AI-ADV-12-2026

GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN ADVERTENCIA SOBRE INSTALACIÓN DE APLICACIONES MEDIANTE MICROSOFT STORE

1. INTRODUCCIÓN

1.1 Origen

La presente Advertencia se origina en cumplimiento del Plan Anual de Trabajo de la Auditoría Interna.

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.

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: ***"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.

El 14 de septiembre de 2026 la Presidencia Ejecutiva y Gerencia General generó una serie de comunicaciones a diferentes personas funcionarias donde se les indicaba que se *"registra instalado en el equipo de cómputo institucional la aplicación o software denominado: Move Mouse".*

En informes de control interno anteriores relacionados con la gestión de la seguridad de la información, la Auditoría Interna identificó debilidades en la implementación de medidas correctivas, la valoración de riesgos de TI, la normativa interna de seguridad y la gestión de Active Directory. Estos aspectos se relacionan con la situación identificada en Microsoft Store, debido a que inciden en la definición y aplicación de controles para restringir permisos, administrar los equipos y prevenir la instalación de aplicaciones no autorizadas.

Microsoft Store se encuentra integrado al entorno de Windows y permite a los usuarios acceder a aplicaciones desde una aplicación propia del sistema operativo. Asimismo, la interfaz utiliza para determinadas aplicaciones opciones como "**Obtener**", mediante las cuales el usuario puede incorporar aplicaciones al equipo. Esta condición adquiere relevancia en un ambiente institucional, debido a que, al tratarse de una aplicación integrada en Windows y disponible en los equipos de trabajo, el usuario podría interpretar que las aplicaciones disponibles mediante esta plataforma se encuentran habilitadas o autorizadas para uso institucional. Además, el término "**Obtener**" no necesariamente permite distinguir con claridad que la acción implica instalar una nueva aplicación al equipo.

Por esta razón, la seguridad no debería depender únicamente de que el usuario identifique cuáles aplicaciones puede o no utilizar, sino de la existencia de controles técnicos preventivos que restrinjan la instalación o incorporación de software no autorizado, de acuerdo con las necesidades y lineamientos institucionales. En ese sentido, la situación evidencia un riesgo que debió ser considerado durante la configuración y administración de los equipos institucionales, particularmente respecto al acceso a Microsoft Store, los privilegios otorgados a los usuarios, las aplicaciones permitidas y los mecanismos para prevenir la incorporación de software que no haya sido previamente evaluado y autorizado.

En las Normas de Control Interno para el Sector Público, se establece:

> *"**4.3.3. Regulaciones y dispositivos de seguridad.***
> *El jerarca y los titulares subordinados, según sus competencias, deben disponer y vigilar la aplicación de las regulaciones y los dispositivos de seguridad que se estimen pertinentes según la naturaleza de los activos y la relevancia de los riesgos asociados, para garantizar su rendimiento óptimo y su protección contra pérdida, deterioro o uso irregular, así como para prevenir cualquier daño a la integridad física de los funcionarios que deban utilizarlos".*

Asimismo, en el Manual de Normas Técnicas de Tecnologías de la Información del Instituto Nacional de Aprendizaje, se dispone lo siguiente:

> *"2.4.4 Control de acceso*
> *La organización debe proteger la información de accesos no autorizados.*
> *Para dicho propósito debe:*
> *(…)*
> *e. Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de necesidad de saber o menor privilegio. Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones.*
> *f. Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. Ello debe acompañarse de un procedimiento que contemple la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares.*
> *(…)*
>
> *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.*
> *b. Contar con procedimientos claramente definidos para el mantenimiento y puesta en producción del software e infraestructura.*
> *c. Mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, mantenimiento y producción.*
> *d. Controlar el acceso a los programas fuente y a los datos de prueba".*

Según lo definido en el Marco Normativo (Manual de Normas y estándares de seguridad de la información), se indica:

> *"**11.2 Restricciones en la instalación de software**.*
> *• Es responsabilidad de la GTIC definir el software y hardware autorizado, estableciendo los mecanismos respectivos para instituir su operatividad. Esta definición debe estar alineada con los objetivos del INA.*
> *• Se prohíbe la descarga, instalación, implementación o uso de software no autorizado y/o sin licenciamiento.*
> *• La GTIC debe llevar a cabo revisiones periódicas del software instalado y los datos almacenados en los equipos de la Institución. En caso de que se detecte la presencia de software no autorizado, la GTIC debe investigar y recomendar lo que corresponda.*
> *• La GTIC debe definir y aplicar unas normas estrictas sobre qué tipos de software pueden instalarse.*
> *• La GTIC debe aplicar el principio de menor privilegio en la asignación de derechos y accesos a los recursos informáticos de las personas funcionarias tomando en cuenta sus funciones.*
> *//*
> ***22.5 Control de Acceso al Sistema Operativo***
> *22.5.1 Identificación Automática de Terminales*

El Responsable de Seguridad de la Información junto con la GTIC realizarán una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

22.5.5 Uso de Utilitarios de Sistema
Existen programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Su uso será limitado y minuciosamente controlado".

Adicionalmente, el marco de referencia COBIT 2019, un manual internacional que sirve como guía de mejores prácticas, propone en el dominio Entregar, Dar Servicio y Soporte, específicamente en los objetivos de gestión DSS05 - Gestionar los servicios de seguridad:

*"**DSS05.03 Gestionar la seguridad de endpoint**.*
Garantizar que los dispositivos de punto final (Endpoint, término en inglés) (p.ej., ordenador portátil, ordenador de sobremesa, servidor y otros dispositivos móviles o de red o software) tengan una seguridad a un nivel igual o superior al de los requisitos de seguridad definidos para la información procesada, almacenada o transmitida.

***DSS05.04: Gestionar la identidad del usuario y el acceso lógico**.*
Asegurarse de que todos los usuarios tienen derechos de acceso a la información de acuerdo con los requisitos del negocio. Coordinarse con las unidades del negocio que gestionan sus propios derechos de acceso en los procesos de negocio".

Derivado de lo anterior y en atención a la situación identificada, conforme a la estructura de riesgos institucional (SICOI), se identifica la posible materialización de los siguientes riesgos:

Tipo	Riesgo	Posible materialización
Operativos	R026 Atención de servicios	Suspensión o disminución de servicios institucionales como consecuencia de incidentes originados por aplicaciones instaladas en los equipos.
	R028 Eficiencia	Controles de seguridad implementados insuficientes para gestionar adecuadamente los equipos y prevenir instalaciones no autorizadas.
	R029 Normativa interna inadecuada	Existencia de normas o procedimientos insuficientes o desactualizados para regular la instalación, autorización y control de aplicaciones en los equipos institucionales.
Sistemas de Información	R043 Confiabilidad de la información	Alteración, eliminación o modificación no autorizada de información institucional por aplicaciones instaladas sin evaluación previa.
	R044 Sistemas de información	Afectación del funcionamiento de los sistemas institucionales por incompatibilidades, conflictos o interferencias generadas por aplicaciones no autorizadas.

Tipo	Riesgo	Posible materialización
	R066 Confidencialidad	Acceso, recopilación o transmisión no autorizada de información restringida disponible desde los equipos institucionales.
	R068 Ataque cibernético	Ingreso de software malicioso o aprovechamiento de vulnerabilidades que pueda ocasionar daños, robo de información o interrupción de servicios.
Integridad	R033 Cumplimiento de normativa jurídica y técnica	Incumplimiento de normativa técnica o disposiciones institucionales aplicables al control de software y seguridad de los equipos.
	R036 Seguridad	Exposición de las personas funcionarias a riesgos de seguridad derivados del uso de aplicaciones no evaluadas que podrían comprometer la confidencialidad, integridad o disponibilidad de la información y de los equipos institucionales.

3. RESUMEN DE LO ADVERTIDO

Por lo expuesto anteriormente, se advierte a la Gestión de Tecnologías de Información y Comunicación sobre la necesidad de revisar y fortalecer los controles de seguridad establecidos en los equipos institucionales para la instalación y ejecución de aplicaciones, incluyendo Microsoft Store y otros mecanismos disponibles en Windows, de manera que:

- Se permita únicamente la instalación y ejecución de aplicaciones previamente revisadas y autorizadas por la institución.

- Se restrinjan los permisos de los usuarios para instalar o modificar aplicaciones sin la autorización correspondiente.

- Se establezcan configuraciones de seguridad que reduzcan la posibilidad de incorporar aplicaciones que puedan representar un riesgo para los equipos o la información institucional.

- Se mantengan actualizados los mecanismos de protección contra amenazas en los equipos y activos tecnológicos.

Lo anterior, considerando el principio de menor privilegio, según el cual los usuarios deben disponer únicamente de los permisos necesarios para el desempeño de sus funciones, evitando que puedan instalar o ejecutar aplicaciones no autorizadas cuando dicha capacidad no sea requerida para sus labores, de manera que la seguridad no dependa exclusivamente de las decisiones de las personas usuarias.

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, todos los funcionarios públicos (titulares subordinados) 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, de manera respetuosa, 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 Fiscalización las acciones que se aplicarán en relación con lo indicado.

4.3. Responsables de la advertencia

La advertencia fue realizada por la persona funcionaria de esta Auditoría: Albertina Cruz Casco, bajo la supervisión de Didier Chavarría Chaves, Encargado del Proceso de Auditoría de Tecnologías de la Información y Comunicación.

Firmado digitalmente
Albertina Cruz Casco
Auditora Encargada de la Advertencia

Firmado digitalmente
Didier Chavarría Chaves
Encargado de Proceso

Firmado digitalmente
Alfredo Hasbum Camacho
Auditor General