San José, 04 de abril de 2017
AI-SAD-002-2017

Máster
Guillermo Sandí Baltodano
Director Ejecutivo

Asunto: Servicio preventivo de advertencia sobre el control y uso de los roles autorizados a los funcionarios de la DNN en el Sistema Notarial.

Estimado señor:

Éste servicio, se realiza con fundamento en la competencia de asesoría y advertencia establecida a la Auditoría Interna en el inciso d) del artículo 22 de la Ley General de Control Interno sobre los servicios preventivos de asesoría y advertencia, así como lo señalado en la norma 1.1.4. del documento denominado Normas para el ejercicio de la Auditoría Interna en el Sector Público, emitidas por la Contraloría General de la República; disposiciones referidas al deber de asesorar, en materia de su competencia, al jerarca del cual depende, y advertir a los órganos pasivos que fiscaliza, sobre las posibles consecuencias de determinadas conductas o decisiones contrarias al ordenamiento jurídico o técnico, cuando sean de su conocimiento.

El servicio tiene como objetivo advertir al señor Director Ejecutivo, sobre el control de acceso a los roles y autorizaciones para el uso del Sistema Notarial.

La Dirección Nacional de Notariado, cuenta con un Sistema Notarial Automatizado, se evidencio en los acceso de claves de ese sistema que se le asigna a diferentes usuarios el ingreso a las aplicaciones de ingresar, modificar y eliminar cualquier producto que genera el mismo, en otras palabras, no existe ninguna limitación sobre la segregación de funciones, la situación hallada representa un debilitamiento al control interno y a las Normas Técnicas para la gestión y el control de las Tecnologías de Información emitidas por la Contraloría General de la Republica,

Por lo que seguidamente se expone en detalle lo revisado:

El 14 de marzo, se solicita a la unidad de Tecnología de Información por vía correo un detalle de los roles de cada funcionario y área donde se aplica el procedimiento y cuáles labores realizan según el rol asignado. La Unidad Tecnología de Información nos emite un inventario que detalla el responsable y sus roles de accesos para el uso del sistema.

En la revisión de dicho inventario se identificó un usuario que no tiene limitación a los accesos por ser el jefe encargado de las Unidades de Servicio al Cliente Notarial y con recargo de la Unidad de Fiscalización Notarial, en otros tres usuarios se identificó permisos de más, que no corresponden a sus funciones según el puesto que ocupa y en las reentrar expedientes los jefes tienen autorización.

Se detalla en el siguiente cuadro los casos del usuario que tiene todos los permisos para ingresar, modificar y eliminar la información del sistema sin limitaciones y se detalla lo que puede realizar con dichos permisos.

Usuario. csanabria.

Nombre ROL	Lo que se puede realizar con el permiso.
ADMINISTRACION CATALOGOS	Permite la modificación de los catálogos del sistema, provincias, estados, tipos entre otros.
ADMINISTRADOR DNN	Administrador de catálogos, administrador de sanciones, administrador de tomos de protocolo, administrador cuotas, administrador de estados, **Habilitaciones de notarios**, administrador documentos, notificación, interfaces.
ADMNISTRAR NOTARIOS ELIMINAR	Permite administrar información del notario, **habilitacione**s, direcciones, denuncias del juzgado, medidas cautelares, teléfonos.
CERTIFICACIONES	Impresión y consulta de notificación.
CONSULTA A BITACORA	Consulta la bitácora del sistema,
CONSULTAR RNN	Consulta de sanciones, consulta de notarios, consulta de expedientes, consulta de régimen disciplinario.
DENUNCIAS JUZGADO NOTARIAL	Consulta de denuncias, seguimientos de denuncias al juzgado, acceso al menú de registro de notarios.
INTERFACES	Acceso a las interfaces del sistema como menú de procesos, menú de notarios, administrador de plantillas, administrador de catálogos, administrador de documentos
MANIFESTADOR PUBLICO	consulta de solicitudes, menú principal de mensajería, administrador de documentos
NOTIFICADOR	administrador de notificaciones permite imprimir, guardar o realizar nuevas notificaciones
PERFIL DE MACHOTES	Administración de plantillas,
PROCESOS ELIMINAR	Administra la información de los procesos, partes involucradas, resoluciones, medidas cautelares administra toda la información relacionada con procesos.
PROCESOSTODOS ELIMINAR	Consulta de registros de procesos, administra resoluciones, administra catálogos, administración de toda la información de los notarios y de los procesos.

REENTRAREXPEDIENTES	Permite la reentrada de un expediente, el cual cambia el número interno y el estado del mismo.
REGISTRO NACIONAL DE NOTARIOS	Este rol permite la modificación del perfil del notario, fechas, nombramientos, salidas del país.
SECRETARIA	Menú principal de mensajería, administración de documentos recibidos, comunicados y reportes de distribución.

Como se puede observar en el cuadro anterior en el caso de los roles de **ADMINISTRADOR DNN y ADMNISTRAR NOTARIOS ELIMINAR** puede gestionar información pertinente a la funciones Registro Notarios en este caso sólo debería tener permisos los encargados de registrar la información del **REGISTRO NOTARIAL** por sus funciones y competencias de los cambios que se van a registrar.

En el rol de **PERFIL DE MACHOTES** de igual manera tiene la autorización de crear modificar y eliminar las plantillas utilizadas en certificaciones, autenticaciones, apertura de tomos de protocolo entre otros, siendo esta una tarea sensible en cambios que se pueda dar sin un control de las mismas ya que se puedan presentar inconsistencias de la información. De igual forma en los otros roles que permiten eliminar, modificar o incluir información debería ser únicamente los funcionarios responsables de llevar acabo esa función específica.

Con respecto a los otros tres usuarios que tienen roles que no le corresponden según sus funciones del puesto se detalla.

Usuarios. vrodriguez, agarcia, dsolis.

Nombre ROL	Lo que se puede realizar con el permiso.
AREA LEGAL	Permite a los usuarios crear resoluciones.

Se identificó tres funcionarios con autorización del rol AREA LEGAL, este acceso permite realizar resoluciones, sin embargo la asignación a ese módulo, lo tiene funcionarios responsables de ejecutar las tareas como call center, secretariado de la unidad legal y registro de notarios, o sea este acceso, es una tarea atinente a los abogados de las diferentes unidades.

En caso del rol de **REENTRAREXPEDIENTES** esta tarea la tienen asignada tres jefes, siendo una función de los colaboradores que gestionan un nuevo proceso en el expediente del Notario

Público y principalmente velar el estado del expediente para asignar el responsable y centralizar esta tarea.

Así las cosas, es importante, recordar alguna normativa referente al tema en mención, ya que, toda organización debe proteger la información de accesos no autorizados y para ello se establece en las Normas de TI, específicamente en el punto 1.4.5 inciso a) y e), Control de Acceso, lo siguiente:

> *a. Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base de datos y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación.*
>
> *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 los responsables de definir quienes tienen acceso a la información y con qué limitaciones o restricciones.*

La Política de Contraseñas emitida para la Unidad de Tecnología de la Dirección Nacional de Notariado, indica:

> **h. Políticas relativas a seguridad**
> *Políticas generales de seguridad de acceso.*
>
> *1. La Unidad de Tecnologías de Información y Comunicación es el responsable de la seguridad de acceso a los sistemas operativos, sistemas de información, bases de datos, y redes que operen en los equipos de cómputo de la organización.*
>
> *2. La Unidad de Tecnologías de Información y Comunicación establecerá los mecanismos adecuados para el control, verificación y monitoreo de cambios en passwords, número de sesiones activas, seguridad lógica, física de todas las actividades relacionadas con el uso de tecnologías de información.*
>
> *3. Para evitar situaciones de peligro para la organización, se desactivarán o bloquearán las cuentas de usuario a aquellas personas que estén en vacaciones, con permisos o incapacidades mayores a una semana.*
>
> *4. En caso de despido, el permiso de acceso deberá desactivarse o bloquearse previamente a la notificación de la persona sobre la situación.*
>
> *5. En todos los casos, el jefe inmediato debe hacer la solicitud por escrito al administrador de seguridad, para la desactivación de la cuenta de algún usuario.*
>
> *6. El administrador de sistemas operativos, sistemas de información, bases de datos o redes asignará la clave de acceso al usuario.*
>
> *7. **Hasta donde sea posible, no se debe otorgar permisos de acceso ilimitado.***

> *8. Las jefaturas de Unidad deben solicitar formalmente la apertura, modificación o cierre de las cuentas de usuario. Cuando sea una apertura, deben indicar el perfil que se le debe asignar.*

Además, el estándar Cobit (Control Objectives for Information and related Technology) ofrece un conjunto de "mejores prácticas" para la gestión de los Sistemas de Información de las organizaciones y estipula en el punto 4.1 en su Norma PO4.11, Planificación y Organización.

> ***Segregación de Funciones**. Implementar una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico. La gerencia también se asegura de que el personal realice sólo las tareas autorizadas, relevantes a sus puestos y posiciones respectivas.*

Las situaciones expuestas evidencian debilitamiento al control, aspecto que recobra mayor importancia al considerar que se maneja información sensible de los Notarios Públicos y pudieran incrementan la posibilidad de materialización del riesgo de extracción de información de los Notarios Públicos, de errores en la información, delitos relacionados con la venta de los datos a un tercero o del uso indebido de información crítica, entre otros.

Aspectos que pueden representar para la Institución un alto costo económico y de afectación a su imagen al tener que enfrentar posibles reclamos o demandas por parte de los Notarios Públicos en caso de acontecer violaciones a su Informaciones personales y divulgación de datos.

Ante lo expuesto, es trascendental que se cuente con un plan de continuidad de la acción que garantice de manera pertinente la continuidad e integridad de los permisos de accesos al Sistema como lo indica las políticas establecidas por la Unidad de TI.

Además, también es necesario que se pueda determinar fehacientemente la relación de uso entre los equipos de TI y sus usuarios, así como la revisión de la asignación de permisos al Sistema Notarial.

La Unidad de Tecnología de Información debe valorar el efectuar una campaña interna por medio de una charla o vía correo interno sobre la Seguridad de la Información, donde se expliqué el uso y control de los usuarios y contraseñas de los sistemas de información de la institución. Así dar seguridad del buen uso y responsabilidad de los usuarios de sus accesos a los Sistemas.

Se espera que los aspectos detallados sean valorados y se tomen las medidas para mitigar los riesgos señalados, y que se aplique a todos los Sistemas actuales en uso y los nuevos para implementar en la Institución, se otorga el plazo establecido en el artículo 37 de la Ley General de Control Interno para su ejecución y comunicación de las acciones para corregir.

Atentamente,

MAFF. Xinia Solís Torres
Auditora Interna
CPA-5343

C: Archivo A.I.