# Informe sobre el cumplimiento del Decreto Nº 37549-JP Protección de los Programas de Cómputo DNN.

## INF-03-2016

## Tabla de contenido

## Resumen Ejecutivo

Este informe es el resultado de un estudio de auditoría programado en el Plan de trabajo de la Auditoría del año 2016, orientado a evaluar los controles establecidos en la Unidad de Administración de Software de la Unidad de Tecnología de Información y Comunicación sobre los programas contenidos en los equipos de cómputo de la Dirección Nacional de Notariado, para efectos de determinar la razonabilidad , garantizar el uso autorizado, la salvaguarda de los recursos públicos, y el cumplimiento de la normativa.

El estudio comprendió la revisión de los controles establecidos para administración de las Licencia de Software que es una especie de contrato, en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado programa, principalmente se estipulan los alcances de uso, instalación, reproducción y copia de estos productos.

La Dirección Nacional de Notariado cumple con lo establecido en el decreto Ejecutivo No 37549-JP.

Se revisaron los servicios contratados con la empresa Racsa, llamados escritorios virtuales, se identificó que cinco de éstos se han asignado en forma no oportuna.

Además se observa que la administración en el Sistema Bos TecApro no se da una segregación de control con los permisos de este sistema, ya que la persona que lleva el control de los roles de autorización y los permisos del sistema es la misma que coordina las tareas en las áreas de trabajo.

## I. Introducción

### 1.1 Origen del Estudio

El presente estudio se realizó de conformidad con el Plan de Trabajo Anual del año 2016, de esta Auditoría Interna. En cumplimiento con el Decreto 37549-JP, sobre la aplicación del Reglamento para la protección de los programas de cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central.

### 1.2 Objetivo del Estudio

Evaluar los controles establecidos sobre las licencias de los sistemas informáticos de la Institución, para efectos de determinar la razonabilidad de estos para garantizar el cumplimiento de la normativa vigente.

### 1.3 Alcance

Comprendió la evaluación de los controles existentes en la Unidad de Tecnologías de Información y Comunicación, sobre las licencias de los sistemas informáticos de la Dirección Nacional de Notariado, así como de las acciones realizadas por esa Unidad para cumplir con las disposiciones contenidas en el Decreto Ejecutivo No 37549-JP, orientado al uso legal de software en el Gobierno Central comprendido en los periodos del 2015 a la fecha. Este estudio se realizó de acuerdo con la normativa aplicable a la Ley General de Control Interno, Nº. 8292, Normas de Control Interno para el Sector Público, el Manual de Normas Generales de Auditoría para el Sector Público", R-DC-064-2014, dictadas por la Contraloría General de la Republica, Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE).

### 1.4 Comunicación oral de resultados

Los resultados que contiene este informe fueron presentados el 28 de mayo del 2016, con los señores: M.Sc. Guillermo Sandi Baltodano, Director Ejecutivo y Lic. Adolfo Barquero Picado, Coordinador de Unidad de Tecnologías de Información y Comunicación.

### 1.5 Normativa relacionada en materia de control y atención de informes.

A fin de prevenir efectos negativos por inobservancia de la legislación vigente, a continuación se transcriben los artículos de la Ley General de Control Interno N° 8292 (LGCI), que regulan los deberes del jerarca y titulares subordinados en materia de control y atención de informes.

*Artículo 36. —Informes dirigidos a los titulares subordinados.// Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera: a) El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados .b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además, deberá ordenar la implantación de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes. c) El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda."*

*"Artículo 39. —Causales de responsabilidad administrativa. // El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios.//El jerarca, los titulares subordinados y los demás funcionarios públicos incurrirán en responsabilidad administrativa, cuando 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.//(…) Igualmente, cabrá responsabilidad administrativa contra los funcionarios públicos que injustificadamente incumplan los deberes y las funciones que en materia de control interno les asigne el jerarca o el titular subordinado, incluso las acciones para instaurar las recomendaciones emitidas por la auditoría interna, sin perjuicio de las responsabilidades que les puedan ser imputadas civil y penalmente…"*

## II- Resultados

### 2.1 Cuestionario sobre el cumplimiento del Decreto Nº 37549-JP.

Se aplicó cuestionario relacionado con los controles y cumplimientos del Decreto Nº 37549-JP del Reglamento para la protección de los programas de cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central, al encargado de la área de Tecnología de Información, el señor Adolfo Barquero picado, mediante el correo electrónico del día 19 de abril de 2016. Dicho cuestionario contemplo los siguientes aspectos como mantener los sistemas de inventarios actualizados y la documentación probatoria de las licencias de software adquiridas e instaladas en los equipos y cuáles son estos métodos de recuperación por pérdidas de documentación.

Según respuesta del cuestionario enviado a esta Auditoría Interna el día 04 de mayo del 2016, se observa que esta Unidad de Tecnología de Información cumple con los requerimientos que dicta el Decreto Nº 37549-JP.

**Sobre el Sistema de Inventario de Software**

## 2.2 Licencias de Sistemas Operativos Microsoft Windows 7 y 8.

Quien tiene a cargo las licencias de Software es la Lic. Magda Gutiérrez Duran, según lo indicado por ella verbalmente, el día 06 de mayo del 2016 el proveedor Consulting Group "*lleva un control y administra las licencias en medida que la institución va evolucionando, se verifica y efectivamente se lleva con el programa SAM, este lo que buscan es dar visibilidad de que la organización no tenga mayor número de instalaciones en comparación a la cantidad de licencias y versiones que han comprado atravez de algún esquema de licenciamiento autorizado por Microsoft, indicando que cada licencia puede ser actividad solamente una vez en el equipo correspondiente".*

Las licencias están relacionadas con el equipo adquirido por lo tanto cada equipo tiene su control y licencia o clave de producto desde el momento de la compra del equipo. Se realizó el inventario y se verificaron la totalidad de las licencias de Microsoft office que se encuentran instaladas y autorizadas por el proveedor y la institución. Existen 44 licencias con equipo de escritorio con Windows 7 y 21 Tablet con Windows 8 sumando un total de 65 licencias instaladas.

## 2.3 Licencias de Sistemas Operativos Plataforma Virtual.

La Dirección Nacional de Notario cuenta con un contrato de servicio de 44 Remote DESKTOP Services (Usuarios de escritorios compartidos) con la compañía Racsa, esta empresa es la encargada de dar esos servicios.

Se verificó el uso y las instalaciones de estos cuarenta y cuatro escritorios virtuales, y se observó que treinta y nueve de estos se encuentran en uso por los funcionarios de la Institución y los cinco restantes están instalados en lugares distintos en la administración (sala de capacitación, sala consejo y sala de reuniones y los dos restantes asignados a funcionarios pero sin instalar). Éstos cinco escritorios virtuales no se están aprovechando de manera eficiente y eficaz, ya que en los lugares que se encuentran instalados no hay

necesidad de establecer seguridad con la información e incluso no se utilizan continuamente estos escritorios virtuales.

Se le consultó vía correo electrónico el día 19 de mayo del año en curso, al señor, Adolfo Barquero Picado, encargado de la Unidad de Tecnología de Información y a cargo de administrar este contrato, las razones de gestionar estos cinco escritorios virtuales de esta forma. El señor Barquero, el día 20 de mayo 2016, responde lo siguiente:

> *"Cuando se inició con el proceso de compra de equipos livianos como Thin clients y tabletas, se había establecido que cada uno tendría asignado un escritorio virtual. Con la última compra de Tablets , se solicitaron 3 adicionales para las pantallas en las áreas de capacitación y para estas tablets había asociado un escritorio virtual.*
>
> *La idea original era de tener la posibilidad de acceso a los sistemas a través de estos equipos por medio escritorio virtual, sin embargo, se han usados los escritorios virtuales a través de estos equipos solo en algunas ocasiones , pero no con la frecuencia que se esperaba. Ante esto, estaba dentro de nuestros planes reasignarlos pero por la atención de otros asuntos prioritarios no los habíamos podido asignar. Los otros dos escritorios no asignados son de los funcionarios Melvin Rojas y Alexander Zeledón, que por en su momento y por la naturaleza de su trabajo prefirieron no usarlos todavía, y no habían sido asignados por la razón anterior.*
>
> *Para resolver la situación de inmediato, se están asignando dichos escritorios a otros funcionarios.*
>
> *Inmediatamente después de que todos los escritorios virtuales estén asignados, le proporcionaré la lista completa. No omito manifestarle que quedarán algunos sin funcionario asignado y quedarán a nombre del*
>
> *Puesto, dado que los funcionarios están por contratarse y el escritorio virtual para ellos debe estar disponible para cuando se presenten a laborar".*

Al no tener un control oportuno para administrar estos escritorios virtuales la administración podría estar asumiendo gastos de alquiler de estos servicios en forma

ineficiente. Ya que el costo mensual de este servicio equivale por cada uno a ¢36.266.65, quiere decir que la administración están pagando ¢181.333.26 colones al mes por los cinco escritorios virtuales sin uso adecuado.

La Unidad de Tecnología Información debe administrar este contrato con la empresa RACSA, en forma eficaz, eficiente y oportuna, y distribuir estos escritorios virtuales a funcionarios que ejecuten diariamente información sensible, y así minimizar el riesgo con la información manipulada por los funcionarios y sus respaldos de seguridad que da esta empresa a la Institución.

## 2.4 Licencias de Microsoft Office Professional 2010 y Standart 2013.

Esta Auditoría Interna verificó la totalidad de las licencias de Microsoft office profesional 2010 y Standart 2013, las que se encuentran instaladas por la institución y autorizadas por el proveedor. Se identificaron 86 licencias en total, derivándose en 50 licencias de Microsoft Office 2013 y 36 Microsoft Office 2010.

## 2.5 Licencia Newlicense Eset Endpoint Security

Se revisó la licencia Newlicense Eset Endpoint Security, esta se utiliza para detectar todo tipo de amenazas que circulen por la web; el motor heurístico le permite detectar amenazas nuevas aún desconocidas o del tipo 0-day.

Además puede administrar completamente todas las soluciones de ESET desde una única consola de administración. Se realizó una muestra y no se determinó ninguna inconsistencia.

Esta licencia le garantiza a la Dirección Nacional de Notariado, instalar en 80 equipos hasta el 17 noviembre del 2016, de lo cual se verificó que dichas licencias están instaladas en los equipos de los funcionarios de la Institución.

**2.6 Licencia del Sistema Bos TecApro.**

En cuanto al Sistema de información utilizado en la Unidad de Administración denominado BOS de TecApro, se utiliza los módulos de Contabilidad, Control Bancario, Activos Fijos, Presupuesto, Inventarios y Nómina, de lo cual se encuentra la certificación firmada el 20 de noviembre del 2013 de dicha compra con la empresa TecApro de Costa Rica S.A.

Se verificaron los procedimientos definidos para los perfiles, roles y niveles de privilegio de los usuarios del Sistema de Bos7- TecApro y para la identificación y autenticación para el acceso a la información y se solicitó por medio de correo electrónico el día 05 de abril del 2016, al Jefe de la Unidad Administrativa para verificar lo siguiente:

1¿Cuáles son los procedimientos definidos para los perfiles, roles y niveles de privilegio de los usuarios del Sistema de Bos7- TecApro y para la identificación y autenticación para el acceso a la información. El señor Zeledon indica:

> *En relación con los perfiles, roles y niveles de privilegio, los mismos se definieron desde la adquisición del Sistema con la guía y apoyo del Proveedor de la herramienta y la Jefatura de Informática y de conformidad con el área de trabajo del usuario. A cada uno de los funcionarios de la Unidad Administrativa que laboran en cada uno de los módulos que componen el Sistema Bos, a saber, Presupuesto, Contabilidad, Inventario, Compras, Cuentas por pagar, Control Bancario y Nómina se les asignó perfil, rol y nivel de privilegio conforme a sus obligaciones. A este servidor, junto con el Jefe de la Unidad de Informática se les asignó en ese mismo momento el perfil de Administrador del Sistema para que designaran los perfiles y roles conforme a las responsabilidades asignadas a cada persona. Así mismo a este servidor se le asignó rol de aprobación para aquellos procedimientos que así lo requirieran.* (El destacado no es del original).

2- ¿A quién se le asignó oficialmente la administración del Sistema Bos7- TecApro? El señor Zeledon indica.

*Como le expliqué en el punto anterior entre el Proveedor del Sistema, la Jefatura de Informática y este servidor como órgano fiscalizador de la contratación se me asignó el rol de administrador del Sistema Bos7-Tecapro.*

Se observa que el proceso de control de los roles y niveles de privilegio de los usuarios del Sistema de Bos7- TecApro lo ejecuta el Jefe de la Unidad de la Administrativa-Financiera, quién es el mismo que tiene a cargo la coordinación de todo lo relacionado con la materia financiero-contable, contratación administrativa; aprueba gastos y cuenta con autoridad financiera.

La Institución está incumpliendo con las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) que indica:

***1.4.4 Seguridad en las operaciones y comunicaciones***

*La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información.*

*Para ello debe:*

*a. Implementar los mecanismos de control que permitan asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información.*

*b. Establecer procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativos al manejo y desecho de esos medios.*

*c. Establecer medidas preventivas, detectivas y correctivas con respecto a software "malicioso" o virus.* (El destacado no es del original).

***1.4.5 Control de acceso***

***La organización debe proteger la información de accesos no autorizados.***

*Para dicho propósito debe:*

*a. Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación.*

*b. Clasificar los recursos de TI en forma explícita, formal y uniforme de acuerdo con términos de sensibilidad.*

*c. Definir la propiedad, custodia y responsabilidad sobre los recursos de TI.*

*d. Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI.*

*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.*

*i. Establecer controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios.*

*j. Establecer los mecanismos necesarios (pistas de auditoría) que permitan un adecuado y periódico seguimiento al acceso a las TI.*

*k. Manejar de manera restringida y controlada la información sobre la seguridad de las TI.* (El destacado no es del original).

***1.4.6 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.* (El destacado no es del original).

No es conveniente que una misma persona tenga concentradas todas las tareas de control del Sistema Bos TecApro, y este sea el jefe que coordina y ejecuta las tareas con estas áreas que utilizan el sistema, no habría imparcialidad y objetividad con el uso y administración del Sistema.

La Institución podría asumir responsabilidades al no proteger y establecer controles para 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. Además, el propósito de establecer una adecuada planificación, organización, dirección, control y evaluación de los sistemas de información computadorizados es de la Unidad de Tecnología de Información, como lo indican las Normas técnicas para la gestión y el control de las Tecnologías de Información, emitidas por la Contraloría General de la República.

## 2.7 Licencias Windows Server 2008 R2.

Windows Server es una línea de productos para servidores de Microsoft Corporation. El nombre se ha utilizado en las versiones de Microsoft Windows para servidores.

Se verificó con el Ing. Fabián Mora Hernández de la Unidad de Tecnología de Información la existencia de los permisos utilizados y aprobados por el proveedor y cumple con lo establecido por el proveedor.

# III CONCLUSIONES

Se determinó que las licencias utilizadas por la Dirección Nacional de Notariados, a saber: Microsoft Office 2010 y 2013, Microsoft Windows, Windows Server 2008 R2 y la Licencia Newlicense Eset Endpoint Security, están todas las que se adquirieron, no existen faltantes.

Se revisó los servicios contratados con la empresa Racsa, llamados escritorios virtuales, se comprobó que cinco de estos los asignaron a las diferentes salas de reuniones y los dos restantes se le asignaron a funcionarios que no les fue instalado, lo que implica que no se está siendo eficiente y eficaz con el manejo de los recursos públicos.

Además, se observa que la administración en el Sistema Bos TecApro, no se da una segregación de control de los permisos, ya que la persona que lleva el control de los roles de autorización y los permisos del sistema, para cualquier cambio que se deba realizar, es el mismo que coordina y ejecuta las tareas en las áreas de trabajo.

## V RECOMENDACIONES.

**Señor Director Ejecutivo.**

Con el propósito de cumplir con el Decreto N° 37549-JP e impulsar avances efectivos en el desempeño de la organización que a su vez, se traduzcan en el logro de una gestión más eficaz, eficiente, orientada a la satisfacción oportuna de las necesidades de sus ciudadanos y apegada al ordenamiento jurídico, se emite las siguientes recomendaciones.

1- Analizar lo antes posible el traslado del control de los roles existentes en el Sistema de Bos TecApro, para que sea únicamente la Unidad de Tecnología de Información quien administre los perfiles, privilegio de los usuarios de dicho Sistema. (Ver punto 2.3).

2- Girar instrucciones a la Unidad de tecnología de información para que administre los escritorios virtuales de forma oportuna y que después de comunicado este informe, asigne estos cinco escritorios a funcionarios que realicen tareas diarias con información sensibles. (Ver punto 2.6).

MAFF. Xinia Solís Torres
Auditora Interna