# Auditoría Interna

20 de febrero de 2026
**AI-Ad-02-2026**

Señor
Alberto López Chaves
Gerente general
Departamento Tecnologías de Información y Comunicación

*Asunto:* *Servicio Preventivo sobre Políticas de Seguridad de la Información en el ICT*

Estimado señor:

La Auditoría en cumplimiento del Plan Anual de Trabajo, realiza el servicio preventivo sobre "*Políticas de Seguridad de la Información en el ICT*", con el objetivo de verificar la suficiencia de las Políticas de Seguridad de la Información del ICT, con el fin de determinar si están alineadas con la normativa legal vigente, los marcos de referencia internacionales y las mejores prácticas en gestión de seguridad de la información.

El alcance del estudio comprende el período del 01 de enero de 2025 al 30 de diciembre de 2025.

**Condición -lo que encontramos-**

1. **Riesgos tecnológicos sobre seguridad y ciberseguridad de la Información**

La información facilitada por la Unidad de Planificación Institucional[1] evidencia que no todas las dependencias del ICT gestionan riesgos de seguridad y ciberseguridad, dado que únicamente diez departamentos y unidades incorporan dichos riesgos, además no se contempla una gestión de riesgos integral para todo el Instituto.

El Departamento de TIC en su gestión de riesgo identifica el riesgo: "Que la información sensible del ICT sea vulnerada debido a un ataque cibernético", con un

[1] Correo del 09/10/25



(506) 2299.5800
San José, Costa Rica
www.ict.go.cr
www.visitcostarica.com

resultado residual alto. Además, indica que, ante una eventualidad de vulneración a la información sensible del ICT debido a un ataque cibernético, no se cuenta con el recurso humano para el manejo de la seguridad, que permita prevenir ataques, tomar medidas preventivas y resolver problemas.

Los controles establecidos por TIC para administrar el riesgo anterior son los siguientes:

- Herramientas de protección contra virus, spyware, hardware y otros. (Alto) [2]
- Dispositivos de seguridad instalados para garantizar la seguridad. (Alto)
- Políticas informáticas dirigida a todas las personas colaboradoras. (Medio)

Las acciones tomadas por TIC son:

- Solicitar mediante DTIC-349-2025 a la Administración dotar a TIC del personal para atender temas de seguridad.

- Reiterar semestralmente a todas las personas funcionarias, mediante correo electrónico, la responsabilidad de cumplir con las políticas de seguridad, como recordatorio de la importancia del uso adecuado de las políticas informáticas relacionadas con la seguridad de la información.

**Normativa técnica relacionada -criterio-**

El Código Nacional de Tecnologías Digitales del MICITT, Capítulo 3 Seguridad tecnológica, Seguridad de la Información y Ciberseguridad en sus Políticas Específicas, cita:

> *"Gestión integral del riesgo:*
> *La organización comprende el gobierno y la gestión de los riesgos de seguridad de la información y la ciberseguridad y su importancia para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas. Se establecen las prioridades, restricciones, tolerancias de riesgo, tratamiento y suposiciones de la organización, que se usan para respaldar las decisiones de riesgos operacionales."*

Las Normas técnicas para la gestión y el control de las tecnologías de información del MICITT, en el Proceso IV, cita:

[2] Nivel de riesgo asignado por la Administración

*"GESTIÓN DE RIESGOS TECNOLÓGICOS*
*La institución debe establecer un proceso formal de gestión de riesgos que responda a las amenazas que puedan afectar el logro de los objetivos institucionales, basado en una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considerando el marco normativo que le resulte aplicable.*

*La Unidad de TI debe aplicar el marco de gestión de riesgo tecnológico, con el fin de identificar, valorar, priorizar y gestionar los riesgos al nivel de TI en cualquiera de sus escenarios, que impliquen una eventual afectación a la continuidad operacional, así como la integridad y confidencialidad de la información y el cumplimiento regulatorio de la institución."*

Los objetivos de gobierno y gestión de COBIT2019, en el objetivo de gestión: APO12 Gestionar el riesgo, para la práctica de gestión APO12.01 cita:

*"Recopilar datos.*
*Identificar y recopilar datos relevantes para habilitar una efectiva identificación, análisis y reporte de los riesgos relacionados con I&T.*

*1. Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con el riesgo de I&T.*
*2. Registrar datos relevantes y significativos relacionados con los riesgos de I&T en el entorno operativo interno y externo de la empresa.*
*3. Adoptar o definir una taxonomía de riesgo para las definiciones consistentes de escenarios de riesgo y categorías de impacto y probabilidad.*
*4. Registrar datos de eventos de riesgo que han causado o podrían causar impacto en el negocio conforme a las categorías de impacto definidas en la taxonomía de riesgo. Capturar datos relevantes de cuestiones, incidentes, problemas e investigaciones.*
*5. Estudiar y analizar los datos históricos de riesgo de I&T y de pérdidas experimentadas a partir de datos y tendencias externos disponibles, homólogos de la industria a través de logs de eventos de la industria, bases de datos, y acuerdos de la industria, para la publicación común de eventos.*


(506) 2299.5800
San José, Costa Rica
www.ict.go.cr
www.visitcostarica.com

*6. Para clases de eventos similares, organizar los datos recopilados y resaltar los factores causantes. Determinar los factores causantes comunes en múltiples eventos.*
*7. Determinar las condiciones específicas que existieron o estuvieron ausentes cuando tuvieron lugar los eventos de riesgo y la forma en que las condiciones afectaron a la frecuencia del evento y la magnitud de la pérdida.*
*8. Realizar un análisis periódico de eventos y factores de riesgo para identificar riesgos nuevos o emergentes y para mejorar el entendimiento de los factores de riesgo internos y externos asociados."*

**Causa**

TIC no cuenta con personal técnico especializado para la gestión de la seguridad de la información. Ante esta situación, la Gerencia General ha priorizado la contratación de una firma reclutadora, debido a que los procesos internos no han permitido cubrir las plazas vacantes[3].

**Efecto**

La ausencia de una gestión de riesgos tecnológicos liderada por un especialista en seguridad y ciberseguridad de la información puede dar lugar a la materialización de los riesgos siguientes[4]:

- Omisión de amenazas emergentes tales como: ransomware avanzado, ataques a cadena de suministro, explotación de APIs.
- Subestimación de vulnerabilidades técnicas críticas.
- No consideración de riesgos derivados de terceros o proveedores.
- Evaluaciones subjetivas sin criterios técnicos consistentes.
- Falta de metodologías formales tales como ISO 31000, NIST RMF Risk Management Framework (Marco de Gestión de Riesgos del NIST).

[3] Oficio G-0273-2026 (12/02/2026)
[4] Realizado con apoyo de Inteligencia Artificial Generativa Microsoft Copilot 365 (30/01/2026)

- Implementación de controles reactivos en lugar de preventivos.
- Configuraciones débiles en firewalls, Security Information and Event Management (Gestión de Información y Eventos de Seguridad).
- Falta de segregación de funciones y control de accesos basado en riesgos.
- Seguridad vista como tema operativo y no estratégico.
- No integración con el PETIC o plan estratégico institucional.
- Falta de indicadores (KPIs/KRIs) de ciberseguridad.

**Condición -lo que encontramos-**

2. **Prácticas de gestión para la seguridad y la ciberseguridad de la información fundamentadas en iniciativas o proyectos del Plan Estratégico de Tecnologías de Información y Comunicación -PETIC-.**

El PETIC cuenta con una propuesta cuyo borrador lo elabora la empresa DCI Dinámica Consultores Internacional S.A. mediante procedimiento 2024LE-000006-0001200001[5].

TIC indica que varias prácticas o elementos para desarrollar la gestión de la seguridad y ciberseguridad de la información están relacionadas o fundamentadas en medidas, actividades y proyectos contenidos en la propuesta del PETIC. A la fecha de emisión de este servicio, este plan no está aprobado por las autoridades correspondientes.

Los elementos o prácticas relacionados con la seguridad de la información y ciberseguridad que están incluidos en la propuesta del PETIC son las siguientes:

- Proyecto sobre arquitectura de la información, que se encargará de clasificar, gestionar y proteger la información institucional. Además de la gestión técnica

[5] Propuesta de Plan Estratégico de Tecnologías de Información y Comunicación (PETIC) 1.5 del 15 de diciembre del 2025

de la Ley de Protección de la Persona frente al tratamiento de sus datos personales con una inversión estimada en $48 000,00.

- Iniciativas para realizar políticas y procedimientos administrativos para apoyar el control interno de la seguridad de la información y el inventario de activos de Información.

- Serie de acciones relacionadas con la seguridad de la información y ciberseguridad para la implementación de las medidas -atención de lineamientos, políticas, recomendaciones, entre otros- dadas por el MCITT.

- La estructura organizacional propuesta en este plan no contempla personal especializado para la seguridad y ciberseguridad de la Información sino como funciones asignadas a otros perfiles de Administración de la Plataforma en la línea de Seguridad Informática.

- Iniciativas para servicios administrados en infraestructura de seguridad de la información y ciberseguridad para asegurar una infraestructura estable, continua, disponible e íntegra para la continuidad y efectividad de la infraestructura tecnológica con una inversión estimada en $2 663 752.

- Diseño de objetivos de control para la gestión de la seguridad para evaluar los indicadores: incidentes de seguridad, nivel de exposición de los activos tecnológicos y efectividad en la continuidad del servicio.

**Normativa técnica relacionada -criterio-**

Las Normas técnicas para la gestión y el control de las tecnologías de información del MICITT, en el Proceso III, cita:

> *"PLANIFICACIÓN TECNOLÓGICA INSTITUCIONAL*
> *La Institución debe instaurar un modelo estratégico formal que permita establecer la dirección organizacional, iniciativas a corto, mediano y largo plazo, incorporando las necesidades y oportunidades tecnológicas que permita establecer los requerimientos al nivel tecnológico para la sostenibilidad de las operaciones institucionales, así como cambio y mejora a los recursos tecnológicos instalados y las oportunidades de crecimiento y entrega de valor público. Adicionalmente, que incorpore*


(506) 2299.5800
San José, Costa Rica
www.ict.go.cr
www.visitcostarica.com

*indicadores que permitan valorar el nivel de cumplimiento de los objetivos estratégicos, las acciones de revisión y ajuste a la estrategia.*

*La Unidad de TI debe disponer de un plan de infraestructura e inversiones que permita proyectar los requerimientos de licenciamiento, mantenimiento de infraestructura tecnológica (preventiva, por obsolescencia, mejora), adquisición de nuevos recursos tecnológicos, basados en la línea estratégica institucional establecida.*

*La entidad debe establecer una Política de Innovación e investigación tecnológica donde se determinen los mecanismos necesarios para asegurar el establecimiento de un proceso continuo por medio de la Unidad de TI.*

*La Unidad de TI debe disponer de un programa de iniciativas institucionales que pueden ser habilitadas a través de la incorporación de recursos y servicios tecnológicos, respaldados debidamente por la valoración de la factibilidad y entrega de valor respectivos.*

*La Unidad de TI debe desarrollar la planificación anual operativa que oriente las acciones para asegurar la mantenibilidad y disponibilidad de los recursos tecnológicos, la incorporación de nuevas facilidades (a través de proyectos) y el presupuesto asociado a las actividades y tareas, debidamente alineadas con los objetivos estratégicos establecidos por la institución.*

*La entidad debe optimizar el uso de los recursos financieros invertidos en la gestión de TI procurando el logro de los objetivos de esa inversión, controlando en forma efectiva dichos recursos y observando el marco jurídico que al efecto le resulte aplicable."*

COBIT2019 en los Objetivos de gobierno y gestión, en el Objetivo de gestión: APO02 Gestionar la estrategia, para la Práctica de gestión APO02.05 cita:

*Definir el plan estratégico y el mapa de ruta.*
*Desarrollar una estrategia digital holística, en cooperación con las partes interesadas relevantes, y detallar una hoja de ruta que define los pasos incrementales a seguir requeridos para lograr las metas y objetivos. Asegurar el foco en la ruta de transformación, mediante el nombramiento*

*de una persona que ayude a liderar la transformación digital e impulse el alineamiento entre I&T y la empresa.*

*1. Definir las iniciativas requeridas para eliminar las brechas entre los entornos actual y el objetivo. Integrar las iniciativas en una estrategia de I&T coherente que alinee a la I&T con todas las facetas empresariales.*
*2. Detallar una hoja de ruta que defina los pasos incrementales requeridos para lograr las metas y objetivos de la estrategia de I&T. Garantizar que se incluyan acciones para formar al personal en nuevas habilidades, apoyar la adopción de nueva tecnología, mantener el cambio en toda la organización, etc.*
*3. Considerar el ecosistema externo (socios empresariales, proveedores, startups, etc.) para que contribuya a apoyar la ejecución de la hoja de ruta*
*4. Agrupar las acciones en programas y/o proyectos con una meta o entregable claros. Identificar para cada proyecto los requisitos de recursos de alto nivel, la programación de actividades, el presupuesto para la inversión/operativo, el riesgo, el impacto del cambio, etc.*
*5. Determinar las dependencias, solapamientos, sinergias e impactos entre proyectos, y priorizar.*
*6. Finalizar la hoja de ruta, indicando una programación relativa de actividades y las interdependencias entre proyectos.*
*7. Garantizar el foco en la ruta de transformación. Designar a un campeón de transformación y alineamiento digital entre la empresa y la I&T (el director de tecnologías digitales (CDO) u otro rol tradicional directivo).*
*8. Obtener el apoyo y aprobación formal del plan de las partes interesadas.*
*9. Trasladar los objetivos a resultados medibles representados por métricas (qué) y objetivos (cuánto). Asegurar que los resultados y medidas se correspondan con los beneficios empresariales.*

**Causa**

La falta de aprobación del PETIC versión 1.5 obedece a la persistencia de debilidades en su estructura, formulación y alineación estratégica con el Plan Estratégico Institucional y las guías vigentes, pese a haber transcurrido un año desde la entrega del PETI 2024–2028 por parte de la empresa proveedora y a las observaciones reiteradas por la Auditoría Interna.


(506) 2299.5800
San José, Costa Rica
www.ict.go.cr
www.visitcostarica.com

**Efecto**

Los riesgos asociados a no contar con un PETIC que autorice las medidas, actividades, iniciativas y proyectos de seguridad y ciberseguridad de la información[6] son los siguientes:

- La seguridad de la información opera de forma aislada, sin conexión con los objetivos institucionales.
- Proyectos de ciberseguridad no priorizados conforme al riesgo organizacional.
- Falta de vinculación con el Plan Estratégico Institucional.
- Dificultad para justificar presupuesto de forma técnica conforme a objetivos institucionales.
- Iniciativas sujetas a decisiones operativas coyunturales y no conforme a una estrategia.
- Prioridades determinadas por urgencias, no por análisis de riesgo.
- Ausencia de hoja de ruta plurianual para lograr las metas de implementación de seguridad.
- Percepción de la seguridad de información como función técnica y no como una estrategia integral para el Instituto.

**Conclusión**

La implementación de la segunda versión de las Políticas de Seguridad Informática, emitida en diciembre de 2022, no se ha concretado, debido a que la fase inicial de la gestión de la seguridad de la información requiere una gestión de riesgos tecnológicos liderada por personal especializado en Seguridad y Ciberseguridad de la Información, cuya ejecución es clave para la prevención de riesgos, el fortalecimiento del gobierno de TI y la protección del interés público.

[6] Realizado con apoyo de Inteligencia Artificial Generativa Microsoft Copilot 365 (16/01/2026)


(506) 2299.5800
San José, Costa Rica
www.ict.go.cr
www.visitcostarica.com

La aprobación del PETIC es un requisito previo indispensable para garantizar la validez, coherencia y efectividad de las medidas, actividades e iniciativas en Seguridad y Ciberseguridad de la Información, en apego al marco normativo técnico y a las mejores prácticas internacionales.

**Advertencia**

La Ley Orgánica del ICT, artículo 32, establece que la Gerencia es el responsable del eficiente y correcto funcionamiento administrativo de la Institución y debe ejercer las funciones inherentes a su condición de administrador general y jefe superior del Instituto, vigilando la organización, el funcionamiento y la coordinación de todas sus dependencias y la observación de las leyes, reglamentos y resoluciones de la Junta Directiva, razón por la cual, se advierte sobre:

1. La importancia de implementar una gestión de riesgos tecnológicos liderada por un especialista en seguridad y ciberseguridad de la información, que cuente con la debida independencia organizacional para la evaluación, corrección e implementación de las acciones correspondientes.

2. La necesidad y urgencia de que el ICT apruebe el PETIC, a fin de formalizar y dar sustento a las prácticas, proyectos e inversiones en materia de seguridad y ciberseguridad de la información contempladas en dicho instrumento de planificación.

Lo anterior, a efecto de valorar la posible materialización de los riesgos identificados y fortalecer el diseño y la eficacia de los controles institucionales.

**Valor agregado de la Auditoría**

El valor agregado que la Auditoría aporta a la Administración mediante la prestación de este servicio es el siguiente:

- Contribuir con el objetivo estratégico 7 “Optimizar los procesos institucionales”.

- Fortalecer el sistema de control interno cuyos objetivos se enfocan en garantizar la confiabilidad y oportunidad de la información, la eficacia y eficiencia de las operaciones y el cumplimiento normativo.


(506) 2299.5800
San José, Costa Rica
www.ict.go.cr
www.visitcostarica.com

El presente servicio se realiza con fundamento en las competencias conferidas a la Auditoría Interna en la Ley Orgánica del ICT, artículos 33 y 35, la Ley General de Control Interno, artículo 22, inciso d), las “Normas para el Ejercicio de la Auditoría Interna en el Sector Público”, norma 1.1.4 y en atención del Plan Anual de Trabajo.

Atentamente,

Romel Álvarez Navarro
Auditor interno

Félix Mata García
Auditor de TI

**ICT**
**Firmado**
**Digitalmente**
**Valide las firmas digitales**

C. Sra. Milena Moreno Rojas
Gerencia General

RAN/ fmg