AI-ADV-11-2026

GERENCIA GENERAL
AUSENCIA DE CONTRATO VIGENTE PARA LA SOLUCIÓN DE ANTIVIRUS INSTITUCIONAL

1. INTRODUCCIÓN

1.1 Origen

Esta Advertencia se origina en cumplimiento del Plan Anual de Trabajo del año 2026.

1.2 Objetivo

Advertir sobre las posibles consecuencias de determinadas conductas o decisiones a los órganos pasivos que se fiscalizan, con el fin de brindar un servicio preventivo oportuno a la administración activa de la institución.

1.3. Terminología y siglas utilizadas en la Advertencia

APO: Alinear, Planificar y Organizar.

BAI: Por sus siglas de (Build, Acquire and Implement) en español Construir, Adquirir e Implementar.

BOTNET: Red de dispositivos comprometidos controlados por un actor malicioso. En protección DNS, pueden bloquearse dominios utilizados para coordinación, comunicación o control de estos dispositivos.

COBIT: Por sus siglas de (Control Objectives for Information and Related Technologies) en español Objetivos de Control para las Tecnologías de la Información y Relacionadas.

C&C: Por sus siglas de Command and Control (Comando y Control). Se refiere a la infraestructura y los canales de comunicación que un atacante utiliza para mantener el control remoto sobre sistemas comprometidos, como parte de una botnet o tras una intrusión.

DNS: Sistema de Nombres de Dominio, por sus siglas en inglés Domain Name System. Servicio que permite traducir nombres de dominio legibles para las personas en direcciones IP u otros registros utilizados por los sistemas para establecer comunicaciones en red.

ENDPOINT: Dispositivo final que utiliza servicios tecnológicos institucionales, tales como estación de trabajo, computadora portátil, servidor, dispositivo móvil u otro equipo que pueda realizar consultas DNS y estar dentro del alcance del servicio de protección.

GTIC: Gestión de Tecnologías de la Información y Comunicación.

MALWARE: Software malicioso diseñado para afectar la confidencialidad, integridad o disponibilidad de sistemas, datos o servicios.

MICITT: Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones.

SERVICIO MDR: Servicio gestionado de ciberseguridad orientado a la detección, análisis, investigación, alertamiento, escalamiento y apoyo en la respuesta ante amenazas o incidentes de ciberseguridad, conforme al alcance definido en el pliego de condiciones, el FC y el modelo operativo ofertado.

SIREMA: Sistema de Recursos Materiales.

SICOP: Sistema Integrado de Compras Públicas.

USIT: Unidad de Servicios de Informática y Telemática.

2. DESARROLLO DE LA ADVERTENCIA

Como parte de los servicios preventivos que debe brindar la Auditoría Interna, y en el marco de cumplimiento de sus obligaciones y competencias establecidas en el artículo 22 de la Ley General de Control Interno, 8292, especialmente el inciso d); donde se dispone que: ***"d) Asesorar, en materia de su competencia, al jerarca del cual depende; además, advertir a los órganos pasivos que fiscaliza sobre las posibles consecuencias de determinadas conductas o decisiones, cuando sean de su conocimiento";*** así como lo establecido, en igual sentido, por las *Normas para el Ejercicio de la Auditoría Interna en el Sector Público*, aprobadas por la Contraloría General de la República mediante resolución R-DC-064-2014 del 11 de agosto de dos mil catorce; se presenta la siguiente información referente a algunos temas que se consideran de relevancia por las implicaciones que tienen en el cumplimiento de objetivos institucionales y las que pudieran derivarse en adelante y que se detallan seguidamente.

2.1 Vencimiento de contrato de Antivirus Institucional

El 13 de agosto de 2026, en el ejercicio de las labores ordinarias de planificación anual, esta Auditoría Interna realizó un análisis en el Sistema Integrado de Compras Públicas (SICOP) sobre el procedimiento de contratación directa 2022CD-000050-0002100001, correspondiente al licenciamiento de software y mantenimiento preventivo del antivirus institucional.

Se constató que, para el 23 de mayo de 2026, finalizó de manera definitiva e improrrogable el licenciamiento de la solución WithSecure (adquirida originalmente bajo la marca comercial F-Secure Business Suite Premium), así como su servicio de soporte técnico conexo, cuya vigencia de 4 años quedó establecida en la orden de inicio UCI-PA-973-2022, emitida por la Unidad de Compras Institucionales para el periodo del 24 de mayo de 2022 al 23 de mayo de 2026.

A raíz de lo identificado, y con el fin de ampliar la información sobre la situación del licenciamiento, esta Auditoría procedió a realizar una consulta a la USIT. Mediante oficio USIT-414-2026 del 17 de setiembre de 2026, la USIT atendió la solicitud de información formulada por esta Auditoría (AI-PTIC-092-2026). De dicho oficio se desprenden los siguientes hechos:

a) Situación Actual

La USIT indica textualmente:

> *"La contratación correspondiente a la solución de antivirus institucional WithSecure para 6.500 endpoints... finalizó el 23 de mayo de 2026 y, a la fecha de esta respuesta, no se cuenta con un instrumento jurídico vigente (contrato, adenda, prórroga u orden de pedido) que ampare la continuidad de la relación contractual con el fabricante o su representante para dicho servicio".* El subrayado no pertenece al original.

Asimismo, señala que:

> *"no existe a la fecha un instrumento jurídico vigente que respalde o regule las descargas de actualizaciones posteriores al vencimiento contractual señalado".*

Lo anterior implica que, a la fecha, la institución no dispone de:

- Soporte técnico oficial del fabricante o su representante.
- Derecho contractual a recibir futuras actualizaciones de versión del cliente de seguridad instalado en los equipos.
- Acceso a la consola de administración de la plataforma.

Esta última limitación tiene consecuencias directas sobre la capacidad de la institución para conocer el estado real de protección de sus equipos. En efecto, ante la consulta sobre la cantidad y porcentaje de los 6.500 endpoints que cuentan con el agente instalado, activo, conectado a la consola y sincronizado con las bases de firmas actualizadas, la USIT respondió:

> *"No se cuenta acceso a la consola de administración de la plataforma por lo que no es factible suministrar esta información".*

La misma respuesta se dio respecto a la fecha y versión de la última actualización exitosa de las bases de datos de virus y amenazas. Esto confirma que la USIT no cuenta con los mecanismos para determinar cuántos equipos están desactualizados, infectados o desprotegidos, tanto en la Sede Central como en las sedes regionales.

b) Trámite de compra para el relevo de la contratación vencida de Antivirus

Con el fin de conocer las gestiones realizadas por la Administración para renovar el licenciamiento del antivirus institucional una vez vencida la contratación, esta Auditoría indagó sobre el trámite planificado al efecto, obteniéndose los siguientes hechos:

La USIT inició las gestiones de contratación el 30 de julio de 2025, mediante el oficio USIT-381-2025, con la solicitud de publicación del sondeo de mercado en la plataforma de compras públicas. El aviso se publicó el 4 de agosto de 2025 y finalizó el 11 de agosto de 2025. Posteriormente, mediante el oficio SGA-45-2026 del 18 de febrero de 2026, la Subgerencia Administrativa solicitó incorporar cláusulas de escalabilidad, planes de contingencia, continuidad del servicio y una transición tecnológica hacia una plataforma de detección y respuesta de amenazas en puntos finales (EDR/XDR), lo que obligó a la USIT a reformular parcialmente el trámite. Dado lo anterior, el nuevo estudio de mercado definitivo se remitió el 24 de marzo de 2026, mediante el oficio USIT-POS-19-2026. El detalle de los códigos para el catálogo de bienes y servicios con sus respectivos precios de referencia registrados en el SIREMA, así como de los proveedores que participaron en el sondeo de mercado, se evidencia en el Anexo 1.

No obstante, el 10 de diciembre de 2025 se habían digitado las solicitudes de compra 412232 (mantenimiento) y 412225 (suscripción de licencias), las cuales no incluían las cláusulas solicitadas por la SGA posteriormente; al momento de la revisión, esta última aún se encontraba pendiente de aprobación presupuestaria y por ende no se evidencia su uso en el proceso de compra. El detalle del estado de ambas solicitudes en el SIREMA y las imágenes correspondientes se presentan en el Anexo 2.

La Subgerencia Administrativa mediante oficio SGA-201-2026 del 16 de junio de 2026 solicitó a la GTIC analizar si era conveniente para el INA ser parte del Convenio Marco para la Adquisición de Soluciones Informáticas de Ciberseguridad promovido por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) y dejar sin efecto el procedimiento licitatorio N° 2026LY-000006-0002100001.

Se evidenció la creación del trámite de compra N° 2026LY-000006-0002100001 en SICOP para la adquisición del licenciamiento, y se tenía programada su apertura para el 18 de junio de 2026, sin embargo, el 16 de junio de 2026, mediante el oficio GTIC-212-2026, se remitió una solicitud de desestimación de dicho trámite a la Unidad de Compras Institucionales parte de la GTIC. El detalle de la justificación se transcribe a continuación:

> *"De conformidad con el análisis técnico y el cuadro comparativo presentado anteriormente, se concluye que el alcance funcional, tecnológico y operativo contemplado en el Convenio Marco para Soluciones de Ciberseguridad promovido por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) supera significativamente las especificaciones técnicas establecidas en el procedimiento licitatorio No. 2026LY-000006-0002100001 promovido por el Instituto Nacional de Aprendizaje (INA)*
> *(…) En virtud de lo anterior, esta Gestión considera que la adopción del Convenio Marco promovido por el MICITT representa una alternativa técnicamente superior, más robusta y alineada con las mejores prácticas nacionales e internacionales en materia de ciberseguridad, permitiendo fortalecer significativamente las capacidades institucionales de prevención, detección, análisis, investigación y respuesta ante amenazas informáticas.*
> *Por consiguiente, y considerando el interés institucional de maximizar los niveles de protección de los activos tecnológicos, la información institucional y los servicios digitales del INA, se solicita dejar sin efecto el procedimiento licitatorio No. 2026LY-000006-0002100001 y gestionar la adhesión al Convenio Marco de Soluciones de Ciberseguridad promovido por el MICITT, el cual, según la información suministrada por el señor Gezer Ramiro Molina Colomer, encargado de ciberseguridad de dicho Ministerio, estará disponible en su segunda etapa a partir del 30 de junio de 2026".* El subrayado no pertenece al original.

c) Gestiones de la USIT para la adhesión al Convenio Marco

Se consultó el 28 de agosto de 2026 mediante el oficio AI-PTIC-092-2026 a la USIT, sobre el estado actual de una nueva contratación o el convenio marco mediante la consulta:

> *"Trámite realizado: Describa detalladamente las acciones, gestiones y procedimientos llevados a cabo por la USIT con miras a la nueva contratación (incluyendo fechas, instancias involucradas y documentación generada). Asimismo, informe el estado actual del expediente y especifique los avances en caso de utilizar la modalidad de Convenio Marco".*

La respuesta de la USIT fue la siguiente:

> *"Se adjunta línea de tiempo con el detalle de las gestiones realizadas sobre este trámite. Ver archivo .PDF línea de tiempo".*

En el mencionado documento se detalla que al 2 de setiembre de 2026, y según consta en el archivo "Correo electrónico (6)", en dicha fecha se debe iniciar con el proceso de compra que involucra:

> *"Solicitar visto bueno a la UCI, es necesario al no haberse pre digitado".*
> *"Crear el código en SIREMA y digitar la solicitud de compra".*

Las Normas de Control Interno para el Sector Público (N-2-2009-CO- DFOE) y R-DC-00057-2026, establecen:

> *"**5.7.4 Seguridad** Deben instaurarse los controles que aseguren que la información que se comunica resguarde sus características propias de calidad, y sea trasladada bajo las condiciones de protección apropiadas, según su grado de sensibilidad y confidencialidad. Así también, que garanticen razonablemente su disponibilidad y acceso por parte de los distintos usuarios en la oportunidad y con la prontitud que la requieran.* El subrayado no corresponde al original.
>
> *(…)*
> ***5.9. Control de sistemas de información.** El jerarca y los titulares subordinados, según sus competencias, deben disponer y verificar periódicamente los controles pertinentes para que los sistemas de información institucionales garanticen razonablemente la calidad, trazabilidad, oportunidad y protección de la información y la comunicación, como soporte esencial del sistema de control interno y de la gestión de la integridad pública. Dichos controles deberán asegurar la confidencialidad, integridad, disponibilidad y seguridad de la información, así como la clara asignación de responsabilidades y la adecuada administración de los niveles de acceso a la información y datos sensibles, de conformidad con el marco jurídico aplicable, la naturaleza de los procesos institucionales y los riesgos asociados al uso indebido, alteración, pérdida o divulgación no autorizada de la información.* El subrayado no corresponde al original.
>
> ***5.10 Tecnologías de información** El jerarca y los titulares subordinados, según sus competencias, deben propiciar el aprovechamiento de tecnologías de información que apoyen la gestión institucional mediante el manejo apropiado de la información y la implementación de soluciones ágiles y de amplio alcance. En todo caso, deben instaurarse los mecanismos y procedimientos manuales que permitan garantizar razonablemente la operación continua y correcta de los sistemas de información.*
>
> *En esa línea, de conformidad con el perfil tecnológico de la institución, órgano o ente, en función de su naturaleza, complejidad, tamaño, modelo de negocio, volumen de operaciones, criticidad de sus procesos, riesgos y su dependencia tecnológica, el jerarca deberá aprobar el marco de gestión de tecnologías de información y establecer un proceso de implementación gradual de cada uno de sus componentes (…)".* El subrayado no corresponde al original.

Conforme a la Directriz del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones número MICITT-DAF-DIR-001-2026 MH-DCoP-DIR-0001-2026 Directriz de Uso CM Ciberseguridad Final se indica que:

"La entrada en vigencia de dicho convenio marco, será a partir del día 30 de junio de 2026, fecha en la que dará inicio la ejecución de las opciones de negocio que quedaron en firme en la Licitación Mayor 2025LY-000002-0009300001, denominada Convenio Marco de Servicios de Soluciones de Ciberseguridad (…)

I Cobertura
El presente convenio marco cubrirá a todas las instituciones de la Administración Central y sus adscritas, quienes lo utilizarán en forma obligatoria; además de cualquier otro sujeto cubierto por el ámbito de aplicación regulado en el artículo 1 de la LGCP, como por ejemplo: municipalidades, instituciones descentralizadas , sujetos privados que utilicen fondos públicos, entre otras, los cuales pueden hacer uso del convenio siempre y cuando realicen previamente el proceso de adhesión ante la DCoP, atendiendo los requisitos estipulados en la Circular MH- DCoP - CIR - 0076 - 2024, de fecha 14 de octubre de 2024 y MH- DCoP - CIR - 0042 - 2025 , del 06 de agosto de 2025 (…)

I III. Ejecución Contractual modalidad de cotización
Conforme a lo establecido en el apartado «1.6. Etapas del Procedimiento de Convenio Marco» del pliego de condiciones, durante la etapa de ejecución contractual las instituciones usuarias del Convenio Marco deberán efectuar una adecuada planificación del servicio requerido y realizar un sondeo de mercado, previo a tramitar la solicitud de cotización en el Sistema Digital Unificado (SDU).

Para la elaboración del mismo, en primera instancia, deberá consultarse el banco de precios del SDU y, en caso de que este no cuente con información suficiente, la institución usuaria deberá obtener precios de referencia del servicio a adquirir mediante las fuentes que estime pertinentes. Los precios obtenidos servirán de insumo para determinar las bandas de tolerancia y efectuar el análisis de razonabilidad de precios de las cotizaciones presentadas por los adjudicatarios del presente Convenio Marco, con el fin de verificar que los precios cotizados sean razonables y no resulten ruinosos o excesivos. (…)".

De la Política de Seguridad Institucional del INA, se puede visualizar que:

"(…)
3. Organización del Equipo de Seguridad de la Información La Gerencia debe contar con un equipo encargado de la coordinación, implementación, monitoreo y mantenimiento de los mecanismos de seguridad de la información, asignar roles y responsabilidades, así como la generación y difusión oportuna del marco normativo de seguridad de la información. El subrayado no corresponde al original.

"7. Administración Operaciones de Redes, Comunicaciones y Deben existir mecanismos de control para proteger toda la información que opere en la infraestructura tecnológica del INA, que prevengan y detecten posibles intrusiones o robos a la información, y que de igual forma protejan toda aquella información con carácter confidencial que por necesidades de la institución deba viajar ya sea dentro de la red interna del INA o hacia Internet. Se deben definir y establecer procedimientos de seguridad que proporcionen las acciones a seguir en caso de eventos no programados. Se debe proteger la información residente en los equipos de cómputo del INA, de cualquier tipo de código malicioso". El subrayado no corresponde al original.

Del Marco Normativo Manual de Normas y Estándares de Seguridad de la Información del INA, se desprende que en:

> *"2 Términos y Definiciones (…)*
> *Responsable de Seguridad de Tecnología Informática (Seguridad TI) El Gestor de TIC o quien este designe cumplirá la función de cubrir los requerimientos de seguridad de tecnología informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la institución. (…)"*
>
> *Seguridad Informática La seguridad informática, también conocida como ciberseguridad, es el área que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, esta solamente se encarga de la seguridad en el medio informático.*
>
> *3.3 Objetivos*
> *Establecer prácticas para la implantación y mantenimiento de seguridad de la información que permita la protección de la información de los recursos de tecnología de información del INA, lo cual considera a los sistemas, redes, comunicaciones, bases de datos, y en general sistemas de cómputo; para prevenir, detectar y/o corregir cualquier problema de acceso no autorizado, autenticación, confidencialidad, negación del servicio, integridad de la información, y de no-repudio (…)".*
>
> *11.1 Del uso de los recursos informáticos*
> *Todo equipo de cómputo propiedad de la Institución debe contar con el software oficial autorizado por la GTIC y debe contar con el antivirus del INA, el cual debe ser actualizado de forma periódica y es el único que se puede utilizar para este propósito. Las personas usuarias deben velar por el correcto funcionamiento de la herramienta y reportarlo a la GTIC cuando se encuentra deshabilitado.*
> *(…)*
>
> *20.3.1 Controles Contra Software Malicioso*
> *La GTIC, a través del área de Seguridad de Tecnología Informática, es el único ente autorizado para habilitar o deshabilitar los servicios relacionados con el software de antivirus o aplicaciones instaladas para combatir el software malicioso, tanto a nivel de servidor como de los demás dispositivos. Las demás personas funcionarias de la institución no podrán deshabilitar dichos servicios por cuenta propia.*
> *(…)*
>
> *La GTIC debe velar por que las actualizaciones del software antimalware (Antivirus), así como las actualizaciones del sistema operativo u otras herramientas comerciales proporcionadas por el INA estén al día. (…)".*
>
> *Todo equipo de cómputo propiedad de la Institución debe contar con el software oficial de antivirus del INA, el cual debe ser actualizado de forma periódica y es el único que se puede utilizar para este propósito. Las personas usuarias deben velar por el correcto funcionamiento de la herramienta y reportarlo a la GTIC cuando se encuentra deshabilitado. (…)".* El subrayado no corresponde al original.

En lo referente al manejo de incidentes, el numeral 1.4 en su sección 2.4.5 del Manual de Normas Técnicas de Tecnologías de la Información del Instituto Nacional de Aprendizaje, se dispone lo siguiente:

> *"2.4.5 Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica*
>
> *La organización debe mantener la integridad de los procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o pérdida de información. Para ello debe: a. Definir previamente los requerimientos de seguridad que deben ser considerados en la implementación y mantenimiento de software e infraestructura.* El subrayado no corresponde al original.

Por otra parte, el procedimiento Protocolo de respuesta ante infección por malware se cita que:

> *"(...)*
> *2. PROTOCOLO TÉCNICO: RESPUESTA ANTE INFECCIÓN POR MALWARE*
> *(...)*
> *2.3.2 Contención Inmediata*
> *(...)*
> • *Aislar virtualmente el host si se dispone de control desde consola de gestión (Dominio/Antivirus).*
>
> *(...)*
> *1.3.3 Análisis y Clasificación*
> *(...)*
> • *Analizar logs del sistema, antivirus, tráfico de red y procesos en ejecución.*
> *(...)*
> *2.3.7 Medidas Preventivas*
> • *Todas las computadoras deben tener el antivirus institucional instalado y actualizado.*
> *(...)".*

Adicionalmente, el marco de referencia COBIT 2019, un manual internacional que sirve como guía de mejores prácticas, propone en los dominios de Alinear, Planificar y Organizar APO09 Gestionar Acuerdos de Nivel de Servicio, APO10 Gestionar Proveedores, APO13 Gestionar la Seguridad y el dominio Entregar, Dar Servicio y Soporte, específicamente en el objetivo de gestión DSS04 - Gestionar la continuidad, así como del dominio Construir, Adquirir e Implementar los objetivos BAI09 Gestión de Activos , lo siguiente:

> *"Objetivo de gestión: APO10 — Gestionar los proveedores*
> *Gestionar los productos y servicios relacionados con I&T proporcionados por todo tipo de proveedores para que satisfagan los requisitos de la empresa. Esto incluye la búsqueda y selección de proveedores, gestión de relaciones, gestión de contratos y revisión y monitorización del rendimiento de proveedores y el ecosistema de proveedores (incluida la cadena ascendente de suministro) para que sea efectiva y cumpla con la legislación".*

> *"Objetivo de gestión: APO13 — Gestionar la Seguridad*
> *Definir, operar y monitorizar un sistema de gestión de seguridad de la información.*
>
> *"Objetivo de gestión: BAI09 — Gestionar los activos*
> *Gestionar los activos de I&T a través de su ciclo de vida para asegurarse de que su uso aporta valor a un coste óptimo, continúan operativos (adecuados a su propósito), y se tienen en cuenta y están físicamente protegidos.*
> *Asegurar que aquellos activos que son críticos para soportar la capacidad del servicio son confiables y están disponibles. Gestionar las licencias de software para asegurarse de que se adquiere, retiene y despliega la cantidad óptima en relación con el uso que requiere el negocio, y que el software instalado cumpla con los acuerdos de licencia.* El subrayado no corresponde al original.

Del análisis conjunto de los hechos descritos se desprende que la institución atravesó un proceso de renovación del licenciamiento del antivirus institucional que no ha logrado concretarse desde el 23 de mayo de 2026. Lo anterior implica que la institución opera sin licenciamiento vigente, sin actualización diaria de firmas, sin acceso a la consola de administración y sin soporte del fabricante ante eventos de seguridad. Las medidas perimetrales invocadas por la USIT (antivirus en firewalls y filtrado DNS Botnet C&C) son incapaces de resguardar a las 6.500 estaciones de trabajo frente a vectores de ataque locales —como dispositivos USB o archivos adjuntos cifrados—, mientras que el propio Protocolo de respuesta ante infección por malware exige como insumo primario la realización de escaneos profundos con un antimalware local actualizado. Al encontrarse la consola desactualizada y sin administración, dicho protocolo resulta ineficaz para prevenir una infección o detener el cifrado de datos antes de que el daño se ejecute.

Este escenario expone a la institución a vulnerabilidades tecnológicas críticas al operar sin licenciamiento vigente, sin actualización diaria de firmas, sin acceso a la consola de administración y sin soporte del fabricante ante eventos de seguridad, dado que la Administración no ha realizado las acciones suficientes para garantizar la continuidad del servicio antimalware institucional. Ello podría traducirse en afectación de los servicios que brinda la institución. De ahí que esta Auditoría Interna advierta que podrían estarse materializando los siguientes riesgos:

Tipo	Riesgo	Posible materialización
Operativos	R005 Planificación de recursos	Retraso sistemático de futuros procedimientos al proyectar presupuestos desalineados con la realidad, provocando cuellos de botella recurrentes, reinicios de trámites y la imposibilidad de consolidar contratos críticos para la infraestructura tecnológica.
	R026 Atención de servicios	Parálisis parcial o total de los servicios institucionales (plataformas educativas virtuales, matrícula y sistemas administrativos) ante una eventual infección masiva en la red.

Tipo	Riesgo	Posible materialización
	R028 Eficiencia	Persistencia de una gestión administrativa reactiva, que desgasta la capacidad operativa en gestiones infructuosas, sacrificando la estabilidad de los servicios tecnológicos críticos de la institución sin una visión integral.
Financieros	R059 Ejecución presupuestaria	Riesgo de registrar subejecución presupuestaria al cierre del año, así como la necesidad de reasignar recursos de otros programas institucionales en ejercicios posteriores para solventar la contratación del licenciamiento y soporte.
Contratación e Inventarios	R023 Trámites de compra	Paralización del trámite por Convenio Marco o riesgo de caducidad de los plazos legales, obligando a la institución a recurrir a compras de urgencia, provisionales o fragmentadas que encarecen el costo de los servicios y prolongan la falta de un contrato formal.
Sistemas de información	R044 Sistemas de información	Continuar operando con una infraestructura tecnológica desprovista de plataformas de software efectivas para el monitoreo y respuesta a ciber incidentes.
	R068 Ataque cibernético	Proyección: Infección por ransomware, filtración masiva de información confidencial y destrucción de bases de datos críticas, con consecuencias financieras, operativas y reputacionales graves.

3. RESUMEN DE LO ADVERTIDO

Por lo anterior, se advierte a la Gerencia sobre la necesidad de disponer un Plan de Acción que agilice la migración hacia la solución de detección y respuesta gestionada (MDR) mediante el Convenio Marco con el MICITT.

Este plan deberá ejecutar las correcciones requeridas en SIREMA, SIF y SICOP para completar el trámite de compra con la celeridad que la situación actual demanda, garantizando la reserva presupuestaria, realizando las gestiones administrativas respectivas en la emisión de códigos de servicio y asegurando la protección integral de las plataformas e información del Instituto Nacional de Aprendizaje.

4. OBSERVACIONES

4.1 Responsabilidad del control interno

Desde la competencia de esta Auditoría Interna, es deber recordar a la administración, lo establecido en la Ley General de Control Interno, 8292, artículos 39 y 41, los numerales 38, inciso d) y 39 de la Ley contra la corrupción y el enriquecimiento ilícito en la función pública, 8422, y demás normativa aplicable, en cuanto a que, todas las personas funcionarias públicas (titulares subordinadas) que debiliten con sus acciones el sistema de control interno, u omitan las actuaciones necesarias para establecerlo, mantenerlo, perfeccionarlo y evaluarlo, según la normativa técnica aplicable, o que incumplan injustificadamente con sus deberes y funciones en materia de control interno; incurrirán en responsabilidad administrativa y civil según corresponda.

4.2 Plazo para informar sobre las acciones llevadas a cabo

En el ejercicio de las competencias conferidas legalmente a las auditorías internas, que van desde la prevención hasta el seguimiento de las decisiones y acciones que la Administración deba tomar o ejecutar, se solicita, que, en un plazo no mayor a diez días hábiles, contados a partir de la recepción de esta advertencia, se comunique por escrito a este Órgano de Control las acciones que se aplicarán en relación con lo indicado.

4.3 Responsables de la Advertencia

La Advertencia fue realizada por las personas funcionarias de esta Auditoría Interna: Sergio Daniel Rojas Solano y Silvia Elena Carranza Marín, bajo la supervisión de Didier Chavarría Chaves, Encargado del Proceso de Auditoría de Tecnologías de la Información y Comunicación.

Firmado digitalmente
Sergio Daniel Rojas Solano
Auditor asignado

Firmado digitalmente
Silvia Elena Carranza Marín
Auditora asignada

Firmado digitalmente
Didier Chavarría Chaves
Encargado de Proceso

Firmado digitalmente
Alfredo Hasbum Camacho
Auditor General

Anexo 1

Detalle del sondeo de mercado y precios de referencia registrados en SIREMA

Como parte de las gestiones de contratación para el relevo del licenciamiento del antivirus institucional, la USIT publicó el sondeo de mercado en la plataforma de compras públicas entre el 4 y el 11 de agosto de 2025. De dicho sondeo se recopilaron cotizaciones de los siguientes proveedores:

- Consorcio Fincosta
- Soluciones Digitales de Almacenamiento (SDA)
- ESET Costa Rica
- Alvione

Posteriormente, el Proceso de Operación de Servicios (POS) de la USIT realizó la normalización de códigos institucionales en el catálogo de bienes y servicios del Sistema de Recursos Materiales (SIREMA), registrándose los siguientes precios de referencia en colones (₡):

Tabla 1

Códigos Registrados en SIREMA

Código de catálogo	Descripción	Precio de referencia (₡)
59903-2000-0207	Suscripción de Licencias	186.973.142,69
10808-0001-0286	Mantenimiento preventivo	186.973.142,69

Fuente: Elaboración propia de la Auditoría Interna con base en la información remitida por la USIT en el marco del AI-PTIC-092-2026.

Posterior al oficio SGA-45-2026 del 18 de febrero de 2026, la Subgerencia Administrativa solicitó incorporar cláusulas la USIT publicó el sondeo de mercado en la plataforma de compras públicas entre el 11 de marzo de 2026. De dicho sondeo se recopilaron cotizaciones de los siguientes proveedores:

- SDA-Kaspersky.
- Fincosta – WithSecure.
- Sefisa – Trend Micro.
- Netway – Cortex.

Tabla 2

Costos del contrato vencido vs nuevo estudio de mercado

Concepto de Compra	Contrato Vencido (2022-2026) F-Secure Premium	Nuevo Estudio Mercado (2026) EDR / XDR Avanzado			% Incremento del Costo Promedio
		Precio mínimo	Precio máximo	Costo promedio	
Suscripción de Licencias	$175,306.20 USD (Total 4 años) 6,500 licencias de antivirus estándar	$956, 949.16	$1,987,509.78	$1,472,229.47 USD (Total 4 años) Incluye 3,200 licencias con EDR activo, capacitación	739.8%
Mantenimiento / Soporte	$54,240.00 USD (Total 4 años) 8 horas mensuales fijas ($1,130/mes)	$31, 710.93	$65,861.16	$48,786.05 USD (Total 4 años) Soporte por demanda (384 horas tope)	-10.05%
Presupuesto Total	$229,546.20 USD (Impuestos Incluidos)			$1,521,015.52 USD (Impuestos Incluidos)	562.62%

Fuente: Elaboración propia de la Auditoría Interna con base en la información obtenida de los Sistemas Institucionales y en el marco del AI-PTIC-092-2026.

Anexo 2

Estado de las solicitudes de compra 412232 y 412225 en SIREMA

Para continuar con el proceso de compra respectivo, el 10 de diciembre de 2025 se digitaron las siguientes solicitudes de compra en el SIREMA:

N° de solicitud	Objeto	Estado en SIREMA
412232	Servicio de mantenimiento	Aprobado Presupuestario
412225	Suscripción del licenciamiento	Aprobado (pendiente de Aprobado Presupuestario)

Al momento de la revisión efectuada por este órgano de control, la solicitud número 412225 aún se encontraba pendiente de aprobación presupuestaria para el proceso respectivo de compra.

Imagen 1

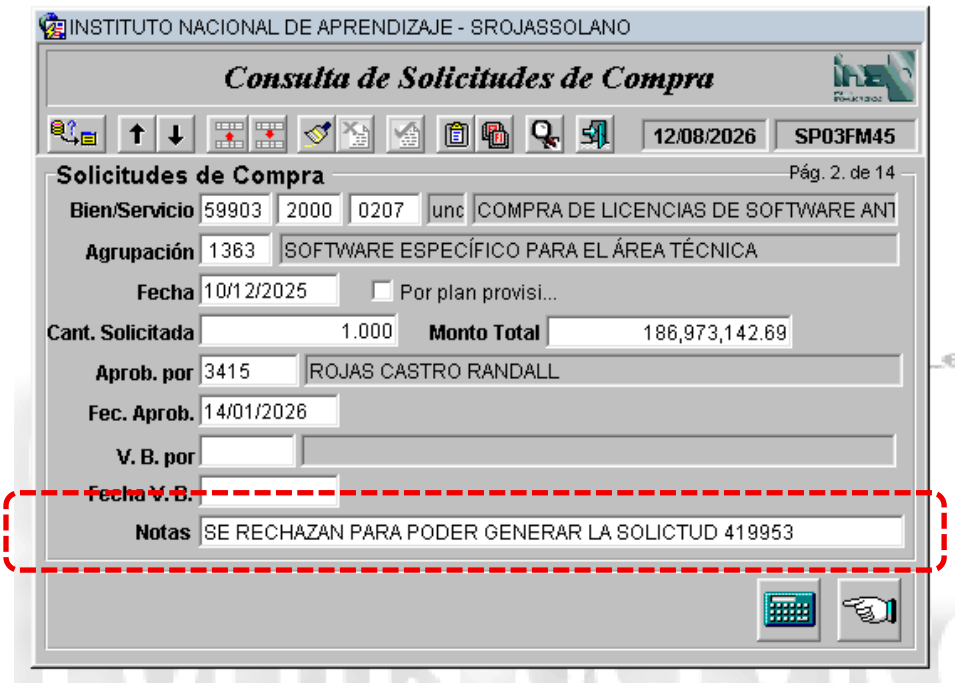
Detalle de solicitud de compra de licencias número 412225



Fuente: SIREMA

Imagen 2

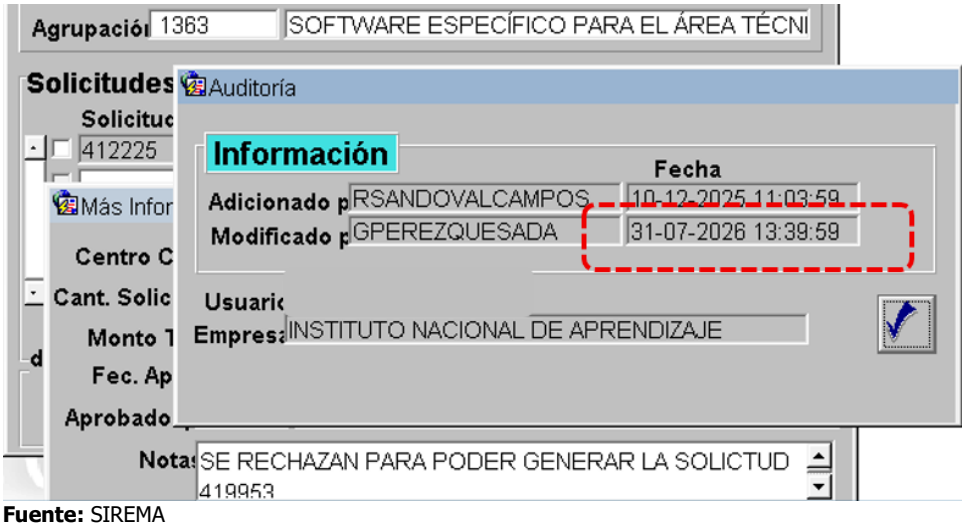
Detalle de falta de V.B presupuestario y rechazo de la solicitud de compra de licencias número 412225



Fuente: SIREMA

Imagen 3

Detalle de cancelación definitiva de solicitud de compra 412225



Fuente: SIREMA

Imagen 4

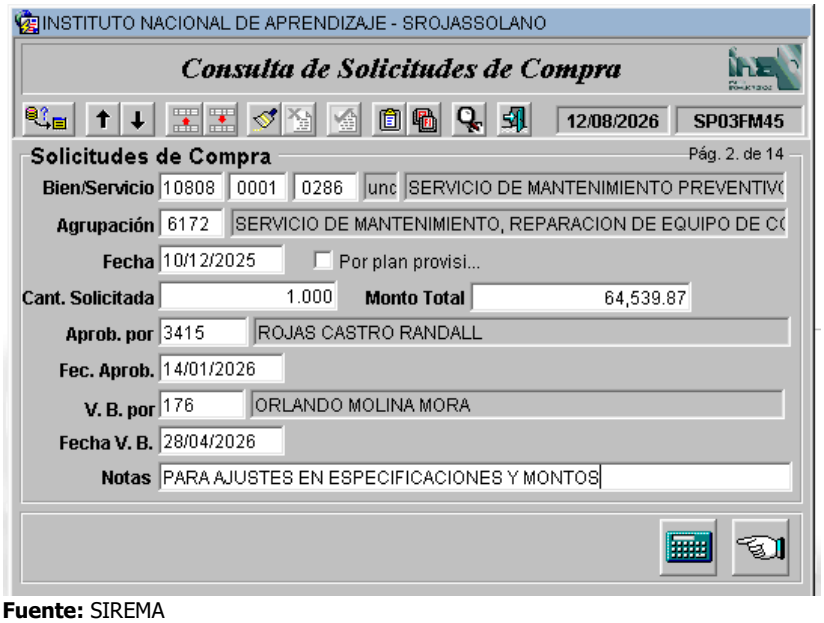
Detalle de solicitud de compra de licencias número 412232



Fuente: SIREMA

Imagen 5

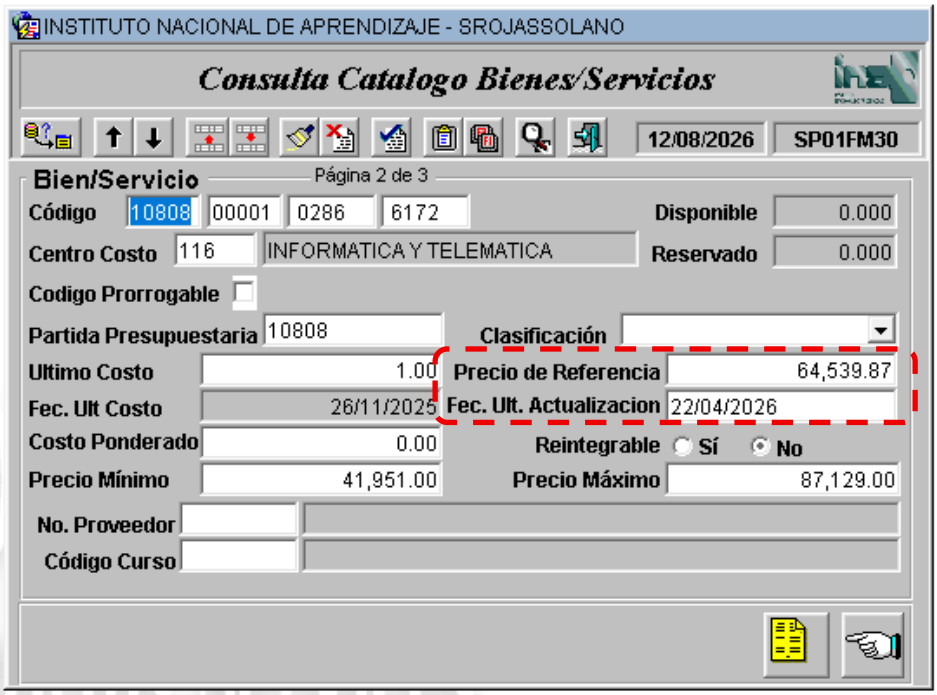
Detalle de V.B presupuestario otorgado a la solicitud de compra de licencias número 412232



Fuente: SIREMA

Imagen 6

Detalle de actualización de información del código para la solicitud de compra 412232



Fuente: SIREMA