



**DIRECCIÓN NACIONAL DE NOTARIADO**

**INFORME Nº DNN-INF-001-2019**

**AUDITORÍA EXTERNA SOBRE PROCESOS DE  
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN  
(TIC)**

**CONTRATACIÓN 2019CD-000046-0007500001**

**NOVIEMBRE 2019**

---

## Resumen Ejecutivo

El estudio de los procesos de la unidad de Tecnologías de Información y Comunicación (TIC), objeto de esta auditoría, se enfoca en la evaluación de la gestión de proveedores, seguridad lógica, organización funcional del área de TIC, sistema de misión crítica, la administración de las bases de datos y la protección de datos personales.

La unidad de TIC se encarga de la administración de los recursos de TI de la DNN, para lo cual cuenta con la jefatura, actualmente incapacitado, y dos funcionarios, uno que se encarga de la infraestructura y telecomunicaciones, y el segundo, de los sistemas de información y las bases de datos.

La DNN cuenta con cinco aplicaciones y una página web. La aplicación de misión crítica es el sistema de gestión de información notarial (SGIN), el cual está en uso desde el 28 de julio del 2017. Actualmente, la ESPH brinda el mantenimiento correctivo/preventivo y evolutivo a este sistema. El sistema FileOn para la gestión de documento está en desarrollo y los demás sistemas (Administración, Acuerdos y Filas) están en Producción.

En este documento se presenta el resultado de la evaluación de los aspectos mencionados previamente, de los procesos de la unidad de Tecnologías de Información y Comunicación; se describen los hallazgos y se presentan recomendaciones para mitigar las vulnerabilidades encontradas.

El anexo número uno de este informe contiene una lista de los documentos consultados para llevar a cabo esta auditoría. En los anexos dos y tres se presenta un resumen de las observaciones y entrevistas realizadas en los temas evaluados. El anexo número 4 muestra el cumplimiento de las Normas Técnicas evaluadas en esta auditoría. El anexo 5 muestra las características de seguridad de los sistemas de información que se revisaron. El anexo 6 muestra el cumplimiento de prácticas de seguridad aplicadas en los sistemas de información evaluados. El anexo 7 presenta los controles recomendados por el estándar ISO/IEC 27001 sobre la gestión de continuidad del negocio; y el anexo 8 presenta un caso particular de debilidad en el control de acceso en el sistema de información notarial (SGIN).

## Control de Revisiones y Socialización

Fecha	Descripción	Responsable/Participantes
28 de octubre, 2019	Definición de plan y metodología de trabajo	Rodolfo Calvo F., Manuel Mairena, Damián Calvo
29 de octubre, 2019	Inicio de ejecución de la auditoría	Roger Ureña, Cristh Bonilla, Rodolfo Calvo F., Damián Calvo, Manuel Mairena, Carlos Cerdas, Fabián Mora
28 de noviembre, 2019	Entrega del borrador del informe.	Rodolfo Calvo F., Manuel Mairena, Damián Calvo
3 de diciembre, 2019	Entrega del 2° borrador del informe.	Rodolfo Calvo F., Manuel Mairena, Damián Calvo
6 de diciembre, 2019	Conferencia final ante DNN.	Guillermo Sandí Baltodano, Roger Ureña, Cristh Bonilla, Rodolfo Calvo F., Damián Calvo, Manuel Mairena, Carlos Cerdas, Fabián Mora
10 de diciembre, 2019	Entrega del informe final.	Rodolfo Calvo F., Manuel Mairena, Damián Calvo

---

## Tabla de Contenido

I. INTRODUCCIÓN.....	4
II. OBJETIVO GENERAL .....	4
III. OBJETIVOS ESPECÍFICOS .....	5
IV. ALCANCE DEL TRABAJO.....	5
V. SUPUESTOS Y LIMITACIONES .....	5
VI. METODOLOGÍA.....	6
VII. NORMATIVA UTILIZADA .....	7
VIII. CONTEXTO DEL ESTUDIO.....	7
IX. EVALUACIÓN SOBRE PROCESOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN .....	11
X. IDENTIFICACIÓN DE OPORTUNIDADES Y HALLAZGOS .....	31
XI. CONCLUSIONES .....	50
XII. RECOMENDACIONES .....	53
ANEXOS.....	58

---

## I. Introducción

Este documento corresponde al Informe de Auditoría Externa sobre procesos de Tecnologías de Información y Comunicación (TIC) de la Dirección Nacional de Notariado (DNN), de acuerdo con los requerimientos de la Auditoría Interna.

El estudio se ejecutó de conformidad con las “Normas Generales de Auditoría para el Sector Público” (R-DC-64-2014) y las “Normas para el Ejercicio de la Auditoría Interna en sector Público” (R-DC-119-2009).

Este informe se entrega como producto de la contratación número 2019CD-000046-0007500001, a solicitud de la Auditoría Interna de la DNN.

### Abreviaturas utilizadas

AIC	Funcionario de la unidad de TIC con el cargo de Analista de infraestructura y telecomunicaciones. Actualmente, es el señor Carlos Cerdas Lazo.
ASB	Funcionario de la unidad de TIC con el cargo de Analista de sistemas de información y bases de datos. Actualmente, es el señor Fabián Mora Hernández.
DNN	Dirección Nacional de Notariado
ESPH	Empresa de Servicios Públicos de Heredia. Ofrece servicios de desarrollo y mantenimiento de sistemas de información.
Normas Técnicas	Normas técnicas para la gestión y el control de las Tecnologías de Comunicación (N-2-2007-CO-DFOE).
SGIN	Sistema de Gestión de Información Notarial
SLA	Acuerdo de Nivel de Servicio (siglas en inglés)
TIC	Tecnologías de Información y Comunicación

## II. Objetivo General

Evaluar el cumplimiento de los criterios básicos de gestión y control que deben observarse en licenciamiento de software, seguridades, continuidad del servicio, estructura de personal, misión crítica y administración de bases de datos, de conformidad con las “Normas Técnicas para la Gestión y el Control de las Tecnologías de Información”

---

emitida por la Contraloría General de la República, resolución R-CO-26-2007 del 07/06/2007, publicada en “La Gaceta N° 119 del 21/06/2007 y verificar el avance del Plan Estratégico de Tecnologías de Información y Comunicación (PETIC).

### **III. Objetivos Específicos**

Los objetivos específicos planteados que se abordan en este informe son los siguientes:

- A. Evaluar la eficacia de los controles establecidos para la gestión de la relación con terceros, acuerdos de servicio y revisión de licenciamiento de software.
- B. Evaluar la eficacia de los controles establecidos relacionados con la seguridad lógica a nivel de redes, sistemas operativos, servicios y bases de datos.
- C. Evaluar la eficacia de los controles implementados para garantizar la continuidad y la disponibilidad del servicio TIC.
- D. Evaluar la organización funcional del área de TIC, el cumplimiento de las funciones asignadas relacionadas y la eficacia de la cobertura de los servicios de Tecnologías de Información y comunicación requeridos por la DNN.
- E. Evaluar los controles implementados a nivel de sistemas de misión crítica de la Entidad, gestión tecnológica y la gestión de la página Web.
- F. Evaluar los controles implementados para la administración de las bases de datos y privacidad de datos.

### **IV. Alcance del Trabajo**

El alcance de este estudio comprende la evaluación de la gestión de terceros, los controles de acceso lógico a los recursos de TIC, la continuidad y disponibilidad de los servicios de TIC, la organización funcional de la unidad de TIC, la seguridad lógica de los sistemas de misión crítica, los controles sobre la administración de las bases de datos y los controles de privacidad de datos personales implementados en los sistemas de información gestionado por la unidad de Tecnologías de Información y Comunicación de la Dirección Nacional de Notariado.

### **V. Supuestos y limitaciones**

- 1. La unidad de Tecnologías de Información y Comunicación (TIC) consta de una jefatura, un profesional encargado de infraestructura y telecomunicaciones y un profesional encargado de sistemas de información y bases de datos.

2. El jefe de la unidad, el señor Oscar Gamboa Jiménez, se encuentra incapacitado desde julio del 2019 y, por ese motivo, no pudo ser entrevistado ni pudo aportar información relacionada con este estudio.

## **VI. Metodología**

Para realizar este estudio se llevaron a cabo las siguientes actividades:

- Entrevistas a funcionarios de Tecnologías de Información y Comunicación relacionadas con:
  - La administración de bases de datos
  - Seguridad de la información y acceso lógico a la red
  - Sistema operativo
  - Servicios y bases de datos.
  - Relación con terceros proveedores de servicios de TI
  - Acuerdos de Servicio (SLAs) internos y externos
  - Gestión del licenciamiento de software Institucional
  - Lineamientos de continuidad y disponibilidad de servicios de TI
  - Organización funcional del área de TI y servicios ofrecidos
  - Ámbito de las funciones y responsabilidades del personal del área de TI
  - Capacidades operativas del área de TI
- Comprobación de la información suministrada en las entrevistas mediante la observación e inspección.
- Revisión de documentos suministrados por los funcionarios de la unidad de Tecnologías de Información y Comunicación.
- Revisión de los controles de acceso en los sistemas de Información Notarial (SGIN), Administrativo (BOS), sistema de Acuerdos (Acuersoft) y el sistema de Filas (QWIZAR).
- Análisis de la información obtenida para identificar debilidades y oportunidades de mejora de los aspectos evaluados.

Las entrevistas y sesiones de trabajo se realizaron entre el 29 de octubre y el 25 de noviembre del 2019. La Auditoría Interna fue facilitadora para la obtención de la información de las entrevistas e inspecciones de la Dirección Nacional de Notariado.

---

## **VII. Normativa utilizada**

Para evaluar los aspectos relacionados con la seguridad de la información se tomaron en consideración las recomendaciones de la Asociación para el Control y Auditoría de los Sistemas de Información (ISACA por sus siglas en inglés) y las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE).

Para evaluar los aspectos relacionados con la relación con terceros, Continuidad y Disponibilidad de Servicios, se tomaron en consideración los lineamientos de la Norma ISO 27000 sobre el Sistema de Gestión Seguridad de la Información y las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE).

Para evaluar los aspectos relacionados con Licenciamiento, Acuerdos de Nivel de Servicio (SLAs), Organización del área y las respectivas funciones y capacidades relacionadas, se tomaron en consideración los lineamientos de las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE).

Para realizar esta auditoría se siguieron las normas establecidas por la resolución R-DC-64-2014, Normas Generales de Auditoría para el Sector Público, emitida por la Contraloría General de la República, del 11 de agosto del 2014.

## **VIII. Contexto del estudio**

### **La unidad de Tecnologías de Información y Comunicación**

La unidad de Tecnologías de Información y Comunicación (TIC) depende directamente de la Dirección Ejecutiva de la DNN. De acuerdo con el Manual Organizacional y Funcional (MOF), su función general es “establecer y conducir el desarrollo informático y de tecnologías de la Dirección Nacional de Notariado.”

Las funciones específicas de esta unidad, según el MOF, son las siguientes:

- I. Promover el uso de las tecnologías de información que sean aplicables en las actividades institucionales.
- II. Promover el uso de infraestructuras tecnológicas modernas que permitan ofrecer a los usuarios y ciudadanos servicios de forma continua y sin interrupciones.
- III. Proveer el servicio de telecomunicaciones de forma eficiente y eficaz, para el acceso veraz de la información.
- IV. Proveer a los usuarios un servicio de bases de datos adecuado a sus necesidades, el cual permita obtener información de forma ágil y oportuna.
- V. Dotar a la institución de los sistemas de información adecuados, para que



---

los usuarios y la ciudadanía en general puedan obtener información en línea o en ventanilla.

- VI. Administrar el portal web de servicios de la institución.
- VII. Administrar todos los servicios tecnológicos que se ofrezcan a los usuarios tanto internos como externos para apoyo a sus actividades.
- VIII. Administrar los contratos tecnológicos suscritos por la institución.
- IX. Asesorar en materia de tecnologías de información al Consejo Superior Notarial, la Dirección Ejecutiva y a las unidades de la Dirección Nacional de Notariado.

### **Redes, sistemas y equipos de la DNN**

La Dirección Nacional de Notariado cuenta con dos cuartos de comunicación que contienen los equipos de la red informática interna, y cuatro servidores virtuales provistos por la empresa Radiográfica Costarricense S.A. (RACSA), según el contrato C-CC-02-07-13-9182.

El sistema Administrativo BOS se encuentra en uno de los servidores locales de la DNN. El sistema de Información Notarial (SGIN), el sistema de Acuerdos (Acuersoft) y el sistema de Filas se encuentran en los servidores del Centro de Datos de la empresa RACSA.

El sistema de gestión de documentos (FileOn) es administrado por la empresa RACSA, con base en la “CONTRATACIÓN DE SERVICIOS DE DIGITALIZACIÓN DE LOS DOCUMENTOS DE LA UNIDAD DE ARCHIVO INSTITUCIONAL CON LA EMPRESA RADIOGRÁFICA COSTARRICENSE RACSA”, del año 2017. El encargado de la ejecución del proyecto es el señor Kenneth Marín Vega de la unidad de Archivo Institucional. La unidad de Tecnologías de Información y Comunicación no tiene acceso al servidor, ni al sistema, ni a los documentos digitalizados.

Las computadoras personales que utilizan los funcionarios de la DNN son alquiladas por la empresa PC CENTRAL, con base en la licitación pública “ARRENDAMIENTO DE EQUIPO DE CÓMPUTO Y SUSCRIPCIÓN PARA SISTEMAS OFIMÁTICOS OFFICE 365 CON EL RESPECTIVO MANTENIMIENTO TANTO A NIVEL DE HARDWARE COMO SOFTWARE”, número de contratación 2018LN-000001-00007500001.

### **Sistemas de información**

La DNN cuenta con los siguientes sistemas de información para brindar sus servicios al público y para su operación interna.



Sistema	Descripción general
SGIN	<p>Sistema de Gestión de Información Notarial.</p> <p>Este sistema se encarga de registrar y administrar la información de los notarios públicos de Costa Rica, su estado y los movimientos relacionados con la función notarial que desempeñan, como apoyo a las funciones y atribuciones de la Dirección Nacional de Notariado, conforme a la Ley 7764, Código Notarial, del 17 de abril de 1998, y su reforma, contenida en la Ley 8795, del 4 de enero del 2010.</p> <p>El sistema fue desarrollado por la empresa Hermes Soft (SGIN 1.0). El desarrollo terminó en diciembre del 2016, y se empezó a utilizar el 28 de julio del 2017, después de agregarle requerimientos no contemplados en la contratación.</p> <p>Desde el 17 de septiembre del 2018 hasta la fecha de esta auditoría, la Empresa de Servicios Públicos de Heredia (ESPH) está brindando el servicio de mantenimiento preventivo, correctivo y evolutivo para actualizar la tecnología de desarrollo utilizada por el sistema, corregir los defectos de la versión 1.0 y agregar mejoras y requerimientos que cumplan con las necesidades actuales de la DNN.</p> <p>La nueva versión del sistema se denomina SGIN 1.1 y se estima que estará en producción en los primeros días de mayo del 2020.</p>
Sistema de Notarios	<p>Sistema de gestión de notarios. Fue sustituido por el SGIN 1.0, en el 2017. Se utiliza, únicamente, para consultar información histórica que no se encuentra en el sistema actual.</p> <p>Este sistema fue cedido por el Poder Judicial, cuando la DNN se separó de ese organismo, en el 2010.</p> <p>Actualmente, no se está proporcionando mantenimiento a este sistema.</p>
BOS	<p>Sistema administrativo desarrollado por la empresa Tecapro S.A. que incluye los sistemas de Contabilidad, Presupuesto, Control Bancario, Compras, Inventario, Cuentas por Cobrar, Cuentas por Pagar y Nómina.</p> <p>Este sistema cuenta con soporte telefónico y conexión remota con la empresa Tecapro, con base en la contratación directa número 2016CD-000017-0007500001.</p>



Sistema	Descripción general
QWIZAR	<p>Sistema de gestión de filas para la atención al público, adquirido a la empresa Soluciones Optimizadas, la cual brinda el servicio de mantenimiento y soporte preventivo y correctivo, por medio de la contratación directa número 2017CD-000011-0007500001.</p> <p>En caso de que este sistema no esté disponible, la atención al público se realiza por medio de <i>tickets</i>.</p>
Acuersoft	<p>Sistema de control de Acuerdos. Este sistema es utilizado por la secretaria del Consejo para llevar el control de las sesiones del Consejo Superior Notarial. Se compró a la empresa Desarrollo Informático S.A. Actualmente, se cuenta con el contrato de mantenimiento y soporte preventivo y correctivo, número 2017CD-000012-0007500001.</p> <p>Todos los usuarios tienen acceso al sistema con el fin de realizar y dar seguimiento a las tareas relacionadas con los acuerdos tomados por el Consejo.</p>
Sitio web	<p>Sitio web de la DNN, desarrollado y mantenido por la empresa MANATI. Es administrado por la funcionaria de Comunicación de la DNN. Se cuenta con el contrato de hospedaje y mantenimiento por demanda, número 2018LA-000004-0007500001.</p>
FileOn	<p>Sistema proporcionado y administrado por RACSA, bajo la modalidad de Software como Servicio (SaaS, por sus siglas en inglés), para el registro, actualización y consulta de documentos digitales.</p> <p>Actualmente, la empresa ServiArchivos realiza la digitalización de los documentos físicos, como parte de la contratación del servicio.</p> <p>Los usuarios de este sistema son las unidades de Fiscalización Notarial, Servicios Notariales, Dirección Ejecutiva, Asesoría Jurídica, Legal Notarial y Archivo Institucional.</p> <p>El encargado de la ejecución del proyecto es el señor Kenneth Marín Vega, encargado de la unidad Archivo Institucional.</p>

---

Con base en las funciones de los sistemas de información, la unidad de TIC considera que el sistema de misión crítica es el Sistema de Gestión de Información Notarial (SGIN), sin el cual la DNN no podría brindar, de forma eficiente, los servicios que requieren los notarios públicos y otros usuarios que realizan trámites y consultas en esta institución.

## **IX. Evaluación sobre procesos de Tecnologías de la Información y Comunicación**

### **1. Evaluación de la gestión de terceros, acuerdos de servicios y licenciamiento de software.**

Reunión de trabajo con el señor Carlos Cerdas sobre el alcance de la gestión de relaciones con terceros, y los controles definidos para velar por el cumplimiento de acuerdos de nivel de servicio de TI internos y externos.

Se revisa la documentación relacionada con contratos y control de servicios otorgados.

Se consulta sobre los controles relacionados con la gestión de acuerdos de nivel de servicio.

#### **1.1 Relaciones con terceros que brindan servicios de TIC y Acuerdos de Nivel de Servicio (SLAs) vinculantes**

1.1.1 Actualmente, se cuentan con los siguientes proveedores de servicio:

- TecApro para el servicio de conectividad con el sistema BOS.
- Tecnova para el servicio administrado de Firewall de seguridad.
- ESPH – Grupo Mas, en convenio interinstitucional, para el servicio de desarrollo evolutivo y mantenimiento de los sistemas sustantivos de la DNN, principalmente el desarrollo de la nueva versión del SEGIN.
- Racsa, en convenio interinstitucional, para el servicio administrado de centro de datos principal y enlaces de comunicación dedicado de la plataforma en producción de la DNN.
- Soluciones Optimizadas, para el mantenimiento del sistema de Filas.
- Time and Attendance, para el mantenimiento del sistema de relojes marcadores.
- Avtec, para el servicio administrado de la telefonía IP y central telefónica.
- ICE, como proveedor de servicio de Internet.

- PC Central, para el servicio de soporte y mantenimiento de equipos de cómputo de uso personal para los funcionarios de la DNN:
  - Manatí, para el servicio de mantenimiento y soporte de la página Web Institucional.
- 1.1.2 La administración de estos contratos recae en la Jefatura del área de TIC; mientras la persona responsable no se encuentre laborando, las responsabilidades de gestión recaen en Carlos Cerdas.
- 1.1.3 La confección, publicación y seguimiento del cartel se realiza a través del área de Proveduría; la decisión inicial de la contratación y los criterios de admisibilidad salen del área de TI, además de las aclaraciones, apelaciones técnicas y evaluación de oferentes.
- 1.1.4 No hay un procedimiento formal con respecto al seguimiento y control de las contrataciones o para realizar evaluaciones periódicas del desempeño del contratista y el aporte de valor.
- La estrategia de gestión del proyecto se define a nivel cartel, pero no hay un estándar que rijan cómo se debe dirigir y fiscalizar la ejecución de un proyecto.
  - El cronograma base se desarrolla en conjunto con el contratista al momento de ejecutar la planificación del proyecto.
  - Los hitos del cronograma definen el desempeño del proyecto y los pagos a realizar.
- 1.1.5 Los proveedores de servicios tercerizados no están clasificados, por lo que no se tiene un control sobre tipo de servicio ofrecido y el alcance relacionado con la plataforma tecnológica.
- En la Unidad de TIC tienen claro el tipo y alcance del servicio, puesto que son ellos quienes lo estructuran y solicitan; sin embargo, la gestión del mismo se mantiene en la práctica por la experiencia del personal, no por seguir un lineamiento de contratación por tipo de proveedor.
  - Rige el criterio experto para valorar el servicio del contratista.
  - No hay un portafolio de proyectos formal que rijan la entrega de servicios según necesidades funcionales y requerimientos de inversión tecnológica.
- 1.1.6 Con respecto a los controles para la validación de Acuerdos de Nivel de Servicio (SLAs) con proveedores:
- Los Acuerdos de Nivel de Servicio (SLAs) se definen a nivel cartelario, pero no hay evidencia de reportes periódicos de servicios otorgados (salvo que sean entregables).

- Los Acuerdos de Nivel de Servicio (SLAs) se orientan a la atención de incidentes y tiempos de respuesta de soporte, pero no incluye niveles de disponibilidad.
  - Racsa si incluye este rubro: 99.8% de la plataforma.
- Con respecto a TecApro, sistema BOS:
  - No acepta la definición de tiempos máximos de atención por Acuerdos de Nivel de Servicio (SLAs).
  - El reemplazo del servicio está sujeto a la respuesta por parte del Ministerio de Hacienda de ofrecer un software que sustituya al BOS; no hay fecha para resolución.
  - No cuenta con soporte y mantenimiento para la herramienta, solo de atención de dudas funcionales, por lo que se está desarrollando un cartel para cubrir esta necesidad.
  - Se cuentan con actualizaciones del sistema siempre y cuando sea sobre la versión vigente (una nueva versión implica un nuevo contrato de servicio).
  - La responsabilidad del contrato recae en la Unidad Administrativa, por lo que el área de TI no ofrece soporte a la gestión.
- Con respecto a ESPH-Grupo Mas:
  - Se validan entregables y documentos de respaldo de trabajos.
  - Se cuentan con un debido proceso de gestión de cambios.
  - La gestión de las actividades y la ejecución de servicios se hace a través de cronograma.
    - Esta gestión recae en la unidad de Servicios Notariales.
    - El área de TI apoya en temas de soporte y mantenimiento de Bases de Datos.
  - No se ejecuta un proceso periódico de revisión del desempeño del servicio adquirido por parte de TI.
- Con respecto a Racsa:
  - No hay métricas de desempeño de la plataforma definidas.
  - Los Acuerdos de Nivel de Servicio (SLAs) son establecidas a nivel convenio, no se pueden incorporar nuevos lineamientos de forma unilateral.
  - Cuenta con una mesa de ayuda que soporta la solución por horas mensuales.



- El área de TI solo puede ver alertas a nivel general, pero no métricas del estado de uso de la plataforma.
  - Los servicios de administración y soporte recaen en Racsa; es rígido con respecto a la incorporación de mejoras a la plataforma identificadas por la DNN (por ejemplo, espacio de almacenamiento disponible).
  - No se cuenta además con un inventario de activos de la Institución en el Centro de Datos principal.
- Con respecto a Tecnova:
  - Con este contrato se cuentan son servicios de soporte y administración, atención de incidentes, soporte correctivo y Acuerdos de Nivel de Servicio (SLAs) de atención.
  - El área de TI puede monitorear el servicio.

#### 1.1.7 Con respecto a Acuerdos de Nivel de Servicio (SLAs) Internos:

- No se gestionan Acuerdos de Nivel de Servicio (SLAs) internos, aunque los usuarios en general no reportan deficiencias en el servicio del área de TI.
- No hay canales formales de atención de incidentes, más allá de llamadas, correos electrónicos o visitas presenciales.
  - Se está en proceso de implementación una mesa de ayuda con métricas de desempeño; se está definiendo la estrategia de la misma.

## 1.2 Licenciamiento del software Institucional

- 1.2.1 El licenciamiento requerido para la creación de ambientes de producción y herramientas de servicio del Centro de Datos principal recae en Racsa. Mantiene las licencias requeridas como parte del servicio administrado, y crece según demanda, previo adendum del convenio.
- 1.2.2 Licencias con respecto a los servicios y ambientes requeridos para los equipos personales de la DNN y herramientas ofimáticas recaen en PC Central. Mantienen las licencias vigentes, activas y pueden crecer según demanda.
- 1.2.3 El SGIN actual cuenta con permisos de uso, pero no puede crecer en capacidades (no hay contrato con Hermes, quien es el dueño de los utilitarios sustantivos del sistema). Con la creación del nuevo sistema, la propiedad pasa a DNN.

- 
- 1.2.4 Como utilitarios, solo se utilizan las herramientas del MICIT para el uso de firma digital.
- Las aplicaciones adicionales no requieren de licencias de cobro, y su uso es vigente para las necesidades de la DNN.
- 1.2.5 Hay políticas sobre la instalación y uso de software en la Institución, y se tienen controles a nivel administrados para realizar instalaciones.
- 1.2.6 No hay claridad con respecto a la custodia y propiedad de los activos del Archivo Digital; no hay términos definidos en el convenio sobre el traspaso de documentos y estructuras de expedientes al momento de terminar con el servicio.
- Actualmente es otorgado por Servearchivos a través de un convenio con Racsa.

## **2. Evaluación de la seguridad lógica a nivel de redes, sistema operativo, servicios y bases de datos.**

Se realiza la evaluación de la seguridad lógica de la DNN, la cual involucra los controles de acceso lógico a la red de la institución, los controles sobre la creación de usuarios en el Active Directory y los controles de acceso lógico a las bases de datos.

Se revisan los perfiles de usuarios de la base de datos, las políticas para la creación de usuarios y asignación de privilegios, y el procedimiento de cambio y eliminación de privilegios.

### **2.1 Marco de seguridad de la información**

- 2.1.1 La DNN no cuenta con el marco de seguridad requerido por la cláusula 1.4.1 de las Normas Técnicas, la cual establece la implementación de un marco de seguridad de la información que incluya la clasificación de los recursos de TI, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento y evaluación de medidas de seguridad y la ejecución de procesos de concientización y capacitación del personal.

El marco de seguridad de la información es la base para la protección de la confidencialidad, integridad y disponibilidad de la información y los recursos de TI.

- 2.1.2 La DNN cuenta con un manual de políticas para tecnologías de información, con fecha de noviembre del 2013. Este manual define un conjunto de políticas para la protección y uso de los recursos de TIC, pero la institución no cuenta con un sistema de gestión para la selección, implementación,



monitoreo, revisión y mantenimiento de los controles necesarios para proteger estos recursos.

- 2.1.3 El señor Carlos Cerdas Lazo indica que el Manual de Políticas de TI no se ha revisado desde su ingreso a la DNN y que no cuenta con documentos para comprobar si ha sido revisado desde su elaboración. Con base en manifestaciones del señor Cerdas Lazo y la revisión del Manual de Políticas de TI, se detectó que la “Política de nomenclatura en Carpetas de almacenamiento y en documentos de trabajo” (Manual de Políticas, pág. 35) está desactualizada.

La política mencionada está desactualizada porque no corresponde con la forma en la que se trabaja actualmente, con respecto a las carpetas compartidas para cada unidad organizacional.

Este año la forma de trabajo actual se está migrando para utilizar el SharePoint de Office 365, por lo que el Manual de Políticas de TI debería ser actualizado.

La evidencia indica que no se ha seguido el procedimiento de revisión periódica y actualización del Manual cuando se requiere un cambio; en este caso, primero debe actualizarse la política y después implementar el cambio en la organización.

- 2.1.4 La DNN no cuenta con una clasificación formal ni con criterios de clasificación de sus activos de información, en términos de su criticidad y confidencialidad.

- 2.1.5 En una encuesta realizada el 22 de noviembre del 2019 a 10 funcionarios de la DNN, se encontraron las siguientes brechas de seguridad:

- a. El 60% contestó que no conocían las políticas para el control de acceso de la DNN.
- b. El 90% indicó desconocer el Manual de Políticas para el acceso a las tecnologías de información de la DNN.
- c. Ningún usuario ha recibido capacitación relacionada con la seguridad de la información.
- d. El 60% manifestó que utilizaba dispositivos externos de almacenamiento para copiar archivos a estos dispositivos, o de estos a la computadora asignada por la DNN, con fines de respaldo o laborales; sin embargo, la DNN no cuenta con políticas ni mecanismos para la protección de la información confidencial o privada que se puede copiar a dispositivos móviles.
- e. El 70% contestó desconocer criterios de clasificación de la información que maneja la DNN. Y el 50% contestó que desconoce cómo reconocer la información pública, privada o confidencial y cómo tratarla.

f. El 80% afirma no haber recibido ninguna comunicación (correo, circular, etc.) relacionada con el tratamiento de documentos físicos o digitales.

2.1.6 El señor Carlos Cerdas Lazo manifiesta que ningún funcionario de la DNN revisa los derechos de acceso de los usuarios ni los privilegios asignados a los perfiles de usuario de los sistemas de información ni del sistema operativo. A la fecha en que se realiza esta auditoría, el señor Fabián Mora Hernández está elaborando una lista con los accesos asignados a los perfiles de usuario en los sistemas de información, para validarlos con la unidad organizacional que corresponda, según el sistema de información.

La revisión de los perfiles y privilegios de acceso es un control de seguridad, para evitar que las personas tengan acceso no autorizado a recursos de TI, dependiendo de las funciones que realizan y de acuerdo con el principio de “necesidad de saber” y “necesidad de hacer”.

## **2.2 Administración de cuentas de usuario y asignación de accesos**

2.2.1 Aunque el Manual de Políticas de TI contiene políticas para la creación y deshabilitación de cuentas de usuario, en el Manual de Procedimientos de la unidad de TIC no se encontraron procedimientos para la creación de usuarios ni para la inactivación o deshabilitación de usuarios.

El procedimiento es la herramienta para que los responsables de las unidades soliciten a la unidad de TIC la creación de cuentas de usuario para nuevos empleados y para la desactivación de la cuenta, de acuerdo con las políticas de control de acceso.

2.2.2 El señor Carlos Cerdas Lazo manifiesta que cuando ingresa un nuevo funcionario, la solicitud para la creación de usuarios y asignación de accesos no se realiza con la suficiente anticipación para que TIC tenga creados los accesos a la red, correo electrónico, Internet y a los sistemas de información, antes del primer día de labores del funcionario. El problema que esto genera es el atraso en el inicio de labores del nuevo funcionario.

2.2.3 El señor Carlos Cerdas Lazo manifiesta que los jefes de unidad no solicitan a TI la deshabilitación de cuentas de usuario de funcionarios que estén de vacaciones, con permiso o en incapacidad por más de una semana, como se especifica en las “Políticas relativas a seguridad”, establecidas en el Manual de Políticas de TI.

2.2.4 El señor Carlos Cerdas Lazo manifiesta que los jefes de unidad no solicitan a TI la deshabilitación de las cuentas de usuario de funcionarios que terminan la relación laboral con la institución, como se establece en las “Políticas relativas a seguridad”, del Manual de Políticas de TI.

Al no realizar la deshabilitación de exfuncionarios de forma oportuna, estos pueden hacer uso de la cuenta de correo institucional y tener acceso a los archivos compartidos en el SharePoint de Office 365 ®.

El 11 de noviembre del 2019, la unidad de TIC recibió la nota DNN-DE-834-2019, de la Dirección Ejecutiva para eliminar (deshabilitar) cuentas activas de exfuncionarios de la DNN, con acceso a cualquier recurso tecnológico de la institución, debido a que se detectó la recepción de correos a una exfuncionaria.

### **2.3 Controles de acceso a las bases de datos**

Con excepción del analista de infraestructura y telecomunicaciones (AIC) y el analista de sistemas de información y bases de datos (ASB) de la unidad de TIC, los demás funcionarios de la DNN no tienen cuentas de usuario en el Gestor de la base de datos de Producción. El acceso de los demás funcionarios a la base de datos se realiza a través de los sistemas de información que utiliza, según sus funciones.

La creación de usuarios y la asignación de privilegios de acceso se administra por medio del módulo de Administración de usuarios (o módulo de Configuración) de los sistemas de información de la DNN.

El señor Carlos Cerdas Lazo manifiesta que ningún proveedor ni personas ajenas a la DNN tienen acceso a las bases de datos de Producción. Al revisar las cuentas de usuario creadas en el Gestor de la Base de Datos, se pudo comprobar que solo existen los usuarios “sa”, “admin” y los usuarios que utilizan los sistemas de información para conectarse a la base de datos correspondiente.

El usuario “admin” corresponde al usuario administrador a nivel del sistema operativo. Esta cuenta es utilizada, únicamente, por el encargado de bases de datos y, solo en casos de emergencia, sería utilizada por el Carlos Cerdas.

Las debilidades detectadas en el acceso a la base de datos son las siguientes:

- 2.3.1 El usuario “sa” se encuentra habilitado. Esta cuenta corresponde al administrador del sistema del Gestor de Base de Datos SqlServer, el cual está asignado al rol “sysadmin”, con los privilegios más altos en la base de datos.

La empresa Microsoft recomienda no utilizar esta cuenta para ingresar a la base de datos, cambiar la contraseña inicial por una contraseña segura y deshabilitarla, para evitar que un atacante la utilice si logra descubrirla. (<https://docs.microsoft.com/es-es/dotnet/framework/data/adonet/sql/authentication-in-sql-server>)

- 2.3.2 Los funcionarios de la unidad de TIC no deben compartir la misma cuenta de usuario, ya que no es posible identificar a la persona que ingresa a la

base de datos. El inciso f de la cláusula 1.4.5, “Control de acceso” de las Normas Técnicas, especifica que la organización debe:

“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.”.

2.3.3 La hilera de conexión a las bases de datos utilizada por los sistemas de información SGIN, Acuersoft y QWIZAR no están encriptadas, con lo que abre la posibilidad de que una persona utilice esta información para acceder a las bases de datos, de forma indebida.

2.3.4 No existe una definición ni autorización escrita y aprobada de los privilegios que deben tener las cuentas de usuario utilizadas por los sistemas de información.

Los privilegios de las cuentas de usuario con acceso a las bases de datos deben ser definidos, escritos y autorizados por quien corresponda, de acuerdo con las políticas y procedimientos de seguridad de la información.

2.3.5 La cuenta de usuario del sistema QWIZAR (sistema de Filas) tiene asignado el rol “sysadmin”, con el cual se puede realizar cualquier actividad en la base de datos. Véase la figura 1.

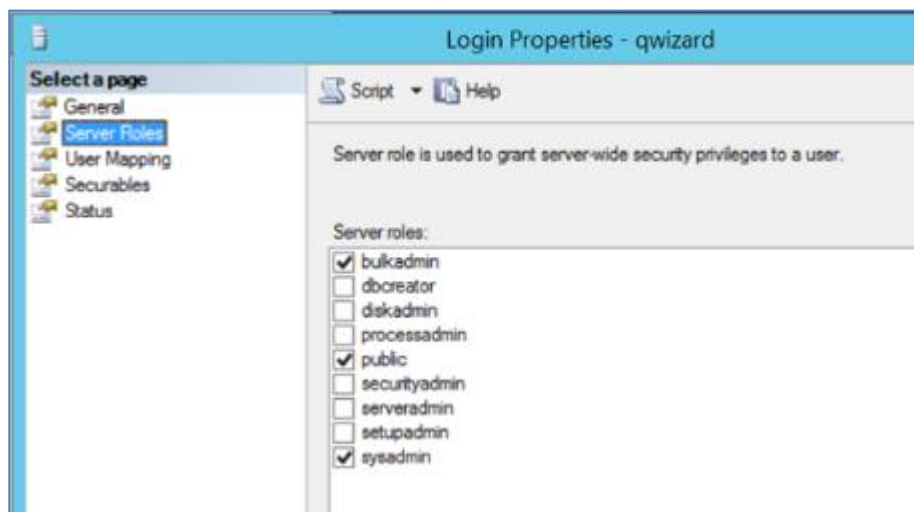


Figura 1. Roles de servidor asignados al usuario qwizard.

### 3. Evaluación de la continuidad y la disponibilidad del servicio de TIC.

Reunión de trabajo con el señor Carlos Cerdas sobre el alcance de la gestión de la continuidad de la plataforma y los servicios asociados con las TIC Institucionales.

Se revisan políticas de gestión de continuidad, recuperación de servicios y priorización de atención.



---

### **3.1 Continuidad y disponibilidad de servicios**

- 3.1.1 No se cuenta con un análisis de riesgos en el SEVRI relacionado con la necesidad de desarrollar planes de continuidad y contingencia a nivel Institucional, con su vinculación a la plataforma tecnológica asociada.
- 3.1.2 No se cuenta con un inventario de activos clasificados para valorar nivel de criticidad, capacidad de soporte en contingencia o reemplazos.
- 3.1.3 No hay controles implementados con respecto a la seguridad e integridad de la plataforma tecnológica de la DNN, con sus respectivos acuerdos de soporte y disponibilidad.
- 3.1.4 No se cuentan con planes de continuidad o contingencia de TI.
- 3.1.5 No está definida una estrategia de atención y recuperación de desastres.
- 3.1.6 No se cuenta con un sitio alternativo de procesamiento de datos adicional al de Racsá.
  - Se está desarrollando una iniciativa de robustecer la plataforma interna para atender estas necesidades con un centro de datos alternativo Tier III.
- 3.1.7 El cableado estructurado de comunicaciones y datos se encuentra en garantía con el proveedor de la instalación ICM Empresarial, pero no se cuenta con servicios de soporte y mantenimiento que garantice su disponibilidad y atención ante incidentes.
- 3.1.8 Los equipos de gestión de la red interna de datos (LAN) son equipos obsoletos que dificultan su control y recuperación ante desastres, además de no contar con soporte.

### **4. Evaluación de la organización funcional del área de Tecnología de Información y Comunicación.**

Entrevista al señor Carlos Cerdas sobre la estructura funcional del área de TIC Institucional y su ámbito de trabajo.

Se revisan los alcances y ámbitos de trabajo interno de los funcionarios y los servicios tercerizados.

Se identifica la brecha de servicios requeridos sobre los facilitados por el área y los servicios tercerizados.

Se revisan los lineamientos relacionados con las funciones específicas del área, descritos en el manual organizacional y funcional de la Institución.

Se identifica la brecha de servicios requeridos sobre los facilitados por el área y los servicios tercerizados.

---

## 4.1 Organización funcional del área de TIC

- 4.1.1 El área de TI cuenta con tres personas de tiempo completo; actualmente la persona responsable de la Jefatura del área se encuentra incapacitada, sin una fecha estimada de reincorporación.
- Se está valorando la posibilidad de nombrar un Jefe de asignación temporal y abrir una plaza para responsabilidades de soporte.
- 4.1.2 Los funcionarios actuales atienden los siguientes servicios:
- Como Jefe del área: Gestión de TI, monitoreo de servicios otorgados, métricas de la plataforma disponibles.
  - Como profesional nivel 2: Telecomunicaciones, servidores e infraestructura tecnológica.
  - Como profesional nivel 1A: Gestión de sistemas y Bases de Datos.
- 4.1.3 Los servicios de soporte técnico y de atención de incidentes para usuarios Institucionales se atienden entre los dos profesionales del área.
- 4.1.4 Los servicios de desarrollo evolutivo para los sistemas se encuentran tercerizado o en proceso de contratación para los sistemas sustantivos de la DNN.
- 4.1.5 Se cuenta con servicios de soporte a la plataforma de Centro de Datos, telefonía y mantenimiento de equipos personales, pero no se cuenta con servicios de soporte y atención de incidentes.
- Se atienden de forma reactiva.
  - Se espera contar con un contrato que apoye en el soporte de incidentes en equipos en temas de actualizaciones, seguridad y soporte a la plataforma.
- 4.1.6 Para asuntos de proyectos, los funcionarios del área cumplen como apoyo en la gestión de proyectos de TI, analistas técnicos y arquitectos de solución.
- Se apoyan además con usuarios expertos de las áreas objeto de los proyectos.
- 4.1.7 Se considera que los servicios tercerizados, si bien pueden mejorarse a nivel de gestión, son necesarios para cumplir con las necesidades Institucionales en temas de TI; el personal interno puede cumplir con sus funciones sustantivas.
- Sin embargo, en la condición actual de dos funcionarios activos, los requerimientos de gestión del área y soporte a usuarios está impactada en temas de tiempo y divide la atención del personal.

---

## 4.2 Funciones específicas del área

- 4.2.1 No se cuenta con un PETI que delimite el nivel de servicio y atención de necesidades de las áreas usuarias de la DNN.
- 4.2.2 No se cuentan con la atención de servicios relacionados con la Seguridad de la Información.
- 4.2.3 Puede haber dificultades para la atención de proyectos con el personal actual si se gestiona a lo interno, según el plazo, dificultad y ámbito de atención interna y externa a la DNN.
- 4.2.4 No se cuenta además con planes de capacitación en temas de desarrollo estratégico de TI para la Institución, o entrenamientos para certificar a los funcionarios del área sobre tecnologías emergentes.
- 4.2.5 Los servicios de soporte sustantivo a la infraestructura tecnológica (plataforma y sistemas) son atendidos por el personal del área, pero el soporte técnico y atención de usuarios consume tiempo importante que limita la capacidad de acción de los funcionarios, principalmente con temas de gestión y estrategia.
- 4.2.6 No se cuenta con personal disponible para los servicios requeridos de Calidad de la Información.
- 4.2.7 No se cuenta con una plataforma y una estrategia de gestión para teletrabajo.
- 4.2.8 No se cuenta con personal suficiente que pueda atender lineamientos de contingencia y recuperación de ambientes de producción Institucional.
- 4.2.9 Por otro lado, se considera que los servicios tercerizados no pueden ser atendidos por el personal interno, con la estructura actual.
  - Es importante valorar si el personal del área puede atender el soporte y mantenimiento de una plataforma tecnológica interna, si terminan con el convenio de servicio con Racsa.

## 5. Evaluación del sistema de misión crítica de la entidad

Se revisan los controles implementados en el sistema de misión crítica de la DNN: Sistema de Información Notarial (SGIN). Adicionalmente, se revisan los controles de seguridad en los sistemas Administrativo (BOS), Filas (QWIZAR) y el sistema de Acuerdos (Acuersoft).

En cada sistema, se evalúa la creación de perfiles, usuarios y contraseñas, la asignación, cambio y eliminación de accesos, el registro de pistas para auditoría (bitácora), y el procedimiento de revisión de la bitácora de transacciones. El anexo

---

número 5 presenta una tabla con las características de seguridad de cada sistema evaluado.

A continuación se presenta el resultado de la evaluación en el sistema de misión crítica SGIN.

## **5.1 Controles de seguridad en el sistema de información notarial.**

- 5.1.1 El señor Fabián Mora Hernández indica que el sistema presenta problemas relacionados con la asignación de accesos a los usuarios. El sistema permite asignar uno o más roles a un usuario bajo el concepto de herencia, en el cual un rol de menor nivel no puede tener permisos que no tenga el rol “padre”. Sin embargo, cuando se asignan dos o más roles a un usuario, puede ocurrir que el usuario no tenga acceso a todas las acciones asociadas a esos roles. El señor Mora Hernández manifiesta que esto se comunicó a la empresa desarrolladora, pero esta no brindó una solución.
- 5.1.2 En el sistema actual, la contraseña no tiene vigencia. El usuario nunca tiene que cambiarla, a menos que la olvide. Es una buena práctica que las contraseñas se cambien cada cierto tiempo, para reducir la posibilidad de que descubran la contraseña de un usuario.
- 5.1.3 La cuenta de usuario no se bloquea después de tres intentos de ingreso fallidos. Es una buena práctica que la cuenta del usuario se bloquee después de al menos tres intentos de ingreso fallidos, y que se envíe un correo al encargado de la seguridad para comprobar que no se trate de un intento de ingreso no autorizado.
- 5.1.4 No tiene acceso con firma digital. El sistema tiene un ícono para ingresar con firma digital; pero el señor Mora Hernández indica que esto era una prevista para un mantenimiento futuro. El señor Mora indica que el acceso con firma digital se implementará en la versión 1.1 del sistema.
- 5.1.5 Uno de los problemas de acceso encontrados en el sistema tiene que ver con la asignación de acceso a los funcionarios de la unidad de Fiscalización Notarial para poder ver la fecha de autorización en la ventana de edición de tomos de los notarios. El problema se debe a que los funcionarios de la unidad mencionada necesitan consultar la fecha de autorización, pero el sistema no provee una opción de consulta en donde se muestre ese dato. Solo la pueden ver si a los funcionarios de esa unidad se les concede acceso a la opción de edición, aunque no deberían tener acceso a ella.

La descripción ampliada de esta brecha de seguridad se describe en el anexo número 8.



---

## **5.2 Evaluación de la vigencia tecnológica, gestión de cambios, costo operativo y calidad del soporte técnico.**

La información sobre el sistema SGIN desarrollado por la empresa Hermes Soft fue suministrada por Carlos Cerdas Lazo y Fabián Mora Hernández, de la unidad de TIC.

- 5.2.1 El desarrollo del sistema SGIN terminó en diciembre del 2016, pero no se pudo poner en Producción, porque las necesidades de los usuarios habían variado durante el desarrollo y estas no se habían incorporado porque no estaban contempladas en el alcance del sistema.
- 5.2.2 Entre enero y julio del 2017, la empresa desarrolladora incorpora las funcionalidades adicionales para que el sistema pueda ser utilizado.
- 5.2.3 El sistema se empieza a utilizar en Producción el 28 de julio del 2017 y, debido a las fallas presentadas, la unidad de TIC decide licitar el servicio de mantenimiento correctivo, preventivo y evolutivo. El proceso de evaluación de las ofertas adjudica el mantenimiento a la empresa ESPH, la cual inicia el trabajo el 17 de septiembre del 2018.
- 5.2.4 Como parte del contrato de mantenimiento, la empresa ESPH realiza un diagnóstico del sistema SGIN, cuyo resultado se encuentra en el documento "Diagnóstico Sistema SGIN - DNN.docx", el cual sirve de base para desarrollar los requerimientos del contrato de mantenimiento.
- 5.2.5 Uno de los problemas relevantes señalados en el diagnóstico es la dificultad que se encontró para hacer cambios y mejoras en la base de datos, ya que los componentes de acceso a datos de la empresa desarrolladora no permitían que se hiciera ningún cambio, y la empresa no cedió el código fuente de esos componentes. Si se hacía algún cambio en la base de datos, el sistema no funcionaba.
- 5.2.6 El señor Fabián Mora Hernández, de la unidad de TIC, indica que con el mantenimiento se están desarrollando nuevos componentes de acceso a datos para dejar de utilizar los componentes originales del sistema y se están reemplazando las interfaces y flujos desde la interfaz gráfica hasta el acceso a la base de datos, mejorando también el desempeño (tiempos de respuesta) del sistema.
- 5.2.7 Con el mantenimiento de la empresa ESPH, la DNN será la propietaria de la totalidad del código fuente que se desarrolle, lo que facilitará el mantenimiento y evolución de la nueva versión del sistema.
- 5.2.8 El señor Fabián Mora Hernández estima que la nueva versión del sistema podría instalarse en Producción en el transcurso del primer cuatrimestre del 2020.

## Gestión de cambios

5.2.9 El procedimiento para la gestión de cambios se especifica en el punto 7.1, “Procedimiento para la Atención de Requerimientos” de la licitación abreviada N° 2018LA-000003-0007500001. Este procedimiento comprende desde el levantamiento y especificación del requerimiento, la estimación de tiempo, la gestión de cambios durante la implementación del requerimiento, las pruebas técnicas y pruebas del usuario, el tratamiento de los errores de programación, los atrasos no atribuibles al proveedor, el plazo para las revisiones y aprobaciones, la atención de incidentes y consultas y los canales y medios de comunicación; todo lo anterior, con las revisiones y aprobaciones correspondientes por parte de la DNN. Se considera que el procedimiento definido es completo y equilibrado para ambas partes.

## Costo operativo

5.2.10 El señor Carlos Cerdas Lazo no cuenta con datos sobre el costo operativo del sistema SGIN. La información con la que cuenta el señor Cerdas es el costo por hora de desarrollo de las empresas que tienen o han tenido contrato con la DNN. En el siguiente cuadro se presenta la información obtenida.

Empresa	Costo por hora
ESPH + Grupo MAS Horas de servicio por demanda para mantenimiento de software. Fuente: Listado de contrataciones vigentes 2017-2018.	\$36.50
Tecapro (Fuente: Carlos Cerdas)	\$60.00
Hermes Soft (Fuente: Carlos Cerdas)	\$100.00

Con base en este cuadro se puede notar que el costo por hora de ESPH es el 60% del costo por hora de Tecapro y el 36% del costo por hora de Hermes Soft, por lo que esta oferta es la más económica para la DNN.

## Calidad del soporte técnico

5.2.11 El contrato de mantenimiento del SGIN comprende el soporte al sistema actual (SGIN 1.0) y la implementación de mejoras, correcciones y nuevas

funcionalidades. De acuerdo con lo expresado por el señor Fabián Mora, quien funge como *Product Owner* (dueño del producto) del proyecto, el soporte que se ha recibido de la empresa ESPH es de buena calidad, ya que no se han presentado diferencias ni se han generado reportes de inconformidades por el servicio recibido.

### **5.3 Eficiencia, eficacia y economicidad en la gestión de la página web de la institución.**

- 5.3.1 El desarrollo de la página Web actual de la DNN se contrató a la empresa MANATI en el 2018, con base en la licitación abreviada 2018LA-000004-0007500001. Además del desarrollo, la contratación incluye el servicio de *hosting* por un año, prorrogable por tres años más, y un mantenimiento por demanda. El costo del *hosting* es de ₡1.800.000.00 por año, y el costo de mantenimiento es de ₡ 30.000 por hora.
- 5.3.2 La página web se instaló el 12 de diciembre del 2018 y es de acceso público.
- 5.3.3 La persona responsable del mantenimiento de contenido es la señora Vivian García Paniagua, encargada de Comunicación de la DNN. Esta funcionaria tiene privilegios para actualizar, eliminar y agregar contenido a la página.
- 5.3.4 Sobre la eficacia y eficiencia de la página web, la señora García Paniagua manifestó la siguiente:
- a. Dedicar, aproximadamente, 11 horas por mes en el mantenimiento del contenido de la página.
  - b. Su trabajo consiste en:

“Subir el material de información solicitado por la jefaturas o encargados de procesos, por ejemplo, documentos del área administrativa, planificación, actas o acuerdos del Consejo Superior Notarial etc. Subir y redactar noticias o información de interés para luego enlazarla a Facebook y la administración del formulario de Contacto, el cual me llega a mí y yo distribuyo a las personas o unidades que pueden dar respuesta y doy seguimiento a que den la respuesta. Finalmente, manejo de imagen, actualización de fotografías, actualización del carrusel de noticias de la página principal, etc.”. (Vivian García Paniagua, 25/11/2019).
  - c. La facilidad para realizar la actualización de la página la califica con 9, en una escala del 1 al 10, en donde 10 es Excelente.
  - d. El tiempo que invierte en actualizar la página la califica con 10, en una escala del 1 al 10, en donde 10 es Excelente.



- e. Con respecto al grado de satisfacción, la señora García Paniagua expresa que:

“El servicio que da la empresa es de mucha calidad, con excelentes tiempos de respuesta y solución de necesidades. Yo estoy muy conforme.” (Vivian García Paniagua, 25/11/2019).

- f. Con respecto a la cantidad de personas que tienen conocimiento para actualizar la página, la señora García Paniagua manifiesta lo siguiente:

“Solo yo tengo conocimiento, pero existe un manual muy sencillo para realizar las actualizaciones.” (Vivian García Paniagua, 25/11/2019).

## **6. Evaluación de la administración de las bases de datos y los controles de privacidad de datos personales.**

Se revisan los procedimientos de respaldo y recuperación de las bases de datos administradas por la unidad de Tecnologías de Información y Comunicación, así como los procedimientos de monitoreo y mantenimiento (tunning) de las bases de datos.

Con respecto a la protección de datos personales se revisa la Ley 8968, “Protección de la persona frente al tratamiento de sus datos personales” y su reglamento, para determinar cuáles controles requeridos por esta Ley se han aplicado en la DNN.

### **6.1 Administración de las bases de datos**

#### **6.1.1 Control de acceso, integridad y disponibilidad del servicio**

Los controles de acceso a las bases de datos se describen en el apartado 2.3, “Controles de acceso a las bases de datos”.

Las bases de datos de los sistemas en Producción SGIN, Acuersoft y Filas se encuentran en los servidores virtuales contratados a la empresa RACSA, por medio del “Contrato para la prestación del servicio de servidor virtual”, número C-CC-28-02-19-11834, y sus modificaciones.

En este contrato se especifican los controles establecidos por RACSA con respecto a la seguridad perimetral, seguridad física y seguridad lógica de los equipos, así como un nivel de disponibilidad del 99.8% anual de los datos almacenados.

Indica el señor Carlos Cerdas que, en los últimos tres años, han ocurrido dos eventos en los cuales se perdió el acceso a la base de datos. El tiempo que no estuvo disponible la base de datos no está registrado. El primer evento ocurrió, aproximadamente, “a finales del 2018” y el segundo evento ocurrió en noviembre del 2019. En ambos casos, el incidente fue causado

por problemas de comunicación con el Centro de Datos de RACSA. No se perdieron datos y no fue necesario restaurar la base de datos.

Un problema que se detecta en la gestión de la unidad de TIC es la escasez y, en algunos casos, la ausencia de registros de eventos e incidentes que afectan la seguridad de la información (integridad, confidencialidad y disponibilidad).

#### 6.1.2 Respaldo y recuperación de bases de datos

El respaldo de las bases de datos de Producción (SGIN, Acuersoft y Qwizar) se realiza como parte del respaldo de los servidores virtuales contratados a la empresa RACSA. El respaldo de los servidores se realiza todos los días a las 9 pm y tiene una vigencia de 30 días.

El procedimiento de restauración consiste en la restauración del servidor virtual que contiene las bases de datos, por parte de la empresa RACSA, a la fecha que especifique la unidad de TIC de la DNN.

La base de datos del sistema Administrativo (BOS7) es un sistema de archivos tipo ISAM que se encuentra en una carpeta del servidor físico NOTARIADO-HV-01, en las oficinas de la DNN. Esta carpeta se respalda todos los días a las 4 pm. El respaldo se deja en el servidor NOTA-FILESRV-00, contratado a RACSA.

El señor Fabián Mora Hernández manifiesta que hasta la fecha no ha sido necesario restaurar ninguna de las bases de datos.

#### 6.1.3 Monitoreo y mantenimiento

El señor Fabián Mora Hernández, de la unidad de TIC, indica que las bases de datos no se monitorean y no se han realizado tareas de mantenimiento. Esto significa que no se revisa el desempeño de la base de datos, la carga de trabajo del CPU, el uso de la memoria, el espacio utilizado por los datos y archivos *Log* y si se presentan bloqueos de registros, ante solicitudes de consulta o transacción.

Tampoco se realizan tareas de mantenimiento, tales como la desfragmentación y reconstrucción de índices, la gestión de datos históricos para mejorar el rendimiento de los accesos a la base de datos (consultas y actualización).

Además, no se encontraron procedimientos relacionados con el monitoreo y mantenimiento (*Tunning*) de la base de datos en el Manual de Procedimientos de TI.

El monitoreo y el mantenimiento de la base de datos son necesarios para optimizar su desempeño mejorando el tiempo de respuesta y el uso de los recursos.

#### 6.1.4 Gestión de datos históricos

Con respecto a este punto, el Manual de Políticas de TI contempla las “Políticas de tiempos de almacenamiento de información en bases de datos” (Manual de Políticas, pág. 20). Sin embargo, Mora Hernández indica que hasta la fecha no se ha realizado y no se tiene definido el traslado de información histórica a otras estructuras dentro de las bases de datos o a otras instancias de la base de datos.

La DNN no ha definido los criterios ni la tabla de plazos para la conservación de los datos, el traslado de la información histórica, ni el desecho de la información que no es requerida para la operación de la DNN.

No se encontraron procedimientos en el Manual de Procedimientos de TI para la identificación, definición de plazos y tratamiento de la información histórica de la DNN.

#### 6.1.5 Control de modificaciones a procedimientos almacenados

El Manual de Políticas de TI establece las “Políticas sobre Administración y mantenimiento de bases de datos” (Manual de Políticas, pág. 20), que indica que “Todo cambio o ajuste hecho en el proceso de mantenimiento se deberá dejar documentado en una bitácora para control y seguimiento”.

El único sistema que se encuentra en mantenimiento es el SGIN, por medio del contrato de mantenimiento 2018LA-000003-0007500001, “Contratación del servicio de mantenimiento correctivo/preventivo y evolutivo para los sistemas de Administración de la información notarial de la Dirección Nacional de Notariado, según demanda”, suscrito con la empresa ESPH, en septiembre del 2018.

La ESPH maneja un procedimiento para el control de cambios y modificaciones general, que incluye cambios en las interfaces, la funcionalidad y la base de datos del sistema.

La unidad de TIC no lleva hasta el momento una bitácora para el control y seguimiento de los cambios en las bases de datos.

## 6.2 Controles para la protección de datos personales

6.2.1 El Analista de infraestructura y comunicaciones (AIC) de la unidad de TIC manifiesta que no se han definido políticas, procedimientos ni controles con respecto a la identificación y gestión de datos personales registrados en las bases de datos de la DNN, conforme a la Ley N° 8968, “Protección de la persona frente al tratamiento de sus datos personales”, y su reglamento.

El artículo 3 de la Ley 8968 define como datos personales “cualquier dato relativo a una persona física identificada o identificable”, y los clasifica como

- 
- a) Datos personales de acceso irrestricto. Datos de acceso general, para los cuales no existe restricción, tales como el nombre y la identificación de una persona.
  - b) Datos personales de acceso restringido. Datos de interés solo para su titular o para la Administración Pública, tales como la dirección exacta de residencia, fotografía, números de teléfono privados.
  - c) Datos sensibles. Información de una persona relacionados con su origen racial, opiniones políticas, convicciones religiosas, condición socioeconómica, información biomédica o genética, vida y orientación sexual.

El artículo 36 del Reglamento a la Ley N° 8968 especifica las acciones que se deben realizar para la protección de los datos personales que mantiene la DNN en sus bases de datos. Para cada una de las acciones, se indica si la unidad de TIC las ha realizado o si ha establecido el control correspondiente. Las acciones son:

- a) Elaborar una descripción detallada del tipo de datos personales tratados o almacenados;
  - TIC no cuenta con esta información.
- b) Crear y mantener actualizado un inventario de la infraestructura tecnológica, incluyendo los equipos y programas de cómputo y sus licencias;
  - TIC cuenta con un inventario de las computadoras, servidores, equipos de comunicación y sistemas de información de la DNN.
- c) Señalar el tipo de sistema, programa, método o proceso utilizado en el tratamiento o almacenamiento de los datos;
  - No se ha elaborado esta información, con respecto a los datos personales.
- d) Contar con un análisis de riesgos, que consiste en identificar peligros y estimar los riesgos que podrían afectar los datos personales;
  - No se ha elaborado un análisis para evaluar los riesgos en relación con los datos personales almacenados en las bases de datos de la DNN.
- e) Establecer las medidas de seguridad aplicables a los datos personales, e identificar aquellas implementadas de manera efectiva;
  - No se han definido las medidas de seguridad aplicables, de forma exclusiva, a los datos personales.



- f) Calcular el riesgo residual basado en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales;

No se ha determinado.

- g) Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivados del resultado del cálculo del riesgo residual.

No se ha realizado.

En consulta realizada al señor Carlos Cerdas Lazo el 25/11/2019 sobre la existencia de un proyecto o iniciativa para implementar los controles requeridos por la Ley 8968, responde:

“Este tipo de controles se desarrollan en los modelos de seguridad de la información, el cual es todo un proyecto a implementar a nivel institucional, el cual será colocado dentro de la cartera de proyectos que se definan en el desarrollo del PETIC para el próximo año.”.

## **X. Identificación de oportunidades y hallazgos**

### **Hallazgo N° 1: Sobre la gestión de terceros, Acuerdos de Nivel de Servicio (SLAs) y licenciamiento de software:**

#### **Hallazgo N° 1.1**

La DNN no cuenta con un procedimiento formal que estandarice el seguimiento y control de las contrataciones o para definir los lineamientos de evaluación periódica del desempeño del contratista y el aporte de valor.

#### **Hallazgo N° 1.2**

La DNN no cuenta con un inventario de proveedores, categorizados por sus funciones y capacidades, o por el tipo de servicios que ofrece.

#### **Hallazgo N° 1.3**

La DNN no cuenta con Acuerdos de Nivel de Servicio (SLAs) suficientemente robustos que definan la atención, resolución y servicios de mantenimiento de la plataforma tecnológica o de sus componentes, ni para externos como internos del área de Tecnologías de Información.



---

## **Hallazgo N° 1.4**

Hay contratos (como Racsa o Tecapro) que no aceptan la incorporación de Acuerdos de Nivel de Servicio (SLAs) para medir el desempeño de la herramienta y la disponibilidad y atención de incidentes, y que además ofrecen servicios “rígidos” que no aceptan la incorporación de oportunidades o mejoras.

### **Causa**

Esto evidencia una debilidad con respecto al monitoreo y control de seguimiento de la ejecución de los contratos con terceros vinculantes a la entrega de servicios de TI, así como la debida diligencia al estado de cumplimiento de requerimientos conforme fueron establecidos, velando por los intereses de la Institución y el bien público.

### **Efecto**

Este hallazgo representa un Riesgo Alto para la Institución, ya que la ausencia de procesos formales de definición de Acuerdos de Nivel de Servicio (SLAs), además de la falta de mecanismos robustos para su debida gestión y control, limita la capacidad de validar el cumplimiento de las actividades vinculantes con la ejecución y control, dificulta la trazabilidad ante incidentes y factores de riesgo, incumplimientos, entre otros; además de dificultar la transparencia en el cumplimiento del objeto de la contratación.

### **Criterio**

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la CGR, definen, con respecto al seguimiento y control de las contrataciones y la gestión de Acuerdos de Nivel de Servicio (SLAs):

*“4.1 Definición y administración de acuerdos de servicio*

*La organización debe tener claridad respecto de los servicios que requiere y sus atributos, y los prestados por la Función de TI según sus capacidades.*

*El jerarca y la Función de TI deben acordar los servicios requeridos, los ofrecidos y sus atributos, lo cual deben documentar y considerar como un criterio de evaluación del desempeño. Para ello deben:*

*[...]*

- c. Definir con claridad las responsabilidades de las partes y su sujeción a las condiciones establecidas.*



- d. *Establecer los procedimientos para la formalización de los acuerdos y la incorporación de cambios en ellos.*
- e. *Definir los criterios de evaluación sobre el cumplimiento de los acuerdos.*
- f. *Revisar periódicamente los acuerdos de servicio, incluidos los contratos con terceros.”*

Sobre el mismo criterio:

*“4.6 Administración de servicios prestados por terceros*

*La organización debe asegurar que los servicios contratados a terceros satisfagan los requerimientos en forma eficiente. Con ese fin, debe:*

- a. *Establecer los roles y responsabilidades de terceros que le brinden servicios de TI.*
- b. *Establecer y documentar los procedimientos asociados con los servicios e instalaciones contratados a terceros.*
- c. *Vigilar que los servicios contratados sean congruentes con las políticas relativas a calidad, seguridad y seguimiento establecidas por la organización.*
- d. *Minimizar la dependencia de la organización respecto de los servicios contratados a un tercero.*
- e. *Asignar a un responsable con las competencias necesarias que evalúe periódicamente la calidad y cumplimiento oportuno de los servicios contratados.”*

En relación con la gestión de terceros y Acuerdos de Nivel de Servicio (SLAs), la norma ISO 27001 establece:

*“A.10.2 Gestión de la entrega del servicio por terceras partes*

*Objetivo: implementar y mantener un nivel apropiado de la seguridad de la información y la entrega del servicio, acorde con los acuerdos de entrega del servicio por terceras partes.*

*A.10.2.1 Entrega del servicio*

*Control*

*Deben asegurarse de que los controles de seguridad, las definiciones del servicio y los niveles de entrega incluidos en el acuerdo de entrega del servicio por terceras partes son implementados, operados, y mantenidos por las terceras partes.*

*A.10.2.2 Supervisión y revisión de los servicios por terceras partes*

*Control*

*Deben supervisarse y revisarse regularmente los servicios, informes y registros proporcionados por las terceras partes, y deben realizarse regularmente auditorías.*

*A.10.2.3*

*Gestión de cambios en los servicios de terceras partes*

*Control*

*Los cambios a la prestación de los servicios, incluyendo mantenimiento y mejora de las políticas existentes de la seguridad de la información, procedimientos y controles, deben gestionarse tomando en cuenta la importancia de los sistemas y procesos de negocio que impliquen una nueva valoración de riesgos.”*

**Hallazgo N°2: Sobre la seguridad lógica a nivel de redes, sistema operativo, servicios y bases de datos:**

**Hallazgo N° 2.1**

La unidad de TIC cuenta con el Manual de Políticas de TI, el Manual de Procedimientos de la Unidad de Tecnologías de Información y Comunicación y el instrumento del Sistema Específico para la Valoración de Riesgo Institucional (SEVRI), pero no ha formulado los criterios para la clasificación de los recursos de TI, según su criticidad; no se ha implementado el sistema de gestión de la seguridad de la información (SGSI), que incluya la selección de los controles de acuerdo con la evaluación de riesgos de los activos de información, los procedimientos de monitoreo, registro, revisión y mantenimiento del sistema de gestión, y el proceso y plan de concientización y capacitación a todos los funcionarios.

**Hallazgo N° 2.2**

No se encontraron registros que muestren la revisión de los manuales antes mencionados, de acuerdo con la política de revisión de los documentos. En el Manual de Políticas de TI se encontró que la “Política de nomenclatura en Carpetas de almacenamiento y en documentos de trabajo” está desactualizada, como se describe en el punto 2.1.3

**Hallazgo N° 2.3**

La DNN no cuenta con procedimientos para revisar los roles y los derechos de acceso definidos en el sistema operativo, sistemas de información, bases de datos y otros recursos de TI, que deben ser protegidos, para garantizar la integridad, confidencialidad y disponibilidad de la información.

---

### **Hallazgo N° 2.4**

El Manual de Políticas de TI hace referencia a procedimientos que no están descritos en el Manual de Procedimientos de TIC, tales como la política número 13 de las políticas generales de seguridad de acceso (Manual de Políticas de TI, pág. 30), la cual se refiere a la creación de “*un procedimiento especial para la creación de perfiles y roles de usuario*”.

### **Hallazgo N° 2.5**

La DNN no cuenta con un Plan de Capacitación para dar a conocer y reforzar periódicamente, las políticas, controles y procedimientos de seguridad de la información, que los funcionarios deben conocer y aplicar, para prevenir e informar de forma oportuna sobre vulnerabilidades o amenazas que puedan causar un perjuicio a la organización.

### **Causa**

La DNN no cuenta con un funcionario con rol de oficial de seguridad que se encargue de gestionar la elaboración, revisión y mantenimiento de planes, políticas y procedimientos, así como las actividades para la operación, evaluación y mantenimiento del sistema de gestión de la seguridad de la información de la organización.

### **Efecto**

Este hallazgo representa un riesgo alto, ya que al no disponer de un marco metodológico completo para la seguridad de la información, no mantener actualizadas las políticas y procedimientos, y no realizar una adecuada capacitación y concientización de las políticas y procedimientos de seguridad, la institución se expone a la pérdida de información, debido a la explotación de vulnerabilidades no atendidas, o bien, a la divulgación o modificación no autorizadas de información privada o confidencial.

### **Criterio**

La cláusula 1.4.1, *Implementación de un marco de seguridad de la información*, de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la CGR, establece que:

*“La organización debe implementar un marco de seguridad de la información, para lo cual debe:*



- a. *Establecer un marco metodológico que incluya la clasificación de los recursos de TI, según su criticidad, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concienciación y capacitación del personal.*
- b. *Mantener una vigilancia constante sobre todo el marco de seguridad y definir y ejecutar periódicamente acciones para su actualización.*
- c. *Documentar y mantener actualizadas las responsabilidades tanto del personal de la organización como de terceros relacionados.”*

Adicionalmente, los objetivos de control del anexo A de la norma ISO 27001 establecen los siguientes controles, con respecto a la organización de la seguridad de la información:

*“A.6.1 Organización interna*

*Objetivo: Manejar la seguridad de la información dentro de la organización.*

*A.6.1.1 Compromiso de la gerencia con la seguridad de la información.*

*Control*

*La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.*

*A.6.1.2 Coordinación de la seguridad de la información.*

*Control*

*Las actividades de la seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.*

*A.6.1.3 Asignación de responsabilidades de la seguridad de la información.*

*Control*

*Se deben definir claramente las responsabilidades de la seguridad de la información.”*

Con respecto a los hallazgos 2.2, 2.3 y 2.4, el objetivo de control A.5.1.2, “*Revisión de la política de seguridad de la información*”, de la norma ISO 27001 establece:

*Control*



---

*“La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.”*

Sobre el hallazgo 2.5, la cláusula 1.4.2, *Compromiso del personal con la seguridad de la información*, las Normas Técnicas de la CGR, especifican:

*“El personal debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI.”*

Como complemento a lo anterior, la norma ISO 27001, establece:

*A.5.1.1 Documentar la política de seguridad de la información.*

*Control*

*“La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externa relevantes.”*

*A.8.2.2 Capacitación y educación en seguridad de la información.*

*Control*

*“Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.”*

## **Hallazgo N° 2.6**

Cuando se revisaron las cuentas de usuario de la base de datos, se encontró que a) el usuario administrador (“sa”) de la base de datos está habilitado; b) los dos funcionarios de la unidad de TIC utilizan el usuario “admin” para conectarse a la base de datos; c) la hilera de conexión a las bases de datos usadas por los sistemas de información está sin encriptar; d) no existe una autorización escrita y aprobada con los privilegios que deben tener las cuentas de usuario; y e) la cuenta de usuario “qwizard” tiene asignado el rol de servidor de alto nivel “sysadmin”.

## **Causa**

La unidad de TIC no ha establecido buenas prácticas relacionadas con el control de acceso a las bases de datos. Además, la organización no ha elaborado una lista de roles y privilegios para acceder a los recursos de información, la cual debe

---

ser definida, aprobada, revisada y actualizada periódicamente, de acuerdo con las necesidades de protección de datos y apetito de riesgo.

### **Efecto**

Todos los puntos señalados en este hallazgo atentan contra la integridad y confidencialidad de la información y podrían afectar la disponibilidad de la base de datos, en caso de que se realice alguna acción que impida su uso.

El riesgo existe por las siguientes razones:

- 1) El usuario “sa” (administrador del sistema) tiene el mayor privilegio de acceso a la base de datos y no se le puede quitar;
- 2) cuando dos o más usuarios utilizan la misma cuenta, no se puede determinar quién realizó una acción que haya violentado la integridad, confidencialidad o disponibilidad de los datos, además de que no quedan pistas de auditoría;
- 3) la hilera de conexión a la base de datos debe estar encriptada para evitar que una persona no autorizada acceda a ella, haciéndose pasar por otra o, en este caso, por el sistema de información que la utiliza;
- 4) el rol de servidor “sysadmin” es un rol que tiene los mayores privilegios de acceso en la base de datos y solo debe ser otorgado si es estrictamente necesario y está debidamente autorizado.

Este hallazgo representa un riesgo medio, ya que de acuerdo con la cláusula novena del contrato C-CC-28-02-19-11834, la empresa RACSA ofrece los controles de acceso a nivel perimetral, seguridad física y seguridad lógica de los equipos en donde se encuentra la información de la DNN. Adicionalmente, en la cláusula décimo segunda de dicho contrato, se indica que la infraestructura de red y de tecnología de información cuenta con firewall e IPS (sistema de protección de intrusos). No obstante, el nivel de riesgo puede ser alto si disminuyen las medidas de protección de los equipos y de acceso a los datos de la organización.

### **Criterio**

La cláusula 1.4.5, *Control de acceso*, de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la CGR, establecen que:

*“La organización debe proteger la información de accesos no autorizados. Para dicho propósito debe:*

- 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”.*

*Este inciso, además, señala que “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.”*

Por su parte, la norma ISO 27001 establece los siguientes controles:

*“A.11.2.2 Gestión de privilegios.*

*Control*

*“Se debe restringir y controlar la asignación y uso de los privilegios.”*

*A.11.5.2 Identificación y autenticación del usuario.*

*Control*

*“Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal y exclusivo; se debe elegir una técnica adecuada para verificar la identidad del usuario.”*

### **Hallazgo N° 3: Sobre la evaluación de la continuidad y la disponibilidad del servicio de TIC:**

#### **Hallazgo N° 3.1**

No se cuenta con políticas ni lineamientos para desarrollar planes de continuidad y contingencia a nivel Institucional, con su vinculación a la plataforma tecnológica asociada, según la criticidad de las áreas, capacidad de los activos y servicios que requieran trabajar en contingencia.

#### **Hallazgo N° 3.2**

No se cuenta con contratos robustos que brinde la debida contingencia y recuperación de desastres necesario para soportar la plataforma tecnológica gestionada o instalada por proveedores externos.



---

## Causa

Esto indica que la unidad de Tecnologías de Información no ha realizado formalmente el estudio de impacto de negocio que facilite la identificación de los procesos de misión crítica, de gestión y soporte de la DNN. Además, no hay una definición de la criticidad de las funciones que se desarrollan de cara a la atención de las necesidades y requerimientos de los usuarios interesados de los servicios en la Institución (notarios, usuarios internos, entidades fiscalizadoras, público en general, entre otros). La ausencia de estos insumos dificulta la implementación del plan de continuidad de los servicios operativos y tecnológicos tanto soportados por el personal interno del área de TI como de los proveedores de servicios a la infraestructura tecnológica.

## Efecto

Estos hallazgos representan un Riesgo Alto para la Institución, ya que sin un plan formal de continuidad de los servicios TIC, se puede materializar la pérdida de recursos tangibles, informáticos y financieros por una plataforma que no garantice los niveles de continuidad necesarios para cumplir los requerimientos de atención de las partes interesadas en los servicios ofrecidos por la Institución. Además, dificulta la capacidad de recuperación de la plataforma sustantiva de la DNN ante incidentes que impacten la infraestructura tecnológica, o contar con un plan de inversión que no priorice la plataforma de misión crítica de otros activos secundarios<sup>1</sup>.

## Criterio

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la CGR, definen, con respecto a la continuidad de los servicios:

*“1.4.7 Continuidad de los servicios de TI*

*La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios.*

---

<sup>1</sup> Los “Activos secundarios” son aquellos componentes tecnológicos instalados en la plataforma que realizan las siguientes funciones:

- a. Son equipos de respaldo disponibles para reemplazar activos de producción principales ante un desastre que los inhabilite.
- b. Son equipos de soporte que facilitan servicios continuos de TIC que reducen cargas de trabajo a los activos principales, pero que no afectan la calidad y continuidad de la plataforma en caso de que fallen.
- c. Son equipos en producción que se utilizan para la operación de unidades de negocio que no forman parte de la misión crítica institucional.

---

*Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad.”*

## **Hallazgo N° 4: Sobre la evaluación de la organización funcional del área de Tecnología de Información y Comunicación:**

### **Hallazgo N° 4.1**

No se cuenta con un Plan Estratégico de Tecnologías de Información y Comunicaciones (PETIC) que delimite el nivel de servicio y atención de necesidades de las áreas usuarias de la DNN.

### **Hallazgo N° 4.2**

#### Hallazgo N° 4.2.1

No hay Acuerdos de Nivel de Servicio (SLAs) internos que permitan validar el nivel de servicio, capacidad, operatividad y satisfacción de los usuarios en torno a las capacidades operativas y estratégicas de TI.

#### Hallazgo N° 4.2.2

No se cuenta con una plataforma robusta de mesa de ayuda que facilite la solicitud y monitoree los tiempos de atención y respuesta para atender incidentes de la plataforma tecnológica.

### **Hallazgo N° 4.3**

#### Hallazgo N° 4.3.1

En la condición actual de dos funcionarios activos, los requerimientos de gestión del área y soporte a usuarios puede durar un tiempo indefinido para ser resueltos, y divide la atención del personal de TI entre actividades administrativas y operativas.

#### Hallazgo N° 4.3.2

Uno de los profesionales que trabajan en el área de TI excede el nivel actual de funciones que realiza, con base en el Manual de Puestos de Servicio Civil; entre los criterios que justifican un nombramiento nuevo, están:

- Se establece que un profesional en informática nivel 1-A debe “Participar en estudios e investigaciones para determinar factibilidad de un proyecto” según el manual, sin embargo, el profesional realiza el estudio bajo su responsabilidad y criterio experto, lo cual representa un profesional grado 2 o 3.
- También cuenta con un grado de licenciatura, y más de dos años de experiencia en la Institución (su nivel actual requiere solo un grado bachiller, sin un mínimo de años ejerciendo), los cuales son criterios que ameritan una recalificación del puesto.

#### Hallazgo N° 4.3.3

No se cuenta con personal disponible para los servicios requeridos de Calidad de la Información.

#### Hallazgo N° 4.3.4

No se cuenta con personal suficiente que pueda atender lineamientos de contingencia y recuperación de ambientes de producción institucional.

### **Causa**

Con respecto al Hallazgo N° 4.1, la unidad de Tecnologías de Información no ha realizado las actividades pertinentes para formalizar el Plan Estratégico de Tecnologías de Información y Comunicaciones (PETIC) de la DNN, que incluya lineamientos como (pero no limitado a) estructura organizacional, políticas que regulan el ámbito y procesos de la función de TI, procesos y procedimientos de gestión, marco normativo relacionado y un portafolio de proyectos para la inversión de TIC.

Se propuso subcontratar el desarrollo y formalización del PETIC institucional dotando recursos en el Presupuesto Ordinario 2020. Es importante validar que el cartel de contratación relacionado establezca claramente el contenido del Plan Estratégico, los lineamientos a seguir para identificar las necesidades de las áreas funcionales de la Institución, y que tanto los objetivos particulares del área como el portafolio de proyectos estén debidamente alineados con los del Plan Estratégico Institucional (PEI).

Con respecto al Hallazgo N° 4.2, la unidad de Tecnologías de Información no ha realizado las actividades pertinentes para establecer las métricas de atención y resoluciones de incidentes que afecten la plataforma tecnológica Institucional, ni

atiendan requerimientos o necesidades de las áreas usuarias, según su criticidad, o que se cuente con un canal formal centralizado para la debida gestión de acuerdos de nivel de servicios (SLAs) con las partes interesadas de la DNN.

Con respecto al Hallazgo N° 4.3, la unidad de Tecnologías de Información no cuenta con la estructura funcional suficiente para cumplir con las actividades pertinentes para obtener el máximo beneficio ante el cumplimiento de los objetivos Institucionales y las necesidades que tiene la DNN.

### **Efecto**

Estos hallazgos representan un Riesgo Alto para la Institución, ya que sin una estructura efectiva para la función de TI, no se puede delimitar el ámbito de acción y capacidad de trabajo de la unidad de TI Institucional, y por ende no puede ser evaluado para identificar condiciones críticas u oportunidades de mejora que afecten el cumplimiento de los objetivos de la DNN. Además, no puede cuantificarse el cumplimiento de las funciones de TIC, en función de la valoración de los requerimientos de continuidad, las capacidades de trabajo del área y la capacidad de respuesta de sus funcionarios.

### **Criterio**

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la CGR, definen, con respecto a la formalización de la función de TI:

*“2.1 Planificación de las tecnologías de información*

*La organización debe lograr que las TI apoyen su misión, visión y objetivos estratégicos mediante procesos de planificación que logren el balance óptimo entre sus requerimientos, su capacidad presupuestaria y las oportunidades que brindan las tecnologías existentes y emergentes.*

*[...]*

*3.1 Consideraciones generales de la implementación de TI*

*La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica.”*

Con respecto al soporte a los servicios de TI:

*4.1 Definición y administración de acuerdos de servicio*



---

*La organización debe tener claridad respecto de los servicios que requiere y sus atributos, y los prestados por la Función de TI según sus capacidades.*

*El jerarca y la Función de TI deben acordar los servicios requeridos, los ofrecidos y sus atributos, lo cual deben documentar y considerar como un criterio de evaluación del desempeño. Para ello deben:*

- a. Tener una comprensión común sobre: exactitud, oportunidad, confidencialidad, autenticidad, integridad y disponibilidad.*
- b. Contar con una determinación clara y completa de los servicios y sus atributos, y analizar su costo y beneficio.*
- c. Definir con claridad las responsabilidades de las partes y su sujeción a las condiciones establecidas.*
- d. Establecer los procedimientos para la formalización de los acuerdos y la incorporación de cambios en ellos.*
- e. Definir los criterios de evaluación sobre el cumplimiento de los acuerdos.*

*[...]*

#### *4.4 Atención de requerimientos de los usuarios de TI*

*La organización debe hacerle fácil al usuario el proceso para solicitar la atención de los requerimientos que le surjan al utilizar las TI. Asimismo, debe atender tales requerimientos de manera eficaz, eficiente y oportuna; y dicha atención debe constituir un mecanismo de aprendizaje que permita minimizar los costos asociados y la recurrencia.”*

Con respecto a la estructura organizacional:

#### *“2.1 Independencia y recurso humano de la Función de TI*

*[...], debe brindar el apoyo necesario para que dicha Función de TI cuente con una fuerza de trabajo motivada, suficiente, competente y a la que se le haya definido, de manera clara y formal, su responsabilidad, autoridad y funciones. “*

Con respecto a la calidad:

#### *“1.2 Gestión de la calidad*

*La organización debe generar los productos y servicios de TI de conformidad con los requerimientos de sus usuarios con base en un enfoque de eficiencia y mejoramiento continuo.”*

Con respecto a la contingencia y recuperación:

---

*“1.4.7 Continuidad de los servicios de TI*

*La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios.*

*Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad.”*

**Hallazgo N° 5: Sobre los controles de seguridad lógica en el sistema de misión crítica:**

**Hallazgo N° 5.1**

Cuando se revisaron los controles de seguridad del sistema SGIN 1.0 (Hermes Soft), se encontró que a) existen problemas con la asignación de derechos de acceso; b) la vigencia de la contraseña es indefinida (no requiere que se cambie); y c) la cuenta de usuario no se bloquea después de tres intentos de ingreso fallido.

**Causa**

La brecha de seguridad encontrada indica que o bien no se establecieron los requisitos de seguridad apropiados, o no se realizaron las pruebas necesarias para comprobar su implementación.

**Efecto**

Todos los puntos señalados en este hallazgo atentan contra la integridad y la confidencialidad de la información y podrían afectar la disponibilidad de la base de datos, en caso de que se realice alguna acción que impida su uso.

El riesgo existe por las siguientes razones:

- 1) El sistema dificulta la asignación de derechos de acceso, debido a que los privilegios de un rol pueden anular los privilegios de otro, cuando ambos roles se asignan a un funcionario;
- 2) en el caso de la consulta de tomos de los notarios, el sistema permite el acceso a la edición y eliminación de datos a funcionarios (los de la unidad de Fiscalización Notarial) que no deberían tenerlo;
- 3) al ser la contraseña indefinida (el usuario no tiene que cambiarla periódicamente), un atacante, interno o externo, dispone de más tiempo para descubrirla;



- 4) cuando no se bloquea la cuenta del usuario después de al menos tres intentos de ingreso fallido, un atacante podría intentar descubrir la contraseña de un usuario de forma indefinida hasta lograrlo. Al bloquear la cuenta del usuario y cambiar la contraseña por medio de un procedimiento apropiado (por ejemplo, que la restauración de la contraseña envíe una advertencia al oficial de seguridad de la información), se alerta al administrador de la seguridad de la posible ocurrencia de un ataque.

Este hallazgo representa un riesgo alto, ya que, en el primer caso, la aplicación no garantiza el acceso a la información a personas autorizadas (violación de la disponibilidad); en el segundo caso, el sistema obliga a dar acceso a un grupo de funcionarios a opciones no autorizadas (violación de la confidencialidad e integridad); en el tercer y cuarto casos, se facilita el descubrimiento de la contraseña por parte de un atacante.

### **Criterio**

La cláusula 1.4.5, *Control de acceso*, de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la CGR, establece que:

*“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.”*

Adicionalmente, los objetivos de control del anexo A de la norma ISO 27001 establecen los siguientes controles, con respecto al control de acceso:

*“A.11.2 Gestión del acceso del usuario.*

*Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información.*

*A.11.2.2 Gestión de privilegios.*

*Control*

*Se debe restringir y controlar la asignación y uso de los privilegios.*

*A.12.1 Requerimientos de seguridad de los sistemas.*

*Objetivo: Asegurar que la seguridad sea una parte integral de los sistemas de información.*

---

*A.12.1.1 Análisis y especificación de los requerimientos de seguridad.*

*Control*

*Los enunciados de los requerimientos comerciales para sistemas nuevos, o mejorar los sistemas existentes, deben especificar los requerimientos de los controles de seguridad.”*

**Hallazgo N° 6: Sobre la administración de las bases de datos y los controles de privacidad de datos personales:**

**Hallazgo N° 6.1**

Las bases de datos no se monitorean. La unidad de TIC no cuenta con procedimientos de monitoreo y mantenimiento de la base de datos. El monitoreo se realiza para prevenir problemas de rendimiento, espacio y uso de los recursos de TI. El mantenimiento es la aplicación de los procedimientos preventivos o correctivos para optimizar el rendimiento de la base de datos. Esto incluye el tratamiento de datos históricos, el cual está contemplado en las “Políticas de tiempos de almacenamiento de información en bases de datos”.

**Causa**

La unidad de TIC no ha establecido la política ni el procedimiento para realizar las tareas de monitoreo y mantenimiento de las bases de datos, con respecto a la capacidad, rendimiento y afinamiento de este recurso. El Manual de Políticas de TI no cuenta con una política relativa al monitoreo de las bases de datos de la organización, en el sentido relacionado con este hallazgo.

**Efecto**

Este hallazgo representa un riesgo alto, ya que el monitoreo y el mantenimiento de las bases de datos son parte de los controles necesarios para asegurar la disponibilidad de la información. La ausencia de monitoreo y mantenimiento impiden prevenir problemas relacionados con el crecimiento de las bases de datos, el espacio disponible, el rendimiento, y la gestión de datos, bitácoras y datos históricos, así como su vigencia tecnológica.

**Criterio**

La cláusula 4.2, *Administración y operación de la plataforma tecnológica*, de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la CGR, establece que:



---

*“La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:*

- a. Establecer y documentar los procedimientos y las responsabilidades asociados con la operación de la plataforma.*
- b. Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas.”*

## **Hallazgo N° 6.2**

De acuerdo con las “Políticas sobre Administración y mantenimiento de bases de datos”, la unidad de TIC debe llevar un registro de los cambios realizados en la base de datos. Durante la realización de esta auditoría, la unidad de TIC no cuenta con un archivo o base de datos en donde se puedan registrar los cambios que se realicen en las estructuras y procedimientos almacenados, como producto del mantenimiento correctivo o evolutivo de los sistemas de información.

### **Causa**

La unidad de TIC no ha implementado las Políticas sobre Administración y mantenimiento de bases de datos, la cual existe en el marco normativo de TI, relativa al registro de los cambios en la base de datos.

### **Efecto**

El registro de los cambios en la base de datos es una política orientada a mantener actualizada la arquitectura de información de la organización, “con el fin de optimizar la integración, uso y estandarización de sus sistemas de información”, como se establece en la cláusula 2.2 de las Normas Técnicas, la cual se cita en los criterios. La ausencia de estos registros impide comprobar que los cambios sean necesarios, autorizados, que sigan un procedimiento estándar y que contribuyan a mejorar la calidad de los datos y la arquitectura de información de la organización.

Contar con una arquitectura de datos adecuada a las necesidades de la organización, que además esté documentada y actualizada, tiende a reducir los costos de mantenimiento de los sistemas de información, reduce la duplicidad de datos y funciones, facilita la integración entre sistemas y permite la reutilización de funciones y procedimientos para obtener y procesar los datos.

### **Criterio**

---

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la CGR, establecen:

*“2.2 Modelo de arquitectura de información*

*La organización debe optimizar la integración, uso y estandarización de sus sistemas de información de manera que se identifique, capture y comunique, en forma completa, exacta y oportuna, solo la información que sus procesos requieren.*

*4.2 Administración y operación de la plataforma tecnológica*

*La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:*

- d. Controlar la composición y cambios de la plataforma y mantener un registro actualizado de sus componentes (hardware y software) (...).*
- e. Controlar la ejecución de los trabajos mediante su programación, supervisión y registro.”*

Adicionalmente, en las *Políticas sobre Administración y mantenimiento de bases de datos* del Manual de Políticas de TI, se especifica que:

- 3. “Todo cambio o ajuste hecho en el proceso de mantenimiento se deberá dejar documentado en una bitácora para control y seguimiento.”*

### **Hallazgo N° 6.3**

El artículo 36 del Reglamento a la Ley N° 8968, “Protección de la persona frente al tratamiento de sus datos personales”, especifica las acciones que se deben realizar para la seguridad de los datos personales. De los siete controles establecidos por este artículo, la unidad de TIC cumple solo el que corresponde al inciso c, del artículo mencionado: *“Crear y mantener actualizado un inventario de la infraestructura tecnológica, incluyendo los equipos y programas de cómputo y sus licencias.”*. Los demás controles establecidos en el artículo 36 del Reglamento se especifican en el apartado 6.2.1 de este documento.

### **Causa**

No se ha establecido una estrategia formal de implementación de los controles para la protección de datos personales, ya que el señor Carlos Cerdas Lazo manifiesta que la protección de datos “es todo un proyecto a implementar a nivel

---

institucional, el cual será colocado dentro de la cartera de proyectos que se definan en el desarrollo del PETIC para el próximo año.”.

### **Efecto**

La organización corre el riesgo de divulgar información de acceso restringido o datos sensibles de los notarios públicos, causando un perjuicio al propietario de esta información y haciéndose acreedor a las sanciones establecidas en el artículo 28 de la Ley 8968 y a las sanciones penales que se deriven de las demandas interpuestas por los afectados en las instancias judiciales.

### **Criterio**

El artículo 2 de la Ley 8968 especifica:

*“Esta ley será de aplicación a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos.”*

## **XI. Conclusiones**

La Dirección Nacional de Notariado cuenta con controles de acceso lógico a la red institucional, al sistema operativo, a las bases de datos y a los sistemas de información. Sin embargo, no se cuenta con listas de perfiles y derechos de acceso definidos y aprobados, para facilitar tanto la asignación y actualización de accesos como la comprobación de los accesos asignados a los recursos de TI.

La unidad de TIC cuenta con el Manual de Políticas de TI, el Manual de Procedimientos de TIC y un instrumento (en Excel) para la evaluación de riesgos (SEVRI), pero no se han implementado procesos para la clasificación y etiquetado de los recursos de TI, la identificación, diseño e implementación de controles, el monitoreo, evaluación periódica y el mantenimiento de los controles para la seguridad de la información. La DNN tampoco cuenta con un plan de capacitación y concientización sobre la seguridad de la información. La implementación de estos procesos conforma la totalidad del marco metodológico requerido por las Normas Técnicas.

Las políticas y procedimientos sobre la seguridad de la información, definidos en el Manual de Políticas de TI y el Manual de Procedimientos de TIC, son desconocidos por los funcionarios de la DNN. No se encontró evidencia de que estos manuales hayan sido revisados y actualizados desde su elaboración. Además, se pudo comprobar que el Manual de Políticas de TI hace referencia a procedimientos que no están definidos en el Manual de Procedimientos, tales como el procedimiento especial para la creación de

---

perfiles y roles de usuario, al que se hace referencia en las Políticas generales de seguridad de acceso.

Una debilidad importante con respecto al control de acceso es la falta de comunicación inmediata del cese o suspensión de labores de un funcionario debido a permisos, vacaciones, incapacidad o cese de la relación laboral, con lo cual se crea una brecha que atenta contra la seguridad de la información, como se describe en la sección de Identificación de oportunidades y hallazgos. La comunicación del cese o suspensión de labores está contemplada en las Políticas generales de seguridad de acceso, en el Manual de Políticas de TI.

El sistema de misión crítica de la DNN cuenta con los controles usuales de acceso y se están realizando mejoras en este aspecto, como parte del mantenimiento del sistema por parte de la Empresa de Servicios Públicos de Heredia (ESPH), tales como la autenticación por medio del *Active Directory* y la firma electrónica. Sin embargo, las principales debilidades encontradas en el tema de control de acceso son la falta de definición de roles y privilegios por parte del propietario de la información, la ausencia de la figura del “propietario de la información” y la falta de revisión de la bitácora de las acciones realizadas por los usuarios.

Con base en las declaraciones del personal de TIC, el sistema SGIN no se pudo instalar al término de su desarrollo por errores no detectados durante las pruebas y problemas en la vigencia de los requerimientos definidos en el alcance. Fue necesario invertir recursos adicionales para agregar las funcionalidades mínimas para su uso. Desde su inicio, el sistema presentó fallas, problemas de eficiencia y dificultades para darle mantenimiento, por lo que fue necesario contratar una empresa para actualizarlo, mejorarlo y corregir los problemas detectados.

La usuaria del mantenimiento de la página Web manifiesta no tener dificultades ni quejas para actualizar la página, y muestra su conformidad y satisfacción con el soporte que recibe de la empresa desarrolladora.

Como parte de este estudio, se identifica una debilidad sustantiva por parte del área de TI en la gestión y control de entrega de servicios por parte de contratistas externos, ya que están limitados en implementar acciones para validar el cumplimiento de los requerimientos de los servicios contratados; además, el riesgo por incumplimientos se incrementa por no contar con acuerdos formales de Acuerdos de Nivel de Servicio (SLAs), no contar con un inventario ordenado de proveedores de servicios clasificados por la calidad del servicio y capacidad operativa, ni contar con lineamientos para realizar inspecciones.

El área de TI no cuenta con lineamientos de continuidad ni la activación de un centro de procesamiento en caso de contingencia, ni procedimientos de recuperación de desastres a nivel tecnológico; además, hay incertidumbre de que los proveedores de servicios cuenten con la capacidad de operar en caso de contingencia con sus respectivas plataformas.

---

De cara a la organización funcional del área de TI Institucional, se tienen debilidades con respecto al uso y efectividad de la atención a usuarios por medio de un canal formal de mesa de ayuda, los cuales son atendidos por medios informales como correos electrónicos, llamadas o solicitudes presenciales.

Además, al ser una unidad de solo dos personas activas, se identifican las siguientes debilidades:

- Debilidades para dar seguimiento a la gestión administrativa y operativa del área de TI.
- Dificultades para atender necesidades del personal usuario de la DNN de forma eficiente y además cumplir con las funciones internas que demanda el área en cuestión.
- Falta de un PETIC que defina los lineamientos base de gobierno de TI.
- Falta de lineamientos para valorar el nivel de satisfacción del personal de cara a TI.

El control de acceso a las bases de datos es apropiado, ya que los usuarios no tienen acceso directo a ellas y los proveedores no tienen acceso a las bases de datos en Producción. Además, la DNN cuenta con protección de la red institucional por medio de un firewall y protección a nivel de infraestructura (firewall) y antivirus por parte de RACSA. Las bases de datos se respaldan todos los días, como parte del respaldo de los servidores contratados a la empresa RACSA. Sin embargo, la unidad de TIC no realiza tareas de monitoreo ni afinamiento de las bases de datos, lo cual impide prevenir problemas de desempeño y la disponibilidad del servicio. Los datos históricos no se gestionan, ya que toda la información se almacena en las mismas estructuras de datos, sin importar su antigüedad o vigencia.

No se encontró evidencia de que se divulguen datos personales de notarios o funcionarios de la DNN, que no sean de carácter público, de acuerdo con lo previsto en la Ley de la República 8968, Protección de la persona frente al tratamiento de sus datos personales; sin embargo, la unidad de TIC no cuenta con políticas ni procedimientos para la identificación y tratamiento de datos personales, conforme a esta Ley, ni se han implementado los controles especificados en el artículo 36 de su reglamento, por lo que se está incumpliendo con la legislación para la protección de datos personales.

---

## **XII. Recomendaciones**

A continuación, se presentan recomendaciones con base en los hallazgos descritos en la sección IX de este informe. En cada caso se hace referencia a los hallazgos por medio del número que los identifica.

### **A la Dirección Ejecutiva**

1. Definir la estrategia para implementar el sistema de Gestión de Seguridad de la Información, con el fin de establecer, operar, mantener, monitorear y dar mantenimiento a los controles que permitan proteger la confidencialidad, integridad y disponibilidad de la información.

Riesgo Alto, Hallazgo No. 2.1

2. Asignar la función de oficial de la seguridad de la información (OSI) a un funcionario de la organización, que se encargue de coordinar los esfuerzos relacionados con el establecimiento, implementación, operación, monitoreo, revisión y mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI).

El oficial de seguridad de la información debe tener conocimientos en Gestión de seguridad de la información, ya sea de la ISO 27001, CISM (*Certified Information Security Manager*), CISSP (*Certified Information Systems Security Professional*), o alguna otra. Preferiblemente, debe tener formación en el área de cómputo, y es deseable que tenga conocimientos en gestión de riesgos. Puede ser un funcionario de cualquier unidad de la Institución.

Riesgo Alto, Hallazgo No. 2.1

3. Elaborar un Plan de Concientización y Capacitación en Seguridad de la Información que aplique tanto a los nuevos funcionarios, como parte de la inducción, como a los funcionarios actuales, para comunicar las políticas y controles de seguridad física y lógica y reforzar estas prácticas periódicamente para reducir los riesgos debidos al factor humano.

Riesgo Alto, Hallazgo No. 2.1 y 2.5

### **A la unidad de Tecnologías de Información y Comunicación**

4. Desarrollar el Plan Estratégico de Tecnologías de Información, que, entre otros aspectos, incluya (aunque no se limite a):
  - a. Misión, visión y valores para conocer la trayectoria de corto, mediano y largo

---

plazo de la estrategia de la gestión de la Dirección Nacional de Notariado.

- b. Estructura funcional de TI, de cara a: perfiles, responsabilidades, ámbito de acción y categoría de puesto.
- c. Objetivos específicos del área, alineados con los objetivos del Plan Estratégico Institucional y sus métricas, para constituir un plan táctico de atención ordenado y oportuno.
- d. Requerimientos técnicos, funcionales y estratégicos de las distintas áreas de la DNN para que se vean reflejadas como requerimientos del portafolio de proyectos Institucional.
- e. Lineamientos para la constitución de Acuerdos de Nivel de Servicio (SLAs) Institucionales.
- f. Capacitación tanto al área como al personal Institucional.
- g. Metodología de proyectos, de calidad y de gestión de TI.
- h. Marco de gobierno de TI, así como los planes de continuidad de los servicios tecnológicos.

Riesgo Alto, Hallazgos del No. 1 al 6.

- 5. Desarrollar los lineamientos e implementar controles para la debida diligencia en la entrega de servicios de TI por parte de terceros, en especial incluir los instrumentos necesarios para la implementación de Acuerdos de Nivel de Servicio (SLAs).

Riesgo Alto, Hallazgo No 1.

- 6. Revisar, actualizar y gestionar la aprobación de los Manuales de Políticas, Procedimientos y documentos relacionados con la seguridad de la información, de acuerdo con los períodos que se definan para cada uno de ellos. Las políticas y procedimientos también deben ser revisados y actualizados ante una decisión ejecutiva que implique un cambio en las políticas. Las políticas y procedimientos deben actualizarse antes de implementar los cambios en la organización.

Riesgo Alto, Hallazgo No. 2.2

- 7. Revisar, actualizar y gestionar la aprobación del Manual de Procedimientos de TIC para incorporar los procedimientos con base en el Manual de Políticas y los que se deriven de la implementación de controles para proteger los recursos de TI. El Manual de políticas hace referencia a procedimientos que

---

no se encuentran en el Manual de Procedimientos. Los procedimientos deben identificar claramente el responsable de su ejecución y, cuando corresponda, el momento en que se debe iniciar y finalizar.

Riesgo Alto, Hallazgo No. 2.3 y 2.4

8. Se recomienda: 1) Deshabilitar la cuenta de inicio de sesión del administrador del sistema (“sa”); 2) crear cuentas de usuario únicas para cada funcionario, con los privilegios que le correspondan de acuerdo con su función y responsabilidades; 3) definir formal y oficialmente las cuentas que deben existir en las bases de datos y los roles y privilegios que deben tener, de acuerdo con los principios de “necesidad de saber”, “necesidad de hacer” y “menor privilegio”; 4) comprobar si la cuenta “qwizard” debe tener el rol “sysadmin”, en cuyo caso debe quedar justificado y aprobado en un documento formal.

Riesgo Medio, Hallazgo No. 2.6

9. Para futuros sistemas de información, que la DNN adquiera o que se desarrollen de forma interna, se recomienda incluir el requerimiento de que la hilera de conexión a la base de datos esté encriptada por medio de un algoritmo confiable y que la contraseña incluya características de una contraseña fuerte.

Riesgo Medio, Hallazgo No. 2.6

10. Desarrollar los lineamientos necesarios para un plan de continuidad a nivel Institucional, que integre la arquitectura de procesos Institucionales y su debida priorización de atención, contingencia y recuperación, alineado con los sistemas de información y activos tecnológicos sustantivos que soportan los procesos de misión crítica Institucional.

Riesgo Alto, Hallazgo No. 3.1.

11. Formalizar los contratos necesarios de mantenimiento preventivo, soporte correctivo y crecimiento de la plataforma tecnológica que requiere talento especializado de proveedores externos.

Riesgo Alto, Hallazgo No. 3.2.

12. Implementar una plataforma de mesa de ayuda que facilite la formalización de atención a usuarios Institucionales, formalizando los respectivos Acuerdos de



---

Nivel de Servicio (SLAs) según incidentes, requerimientos de atención y prioridad de resolución, que además facilite la evaluación del desempeño de atención y resolución para detectar condiciones sensibles de la infraestructura tecnológica Institucional.

Riesgo Medio, Hallazgos No. 4.1 y 4.4.

13. Realizar un diagnóstico de cargas de trabajo, responsabilidades y ámbito de acción del área de Tecnologías de Información, para constituir una organización funcional óptima para atender las necesidades de operación, soporte y estrategia tecnológica, alineada con los requerimientos del personal Institucional, con su personal debidamente categorizada y justificada a nivel de puesto profesional, máxime que se tiene dependencia de dos funcionarios y en caso de rotación se materializaría un riesgo de continuidad de la operación de la UTIC.

Riesgo Alto, Hallazgos No. 4.2, 4.3, 4.6 y 4.7.

14. Para futuros sistemas de información, que la DNN adquiera o que se desarrollen de forma interna, se recomienda que la cuenta de los usuarios incluya atributos que permitan 1) establecer la vigencia de la contraseña, 2) la obligación de cambiar la contraseña cuando se ingresa por primera vez al sistema, 3) bloquear la cuenta cuando se realicen tres intentos de ingreso fallidos. Adicionalmente, se recomienda implementar los controles de seguridad relacionados con la administración de las cuentas de usuario y contraseñas y la generación de reportes de la bitácora, presentadas en el anexo número 5, así como las prácticas de seguridad descritas en el anexo número 6.

Riesgo Alto, Hallazgo No. 5.1

15. Para futuros sistemas de información, que la DNN adquiera o que se desarrollen de forma interna, se recomienda que se realicen las pruebas técnicas y las pruebas de aceptación del módulo de Administración de usuarios, con pruebas adecuadas para detectar defectos como los descritos en el Hallazgo N° 5.1.

Riesgo Alto, Hallazgo No. 5.1

16. Incluir en el Manual de Procedimientos de TIC los procedimientos para monitorear y dar mantenimiento periódico a las bases de datos de la DNN, con base en la descripción del Hallazgo N° 6.1.

---

Riesgo Alto, Hallazgo No. 6.1

17. Capacitar al Analista de Sistemas de Información y Bases de datos como Administrador de Base de Datos (DBA), con el fin de realizar el monitoreo y mantenimiento adecuados de las bases de datos de la organización.

Riesgo Alto, Hallazgo No. 6.1

18. Revisar las políticas de TI y procedimientos de TIC para aplicar las políticas y procedimientos establecidos por la organización.

Riesgo Alto, Hallazgo No. 6.2

19. Implementar los requerimientos establecidos en el artículo 36 del Reglamento a la Ley N° 8968, "Protección de la persona frente al tratamiento de sus datos personales", los cuales son de acatamiento obligatorio.

Riesgo Alto, Hallazgo No. 6.3

## **ANEXOS**

## Anexo 1: Documentos de referencia

Para realizar este estudio se consultaron los siguientes documentos:

N°	Descripción	Documento
E01	Respuesta de la señora Hazel Mata Hidalgo sobre cláusula de confidencialidad.	\\Respuesta contrato de confidencialidad\\Correo sobre contrato de confidencialidad.PNG
E02	Eliminación de cuentas de correo.	\\Varios\\ DNN-DE-834-2019 (eliminación de cuentas).pdf
E03	Lista de computadoras arrendadas y funcionario responsable. Formato de boleta de entrega.	\\Inventarios y digramas\\Inventario arrendamiento DNN.xlsx
E04	Inventario de sistemas y servidores de la DNN.	\\Inventarios y digramas\\Inventario de sistemas-servidores.xlsx
E05	Diagrama de la red institucional.	\\Inventarios y digramas\\Digrama_de_red_DNN.png
E06	Contrataciones vigentes	\\Lista de contrataciones vigentes\\Contrataciones vigentes.xlsx
E07	ESET License Administrator	Pantallazo de administrador de antivirus ESSET\\ESSET.PNG
E08	Especificación técnica para desarrollo, alojamiento y mantenimiento del sitio Web	\\Contratos con proveedores\\Especificaciones Tecnicas Sitio Web V06 - DE - UTIC.pdf
E09	Contrato para la prestación del servicio de servidor virtual	\\Contratos con proveedores\\doc00095120191031165917.pdf
E10	Oferta ESPH para el mantenimiento del sistema SGIN.	\\05 Documentos DNN\\Oferta ESPH\\ESPH – Oferta DNN 2018LA-000003-0007 Mantenimiento de Sistemas.pdf
E11	Oferta Desarrollo y mantenimiento sitio Web	\\05 Documentos DNN\\Oferta página web\\MANATI Oferta - DNN - con firma.pdf
E12	Diagnóstico sistema SGIN 1.0	\\Diagnostico SGIN 1.0\\Diagnóstico Sistema SGIN - DNN.docx
E13	Manual de políticas de TI	\\Manuales Politicas y procedimientos\\Manual_ Políticas_TI_V2.pdf
E14	Manual de procedimientos de TIC	\\Manuales Politicas y procedimientos\\Manual de Procedimientos de la Unidad de Tecnologías de Información y Comunicación.pdf
E15	Herramienta SEVRI para la gestión de riesgos	\\SEVRI-Riesgos\\HERRAMIENTASEVRI 2018-2019- R-013.xlsm

N°	Descripción	Documento
E16	Manual Organizacional y funcional	\\05 Documentos DNN\02 Manual Organizacional y Funcional Dirección Nacional de Notariado v.3.pdf
E17	Ley 8968, PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES, 7/7/2011.	Ley 8968 - Protección de datos personales.docx
E18	Decreto Ejecutivo n.º 37554-JP REGLAMENTO A LA LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES, 5/3/2013	Decreto_37554JP20102012ReglamentoCosta Rica.pdf

---

## **Anexo 2: Controles implementados**

La DNN, por medio de la unidad de TIC, ha implementado los siguientes controles de seguridad lógica:

1. Todos los usuarios tienen un código de usuario y una contraseña para acceder a la red de la institución.
2. Los parámetros para la creación de contraseñas de usuarios de la red institucional (Active Directory) establecen que las contraseñas deben incluir:
  - Letras mayúsculas y minúsculas.
  - Números y caracteres especiales.
  - Al menos siete caracteres.
  - Las contraseñas no se pueden repetir.
3. Los usuarios no cuentan con permiso de administrador en sus equipos de trabajo y no tienen acceso a los comandos del sistema operativo. Solo el personal de TIC puede instalar software en las computadoras de trabajo de los funcionarios.
4. Las computadoras de trabajo de todos los funcionarios cuentan con el antivirus ESET NOD32 actualizado. La herramienta ESET License Administrator le permite al personal de TIC detectar las computadoras que no tienen el antivirus actualizado [E07]. Cuando esto ocurre, TIC se encarga de investigar el motivo y aplicar la actualización de los equipos.
5. Una computadora puede tener el antivirus desactualizado en los siguientes casos: a) cuando el funcionario está incapacitado, con permiso o de vacaciones; o b) cuando el personal de la unidad de Fiscalización realiza su labor fuera de las oficinas de la DNN.
6. El antivirus se encarga de “escanear” los dispositivos externos que se conectan a la computadora (memoria USB, discos duros, teléfono, etc.), en busca de virus. Si el antivirus detecta alguna amenaza, borra el archivo de inmediato.
7. Los funcionarios de la DNN no tienen acceso directo a las bases de datos de Producción. El acceso se realiza por medio de los sistemas de información que utilizan, según sus funciones. La base de datos solo cuenta con el usuario “sa”, el usuario “admin” para uso del analista de sistemas de información y bases de datos de TIC, y las cuentas de usuario que utilizan los sistemas de información para acceder a los datos.



---

### **Anexo 3: Evaluación con base en las Normas Técnicas**

Como resultado de las entrevistas y la revisión de documentos aportados por los funcionarios de la unidad de TIC, se encontraron los siguientes incumplimientos de las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE).

El anexo número 1, Documentos de referencia, contiene las referencias a documentos relacionados con evidencias o hallazgos producto de esta auditoría. Las referencias se identifican de la siguiente manera: “[E###]”, donde “##” es un número que identifica al documento.

#### **Cláusula 1.1 Marco estratégico de TI**

*El jerarca debe traducir sus aspiraciones en materia de TI en prácticas cotidianas de la organización, mediante un proceso continuo de promulgación y divulgación de un marco estratégico constituido por políticas organizacionales que el personal comprenda y con las que esté comprometido.*

#### **Cláusula 2.1 Independencia y recurso humano de la Función de TI**

*El jerarca debe asegurar la independencia de la Función de TI respecto de las áreas usuarias y que ésta mantenga la coordinación y comunicación con las demás dependencias tanto internas y como externas.*

*Además, debe brindar el apoyo necesario para que dicha Función de TI cuente con una fuerza de trabajo motivada, suficiente, competente y a la que se le haya definido, de manera clara y formal, su responsabilidad, autoridad y funciones.*

#### **Cláusula 1.4.1 Implementación de un marco de seguridad de la información**

*La organización debe implementar un marco de seguridad de la información.*

1. La DNN no cuenta con un marco metodológico como lo especifica el inciso a de la cláusula 1.4.1 de las Normas Técnicas.

La creación del marco metodológico consiste en el establecimiento, implementación y operación, monitoreo y mantenimiento de un sistema de gestión para la seguridad de la información, basado en la clasificación de los activos y su exposición al riesgo.

En la actualidad, la Dirección Nacional de Notariado no sigue ninguna norma, guía o estándar para la gestión de la seguridad de la información.

2. La Dirección Nacional de Notariado cuenta con un manual de políticas de TI,

con fecha de noviembre del 2013. Sin embargo, la unidad de TIC no cuenta con registros que comprueben que este documento haya sido revisado y actualizado desde esa fecha.

En la sección “Actualizaciones de este manual”, en la página número 4 del Manual de Políticas de TI, se establece que este debe ser “revisado y actualizado formalmente por lo menos una vez cada tres años o en las ocasiones en que se considere necesario (...)”.

3. La Dirección Nacional de Notariado no cuenta con una clasificación de sus activos de información para determinar el grado de confidencialidad de estos.

La clasificación de los activos de información y la evaluación de los riesgos a los que están expuestos, son la base para el diseño de controles para su seguridad.

El objetivo de control A.7.2.1 del estándar ISO/IEC 27001:2005 especifica que “La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.”.

#### **Cláusula 1.4.2 Compromiso del personal con la seguridad de la información**

*El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI.*

4. La DNN no cuenta con un plan de capacitación en seguridad de la información. El personal de TIC manifiesta que no se ha brindado capacitación sobre este tema a los funcionarios de la DNN, y que no se brinda información a los nuevos funcionarios en aspectos de seguridad y confidencialidad.

El inciso a de la cláusula 1.4.2 especifica que la organización debe “Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI.”.

5. La DNN no cuenta con mecanismos, tales como revisiones o evaluaciones, para vigilar el cumplimiento de las responsabilidades de los funcionarios, como se estipula en el inciso b de la cláusula 1.4.2 de las Normas Técnicas.

La señora Hazel Mata Hidalgo, de Recursos Humanos, manifiesta, mediante correo [E01], que el contrato de trabajo no contiene una cláusula de confidencialidad, por lo que no existe el compromiso para no divulgar información interna o confidencial de la DNN, por parte de los funcionarios.

El inciso c de la cláusula 1.4.2 de las Normas Técnicas especifica que se debe “Establecer, cuando corresponda, acuerdos de confidencialidad y medidas de seguridad específicas relacionadas con el manejo de la documentación y



rescisión de contratos”.

Los acuerdos de confidencialidad son necesarios cuando la organización recibe, almacena y procesa información confidencial o privada, que no debe ser divulgada por los funcionarios. La clasificación de la información es la herramienta para determinar el grado de confidencialidad y criticidad de este recurso.

#### **Cláusula 1.4.4 Seguridad de 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.*

6. No se encontró en el Manual de Procedimientos de la unidad de TIC, un procedimiento para proteger la información almacenada como se especifica en el inciso b de la cláusula 1.4.4, Seguridad de las operaciones y comunicaciones de las Normas Técnicas.

#### **Cláusula 1.4.5 Control de acceso**

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

7. Las políticas contenidas en el Manual de Políticas TI, para el control de acceso a la información no han sido comunicadas a los funcionarios de la DNN. Se corre el riesgo de que algún funcionario viole alguna norma de seguridad, o que sea víctima de un ataque externo (ingeniería social, *malware*, correo no deseado, etc.) por desconocimiento, y que esto cause algún perjuicio a la Dirección Nacional de Notariado, a un notario público o a otro empleado.

Las políticas de control de acceso deben ser explicadas al inicio de la relación laboral, y deben ser reforzadas periódicamente a todo el personal, para evitar la materialización de riesgos relacionados con su desconocimiento, olvido, u otro factor humano.

8. El Manual de Procedimientos de la Unidad de Tecnologías de Información y Comunicación contiene el procedimiento TI-003-2, Administración de Acceso a Recursos de Sistemas de Información y base de datos, el cual describe los pasos para la modificación de accesos (pág. 37). Sin embargo, este manual no cuenta con procedimientos específicos para la creación de cuentas de usuarios y la deshabilitación de cuentas cuando se termina la relación laboral.

El señor Carlos Cerdas Lazo de la unidad de TIC manifiesta que:

- Cuando ingresa un nuevo funcionario a la DNN, la unidad correspondiente no realiza las gestiones para la creación de las cuentas

de usuario y la asignación de permisos, con suficiente anticipación; la solicitud se hace el primer día de trabajo del nuevo funcionario, lo que atrasa el inicio de sus labores.

- Cuando cesa la relación laboral entre un funcionario y la DNN, la unidad correspondiente no informa a la unidad de TIC para que esta proceda a eliminar los accesos y deshabilitar las cuentas de usuario [E02]. Debido a esto, el exfuncionario podría utilizar la cuenta de correo de la DNN o acceder a los archivos compartidos en el Sharepoint de la institución, por medio de la aplicación de Office 365.

La DNN se expone al uso no autorizado de las cuentas de correo y de la información disponible en el repositorio compartido. Además, se incumplen las políticas generales de seguridad de acceso número 3, 4, 5 y 8 de las políticas relativas a seguridad del Manual de Políticas de TI.

9. La DNN cuenta con un inventario de las computadoras arrendadas a la empresa PC Central [E03] y una lista de los servidores locales y remotos [E04], pero no cuenta con una clasificación de los recursos de TI, en términos de su grado de criticidad y sensibilidad, como lo establece el inciso b de la cláusula 1.4.5 de las Normas Técnicas.

La clasificación de los recursos de TI y el análisis de riesgos son necesarios para la priorización en el diseño, operación y monitoreo de controles de seguridad. La ausencia de esta clasificación aumenta el riesgo de desatender un recurso crítico de TI para las operaciones de la DNN.

10. La DNN no cuenta con procedimientos para la definición de perfiles, roles y niveles de privilegio, para identificar y autenticar el acceso a la información, tanto para usuarios como recursos de TI, conforme a lo establecido en el inciso d de la cláusula 1.4.5 de las Normas Técnicas.

Los funcionarios de TIC utilizan el mismo código de usuario (usuario "admin") para acceder a las bases de datos de Producción.

La política número 13 de las Políticas generales de seguridad de acceso del Manual de Políticas de TI establece que:

"La Unidad de Tecnologías de Información y Comunicación establecerá un procedimiento especial para la creación de perfiles y roles de usuario, tomando en consideración los criterios de las jefaturas de unidad, las recomendaciones de control interno y las políticas de seguridad establecidas en este manual."

11. El señor Fabián Mora de la unidad de TIC manifiesta que no existe la figura de "propietario de la información", el cual es el responsable de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones, conforme a lo establecido en el inciso e de la cláusula 1.4.5 de las Normas Técnicas.

De acuerdo con el estándar ISO/IEC 27001, Requerimientos del Sistema de

---

Gestión de la Seguridad de la Información, “El término ‘propietario’ identifica a una persona o entidad que tiene la responsabilidad gerencial aprobada para controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos.”.

12. La unidad de TIC ha implementado el uso de cuentas de usuario y contraseñas para identificar y responsabilizar a quienes utilizan los recursos de TI (red, sistemas de información), pero no cuenta con los procedimientos para la requisición, aprobación, establecimiento, suspensión y desactivación de las cuentas de usuario, ni procedimientos para su revisión, actualización periódica y atención de usos irregulares, de acuerdo con el inciso f de la cláusula 1.4.5 de las Normas Técnicas.
13. Los funcionarios de la DNN tienen acceso de lectura y escritura a carpetas compartidas de trabajo según el área en la que están asignados. El riesgo es que pueden alterar o borrar, accidentalmente o intencionalmente, información de los archivos creados por otros funcionarios que comparten la misma carpeta.

El mecanismo utilizado por la unidad de TIC para mitigar el riesgo es el respaldo diario de las carpetas compartidas y la restauración de los archivos, en caso de borrado o alteración. La restauración se realiza cuando la jefatura de la unidad lo solicite.

14. La unidad de TIC no ha implementado controles de acceso a la información impresa, ya que la DNN no cuenta con un sistema de clasificación y etiquetado de la información, ni se han establecido los criterios para su uso de acuerdo con su grado de privacidad y confidencialidad, de acuerdo con el inciso i de la cláusula 1.4.5 de las Normas Técnicas.

La unidad de TIC no ha implementado controles para el uso de medios de almacenamiento externo, tales como memorias USB, discos duros externos o teléfonos móviles, para restringir la copia de información no autorizada.

### **Cláusula 3.4 Contratación de terceros para la implementación y mantenimiento de software e infraestructura**

*La organización debe obtener satisfactoriamente el objeto contratado a terceros en procesos de implementación o mantenimiento de software e infraestructura.*

15. Contar con la debida justificación para contratar a terceros la implementación y mantenimiento de software e infraestructura tecnológica.
16. Establecer, verificar y aprobar formalmente los criterios, términos y conjunto de pruebas de aceptación de lo contratado; sean instalaciones, hardware o software.
17. Implementar un proceso de transferencia tecnológica que minimice la

---

dependencia de la organización respecto de terceros contratados para la implementación y mantenimiento de software e infraestructura tecnológica.

#### **Cláusula 4.1 Definición y administración de acuerdos de servicio**

*La organización debe tener claridad respecto de los servicios que requiere y sus atributos, y los prestados por la Función de TI según sus capacidades.*

*El jerarca y la Función de TI deben acordar los servicios requeridos, los ofrecidos y sus atributos, lo cual deben documentar y considerar como un criterio de evaluación del desempeño.*

18. Contar con una determinación clara y completa de los servicios y sus atributos, y analizar su costo y beneficio.
19. Definir con claridad las responsabilidades de las partes y su sujeción a las condiciones establecidas.
20. Establecer los procedimientos para la formalización de los acuerdos y la incorporación de cambios en ellos.
21. Definir los criterios de evaluación sobre el cumplimiento de los acuerdos.
22. Revisar periódicamente los acuerdos de servicio, incluidos los contratos con terceros.

#### **Cláusula 4.2 Administración y operación de la plataforma tecnológica**

*La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas.*

23. Controlar la composición y cambios de la plataforma y mantener un registro actualizado de sus componentes (hardware y software), custodiar adecuadamente las licencias de software y realizar verificaciones físicas periódicas.

#### **Cláusula 4.3 Administración de los datos**

*La organización debe asegurarse de que los datos que son procesados mediante TI corresponden a transacciones válidas y debidamente autorizadas, que son procesados en forma completa, exacta y oportuna, y transmitidos, almacenados y desechados en forma íntegra y segura.*

24. Aunque los sistemas de información SGIN y BOS7 registran información sobre las acciones realizadas por los usuarios, la organización no revisa las bitácoras proporcionadas por estos sistemas para comprobar que las transacciones

---

sean “válidas y debidamente autorizadas”.

**Cláusula 4.6 Administración de servicios prestados por terceros**

*La organización debe asegurar que los servicios contratados a terceros satisfagan los requerimientos en forma eficiente. Con ese fin, debe:*

25. Establecer y documentar los procedimientos asociados con los servicios e instalaciones contratados a terceros.
26. Vigilar que los servicios contratados sean congruentes con las políticas relativas a calidad, seguridad y seguimiento establecidas por la organización.
27. Minimizar la dependencia de la organización respecto de los servicios contratados a un tercero.
28. Asignar a un responsable con las competencias necesarias que evalúe periódicamente la calidad y cumplimiento oportuno de los servicios contratados.

## Anexo 4. Resumen del cumplimiento de las Normas Técnicas

En la siguiente tabla se presentan los requerimientos de las Normas Técnicas evaluados en esta auditoría, indicando si este se cumple, no se cumple, o si se cumple parcialmente (P).

Cláusula	Inciso	Cumple		
		Sí	No	P
1.1 Marco estratégico de TI	El jerarca debe traducir sus aspiraciones en materia de TI en prácticas cotidianas de la organización, mediante un proceso continuo de promulgación y divulgación de un marco estratégico constituido por políticas organizacionales que el personal comprenda y con las que esté comprometido		X	
2.1 Independencia y recurso humano de la Función de TI	El jerarca debe asegurar la independencia de la Función de TI respecto de las áreas usuarias y que ésta mantenga la coordinación y comunicación con las demás dependencias tanto internas y como externas.  Además, debe brindar el apoyo necesario para que dicha Función de TI cuente con una fuerza de trabajo motivada, suficiente, competente y a la que se le haya definido, de manera clara y formal, su responsabilidad, autoridad y funciones			X
1.4.1 Implementación de un marco de seguridad de la información	a. Establecer un marco metodológico que incluya la clasificación de los recursos de TI, según su criticidad, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concienciación y capacitación del personal.		X	
	b. Mantener una vigilancia constante sobre todo el marco de seguridad y definir y ejecutar periódicamente acciones para su actualización.		X	
	c. Documentar y mantener actualizadas las responsabilidades tanto del personal de la organización como de terceros relacionados.	X		
1.4.2 Compromiso del personal con la seguridad de la información	a. Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI.		X	



Cláusula	Inciso	Cumple		
		Sí	No	P
	b. Implementar mecanismos para vigilar el debido cumplimiento de dichas responsabilidades.		X	
	c. Establecer, cuando corresponda, acuerdos de confidencialidad y medidas de seguridad específicas relacionadas con el manejo de la documentación y rescisión de contratos.		X	
1.4.4 Seguridad en las operaciones y comunicaciones	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.	X		
	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.		X	
	c. Establecer medidas preventivas, detectivas y correctivas con respecto a software "malicioso" o virus.	X		
1.4.5 Control de acceso	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.			X
	b. Clasificar los recursos de TI en forma explícita, formal y uniforme de acuerdo con términos de sensibilidad.		X	
	c. Definir la propiedad, custodia y responsabilidad sobre los recursos de TI.	X		
	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.		X	
	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.		X	
	f. Implementar el uso y control de medios de autenticación (identificación de usuario,			X



Cláusula	Inciso	Cumple		
		Sí	No	P
	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.		X	
	j. Establecer los mecanismos necesarios (pistas de auditoría) que permitan un adecuado y periódico seguimiento al acceso a las TI.			X
	k. Manejar de manera restringida y controlada la información sobre la seguridad de las TI.	X		
1.4.7 Continuidad de los servicios de TI	La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios. Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad.		X	
3.4 Contratación de terceros para la implementación y mantenimiento de software e infraestructura	<p>a. Contar con la debida justificación para contratar a terceros la implementación y mantenimiento de software e infraestructura tecnológica.</p> <p>b. Establecer, verificar y aprobar formalmente los criterios, términos y conjunto de pruebas de aceptación de lo contratado; sean instalaciones, hardware o software.</p> <p>c. Implementar un proceso de transferencia tecnológica que minimice la dependencia de la organización respecto de terceros contratados para la implementación y mantenimiento de software e infraestructura tecnológica</p>			X
4.1 Definición y administración de acuerdos de servicio	a. Contar con una determinación clara y completa de los servicios y sus atributos, y analizar su costo y beneficio.		X	





Cláusula	Inciso	Cumple		
		Sí	No	P
	<ul style="list-style-type: none"> <li>b. Definir con claridad las responsabilidades de las partes y su sujeción a las condiciones establecidas.</li> <li>c. Establecer los procedimientos para la formalización de los acuerdos y la incorporación de cambios en ellos.</li> <li>d. Definir los criterios de evaluación sobre el cumplimiento de los acuerdos.</li> <li>e. Revisar periódicamente los acuerdos de servicio, incluidos los contratos con terceros.</li> </ul>			
4.2 Administración y operación de la plataforma tecnológica	a. Definir formalmente y efectuar rutinas de respaldo, custodiar los medios de respaldo en ambientes adecuados, controlar el acceso a dichos medios y establecer procedimientos de control para los procesos de restauración.			X
4.3 Administración de datos	La organización debe asegurarse de que los datos que son procesados mediante TI <u>corresponden a transacciones válidas y debidamente autorizadas</u> , que son procesados en forma completa, exacta y oportuna, y transmitidos, almacenados y desechados en forma íntegra y segura. (Nota: El subrayado no es del original)		X	
4.6 Administración de servicios prestados por terceros	<ul style="list-style-type: none"> <li>a. Establecer y documentar los procedimientos asociados con los servicios e instalaciones contratados a terceros.</li> <li>b. Vigilar que los servicios contratados sean congruentes con las políticas relativas a calidad, seguridad y seguimiento establecidas por la organización.</li> <li>c. Minimizar la dependencia de la organización respecto de los servicios contratados a un tercero.</li> <li>d. Asignar a un responsable con las competencias necesarias que evalúe periódicamente la calidad y cumplimiento oportuno de los servicios contratados.</li> </ul>			X

## Anexo 5- Características de Seguridad de los Sistemas de Información

En la siguiente tabla se presentan las características de seguridad evaluadas en los cinco sistemas de información revisados en esta auditoría. El sistema FileOn está en desarrollo y está fuera del ámbito de TIC. El encargado de la ejecución del proyecto de desarrollo de FileOn es el encargado de la unidad de Archivo Institucional.

Característica	Observaciones	SGIN 1.0	SGIN 1.1	BOS	Acuersoft	Filas	FileOn
El sistema está en producción.		S	N	S	S	S	N
Tiene módulo de Seguridad	Requisito indispensable para la seguridad de la información.	S	S	S	S	S	S
Permite crear grupos de usuario		S	S	S	S	N	S
Permite crear usuarios		S	S	S	S	S	S
El sistema genera la contraseña y la envía al usuario.	El personal de TIC no conoce la contraseña asignada a los usuarios.	S	S	N	N	N	NA
La contraseña se oculta.	Se enmascara con "*" u otro caracter.	S	S	S	S	S	S
La contraseña se pide dos veces para confirmar.		NA	NA	N	S	S	NA
La contraseña tiene vigencia.		N	N	S	N	--	S
El usuario puede cambiar su contraseña.		S	S	S	N	--	S
El sistema permite la recuperación de contraseña sin intervención del personal de		S	S	N	N	N	NA

Característica	Observaciones	SGIN 1.0	SGIN 1.1	BOS	Acuersoft	Filas	FileOn
TIC.							
El código del usuario tiene estado Activo / Inactivo.		S	S	S	S	S	S
La cuenta del usuario se bloquea después de 3 intentos de ingreso fallido.		N	S	S	N	N	S
El sistema obliga a los usuarios a cambiar la contraseña la primera vez que ingresa a la aplicación.		S	S	N	N	N	NA
El sistema obliga a los usuarios a cambiar la contraseña cuando el administrador de la Seguridad asigna una nueva contraseña.		NA	NA	N	N	N	NA
Se valida el código del usuario y la contraseña con el Active Directory.		N	S	N	N	N	S
Tiene autenticación de usuario con firma digital.	El SGIN 1.0 tiene un ícono para el ingreso por firma digital, pero esta función no fue implementada.  El SGIN 1.1 tendrá autenticación con firma digital, a solicitud de la Dirección Ejecutiva.	N	S	N	N	N	S

Característica	Observaciones	SGIN 1.0	SGIN 1.1	BOS	Acuersoft	Filas	FileOn
Tiene consulta o reporte de acciones realizadas (reporte de la Bitácora o reporte de seguridad)	<p>En el BOS se puede seleccionar la empresa y el módulo, y permite especificar rango de fechas, rango de horas. Se puede seleccionar un usuario y generar el reporte para todos los usuarios.</p> <p>El SGIN 1.1 tendrá reportes de la bitácora de transacciones.</p>	S	S	S	N	N	S

S-Sí, N-No, NA-No aplica, “—“No hay información

## Anexo 6. Prácticas de Seguridad en los Sistemas de Información en Producción

En la siguiente tabla se presenta un cuadro comparativo de la aplicación de buenas prácticas relacionadas con la seguridad de información.

Característica	Observaciones	SGIN 1.0	SGIN 1.1	BOS	Acuersoft	Filas
Existe una lista de perfiles de usuario y los derechos de acceso autorizados para cada perfil.	Referencia: Inciso d, cláusula 1.4.5, Control de acceso, Normas Técnicas. Esta lista facilita la creación, asignación e desasignación de accesos a los usuarios, dependiendo del perfil asignado por el propietario de la información. También, es la base para realizar la comprobación de los accesos asignados.	N	NA	N	N	N
Se revisan los perfiles de forma periódica para comprobar y actualizar los accesos autorizados.	Referencia: Inciso f, cláusula 1.4.5, Control de acceso, Normas Técnicas.	N	NA	N	N	N
Se revisan de forma periódica los usuarios asignados a los perfiles.	Referencia: Inciso f, cláusula 1.4.5, Control de acceso, Normas Técnicas.	N	NA	N	N	N
Se comprueba si existen cuentas de usuario activas de exfuncionarios o de funcionarios incapacitados, con permiso o que están de vacaciones.	Referencia: Inciso f, cláusula 1.4.5, Control de acceso, Normas Técnicas.	N	NA	N	N	N
La bitácora se revisa regularmente para detectar acciones no autorizadas.	Referencia: Inciso f, cláusula 1.4.5, Control de acceso, Normas Técnicas.	N	NA	N	N	N

Característica	Observaciones	SGIN 1.0	SGIN 1.1	BOS	Acuersoft	Filas
Se actualizan los accesos de los usuarios cuando el funcionario cambia de puesto o se modifican sus funciones.	Referencia: Inciso e, cláusula 1.4.5, Control de acceso, Normas Técnicas.	S	S	S	S	S
Se eliminan los accesos de los usuarios en el momento en que finaliza la relación laboral de un funcionario.	Referencia: Inciso f, cláusula 1.4.5, Control de acceso, Normas Técnicas. Los accesos se eliminan cuando el personal de TIC se da cuenta del cese de labores de un exfuncionario. Las unidades y áreas de la DNN no comunican a TIC el cese de labores de un funcionario, o no lo hacen de forma oportuna.	N	NA	N	N	N

## Anexo 7. Lineamientos revisados sobre estándares de gestión de continuidad de negocio

En la siguiente tabla se presenta un cuadro con los lineamientos de gestión de continuidad de negocio que la ISO 27001 recomienda como controles.

### A.14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

#### A.14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

*Objetivo: contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos de negocio de los efectos de fallas de gran magnitud o desastres en los sistemas de información, y asegurarse de su reanudación oportuna.*

Objetivo de control	Descripción	Controles
A.14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	Control Se debe desarrollar y mantener un proceso de gestión de la continuidad del negocio en toda la organización, que aborde los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.
A.14.1.2	Continuidad del negocio y evaluación de riesgos	Control Se deben identificar los eventos que pueden causar interrupciones en los procesos del negocio, junto con la probabilidad e impacto de estas interrupciones y sus consecuencias para la seguridad de la información
A.14.1.3	Desarrollo e implementación de planes de continuidad que incluyen seguridad de la información	Control Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurarse de la disponibilidad de información al nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla de los procesos críticos del negocio.



Objetivo de control	Descripción	Controles
A.14.1.4	Estructura Marco de referencia para la planificación de la continuidad del negocio	Control Se debe mantener un solo marco de referencia una sola estructura de los planes de continuidad del negocio para asegurarse de que todos los planes son coherentes, abordan de forma coherente los requisitos de seguridad de la información, e identifican prioridades para prueba y mantenimiento.
A.14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	Control Los planes de continuidad del negocio se deben poner a prueba y actualizar regularmente para asegurarse de que estén actualizados y sean eficaces



## Anexo 8. Acceso a la edición de tomos de los notarios en el SGIN 1.0

En este anexo se describe el problema de acceso a la ventana de edición de los tomos de los notarios en el sistema SGIN 1.0. La información la proporcionó el señor Fabián Morales Hernández, encargado de los sistemas de información y bases de datos, de la unidad TIC de la Dirección Nacional de Notariado.

Descripción:

1. La unidad de Fiscalización Notarial necesita ver la fecha de autorización del tomo de un notario, como se muestra en la figura A8.1.

The screenshot displays a web application interface for the SGIN 1.0 system. A modal window titled "Editar registro" is open, showing a form for editing a notary's protocol volume. The form contains the following fields:

Tipo Nombramiento:	PLENO
No. Tomo:	1
Fecha autorización:	17/10/1983
Ubicación del tomo:	EN USO
Fecha estado:	04/10/2019
No. Folio inicial:	0
No. Folio final:	0
No. Seguridad:	0
Serie inicial:	0
Serie final:	0

The modal also includes an "Actualizar" button at the bottom right. In the background, the main application interface is visible, showing the notary's name "Notario: RAFAEL ANGEL", his ID "Carné: 1352", and his status "Estado: INHABILITADO".

Figura A8.1. Editar notario SGIN 1.0.

2. El sistema SGIN 1.0 no cuenta con una opción (pantalla) de consulta en la que se muestre la fecha de autorización. La consulta tomos presenta los siguientes datos:

The screenshot shows a web browser window with the URL `172.28.12.26/sgin/notario/tomosprotocolo/1347`. The page title is "Tomos de protocolo" and it displays information for Notario RAFAEL ANGEL CAMPOS SOLANO, Carné: 1352, Estado: INHABILITADO. A sidebar on the left lists various menu items like "Perú", "Eventos", "Servicios externos", etc. The main content area shows a table titled "Tomos de protocolo utilizados por notario" with columns for Tipo de Nombramiento, Tomo, Estado del tomo, Fecha estado, Folio inicial, Folio final, Serie inicial, Serie final, and No.Seguridad. A single record is shown: PLENO, Tomo 1, Estado EN USO, Fecha estado 04/10/2019, and all folio and serie fields are 0. The page also includes a search bar, "Crear", "Editar", and "Eliminar" buttons, and a footer with contact information for the Dirección Nacional de Notariado.

Figura A8.2. Consulta de notario en SGIN 1.0.

3. Para que los funcionarios de la unidad de Fiscalización Notarial puedan ver la fecha de autorización, se les dio acceso a la página de Notarios. El problema de este acceso es que en el SGIN 1.0, el usuario que tiene acceso a una página (pantalla), tiene acceso a todas las funciones que se realizan en ella; en este caso, el usuario que tiene acceso a la página de Notarios, puede Consultar, Crear, Editar y Eliminar registros. Las opciones Editar y Eliminar se activan cuando el usuario selecciona un tomo de la consulta (Figura A8.3).

En la versión 1.1 del SGIN, ese problema no existirá porque los permisos se asignan por página y por acción, de tal manera que los funcionarios de Fiscalización Notarial podrán consultar la información que ellos requieren, pero no podrán crear, editar ni eliminar registros.



## Tomos de protocolo

Notario : RAFAEL ANGEL CAMPOS SOLANO

Carné : 1352

Estado : INHABILITADO

### Tomos de protocolo utilizados por notario

Crear Editar Eliminar

Tipo de Nombramiento	Tomo	Estado del tomo	Fecha estado	Folio inicial	Folio final	Serie inicial
PLENO	1	EN USO	04/10/2019	0	0	0

Mostrando registros del 1 al 1 de un total de 1 registros

### Detalle de tomo de protocolo PLENO

Historial Tomo Protocolo

Crear Editar Eliminar

Recibo	Fecha Recibo	Fecha Comunica	Condición
Ningún dato disponible en esta tabla			

Mostrando registros del 0 al 0 de un total de 0 registros

Figura A8.3. Las opciones Crear, Editar y Eliminar están activas.

5. El problema con el SGIN 1.0 consiste en que, si se les quita a los funcionarios de Fiscalización Notarial el acceso a la página de Notarios, no podrán consultar el dato que ellos necesitan, y tendrían que pedirlo a los funcionarios de la unidad de Servicios Notariales cada vez que lo requieran. Con base en la evaluación de los riesgos de seguridad de la información que haga la DNN, la Dirección debe decidir si mantiene el acceso de los funcionarios de la unidad de Fiscalización Notarial, o si les quita este acceso, hasta que se inicie la operación de la versión nueva.