



Seguridad de información y continuidad de los servicios digitales de Correos de Costa Rica

Dirigido a Correos de Costa Rica

Auditoría de Carácter Especial
DFOE-GOB-IAD-00003-2026
25 de setiembre de 2026

¿Qué auditamos?

La seguridad de la información de la plataforma tecnológica y el entorno en el que operan los servicios digitales de Correos de Costa Rica, en cuanto a su preparación para detectar, detener y responder a posibles incidentes de ciberseguridad que puedan afectar la continuidad de negocio. Lo anterior para el periodo comprendido entre el 01 de enero de 2024 y 12 de agosto de 2026.

¿Por qué es importante?

Correos de Costa Rica a través de su plataforma tecnológica presta servicios digitales a las personas usuarias, incluidos trámites, pagos, seguimiento de envíos y otras operaciones asociadas a su actividad. Por ello, su disponibilidad y la protección de la información que procesan son relevantes para mantener la continuidad de los servicios y la confianza de las personas usuarias. Una gestión adecuada de la seguridad de la información permite reducir la exposición a incidentes de ciberseguridad que puedan provocar accesos no autorizados, pérdida o alteración de información e interrupciones en la prestación de los servicios.

¿Qué concluimos?

La seguridad de la información en los servicios digitales presenta un **incumplimiento** en aspectos significativos del marco normativo y técnico aplicable. La naturaleza y el alcance de las debilidades identificadas evidencian una gestión reactiva y desarticulada que limita la capacidad institucional para prevenir, detectar y responder oportunamente ante incidentes de ciberseguridad y para mantener la continuidad de los servicios digitales. En consecuencia, estas deficiencias comprometen de forma integral la razonabilidad de la gestión y requieren acciones correctivas inmediatas y de carácter estructural.

Resultados

Limitaciones en capacidad de respuesta y adaptación institucional por rezagos en el marco estratégico y normativo de TI: La planificación de TI no se encuentra alineada con la estrategia institucional, mientras que la implementación del Marco de Gestión de TI y la actualización del cuerpo normativo presentan rezagos que limitan una gestión integrada de la seguridad de la información.

Riesgo de accesos no autorizados y uso indebido de credenciales en algunos servicios digitales: Plataformas críticas operan fuera del esquema institucional de gestión centralizada de identidades y sin mecanismos de autenticación robustos.

Prevalencia de riesgos de alto impacto por falta de oportunidad en remediación de vulnerabilidades técnicas: La gestión de vulnerabilidades mantiene un enfoque reactivo, con riesgos de alto impacto pendientes de atención y componentes tecnológicos obsoletos que operan sin soporte del fabricante.

Riesgo en la respuesta y recuperación operativa ante eventos disruptivos en seguridad: Los instrumentos de continuidad presentaron rezagos en su actualización y no se ha validado mediante pruebas integrales la capacidad de recuperación y coordinación institucional ante eventos disruptivos.

Auditoría en datos



¿Qué son los servicios digitales de Correos de Costa Rica?

Son el conjunto de soluciones, trámites y procesos que Correos de Costa Rica pone a disposición de las personas usuarias a través de plataformas electrónicas, redes e infraestructura de tecnologías de información, con el fin de optimizar la accesibilidad, trazabilidad, oportunidad y eficiencia en la prestación de servicios, eliminando las barreras presenciales.

¿Cuáles son los servicios digitales en Correos de Costa Rica?

Los servicios digitales de Correos de Costa Rica contemplan plataformas para trámites estatales (citas y pagos de servicios); compras en el exterior; la gestión y canalización de entrega de paquetería, preparación y pre-pago de envíos nacionales; registro para buzones de autoservicio, programación de recolecciones a domicilio y seguimiento en tiempo real. Dichos servicios funcionan en una plataforma tecnológica y entorno común y constituyen activos digitales cuya disponibilidad, integridad y continuidad operativa deben ser resguardadas bajo un marco sólido de seguridad de la información.

¿Por qué es importante la seguridad de la información para los servicios digitales?

La seguridad de la información es el marco integral de medidas destinadas a proteger los activos de información de una organización, garantizando su confidencialidad, integridad y disponibilidad. En un entorno digitalizado, la exposición de trámites e iteraciones electrónicas (como pagos en línea, intercambio de datos personales para gestiones estatales, trazabilidad logística y servicios al usuario) convierte a los activos de información en objetivos críticos ante amenazas cibernéticas. Fallas en la seguridad exponen a la organización a accesos no autorizados, fraudes, alteración o

pérdida de datos; además, compromete directamente la continuidad del negocio y la reputación institucional. Resguardar estos servicios mediante un proceso continuo de políticas, controles y gestión de riesgos es indispensable para proteger la privacidad de las personas usuarias, asegurar la estabilidad del servicio público prestado y mitigar de forma preventiva los impactos financieros, legales y operacionales derivados de eventuales incidentes o vulnerabilidades.

¿Cómo se vincula la gestión de la seguridad de la información con la planificación estratégica y el control interno institucional?

La seguridad de la información de los servicios digitales debe gestionarse como un habilitador crítico de la estrategia institucional, requiere una alineación transversal con los objetivos definidos en el Plan Estratégico Institucional (PEI) y el Plan Estratégico de Tecnologías de Información (PETI), asegurando que las inversiones en ciberseguridad, la remediación de vulnerabilidades y la actualización de políticas respondan a las prioridades del negocio y al apetito de riesgo de la entidad. Un control interno efectivo permite garantizar que las medidas de seguridad no solo mitiguen amenazas, sino que aporten valor, faciliten la continuidad operativa, aseguren el cumplimiento normativo y brinden la trazabilidad necesaria para la rendición de cuentas sobre los recursos públicos invertidos.

La gestión de la seguridad de la información y continuidad en los servicios digitales de Correos de Costa Rica presenta un **incumplimiento generalizado** de los aspectos significativos del marco normativo y técnico aplicable. La valoración integral de la evidencia demuestra que las debilidades identificadas no son aisladas, sino de naturaleza estructural y transversal, por cuanto afectan componentes esenciales para prevenir, detectar y responder oportunamente ante incidentes de ciberseguridad y mantener la continuidad de servicios esenciales.

La gestión opera bajo un enfoque predominantemente reactivo y desarticulado, con debilidades en la gobernanza de TI, la gestión de identidades y accesos, la atención de vulnerabilidades y la continuidad de negocio. Estas condiciones limitan la capacidad institucional para gestionar los riesgos de seguridad de manera integrada y oportuna, mantener controles de acceso consistentes, reducir la exposición derivada de vulnerabilidades y obsolescencia tecnológica, y demostrar mediante pruebas integrales su capacidad efectiva de recuperación ante eventos disruptivos.

Si bien la institución dispone de controles operativos que contribuyen a la protección de su infraestructura tecnológica, estos no compensan la naturaleza y el alcance de las deficiencias identificadas ni permiten sostener un nivel razonable de conformidad con los criterios aplicables. En consecuencia, la magnitud del incumplimiento observado requiere acciones correctivas inmediatas de carácter estructural para fortalecer la gobernanza y el control interno, reducir la exposición a riesgos de ciberseguridad, asegurar la continuidad y la resiliencia de los servicios digitales.

Limitaciones en capacidad de respuesta y adaptación institucional por rezagos en el marco estratégico y normativo de TI

¿Qué encontramos?

- 1.1. El proceso de gobernanza, planificación estratégica y actualización normativa de tecnologías de información en Correos de Costa Rica presenta un rezago en su actualización con respecto al nuevo Plan Estratégico Institucional (PEI 2026-2028), lo que limita la capacidad institucional para adaptarse y responder oportunamente a los desafíos y riesgos del entorno. Esta condición se aleja de las mejores prácticas y estándares internacionales en la materia, que promueven la **oportuna** alineación de la estrategia de TI ante cambios en la estrategia de negocio, la efectividad del control interno y la vigencia formal de los instrumentos normativos.
- 1.2. Sobre el particular, se determinó que existe una desalineación estratégica, entre el PETI vigente (2024-2026) y el PEI 2026-2028, por cuanto este último se encuentra desfasado y principalmente porque se requieren ajustes transversales para apegarse al nuevo paradigma organizacional del PEI que exige un modelo cuantitativo, de monetización (IFA) y de gestión de riesgos, el PETI (2024-2026) mantiene el enfoque cualitativo anterior y carece de métricas para respaldar las metas del negocio. Además, el seguimiento actual de TI en informes trimestrales es descriptivo y no cuenta con indicadores de avance precisos. Asimismo, no existía una hoja de ruta elaborada con anticipación para guiar la correspondiente realineación el PETI.
- 1.3. También, se identificó un **retraso del proyecto sobre el Marco de Gestión de TI**, ya que no se ejecutaron los compromisos de la Fase III del Marco de TI adoptado en julio de 2024. Ante requerimientos de la CGR en julio de 2026, la GTTI remitió únicamente la propuesta inicial del plan de trabajo de noviembre de 2024 en lugar de informes de avance real, constatándose que la implementación se encuentra paralizada y acotada a tareas puntuales de ciberseguridad.
- 1.4. Por otra parte, la institución enfrenta una **desactualización normativa**, donde el 41,94% de las políticas de seguridad (13 de 31) datan del periodo 2018-2021, acumulando entre 5 y 8 años de desfase respecto al entorno tecnológico actual. Asimismo, existen controles normativos indispensables como los **procedimientos de Gestión de Activos Tecnológicos, Monitoreo y Aplicación de Parches**, el Protocolo de Incidentes de Ciberseguridad que se mantienen en condición de borrador sin oficialización, al no contar con aprobación formal.
- 1.5. Finalmente, el inventario institucional de activos de información opera como un registro técnico y operativo independiente, sin integración documental explícita con la gestión de riesgos y controles para su protección, tampoco contempla la clasificación de cada activo bajo los parámetros de confidencialidad, integridad y disponibilidad.

¿Por qué se presenta este resultado?

- 1.6. La falta de capacidad resolutoria de los mecanismos de gobernanza y supervisión, los cuales no han logrado la rendición de cuentas ni la toma de decisiones estratégicas documentadas y

Limitaciones en capacidad de respuesta y adaptación institucional por rezagos en el marco estratégico y normativo de TI

oportunas para priorizar o resolver las situaciones que paralizan o retrasan los proyectos indicados. Esta falta de efectividad en la gobernanza y en la acción institucional propició la paralización en la implementación del Marco de TI, así como la desactualización prolongada de sus políticas y procedimientos.

- 1.7. En cuanto a los activos de información institucionales, la debilidad surge ante la ausencia de mecanismos para operacionalizar y materializar en las herramientas institucionales, su articulación con los riesgos y controles asociados, mediante identificadores y relaciones explícitas que permitan mantener su trazabilidad y actualización bidireccional; situación que se ve acentuada por una cultura organizacional centrada prioritariamente en el enfoque tradicional de inventario físico, que omite comprender la información y los datos como activos estratégicos y componentes fundamentales para la seguridad de los servicios digitales.

¿Cómo se espera que funcione según la normativa?

- 1.8. Correos de Costa Rica debe contar con una gobernanza de TI que asegure la alineación continua de sus estrategias y proyectos tecnológicos con las prioridades del negocio plasmadas en el Plan Estratégico Institucional (PEI). Para ello, las máximas autoridades deben garantizar la implementación¹ de su marco de gestión de TI y mantener un cuerpo normativo oficialmente aprobado, actualizado y conforme² al entorno tecnológico actual, que formalice las operaciones y proteja los activos de información³.
- 1.9. La gestión de activos, su clasificación por valor/criticidad y su vinculación con el marco de riesgos y controles para su protección⁴ es un pilar fundamental de la gobernanza de TI, permite a la organización estructurar, priorizar y normalizar la ciberseguridad a nivel estratégico, por ello, debe trascender el registro independiente para establecer una trazabilidad explícita y bidireccional entre ellos para mantener una visión integrada, facilitar la actualización de la información y determinar oportunamente el impacto de los cambios sobre los elementos relacionados⁵.

Imagen 1

Vinculación estratégica de activos de información con sus riesgos y controles asociados

¹ N-2-2009-CO-DFOE 5.10 Tecnologías de información.

² N-2-2009-CO-DFOE 5.3 Armonización de los sistemas de información con los objetivos, 4.3 Protección y conservación del patrimonio

³ Normas técnicas para la gestión y el control de las tecnologías de información emitidas por el MICITT. Proceso I. Gobernanza de TI.

⁴ N-2-2009-CO-DFOE 5.7.4 Seguridad

⁵ Normas técnicas para la gestión y el control de las tecnologías de información emitidas por el MICITT. Proceso XI. Seguridad y Ciberseguridad.

Limitaciones en capacidad de respuesta y adaptación institucional por rezagos en el marco estratégico y normativo de TI



Fuente: Elaboración CGR.

¿Qué pasa si no se corrige?

- 1.10. Mantener políticas desactualizadas omite regulaciones para riesgos emergentes. A su vez, los procedimientos en condición de borrador carecen de habilitación jurídica para su aplicación vinculante y la solidez requerida para el control interno, afectando el ciclo de **mejora continua de la normativa que soporta el Sistema de Gestión de Seguridad de la Información (SGSI)**. La necesidad de actualización expresada por la propia institución evidencia que la normativa vigente no responde al entorno tecnológico ni a las amenazas actuales. Asimismo, la falta de articulación entre un PETI cualitativo y un PEI 2026-2028 cuantitativo y monetizado no permite que la tecnología sea un habilitador estratégico, y podría impedir priorizar las inversiones según el valor real del negocio, lo que limita la capacidad técnica institucional y eleva el riesgo de incumplimiento regulatorio.
- 1.11. En el ámbito tecnológico, el valor de un activo no está determinado únicamente por su costo económico o valor contable, sino por la sensibilidad y criticidad de la información que procesa. La ausencia de esta clasificación impide a la institución identificar cuáles activos son realmente estratégicos, imposibilitando la priorización de recursos y controles donde el impacto institucional ante una falla sería verdaderamente crítico.

Riesgo de accesos no autorizados y uso indebido de credenciales en algunos servicios digitales

¿Qué encontramos?

- 2.1.** La gestión de identidades y accesos en **algunos de sus servicios digitales** opera de forma desarticulada del modelo centralizado institucional, lo que puede exponer a Correos de Costa Rica a accesos no autorizados y al uso indebido de credenciales. Esta condición se aleja de las mejores prácticas en la materia, orientadas a la administración centralizada de identidades y la exigencia de autenticación robusta. Esta condición se sustenta en las siguientes debilidades específicas:
- 2.1.1. Arquitectura de accesos no centralizada:** Se determinó que algunos servicios digitales considerados críticos por la institución, no están integrados a la gestión centralizada de accesos institucional, ni se dispone de mecanismos de inicio de sesión único (Single Sign-On - SSO), operando bajo esquemas descentralizados de administración de usuarios, esta situación fue identificada por la Administración y está incluida en el plan de trabajo para la implementación de COBIT⁶.
 - 2.1.2. Debilidades en la robustez de la gestión de identidades:** Los accesos a dichos servicios, carecen de un esquema robusto de autenticación, omitiendo la implementación de mecanismos de autenticación o validación adicional.
 - 2.1.3. Gestión rígida e individualizada de políticas de seguridad:** La actualización y administración de las políticas y parámetros de contraseñas de esos mismos servicios, no se administran desde la infraestructura central, lo que dificulta su actualización estandarizada.

¿Por qué se presenta este resultado?

- 2.2.** Esta debilidad proviene del desarrollo y despliegue histórico de aplicaciones heredadas con más de ocho años de antigüedad, implementadas bajo arquitecturas independientes previas a la definición del estándar unificado de identidades. Aunque en el informe DFOE-GOB-IF-00008-2022 se dispuso la inclusión obligatoria de requisitos de seguridad en nuevas adquisiciones tecnológicas, la administración no ha implementado mecanismos para resolver la brecha en las plataformas anteriores, permitiendo que operen de forma aislada sin integración al directorio central ni soporte para protocolos de inicio de sesión único (SSO).

¿Cómo se espera que funcione según la normativa?

- 2.3.** Para asegurar razonablemente la continuidad de sus operaciones y la protección de sus activos de información, Correos de Costa Rica debe implementar controles que protejan la información durante su recopilación, procesamiento, almacenamiento y comunicación⁷. Para ello, se requiere la adopción de medidas de seguridad administrativas, físicas y lógicas que garanticen la autenticación y control de acceso en esas plataformas críticas identificadas. Adicionalmente,

⁶ Plan de trabajo para la implementación del marco de gestión de TI, COBIT 2019, acuerdo Junta Directiva N°10884 (acta 1847 del 09 de julio, 2024)

⁷ Normas de control interno para el Sector Público (N-2-2009-CO-DFOE), norma 4.4.

Riesgo de accesos no autorizados y uso indebido de credenciales en algunos servicios digitales

la institución definió⁸ como objetivo optimizar recursos, gestionar riesgos de TI de manera proactiva y alinear los servicios tecnológicos con las necesidades del negocio, beneficiando tanto a la organización como a los usuarios.

- 2.4.** En ese sentido la institución debe disponer de un mecanismo centralizado (como directorio activo y SSO) que permita ajustar los accesos de manera automática e inmediata ante ingresos, traslados o desvinculaciones de personal. Asimismo, para las aplicaciones establecidas como críticas (según su RTO) que procesan transacciones o datos sensibles, la administración debe implementar esquemas de robustez en la autenticación para mitigar el riesgo de suplantación de identidad. Las políticas de contraseñas, caducidad y bloqueos deben administrarse de forma estandarizada e institucional desde la infraestructura central, sin depender de modificaciones en código fuente.

¿Qué pasa si no se corrige?

- 2.5.** La gestión descentralizada de identidades en algunos de sus servicios digitales críticos rompe el esquema de trazabilidad y gobernanza de accesos, expone a Correos de Costa Rica al posible riesgo de que funcionarios desvinculados o trasladados mantengan accesos activos, lo cual podría habilitar la realización de transacciones no autorizadas o la extracción indebida de información sensible. Asimismo, la insuficiente robustez en la autenticación incrementa el riesgo de suplantación de identidad. Por último, la imposibilidad de aplicar políticas de seguridad centralizadas obliga a ejecutar cambios individuales en el código dificultando el cumplimiento normativo unificado.

⁸ Plan de trabajo para la implementación del marco de gestión de TI, COBIT 2019, acuerdo Junta Directiva N°10884.

Prevalencia de riesgos de alto impacto por falta de oportunidad en remediación de vulnerabilidades técnicas

¿Qué encontramos?

- 3.1. El proceso de atención, seguimiento y remediación de vulnerabilidades en la infraestructura que soporta los servicios digitales de Correos de Costa Rica, es lento e inoportuno, en consecuencia permanecen riesgos de alto impacto, **detectados originalmente en la prueba de penetración (pentest) contratada por la propia institución**, esto con el agravante de no haber analizado e implementado controles compensatorios de mitigación temporal contrario a las mejores prácticas internacionales de ciberseguridad, que promueven la **mitigación** inmediata de hallazgos críticos/altos, la aplicación constante de controles de endurecimiento (hardening) y la sustitución oportuna de activos tecnológicos antes de ser afectados por su obsolescencia.
- 3.2. Se confirmó que 34 de las 70 vulnerabilidades detectadas⁹ permanecen pendientes de atención, de las cuales 18 son de alto impacto y severidad crítica. La persistencia de estas fallas sin resolver, sumada a la ausencia de análisis e implementación de controles compensatorios temporales, evidencia la falta de oportunidad en el proceso de remediación y mantiene a los servicios digitales expuestos a riesgos de seguridad de alta severidad.
- 3.3. Asimismo, se identificaron componentes tecnológicos que alcanzaron el fin de su vida útil y configuraciones que requieren fortalecerse.
- 3.4. Por último, se identificó falta de estandarización y documentación del proceso, específicamente en la matriz de control del proceso de remediación la cual, para algunas vulnerabilidades, omite la identificación de responsables formales, y el detalle de los controles compensatorios para aquellas vulnerabilidades no subsanables o postergadas. Tampoco se actualiza de forma oportuna, ni se respalda con acciones de remediación documentadas y evidenciadas.

¿Por qué se presenta este resultado?

- 3.5. El seguimiento a las vulnerabilidades del pentest ha operado bajo un enfoque reactivo e inoportuno, donde la remediación de los hallazgos críticos depende de proyectos de infraestructura que debieron finalizar en noviembre de 2025, que carecen de un control y seguimiento riguroso por parte de la institución. Aunado a la falta de gobernanza sobre la remediación en la cual se ejerza un seguimiento riguroso de la matriz de control, así como la ausencia de una planificación estratégica orientada a la renovación gradual de la infraestructura en estado de obsolescencia manteniéndola expuesta a vulnerabilidades conocidas.

⁹ Los resultados de las distintas pruebas fueron entregados a Correos de Costa Rica entre octubre de 2025 y abril de 2026.

Prevalencia de riesgos de alto impacto por falta de oportunidad en remediación de vulnerabilidades técnicas

¿Cómo se espera que funcione según la normativa?

- 3.6.** Correos de Costa Rica debe adoptar medidas de seguridad administrativas, físicas y lógicas que contemplen la detección y atención oportuna de vulnerabilidades e incidentes¹⁰, los resultados de los informes de pruebas de penetración (pentest), requieren un flujo estandarizado de atención que priorice los hallazgos según su nivel de criticidad y establezca plazos obligatorios de remediación. Asimismo, en el caso de vulnerabilidades que no puedan subsanarse de forma inmediata, se debe documentar formalmente los responsables, las justificaciones técnicas sustentadas y los controles compensatorios aprobados. Asimismo, los registros del proceso deben actualizarse de forma oportuna y sustentarse en acciones de remediación debidamente documentadas y evidenciadas¹¹.
- 3.7.** Asimismo, la gestión de la infraestructura tecnológica debe contemplar la aplicación continua de medidas básicas de endurecimiento (hardening) —conforme a líneas base de configuración segura reconocidas, aplicadas de forma continua y sin depender de revisiones externas—. Por último, la institución debe contar con una planificación estratégica para la sustitución oportuna y gradual de aquellos activos tecnológicos que alcancen el fin de su vida útil, garantizando que todos los componentes en producción mantengan soporte activo y parches de seguridad del fabricante¹². Este proceso debe estar plenamente articulado e integrado con la matriz institucional de riesgos de la entidad, asegurando trazabilidad y rendición de cuentas sobre el estado real de la ciberseguridad¹³.

¿Qué pasa si no se corrige?

- 3.8.** Mantener 18 vulnerabilidades de alto impacto sin resolver y operar con infraestructura en fin de vida útil incrementa la exposición de la institución ante potenciales ciberataques o incidentes de seguridad que comprometan la disponibilidad, integridad y confidencialidad de la información, limitando la capacidad de prevención y respuesta, lo que coloca a los servicios digitales institucionales en un estado de vulnerabilidad prolongada ante eventuales interrupciones o accesos no autorizados.

¹⁰ Ley General de Control Interno n.º 8292, artículo 12 inciso c.

¹¹ Normas de control interno para el Sector Público (N-2-2009-CO-DFOE), norma 6.4.

¹² Normas técnicas para la gestión y el control de las tecnologías de información, emitidas por el MICITT, proceso XII. Administración Infraestructura Tecnológica.

¹³ Normas técnicas para la gestión y el control de las tecnologías de información, emitidas por el MICITT, proceso XI. Seguridad y Ciberseguridad.

Riesgo en la respuesta y recuperación operativa ante eventos disruptivos en seguridad

¿Qué encontramos?

- 4.1.** La gestión de continuidad de negocio en Correos de Costa Rica operó bajo planes teóricos sin revisión formal desde 2019 el Plan de Continuidad Empresarial (BCP) y el Plan de Gestión de Crisis, y desde 2021 los Análisis de Impacto al Negocio (BIA), y sin validaciones prácticas en su ejecución, potenciando las dificultades de recuperación operativa ante un evento disruptivo o incidente de seguridad.
- 4.2.** Al respecto, Correos de Costa Rica mantuvo desfase de cuatro años en los Análisis de Impacto al Negocio (BIA) —mantenidos sin revisar desde 2021 hasta mayo de 2026— y de seis años en el Plan de Continuidad Empresarial (BCP) y el Plan de Gestión de Crisis, los cuales operaron sin revisión formal desde 2019 hasta su ajuste en julio de 2026, pese a que la actualización debió efectuarse anualmente según su normativa. Si bien los documentos fueron actualizados durante la ejecución de la auditoría, persiste la falta de validación práctica mediante pruebas integrales de continuidad y ejercicios de recuperación de sistemas críticos, limitando la verificación operativa únicamente a revisiones físicas preventivas y pruebas técnicas en ambientes de laboratorio.
- 4.3.** Asimismo, la integración entre el protocolo de atención de incidentes y el plan de continuidad se mantiene únicamente a nivel documental. Al respecto, se incumple lo normado internamente dado que no se ha probado en la práctica si los mecanismos de alerta (triggers) funcionan para articular al equipo técnico con las áreas operativas para activar la continuidad ante incidentes. Por lo tanto, no existe certeza de que las áreas de negocio actúen de forma coordinada y oportuna conforme a lo establecido en el Plan de Continuidad Empresarial (BCP) y el Plan de Recuperación ante Desastres (DRP).

¿Por qué se presenta este resultado?

- 4.4.** La gestión de la continuidad se ha enfocado en el cumplimiento documental, omitiendo su naturaleza de proceso operativo continuo. Lo anterior provocó que las acciones institucionales se limitaran durante años solo a la emisión formal de los planes y su reciente actualización, omitiendo la programación y ejecución oportuna de pruebas de efectividad. Cabe señalar que Correos de Costa Rica agendó estas pruebas para el segundo semestre de este año, ante la reciente aprobación de los documentos señalados.

¿Cómo se espera que funcione según la normativa?

- 4.5.** Correos de Costa Rica debe mantener actualizado su Sistema de Gestión de Continuidad mediante la revisión anual¹⁴ y aprobación formal del Análisis de Impacto de Negocio (BIA), revisen el Plan de Continuidad Empresarial (BCP) y planes de contingencia y recuperación (DRP) y por parte de la Alta Dirección. Asimismo, es indispensable articular las medidas de seguridad con la atención de incidentes a través de simulacros periódicos que prueben la coordinación operativa, validen los tiempos de recuperación (RTO/RPO) que garanticen la continuidad de los servicios públicos.

¹⁴ Política de Continuidad de Negocio (PO.GG.05) apartados 2.4 Dirección de Gestión Integral de Riesgo, 3.1.2 Análisis de Impacto de Negocio (BIA), 5. Régimen Sancionatorio y VII. Control de Versiones y Cambios

Riesgo en la respuesta y recuperación operativa ante eventos disruptivos en seguridad

¿Qué pasa si no se corrige?

- 4.6. La ausencia de un esquema de supervisión continua que garantice la actualización periódica de los planes mantiene una debilidad estructural de gobernanza, genera un riesgo de recurrencia en el corto o mediano plazo propiciando que los instrumentos aprobados recientemente queden obsoletos en el corto plazo ante cambios organizativos o rotación de personal.
- 4.7. Mantener la gestión de continuidad sustentada en instrumentos sin validación práctica y sin pruebas integradas genera incertidumbre sobre la capacidad real de la institución para coordinar y recuperar sus sistemas críticos ante un evento disruptivo. La falta de ejercicios integrales que pongan a prueba los mecanismos de alerta (triggers) entre el equipo técnico y las áreas de negocio expone a la organización al riesgo de incumplir los tiempos de recuperación establecidos y los niveles de servicio acordados.

Responsables

- A José Luis Rodríguez Sibaja en su calidad de Gerente de Transformación y Tecnología o a quien en su lugar ocupe el cargo

Disposiciones	Plazo
D1. Considerando lo establecido en el Plan de Trabajo para la implementación de COBIT aprobado, definir y aprobar el cronograma detallado con las acciones específicas, los plazos y los responsables directos para la implementación formal del subproceso DSS05.04. Esto con la finalidad de contar con un esquema de trazabilidad y gobernanza de accesos que cubra los servicios digitales críticos para mitigar el riesgo de accesos no autorizados, garantizar la confidencialidad y un modelo centralizado de gestión de identidades. Lo anterior, en cumplimiento de lo establecido en el capítulo 5 de las Normas de Control Interno para el Sector Público y las mejores prácticas de gestión DSS05.04: Gestionar la identidad del usuario y el acceso lógico, de COBIT 2019. (Ver párrafos 2.1 a 2.5)	a. Remitir a la Contraloría General un oficio que acredite la definición y aprobación del cronograma detallado con las acciones, los plazos y los responsables directos para la implementación formal del subproceso DSS05.04 a más tardar el 30 de octubre de 2026. b. Remitir a la Contraloría General dos informes de avance acerca de la implementación del cronograma, el primero a más tardar el 30 de agosto de 2027 y el segundo al 10 de diciembre de 2027.
D2. Definir, aprobar, divulgar a quien corresponda e implementar un mecanismo para la gestión de vulnerabilidades, para estandarizar y ordenar el flujo de atención de vulnerabilidades internas o externas, que considere al menos: el escaneo, seguimiento y remediación continua de vulnerabilidades técnicas, definición de plazos y responsables según la criticidad y exposición al riesgo; la validación técnica post-remediación; criterios técnicos para justificar excepciones de no remediación y aprobación de controles compensatorios. Lo anterior, en cumplimiento de lo establecido en el capítulo 5 de las Normas de Control Interno para el Sector Público y el proceso XI de las mejores prácticas: Normas técnicas para el gobierno y gestión de TI (MICITT). (Ver párrafos 3.1 a 3.8).	a. Remitir a la Contraloría General un oficio de comunicación formal en la que acredite las acciones ejecutadas y adjuntar la evidencia de la definición, divulgación y aprobación del mecanismo para la gestión de vulnerabilidades, a más tardar el 13 de noviembre de 2026. b. Remitir a la Contraloría General, informe de avance que acredite la implementación del mecanismo establecido, a más tardar el 11 de febrero de 2027.

Responsable

- A Mauricio Rojas Cartín en su calidad de Gerente General o a quien en su lugar ocupe el cargo

Disposiciones	Plazo
D3. Definir, someter ante la Junta Directiva y divulgar, el Plan Estratégico de TI alineado al Plan Estratégico Institucional 2026-2028, considerando la alineación de los objetivos estratégicos institucionales conforme al apoyo en las tecnologías de información de cada proceso de negocio que interviene; esto con el propósito de maximizar el valor de la inversión tecnológica y que las soluciones de TI impulsen directamente el logro de las estrategias institucionales. Lo anterior, en cumplimiento del apartado III Planificación Estratégica Institucional, de las mejores prácticas: Normas técnicas para el gobierno y gestión de TI (MICITT). (Ver párrafos 1.1 a 1.11)	a. Remitir a la Contraloría General una certificación en la que haga constar la definición, aprobación y divulgación del Plan Estratégico de TI, acompañada de la copia del acuerdo adoptado al respecto por la Junta Directiva, a más tardar el 31 de mayo de 2027.
D4. Revisar, actualizar y oficializar el plan de trabajo para la implementación del Marco de TI que ya fue adoptado por la institución, incluyendo la normativa de Tecnologías de Información y Seguridad de la Información desactualizada. Para ello, deberán definirse las actividades, hitos, responsables, plazos y entregables orientados a la medición e implementación de los procesos clave de COBIT para mejorar la gobernanza de TI. Lo anterior, en cumplimiento de lo establecido en el artículo 5.9 de las Normas de Control Interno (N-2-2009-CO-DFOE). (Ver párrafos 1.1 a 1.11)	a. Remitir a la Contraloría General una certificación que haga constar la revisión, actualización y oficialización del plan de trabajo para la implementación del Marco de TI que ya fue adoptado por la institución, a más tardar el 15 de diciembre de 2026. b. Remitir a la Contraloría General dos informes de avance de la implementación del plan de trabajo a más tardar el 26 de febrero y el segundo al 30 de junio de 2027.
D5. Elaborar, oficializar e implementar un mecanismo que permita vincular el inventario de activos de información con sus respectivos riesgos y controles de seguridad establecidos para su protección, considerando al menos:	a. Remitir a la Contraloría General una certificación en la que acredite la elaboración y oficialización del mecanismo para vincular el inventario de activos de información con sus

- a) Extender la clasificación por criticidad e impacto operacional desde los componentes tecnológicos (hardware/software) hacia los activos de información institucionales que estos soportan.
- b) Reporte o visualización de la relación directa entre el activo de información, los riesgos identificados que podrían afectarlo y los controles específicos (preventivos, detectivos y correctivos) implementados para su mitigación.

El propósito es generar la trazabilidad integral entre los controles de seguridad, así como una inversión proporcional y óptima de recursos en función del nivel real de riesgo de cada activo.

Lo anterior, en cumplimiento de lo establecido en el artículo 14 de la Ley General de Control Interno n.º 8292, así como las mejores prácticas estipuladas en las cláusulas 6.1.2, 6.1.3 y 9.1, los controles 5.9 Inventario de información y otros activos asociados, y 5.12 Clasificación de la información, de la ISO 27001 y las mejores prácticas de gestión APO01.07, APO12.03, APO12.04 y APO12.05, de COBIT 2019 (Ver párrafos 1.1 a 1.11)

D6. Formalizar y ejecutar el programa de pruebas integrales de continuidad de negocio y ejercicios de recuperación de sistemas críticos que al menos considere lo siguiente:

- a) Validar operativamente la articulación entre el Protocolo de Atención de Incidentes de Seguridad de la Información y los planes de continuidad (BCP/DRP)
- b) Verificar los desencadenantes (triggers) de alerta para la activación coordinada entre los equipos técnicos y las áreas de negocio
- c) Documentar formalmente los resultados y lecciones aprendidas.

Con el fin de probar la capacidad de respuesta institucional ante eventos disruptivos, validar los tiempos de recuperación y la resiliencia y disponibilidad

respectivos riesgos y controles, a más tardar el 15 de diciembre de 2027.

- b. Remitir a la Contraloría General informes de avance acerca de la implementación del mecanismo establecido el primero a más tardar el 28 de abril y el segundo al 31 de julio de 2028.

- a. Remitir a la Contraloría General una certificación que acredite la formalización del programa de pruebas integrales de continuidad de negocio y ejercicios de recuperación a más tardar el 30 de octubre 2026.

- b. Remitir a la Contraloría General el informe en el que conste que se ejecutaron las pruebas programadas en el II semestre 2026 detallando los resultados y lecciones aprendidas a más tardar el 29 enero de 2027.

continúa de los servicios digitales esenciales.

Lo anterior, en cumplimiento de lo establecido en el proceso XIII Continuidad y disponibilidad operativa de los servicios tecnológicos de las mejores prácticas: Normas técnicas para el gobierno y gestión de TI (MICITT) y la PO.GG.05 Política de Continuidad de Negocio. (Ver párrafos 4.1 a 4.7)

Marco General de la auditoría

Fundamentación

La CGR realizó una auditoría de carácter especial en Correos de Costa Rica enfocada en la seguridad de la información en los servicios digitales relacionada con su preparación para detectar, detener y responder a posibles incidentes de ciberseguridad. Este tipo de auditoría tiene el propósito de determinar si la seguridad de la información en los servicios digitales de Correos de Costa Rica cumple razonablemente con el marco normativo y buenas prácticas aplicables, a efectos de proteger la información de los usuarios y mantener la continuidad de los servicios. 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.º 7428, en cumplimiento del Plan Anual Operativo de la División de Fiscalización Operativa y Evaluativa.

Validación de términos

Los términos de auditoría fueron comunicados al personal de la institución mediante el oficio DFOE-GOB-0289 del 30 de junio de 2026. Se formalizaron los siguientes términos que consideran las observaciones efectuadas por la Administración:

- **Objetivo:** Determinar si la seguridad de la información en los servicios digitales de Correos de Costa Rica cumple razonablemente con el marco normativo y buenas prácticas aplicables, a efectos de proteger la información de los usuarios y mantener la continuidad de los servicios.
- **Alcance:** La seguridad de la información en los servicios digitales de Correos de Costa Rica relacionada con su preparación para detectar, detener y responder a posibles incidentes de ciberseguridad, que puedan afectar la continuidad de negocio, entre el 01 de enero de 2024 al 12 de agosto de 2026.

Fuentes de criterios: Los criterios de auditoría se fundamentan principalmente en las siguientes fuentes:

Normativa	Artículos relevantes
Ley n.º 8292 Ley General de Control Interno	14, 15 y 16
Normas de Control Interno para el Sector Público	2.5, 3.1, 4.4.1 y Capítulo 5
Normas técnicas para el gobierno y gestión de TI (MICITT)	I, II, III, VII, IV,VIII, X, XI, XIII y XIV
COBIT 2019	APO01, APO01.07, APO01.04, APO12 (3,4,5), APO13 (1,2), BAI09 y MEA03
Norma INTE/ISO/IEC 27001:2022	Tabla A.1
PO.GG.05 Política de Continuidad de Negocio	Apartados 2.4, 3.1.2 y 5

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 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(as) de Correos de Costa Rica, así como las respuestas a las consultas planteadas por escrito ante diferentes funcionarios(as) de esa institución. Adicionalmente, se llevaron a cabo revisiones de documentación y configuración virtuales, así como la inspección física de controles relacionados con la seguridad de la información. Asimismo, se aplicó una herramienta para verificar la existencia de controles de seguridad de la información y ciberseguridad, y se realizaron pruebas sustantivas no intrusivas para validar su efectividad operativa.

Comunicación preliminar

La comunicación preliminar de los resultados, conclusiones y disposiciones que se derivan de la auditoría a la que se hace alusión en el presente informe, se llevó a cabo el 09 de setiembre de 2026, de modo virtual por la plataforma de Google Meet, con la participación de Kattia Bryan Cerdas, Gerente de Recursos Humanos en representación de Mauricio Rojas Cartín, Gerente General; José Luis Rodríguez Sibaja, Gerente de Transformación y Tecnologías de Información; Alejandra Araya Quesada, Encargada Ciberseguridad; Rubén Godínez Álvarez, Director de Gestión Integral de Riesgos; Vladimir Badilla Castro, Director Estrategia y Proyectos; y Lidiette Cruz Rodríguez, Auditora Interna, todas personas funcionarias de Correos de Costa Rica.

El borrador del informe fue remitido mediante el oficio n.º DFOE-GOB-0391(11936) del 04 de setiembre de 2026, dirigido al señor Mauricio Rojas Cartín, Gerente General de esa Institución. Al respecto, mediante oficio n.º CARTA-GG-854-2026 del 14 de setiembre de 2026, Correos de Costa Rica remitió las observaciones sobre el contenido de dicho documento, mismas que una vez valoradas por la CGR, fueron incorporadas en lo pertinente al informe final y atendidas por medio del oficio DFOE-GOB-0416 (12930) del 24 de setiembre de 2026.

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.º 7428, y el artículo 12 inciso c) de la Ley General de Control Interno n.º 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

Marco General de la auditoría

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 la Gobernanza de la División de Fiscalización Operativa y Evaluativa, dirigida por Falón Arias Calero.

CGR | Firmado
digitalmente
Valide las firmas digitales