1. **Debilidades en el proceso de continuidad de negocio afectan la capacidad de recuperación ante incidentes:** Si bien RECOPE S.A cuenta con un modelo de continuidad del negocio, carece de elementos clave como el tiempo máximo de interrupción aceptable, de los pasos a seguir para la recuperación de los sistemas, y no cuenta con un inventario completo de sistemas.

2. **Falta de controles de operación y mantenimiento de los sistemas que inciden la seguridad de la información:** Carece de controles de múltiple factor de autenticación, tiene contraseñas débiles y sin caducidad, y deficiencias en el mantenimiento y la gestión de proveedores.

3. **Debilidades en los controles de Ciberseguridad:** no hay controles para gestionar de forma activa, periódica y permanente las vulnerabilidades de infraestructura tecnológica, además de múltiples cuentas genéricas y cuentas activas de usuarios dados de baja o no conocidos por RECOPE S.A.

Auditoría en datos

8 Meses	0	2 años	270
Desde el incidente de seguridad, sin embargo RECOPE aún no ha reestablecido totalidad de sistemas	Ningún sistema crítico de RECOPE cuenta con múltiple factor de autenticación	Sin dar mantenimiento preventivo a la totalidad a los equipos del Departamento de Automatización y Control Industrial	Total de cuentas genéricas en sistemas y 20 cuentas de personas que Recope no conoce

Contexto

¿Qué es la seguridad de la información?

Es el conjunto de acciones para proteger los activos de información de una organización, buscando asegurar su confidencialidad, integridad y disponibilidad. Busca salvaguardar de manera razonable los datos, aplicaciones, redes y demás recursos tecnológicos frente a cualquier uso fraudulento, acceso no autorizado, pérdida, alteración o destrucción[1].

La seguridad de la información es integral: incluye las estrategias, políticas, procedimientos y controles, integrando la gestión de riesgos para identificar, analizar y mitigar las amenazas y vulnerabilidades. Es una responsabilidad que requiere el apoyo jerárquico, para garantizar la continuidad de los servicios críticos y el logro de los objetivos estratégicos del negocio.

¿Qué sistemas opera RECOPE S.A?

Como parte de las Tecnologías de Información (TI), destacan componentes como servidores, redes, sitios web, equipos de usuario final (computadoras de escritorio y portátiles) y bases de datos en sistemas propios o de terceros.

Por otro lado, se encuentran las Operaciones Tecnológicas (OT), cuyo principal componente es el oleoducto que permite trasladar el combustible de una terminal a otra. Esta red se compone de una gran cantidad de equipos como sensores, válvulas, motores, bombas, medidores de presión, entre otros, que son controlados por los sistemas SCADA[2], que por medio de dispositivos como los PLC[3] controlan el estado y flujo de combustible.

A esto se suman otros sistemas y equipos para la entrega del producto final, como los inyectores, medidores volumétricos, sensores de temperatura, entre otros, para operar adecuadamente y garantizar la seguridad.

Fotografía 1.

Entrega de producto final en plantel Aeropuerto

Fuente: *Fotografía tomada el 15 de mayo de 2025 por el equipo auditor*

¿Cómo se relacionan los ciberataques con la seguridad de la información?

Un ciberataque es una acción maliciosa dirigida contra sistemas, redes, dispositivos o datos, para robar, exponer, alterar, deshabilitar o destruir información, aplicaciones u otros activos mediante el acceso no autorizado a redes, sistemas informáticos o dispositivos digitales. Buscan vulnerar o comprometer la confidencialidad, disponibilidad e integridad de la información, pudiendo resultar en la divulgación no autorizada de datos sensibles, la alteración o destrucción de información, o la interrupción prolongada de sistemas y servicios críticos.

Según reportes de RECOPE S.A., el 27 de noviembre de 2024 la empresa fue víctima de un ataque informático de tipo ransomware, lo que derivó en la desconexión inmediata de sus sistemas informáticos, afectando, entre otros, los sistemas administrativos de ventas, facturación y pagos, y los sistemas de controles administrativos y gestor documental, propiciando que los sistemas de facturación para terminales de distribución y aéreas quedaran fuera de funcionamiento; que durante un mes las ventas de combustibles se realizaran de forma manual; y que RECOPE S.A. incumpliera con la presentación de información financiera ante la SUGEVAL, entre otras afectaciones.

[1] Con base en ISO 27000 y Marco de Ciberseguridad del NIST (Instituto Nacional de Estándares y Tecnología) de Estados Unidos

[2] Supervisory Control and Data Acquisition: Sistema de software y hardware que se utiliza para controlar y supervisar procesos industriales en tiempo real.

[3] Programmable Logic Controller: es una computadora industrial especializada que se utiliza para automatizar procesos electromecánicos en entornos industriales.

Conclusión CGR

Los controles de seguridad de la información implementados por RECOPE S.A. no cumplen en aspectos significativos con los criterios del marco normativo y técnico aplicable. Esta situación compromete la capacidad de la entidad para garantizar la integridad, confidencialidad y disponibilidad de sus sistemas y datos críticos. Si bien existe un modelo de continuidad del negocio y controles de autenticación y entrada de datos, entre otros, los hallazgos identificados apuntan a debilidades sistémicas que exponen a la institución a riesgos que podrían afectar la continuidad de sus operaciones y, en consecuencia, la prestación de servicios esenciales.

Las principales debilidades se concentran en tres áreas clave. En primer lugar, la capacidad de la entidad para responder ante incidentes de seguridad es limitada. Se constató que el análisis de impacto al negocio (BIA), los planes de continuidad del negocio (BCP) y los planes de recuperación de desastres (DRP) carecen de elementos esenciales y no están alineados entre sí. Esta deficiencia quedó evidenciada en el ciberataque de noviembre de 2024, donde la recuperación total de los sistemas aún no se había completado para julio de 2025, lo que se traduce en tiempos de inactividad prolongados que afectan a usuarios internos y externos.

En segundo lugar, se identificaron fallas en los controles de operación y mantenimiento de los sistemas. Se determinó que los sistemas críticos de la entidad carecen de medidas de seguridad fundamentales, como la autenticación de múltiple factor. Además, se permite el uso de contraseñas débiles o que no caducan, contrario a lo que establecen las políticas y buenas prácticas. También se encontró un mantenimiento preventivo deficiente en equipos de operaciones tecnológicas y debilidades en la gestión de contratos con proveedores externos, lo que incrementa las vulnerabilidades de los sistemas y dificulta la trazabilidad y la rendición de cuentas.

Finalmente, existen debilidades en los controles de ciberseguridad. RECOPE S.A. no cuenta con un sistema para gestionar activamente las vulnerabilidades de su infraestructura, y el cifrado de datos es parcial. Se encontraron numerosas cuentas genéricas y de usuarios dados de baja aún activas, lo que constituye un riesgo de acceso no autorizado. Las deficiencias encontradas se originan en la falta de un direccionamiento estratégico claro y en la inobservancia de la normativa interna.

Resultado 1

Debilidades en el proceso de continuidad de negocio afectan la capacidad de recuperación ante incidentes

¿Qué encontramos?

1.1. Se determinó que el análisis de impacto al negocio (BIA) de RECOPE S.A. carece de elementos esenciales como objetivos de punto de recuperación (RPO), objetivos de tiempo de recuperación (RTO), y el tiempo máximo de interrupción que es aceptable (MTD), además no define la relación entre los sistemas y los principales procesos para el giro del negocio, lo cual es un punto de partida en la definición de prioridades en la etapa de recuperación ante un incidente.

1.2. Además, no cuenta con un inventario completo de los sistemas, con su debida definición de propietarios y criticidad, aspecto que resulta relevante para la toma de decisiones sobre los sistemas, los controles que les rodean y principalmente sobre la administración de acceso a esos recursos. Se determinó que si bien la mayoría de procesos institucionales cuentan con un plan de continuidad del negocio, que permita la operación en situaciones de contingencia, no todos presentan esta característica fundamental[4]. Esto es aún más relevante en una institución como RECOPE S.A que tiene dependencias en equipos especializados, como lo son las operaciones tecnológicas en los sistemas de cargaderos de combustible, el sistema de medición de tanques o el sistema de detección de fugas, entre otros.

1.3. A su vez, se encontró que el plan de recuperación en caso de desastre (DRP) no está alineado con el análisis de impacto al negocio (BIA) ni con el plan de continuidad de negocio (BCP)[5]. Este plan (DRP) fue desarrollado por la Dirección de Tecnología como un esfuerzo previo a la existencia del Sistema de Gestión de Continuidad de Negocio (SGCN) y carece de elementos importantes, como por ejemplo los pasos para la recuperación de sistemas particulares, los protocolos para actuar en caso de un desastre natural, y criterios del negocio para el respaldo de la información.

1.4. Finalmente, no existe un sitio de procesamiento alterno para el negocio o para la Dirección de Tecnología que permita asegurar la continuidad de la infraestructura tecnológica en todo momento ante eventos fortuitos, a pesar de la criticidad tanto de la información como de los sistemas que la resguardan. En ese sentido, tampoco se localizó un estudio que analice los riesgos y la factibilidad tanto técnica como financiera de no contar con este sitio.

¿Por qué se presenta este resultado?

1.5. Las situaciones encontradas se deben a una falta de articulación institucional para asumir la continuidad del negocio como una responsabilidad esencial y priorizada en la organización. A su vez, debido a deficiencias en la formulación y seguimiento del Análisis de Impacto al Negocio, planes de continuidad y planes de recuperación para validar que puedan funcionar ante posibles eventos disruptivos.

[4] De los 29 procesos críticos establecidos en el BIA, 2 aún están pendientes y otros 2 fueron desestimados por RECOPE S.A.
[5] No obstante, RECOPE S.A. ha actualizado el DRP recientemente, en un esfuerzo por alinearlo progresivamente con el BIA vigente (oficio N.° P-0473-2025 del 04 de setiembre, 2025 en atención a las observaciones al borrador del informe).

Resultado 1

Debilidades en el proceso de continuidad de negocio afectan la capacidad de recuperación ante incidentes

¿Cómo se espera que funcione según la normativa?

1.6. En el proceso de continuidad del negocio, es importante que las instituciones cuenten con controles de tecnologías de información y operaciones tecnológicas para asegurar la disponibilidad de recursos informáticos y operativos, que identifique cuales son los procesos sustantivos y sistemas de misión crítica y establezca los planes de continuidad y recuperación. Además, debe definir escenarios y estrategias de continuidad, roles y responsabilidades claras, procedimientos operativos y un modelo de pruebas para la continuidad del negocio; así como la estrategia, frecuencia, cobertura y ubicación de los respaldos; todo ello con un enfoque en la mejora continua y en apego a las buenas prácticas y la normativa nacional aplicable.

1.7. En ese sentido, Cobit 5 en su proceso DSS04 Gestionar la Continuidad[6], tiene como objetivo principal asegurar que las operaciones críticas y la información del negocio se mantengan disponibles incluso después de una interrupción significativa. Para lograrlo, establece prácticas como: i) Desarrollar y probar un plan de continuidad, ii) Capacitar a los empleados en dicho plan, y iii) Gestionar acuerdos de respaldo. Dentro de estas prácticas, se incluyen controles más específicos como la identificación de procesos de negocio críticos, la realización de un análisis de impacto en el negocio (BIA) para evaluar los efectos de una interrupción, y la definición de los tiempos mínimos de recuperación.

¿Qué pasa si no se corrige?

1.8. Se limita la capacidad de respuesta y recuperación ante incidentes, que se traduce en tiempos de recuperación excesivos que pueden paralizar la operación de servicios críticos por periodos prolongados y afectar a los usuarios internos y externos. Por ejemplo, ante el incidente de ciberseguridad del 27 de noviembre de 2024, a julio de 2025 aún no se han restablecido la totalidad de los sistemas afectados.

Fotografía 2.

Cargaderos de combustible de RECOPE S.A., plantel La Garita

Fuente: *Fotografía tomada el 30 de julio de 2025 por el equipo auditor en visita a Plantel La Garita*

[6] En concordancia además con el capítulo XIII Continuidad y Disponibilidad Operativa de los Servicios Tecnológicos; de las Normas técnicas para el gobierno y gestión de las tecnologías de la información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt).

Resultado 2

Falta de controles de operación y mantenimiento de los sistemas que inciden en la seguridad de la información

¿Qué encontramos?

2.1. Se determinó que ningún sistema crítico de RECOPE S.A. cuenta con múltiple factor de autenticación de forma nativa, es decir, la función para verificar la identidad de un usuario a través de un segundo método (además de la contraseña) no está incorporada. Además, se encontró que se permiten varias sesiones en simultáneo; y en algunos sistemas no existe suspensión automática por desatención del equipo (solo para el Sistema de Administración de Usuarios).

2.2. A su vez, varios de los sistemas evaluados incumplen con la política de gestión de contraseñas, por ejemplo contraseñas que no caducan o que son débiles. Se encontró además que en los sistemas industriales se comparten las cuentas de usuario entre colaboradores[7]; y al analizar las cuentas de usuario activas que hacen parte del Sistema de Administración de Usuarios, se encontró que 143 usuarios finales activos no han cambiado su contraseña en más de 90 días; para 117 cuentas activas la contraseña no expira; y un total de 272 cuentas de usuario no se han autenticado en el año 2025, de las cuales 111 son cuentas activas[8].

2.3. Por otra parte, se encontró debilidades en el proceso de mantenimiento preventivo a los equipos de Operaciones Tecnológicas (OT), ya que no existe un inventario completo de dichos equipos[9] y el Departamento de Automatización y Control Industrial (DACI) no alcanza a dar mantenimiento preventivo a la totalidad a los equipos que gestiona esta unidad en los últimos 2 años[10]. Además, se determinó que no se realiza mantenimiento predictivo (en oposición a lo que establece el Reglamento de Organización[11]). A eso se suma que no fue posible determinar el estado de las actualizaciones de software en los equipos de usuarios final y equipos servidores de TI que administra la Dirección de Tecnología[12].

2.4. Finalmente, se determinó la ausencia de acuerdos de nivel de servicio suscritos con proveedores externos, así como debilidades en los contratos y convenios[13]; ya que no se cuenta con cláusulas relevantes como auditabilidad, proceso de salida, obligaciones en materia de seguridad y acceso,

---

[7] La administración expresó mediante oficio n.° DT-0355-2025 del 12 de agosto de 2025 las razones por las cuales los sistemas de operaciones tecnológicas (OT) deben exceptuarse del cumplimiento de ciertas directrices principalmente en el tema de gestión de contraseñas, sin embargo esto no se ha documentado como una excepción a la política o en su defecto como una aceptación de riesgo.

[8] Una cuenta de usuario que no muestra actividad en varios meses indica que probablemente esa cuenta no sea necesaria o que deba estar temporalmente suspendida.

[9] Mediante oficio n.° DT-0335-2025 del 30 de julio de 2025 se indicó respecto a los inventarios de operaciones tecnológicas que: *"(...) es necesario indicar* ***que no se cuenta con la totalidad de la información por cuanto el ciberataque ocurrido meses atrás, afectó la disponibilidad de la información que se encontraba en respaldos en las redes afectadas."*** Lo resaltado no corresponde al original.

[10] Análisis de muestra con información suministrada mediante oficio n.° ACI-0175-2025 del 21 de julio de 2025 relacionada con información sobre el proceso de mantenimiento preventivo para equipos de operaciones tecnológicas en RECOPE S.A.

[11] Artículo 34 Unidad de Automatización y Control Industrial, inciso 4, *"Conformar un plan anual empresarial de mantenimiento, ejecutar el* ***mantenimiento predictivo, preventivo y correctivo*** *sobre la plataforma de automatización y control industrial, para mantenerla en las mejores condiciones físicas y ambientales, con la debida documentación, en observación de las recomendaciones de los fabricantes, las regulaciones nacionales e internacionales y las mejores prácticas de la industria."* Lo resaltado no corresponde al original.

[12] Mediante oficio n.° DT-0335-2025 del 30 de julio de 2025, se indicó que esta información no está disponible en su totalidad como consecuencia del ciberataque sufrido en noviembre de 2024.

[13] Mediante oficio n.° DT-0145-2025 del 04 de abril de 2025 se indicó que no se contaba con la información relacionada con Acuerdos de nivel de servicio suscrito con proveedores externos.

respaldos de información, entre otras[14].

¿Por qué se presenta este resultado?

2.5. Debido a una débil política de contraseñas y ausencia de monitoreo y control sobre la gestión de contraseñas por parte de RECOPE S.A.; además, hay inobservancia de normativa interna para la operación y mantenimiento preventivo, así como para los procesos de parcheo y actualización de software; también debido a la ausencia de protocolos y coordinación para la gestión de relaciones contractuales en seguridad de la información.

¿Cómo se espera que funcione según la normativa?

2.6. En el proceso de operación y mantenimiento de los sistemas, es importante que las instituciones cuenten con controles robustos para la operación de sus sistemas críticos, tales como políticas de seguridad, autenticación multifactor, y controles de entrada. Además, debe asegurar que su software y hardware reciban mantenimiento preventivo, se mantengan actualizados y que los sistemas críticos tercerizados cuenten con soporte y supervisión continua, además de cláusulas que busquen garantizar la seguridad de la información.

2.7. RECOPE S.A. en su Manual de Directrices en Materia de Seguridad de la Información PE-10-12-005 establece reglas con respecto a usuarios y contraseñas, por ejemplo como mínimo y obligatorio el cambio de la clave cada 30 días naturales o en el caso de ausencia temporal superior a dos semanas, establece que los accesos a los sistemas de información deberán ser inhabilitados con excepción del correo electrónico empresarial. Asimismo, respecto a acuerdos de nivel de servicio indica que se debe incluir una cláusula en la cual se especifique que el servicio proporcionado por la contraparte está sujeto a revisión por parte de la Dirección de Tecnología.

¿Qué pasa si no se corrige?

2.8. Las situaciones encontradas aumentan las vulnerabilidades de los sistemas críticos y aumentan el riesgo de comprometer la seguridad de la información, dejando a los sistemas más expuestos a ataques pues son puertas abiertas a accesos no autorizados. También se dificulta la trazabilidad operativa y la rendición de cuentas.

[14] Análisis de información sobre acuerdos remitidos en el oficio n.° DT-0145-2025 del 04 de abril de 2025

¿Qué encontramos?

3.1. Se determinó que RECOPE S.A. no ha establecido ni implementado controles para gestionar de forma activa, periódica y permanente las vulnerabilidades de infraestructura tecnológica[15]. Sobre este tema, la Contraloría General remitió el oficio DFOE-SOS-0226 (09912) del 22 de mayo de 2025, con carácter de acceso restringido, comunicando la identificación de un total de 19 posibles vulnerabilidades de ciberseguridad, clasificadas según su severidad (2 críticas, 13 altas y 4 medias), para que RECOPE S.A. implementara acciones correctivas y preventivas oportunas. A la fecha, no se ha remitido información que acredite su corrección ni un plan de remediación.

3.2. Además, se encontró que 5 cuentas de usuario activas en el Sistema de Administrador de Usuarios corresponden a ex colaboradores y 20 cuentas activas corresponden a personas que no son identificadas por el departamento de Capital Humano[16]. En el caso del sistema de control y carga de combustible, se encontró que 3 usuarios activos no son conocidos para el departamento de Capital Humano de RECOPE S.A., lo mismo ocurre con 6 usuarios del sistema de gestión de información de laboratorio (LIMS). Además en el sistema SAP se localizan 3 cuentas activas que corresponden a ex colaboradores, así como 70 usuarios genéricos o de servicio; de los cuales uno tiene privilegios de superusuario. A esto se suma que no se suspenden cuentas de usuario automáticamente en los sistemas de aplicación (SAP, cargaderos, Alfresco, SCADA) por ausencias prolongadas como incapacidad, vacaciones, licencias; en el caso del sistema LIMS esta suspensión se realiza manualmente.

3.3. Por otra parte, si bien existe un Manual de Directrices en Materia de Seguridad de la Información (PE-10-12-005), se determinó que no se ha implementado cifrado de datos en equipos de usuario final y en el caso de bases de datos se cifran solamente las tablas de usuarios y contraseñas, lo que no es extensivo para la totalidad de sistemas[17].

3.4. Finalmente en cuanto a las transmisiones por medio de los radios de comunicaciones para el traslado de combustibles, se determinó que para el resguardo de dichas comunicaciones se utiliza mecanismos de cifrado donde la configuración del canal de coordinación de operaciones del poliducto utiliza un algoritmo de encriptación débil en relación con las buenas prácticas, y no se considera efectivo para prevenir algunos tipos de ataques. Además el personal de RECOPE S.A. que tiene acceso a estas comunicaciones no cuentan con acuerdos de confidencialidad laboral suscritos.

---

[15] Mediante oficio n.° DT-0335-2025 del 30 de julio de 2025 se indicó por parte de RECOPE S.A. que se contaba con una contratación vigente de análisis de vulnerabilidades, que incluyen servicios para pruebas de ingeniería social, penetración y análisis en la red y dispositivos, sin embargo no se ha acreditado si todo el ciclo de gestión de las vulnerabilidades se realiza de manera activa, periódica y permanente como parte de la labor de la Dirección de Tecnología.

[16] Verificación mediante información del reporte de colaboradores registrados como activos ante Capital Humano, suministrado mediante oficio n.° DCH-0435-2025 del 14 de julio de 2025. Al respecto, el Manual de Directrices en Materia de Seguridad de la Información PE-10-12-005 establece que "El Departamento de Reclutamiento y Compensaciones deberá notificar oportunamente y por los canales establecidos a la Dirección de Tecnología, cuando un empleado deje de laborar o cambie de cargo en RECOPE S.A., con la finalidad de que sus accesos sean revocados o modificados"

[17] La administración indicó que en equipos de usuario final (laptops y equipos de escritorio), con sistema operativo Windows se puede cifrar datos utilizando las herramientas que ofrece el mismo sistema operativo, sin embargo, esta medida no es mandatoria y no se conoce de su implementación en la totalidad de los equipos.

¿Por qué se presenta este resultado?

3.5. Debido a la ausencia de un sistema de gestión de vulnerabilidades que defina cómo se deben identificar, analizar, monitorear y remediar las vulnerabilidades. Además, debido a la ausencia de un análisis de riesgos integral acerca de la criticidad y sensibilidad de todos los datos para el establecimiento de la necesidad de cifrado y su tipificación en reposo o en tránsito. Finalmente, debido a la inobservancia de los procedimientos de gestión y monitoreo de identidades y accesos para la creación, modificación y asignación de privilegios así como baja de usuarios.

¿Cómo se espera que funcione según la normativa?

3.6. En cuanto a los controles de ciberseguridad, es deber de las instituciones implementar medidas para proteger sus activos digitales (información, infraestructura, redes, bases de datos), incluyendo seguridad física y ambiental. Sus sistemas críticos deben estar controlados y libres de vulnerabilidades conocidas; y además debe tener un proceso que regule las cuentas de usuarios y contraseñas, de conformidad con las buenas prácticas y la normativa de seguridad de la información.

3.7. En cuanto a las vulnerabilidades de ciberseguridad detectadas, se debe considerar que las Normas de Control Interno para el Sector Público[18], señalan que cuando se detecte alguna deficiencia o desviación en la gestión o en el control interno, se deben emprender oportunamente las acciones preventivas o correctivas pertinentes para fortalecer el Sistema de Control Interna (SCI), de conformidad con los objetivos y recursos institucionales. En lo referente al cifrado de información, el marco de gestión del COBIT 5, 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 que ante situaciones donde la confidencialidad es de importancia, los respaldos deberían ser protegidos por medio del cifrado.

¿Qué pasa si no se corrige?

3.8. Se podría comprometer la integridad, disponibilidad y confidencialidad de la información. Ejemplo de ello es que la gestión de las vulnerabilidades tiende a ser reactiva ante el suceso de eventos, así como el riesgo de accesos no autorizados que atenta contra la rendición de cuentas y la confidencialidad. Finalmente aumenta la susceptibilidad a ciberataques e incidentes de seguridad, como por ejemplo el ciberataque acontecido el 27 de noviembre de 2024 en RECOPE S.A. que ha interrumpido servicios y operaciones.

[18] Norma 6.4 Acciones para el fortalecimiento del SCI de la Norma N-2-2009-CO-DFOE (NCISP).

Responsables

- A Karla Montero Víquez en su calidad de Presidenta Ejecutiva o a quien en su lugar ocupe el cargo

Disposiciones	Plazo
D1. Elaborar, formalizar e implementar un Sistema de Gestión de la Continuidad del Negocio (SGCN) integral a nivel institucional, que cubra la totalidad de los procesos de negocio críticos y los sistemas de información que los soportan, que considere al menos: i. Actualizar el Análisis de Impacto del Negocio (BIA) para que cubra la totalidad de los procesos. ii. el Plan de Continuidad del Negocio (BCP). iii. el Plan de Recuperación de Desastres (DRP). iv. la estrategia de respaldo y recuperación. Lo anterior, con la participación conjunta de cada una de las áreas de negocio y de la Dirección de Tecnologías, en atención a la infraestructura tanto de Tecnologías de Información (TI) como de Operaciones Tecnológicas (OT). (Ver párrafos 1.1 al 1.8).	Para dar por acreditada esta disposición se deberá remitir al Área de Seguimiento para la Mejora Pública de la Contraloría General, lo siguiente: a. A más tardar el 30 de octubre de 2026, un informe de avance de la elaboración del Sistema de Gestión de Continuidad de Negocio (SGCN) b. A más tardar el 18 de diciembre de 2026, una certificación en la que se haga constar que se elaboró y formalizó el SGCN c. A más tardar el 30 de junio de 2027, un primer informe de avance en la implementación del SGCN d. A más tardar el 17 de diciembre de 2027, un segundo informe de avance en la implementación del SGCN

- A Karla Montero Víquez en su calidad de Gerente General o a quien en su lugar ocupe el cargo

Disposiciones	Plazo
D2. Elaborar, formalizar e implementar el programa de seguridad de información con sus respectivos proyectos y actividades, cronograma, roles y responsables e incluya al menos actividades periódicas relacionadas con el mantenimiento preventivo y predictivo de las operaciones tecnológicas .(Ver párrafos 2.1 al 2.8).	Para dar por acreditada esta disposición se deberá remitir al Área de Seguimiento para la Mejora Pública de la Contraloría General, lo siguiente: a. A más tardar el 30 de mayo 2026, una certificación que acredite la elaboración y formalización del programa de seguridad de la información. b. A más tardar el 18 de diciembre de 2026, una certificación en la cual conste la implementación de dicho programa.

Disposiciones	Plazo
D3. Elaborar, aprobar e implementar mecanismos de control para monitorear e identificar posibles riesgos y vulnerabilidades de la infraestructura tecnológica de RECOPE S.A., que permita tomar decisiones oportunas para reducir el impacto de estos riesgos en los procesos del negocio, considerando al menos las acciones, responsables, informes requeridos y su periodicidad (frecuencia de monitoreo, análisis y medidas de gestión). (Ver párrafos 3.1 al 3.8)	Para dar por acreditada esta disposición se deberá remitir al Área de Seguimiento para la Mejora Pública de la Contraloría General, lo siguiente: a. A más tardar el 19 de diciembre de 2025 una certificación que acredite la elaboración y formalización de dichos mecanismos de control. b. A más tardar el 30 de junio de 2026, una certificación en la que conste la implementación de dichos mecanismos.
D4. Elaborar, aprobar e implementar un plan de remediación de las vulnerabilidades sobre seguridad de la información comunicadas mediante el oficio n.° 09912 (DFOE-SOS-0226) del 22 de mayo de 2025, mediante el cual se subsanen las debilidades identificadas, que contenga los plazos de ejecución, los responsables y los mecanismos para supervisar el avance en dicha remediación. (Ver párrafos 3.1 al 3.8)	Para dar por acreditada esta disposición se deberá remitir al Área de Seguimiento para la Mejora Pública de la Contraloría General, lo siguiente: a. A más tardar el 09 de enero de 2026 una certificación que acredite la elaboración y aprobación del plan de remediación. b. A más tardar el 27 de febrero de 2026, una certificación en la que conste la implementación de dicho plan.

Disposiciones	Plazo
D5. Incorporar en la política de seguridad de la información institucional, lo siguiente: i) las orientaciones sobre la implementación del cifrado de datos, así como su tipificación en reposo o en tránsito, y sobre las transmisiones en tránsito de las comunicaciones de radio utilizadas; con base en un análisis de riesgos integral acerca de la criticidad, sensibilidad y pertinencia de todos los datos. (Ver párrafos 3.1 al 3.8) ii) mayor detalle acerca de la gestión de las contraseñas para los sistemas de tecnologías de información y de operación; incluyendo al menos: longitud, complejidad, caducidad, reutilización, uso de palabras conocidas, combinación de factores, cifrado de tabla de usuarios y contraseñas; además, definir los roles y responsables del monitoreo y verificación del cumplimiiento de la politica de gestión de contraseñas. (Ver párrafos 2.1 al 2.8)	Para dar por acreditada esta disposición se deberá remitir al Área de Seguimiento para la Mejora Pública de la Contraloría General, lo siguiente: a. A más tardar el 30 de enero de 2026 una certificación que acredite la incorporación de las orientaciones sobre el cifrado de datos en la política de seguridad de la información b. A más tardar el 30 de enero de 2026, una certificación que acredite la incorporación del detalle de la gestión de contraseñas en la política de seguridad de la información. c. A más tardar el 18 de diciembre de 2026, una certificación sobre la elaboración de un reporte acerca del resultado del monitoreo y verificación del cumplimiento de esos requisitos.
D6. Elaborar, en coordinación con la Dirección de Tecnología, lo siguiente: a. El inventario total de los equipos de tecnología operativa (OT) del sector industrial, que contenga al menos la siguiente información: i) Fabricante y Modelo (y versión vo si aplica), ii) Ubicación, iii) Responsable, iv) Estado y nivel de criticidad, v) Fecha de adquisición y fecha de caducidad (vida útil); y además, que se incorpore para su gestión, en el sistema de inventarios correspondiente. b. El inventario total de las actualizaciones de los equipos de usuarios final y equipos servidores (TI), que contenga al menos la siguiente información: i) Fecha de liberación de la actualización, ii) Fecha de instalación de la actualización, iii) Nombre del equipo, y iv) Ubicación. (Ver párrafos 2.1 al 2.8)	Para dar por acreditada esta disposición se deberá remitir al Área de Seguimiento para la Mejora Pública de la Contraloría General, lo siguiente: a. A más tardar el 30 de junio de 2026, una certificación que acredite la elaboración del inventario total de los equipos de tecnología operativa. b. A más tardar el 18 de diciembre de 2026, una certificación que acredite la elaboración del inventario total de las actualizaciones de los equipos.

Disposiciones	Plazo
D7. Establecer, formalizar e implementar los mecanismos de control para asegurar la inclusión, revisión y aprobación de cláusulas de seguridad de la información y acuerdos de nivel de servicio con proveedores de Tecnologías de Información y operadores de servicios, sobre confidencialidad de la información y garantía de continuidad del servicio, que incluya al menos: a. Los aspectos de: auditabilidad, propiedad de información, proceso de salida, obligaciones en materia de seguridad y acceso, y respaldos de información; así como mecanismos para la supervisión y control que incluyan roles y responsabilidades para el cumplimiento de esas cláusulas. (Ver párrafos 2.1 al 2.8) b. Inclusión de acuerdos de no divulgación de información entre RECOPE S.A. y los operadores de traslado de combustibles (Ver párrafo 3.4)	Para dar por acreditada esta disposición se deberá remitir al Área de Seguimiento para la Mejora Pública de la Contraloría General, lo siguiente: a. A más tardar el 29 de mayo de 2026, una certificación que acredite la elaboración y formalización de dichos mecanismos de control. b. A más tardar el 30 setiembre de 2026, una primera certificación en la que conste la implementación de dichos mecanismos. c. A más tardar el 18 de diciembre de 2026, una segunda certificación en la que conste la implementación de dichos mecanismos.

- A Alexander Fonseca Moya en su calidad de Director de Tecnología o a quien en su lugar ocupe el cargo

Disposiciones	Plazo
D8.Elaborar, divulgar e implementar mecanismos de control de ciberseguridad, que al menos contenga los siguientes aspectos: i) Concurrencia de sesiones en los sistemas y servicios de RECOPE S.A, ii) suspensión automática de sesión de sistemas de aplicación y sistemas operativos por desatención, iii) múltiple factor de autenticación de forma nativa, iv) la supervisión de los usuarios privilegiados, suspensión de usuarios por ausencias prolongadas y vi) la depuración de las cuentas de usuarios genéricos, en el Sistema de Administración de Usuarios así como en los sistemas de aplicación con base en su pertinencia y utilidad. (Ver párrafos 3.1 al 3.8)	Para dar por acreditada esta disposición se deberá remitir al Área de Seguimiento para la Mejora Pública de la Contraloría General, lo siguiente: a. A más tardar el 19 de diciembre de 2025, una certificación de la elaboración y divulgación de dichos mecanismos de control de ciberseguridad. b. A más tardar el 21 de agosto de 2026, una certificación en la que conste el avance en la implementación de dichos mecanismos. c. A más tardar 18 de diciembre de 2026, una certificación en la que conste la implementación de dichos mecanismos
D9. Realizar un análisis de riesgos integral, con respecto a la ausencia de un sitio alterno de procesamiento para la recuperación de desastres; y definir e implementar una estrategia para administrar los riesgos identificados en dicho análisis. (Ver párrafos 3.1 al 3.8)	Para dar por acreditada esta disposición se deberá remitir al Área de Seguimiento para la Mejora Pública de la Contraloría General, lo siguiente: a. A más tardar el 16 de enero de 2026, una certificación que acredite la elaboración de dicho análisis. b. A más tardar el 27 de marzo de 2026 la remisión de la estrategia a la Gerencia General para administrar los riesgos identificados. c. A más tardar el 26 de junio de 2026 un informe de avance de la implementación de la estrategia.

Marco General de la auditoría

Fundamentación

La CGR realizó una auditoría de carácter especial acerca de los controles establecidos por la Refinadora Costarricense de Petróleo S.A. (RECOPE S.A) para implementar la seguridad de la información. Este tipo de auditoría tiene el propósito de determinar si las instituciones públicas actúan conforme a las disposiciones legales, reglamentarias y normativas aplicables, así como a los principios de buena administración. Esta auditoría se efectuó con fundamento en las competencias conferidas a la CGR en los artículos 183 y 184 de la Constitución Política, y los numerales 17, 21 y 37 de su Ley Orgánica n.° 7428, en cumplimiento del Plan Anual Operativo de la División de Fiscalización Operativa y Evaluativa.

Validación de términos

Los términos de auditoría fueron comunicados a RECOPE S.A. mediante el oficio n.° 11391 (DFOE-SOS-308) del 24 de junio de 2025. Se formalizaron los siguientes términos que consideran las observaciones efectuadas por la(s) Administración(es):

- **Objetivo:** Determinar si los controles establecidos por RECOPE S.A para implementar la seguridad de la información se ajustan al marco regulatorio y buenas prácticas aplicables, a efectos de prevenir afectaciones en la prestación de los servicios.
- **Alcance:** El periodo del estudio abarca los años 2023-2024, ampliándose de ser necesario
- **Fuentes de criterios:** Los criterios de auditoría se fundamentan principalmente en las siguientes fuentes:

Normativa	Artículos relevantes
Ley General de Control Interno, n.° 8292	12 - 18
Normas de Control Interno para el Sector Público	6.4
Normas técnicas para el gobierno y gestión de las tecnologías de la información, Micitt	XII, XIII, XII y XIV
Control Objectives for Information and Related Technologies (COBIT 5), ISACA	DSS04, DSS06.02, BAI02.01, APO10
Normas ISO 27002, Organización Internacional de Normalización	9-12, 15-17
Normas ISO 22301, Organización Internacional de Normalización	4.3, 5, 6, 8

Marco General de la auditoría

Metodología

La auditoría se realizó conforme a las Normas Generales de Auditoría para el Sector Público, el Manual General de Fiscalización Integral de la CGR, el Procedimiento de Auditoría vigente, 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). Para el desarrollo de esta auditoría se utilizó la información suministrada en las entrevistas a funcionarios de RECOPE S.A, así como las respuestas a las consultas planteadas por escrito ante diferentes funcionarios de esa institución.

Comunicación preliminar

El borrador del informe fue remitido mediante el oficio n.º 15362 (DFOE-SOS-0444) del 26 de agosto de 2025, y comunicado en reunión virtual el 29 de agosto de 2025 con la participación de la Presidenta Ejecutiva, Auditor Interno, Director de Tecnologías, Gerente de Desarrollo, Jefe de Control Interno, Jefe Automatización Industrial, Jefe de Soporte Técnico, entre otros funcionarios de esas dependencias, con el propósito de que se formularan, en el plazo otorgado, las observaciones pertinentes al contenido del documento citado. Al respecto, RECOPE S.A. envió observaciones con el oficio n.º P-0473-2025 del 4 de setiembre de 2025, las cuales fueron atendidas en el oficio n.º 16097(DFOE-SOS-0600) de 05 de setiembre de 2025.

Cumplimiento de disposiciones

De conformidad con 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 n.° 7428, y el artículo 12 inciso c) de la Ley General de Control Interno n.° 8292, las disposiciones contenidas en este informe son de acatamiento obligatorio y deberán cumplirse dentro del plazo establecido, siendo su incumplimiento injustificado causal de responsabilidad. Para su observancia, se deberán aplicar los Lineamientos Generales para el Cumplimiento de las Disposiciones y Recomendaciones de la CGR, Resolución R-DC-144-2015. La CGR se reserva el derecho de verificar la implementación efectiva de estas disposiciones y de valorar las responsabilidades correspondientes en caso de incumplimiento.

Equipo auditor

Esta auditoría fue realizada por un equipo multidisciplinario del Área de Fiscalización para el Desarrollo de Sostenible de la División de Fiscalización Operativa y Evaluativa, dirigida por Lía Barrantes León.