DIRECCIÓN NACIONAL DE NOTARIADO (DNN)

Informe de Auditoría de Tecnologías de Información y Comunicación

CG-I-TI 2021

Informe Final

San José, 13 de diciembre del 2022

Al Consejo Superior Notarial y a la Dirección Ejecutiva
Dirección Nacional de Notariado

Según nuestro contrato de servicios, efectuamos la visita de auditoría externa del período 2021 a la DNN y con base en el examen efectuado, observamos ciertos aspectos referentes al sistema de control interno y procedimientos de Tecnología de Información, basados en las normas de control interno para el sector público, marco de gestión de tecnologías de información de la Dirección Nacional de Notariado y en los estándares establecidos según los Objetivos de Control para Información y Tecnología Relacionada – CobiT®., los cuales sometemos a consideración de ustedes en esta carta de gerencia CG-I-TI 2021.

Considerando el carácter de pruebas selectivas en que se basa nuestro examen, ustedes pueden apreciar que se debe confiar en métodos adecuados de comprobación y de control interno, como principal protección contra posibles irregularidades que un examen basado en pruebas selectivas puede no revelar, si es que existiesen. Las observaciones no van dirigidas a funcionarios o empleados en particular, sino únicamente tienden a fortalecer el sistema de control interno y los procedimientos relacionados con la tecnología de información.

DESPACHO CARVAJAL & COLEGIADOS
CONTADORES PÚBLICOS AUTORIZADOS

IVAN GUSTAVO BRENES PEREIRA (FIRMA)

Firmado digitalmente por IVAN GUSTAVO BRENES PEREIRA (FIRMA)
Fecha: 2022.12.23 10:43:58 -06'00'

Lic. Iván Brenes Pereira
Contador Público Autorizado No. 5173
Póliza de Fidelidad número N° 0116 FIG 7
Vence el 30 de setiembre de 2023.

San José, 16 de diciembre de 2022.

"Exento timbre de Ley número 6663, del Colegio de Contadores Públicos de Costa Rica, por disposición de su artículo número 8".

I. CONTENIDO

INTRODUCCIÓN *5*

ORIGEN DEL ESTUDIO 5

ALCANCE 5

PERIODO DE LA AUDITORÍA 6

LIMITACIONES DEL ESTUDIO 6

METODOLOGÍA 7

HALLAZGOS Y RECOMENDACIONES IDENTIFICADAS EN LA EVALUACIÓN *8*

HALLAZGO 01: DEBILIDADES EN EL MARCO DE GOBIERNO Y GESTIÓN DE TI EN LA DNN. RIESGO MEDIO. 8

HALLAZGO 02: DESBILIDADES EN LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. RIESGO ALTO.9

HALLAZGO 03: AUSENCIA DE UN PROCEDIMIENTO PARA LA GESTIÓN DE ACTIVOS. RIESGO MEDIO. 11

HALLAZGO 04: AUSENCIA DE UN PROCEDIMIENTO FORMAL PARA LA GESTIÓN DE ROLES Y PERFILES RIESGO MEDIO. 12

HALLAZGO 05: AUSENCIA DE UNA METODOLOGÍA PARA LA ADMINISTRACIÓN DE PROYECTOS DE TECNOLOGÍAS DE INFORMACIÓN. RIESGO MEDIO. 13

HALLAZGO 06: AUSENCIA DE UN PROCEDIMIENTO PARA LA GESTIÓN DE CAMBIOS DE TI. RIESGO MEDIO. 16

HALLAZGO 07: AUSENCIA DE UN PROCEDIMIENTO PARA LA GESTIÓN DE SOLICITUDES, INCIDENTES Y PROBLEMAS DE TI. RIESGO MEDIO. 18

HALLAZGO 08: AUSENCIA DE UNA METODOLOGÍA PARA LA EVALUACIÓN DEL CONTROL INTERNO DE TECNOLOGÍAS DE INFORMACIÓN. RIESGO MEDIO. 19

HALLAZGO 09: AUSENCIA DE UN PROCEDIMIENTO PARA LA GESTIÓN DE LA CONTINUIDAD, CAPACIDAD Y DISPONIBILIDAD DE LA PLATAFORMA TECNOLÓGICA. RIESGO MEDIO. 21

HALLAZGO 10: AUSENCIA DE UN CATÁLOGO DE SERVICIOS POR PARTE DE LA UNIDAD DE INFORMÁTICA DE LA DNN. RIESGO BAJO. 23

HALLAZGO 11: AUSENCIA DE UN CORRECTO SEGUIMIENTO Y COMUNICACIÓN DURANTE LA GESTIÓN DE RIESGOS DE T.I. RIESGO MEDIO. 24

HALLAZGO 12: AUSENCIA DE ACUERDOS DE NIVEL DE SERVICIO PARA LOS SERVICIOS BRINDADOS AL DNN. RIESGO BAJO. 26

HALLAZGO 13: DEBILIDADES EN LA SEGURIDAD FISICA DEL CUARTO DE COMUNICACIONES DE LA DNN. RIESGO MEDIO. 27

APÉNDICE *29*

APÉNDICE I: ANÁLISIS DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN. 29
I. PLANIFICACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN. 30
A. PLANIFICACIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN. 30
B. GESTIÓN DEL PRESUPUESTO DE TECNOLOGÍAS DE INFORMACIÓN. 30
C. GESTIÓN DE PROVEEDORES DE TECNOLOGÍAS DE INFORMACIÓN. 31
D. GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN. 32
E. GESTIÓN DE ACUERDOS DE NIVEL DE SERVICIO. 32
II. IMPLEMENTACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN. 33
F. GESTIÓN DE PROYECTOS DE TECNOLOGÍAS DE INFORMACIÓN. 33
G. GESTIÓN DE LA CAPACIDAD Y DISPONIBILIDAD. 34
H. GESTIÓN DE CAMBIOS. 35
III. OPORTE Y SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN. 35
I. GESTIÓN DE INCIDENTES. 35
J. GESTIÓN DE PROBLEMAS. 36
K. GESTIÓN DE LA CONTINUIDAD DE TECNOLOGÍAS DE INFORMACIÓN. 37
L. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. 38
M. GESTIÓN DE LA SEGURIDAD FÍSICA Y AMBIENTAL. 39
IV. EVALUACIÓN DE TECNOLOGÍAS DE INFORMACIÓN. 41
N. VALORAR EL CONTROL INTERNO. 41
RECOMENDACIONES GENERALES PARA LA CIBERSEGURIDAD 42

II. INTRODUCCIÓN

ORIGEN DEL ESTUDIO

Evaluar el cumplimiento de los sistemas de control interno para determinar si las actividades relacionadas con los procesos de tecnologías de información y comunicación se realizan cumpliendo las normas, estándares, procedimientos y cualquier otra regulación interna o externa emitida para el manejo de las tecnologías de información.

ALCANCE

En esta visita el trabajo fue enfocado principalmente a las siguientes áreas:

1. Valoración del grado de avance del Marco de Gestión de la DNN conforme al cronograma que debe cumplir la institución.
2. Revisar el Plan de Tecnologías de Información y Comunicación (PETIC). Analizar si se efectúa una planificación Estratégica tomando en cuenta el análisis de la capacidad de las necesidades de los diferentes departamentos de la DNN, así como verificar las acciones plasmadas en el cumplimiento de dichos Planes Estratégicos.
3. Analizar y evaluar si existe un control adecuado de los proyectos presentados por las diferentes unidades de la DNN.
4. Analizar y evaluar el control sobre los requerimientos presentados para las mejoras a los sistemas por las diferentes unidades de la DNN.
5. Analizar si se diseña, desarrolla, compra o arrienda software de acuerdo con las necesidades de las diferentes unidades de la DNN y de acuerdo con la metodología aprobada a nivel institucional.
6. Analizar y evaluar si se cumple con una adecuada segregación de funciones en los procesos manuales y automatizados para que no se concentren en una sola persona.
7. Analizar y evaluar el control y seguridades físicas en el área de tecnología.
8. Analizar el ambiente de control de la información que es gestionada y almacenada dentro y fuera de los sistemas informáticos con el objetivo de identificar enumerar y evaluar los controles que se tengan implementados para garantizar la confidencialidad, integridad y disponibilidad de la información.
9. Analizar y evaluar si se cuenta con un plan de contingencia o continuidad del servicio en caso de presentarse una eventualidad.
10. Analizar el ambiente de control de los procesos y activos de cómputo central, computo personal, telecomunicaciones, accesos locales y remotos, servicios en la nube, entre otros., para identificar riesgo de negocio y ofrecer recomendaciones factibles, que solventen o mitiguen estos riesgos.
11. Analizar y evaluar si se administra adecuadamente la red que soporta tanto el área de comunicación entre las diferentes oficinas de la dependencia, así como las oficinas remotas ubicadas en otras localizaciones, y los accesos a la nube.
12. Evaluar si se realizan análisis de la capacidad de los sistemas y bases de datos.
13. Analizar si se realizan informes de rendimiento de los equipos en producción.

14. Analizar y evaluar si se coordina y realizan labores de capacitación y concientización en materia de seguridad de acuerdo con los lineamientos institucionales y con los objetivos estratégicos de TI.
15. Analizar si se cuenta con una plataforma tecnológica Institucional con esquemas de seguridad como Firewalls entre otros que garanticen la integridad y confidencialidad de los datos.
16. Verificar que los servicios de TI se encuentran al nivel que la organización requiere para habilitar, potenciar y soportar de manera efectiva y eficiente sus funciones.
17. Analizar y evaluar si se efectúan evaluaciones a la plataforma tecnológica Institucional sobre aspectos de esquemas de seguridad (Firewalls, entre otros) que garanticen la integridad y confidencialidad de los datos.
18. Evaluar si se cuenta con un Esquema de Seguridad, que controle tanto la salida como el ingreso de información hacia y desde la red interna de la Institución.
19. Evaluar si la unidad de tecnologías realiza investigaciones de las nuevas tendencias en seguridad informática.
20. Evaluar si se planifica, coordina y realiza las labores de capacitación y concientización en materia de seguridad de acuerdo con los lineamientos institucionales y con los objetivos estratégicos de TI, generando la evidencia respectiva Informes de Capacitación y cierre del proceso.
21. Analizar y evaluar si se lleva un adecuado seguimiento de los Proyectos de Inversión que estén relacionados con Tecnologías de Información
22. Evaluar si los requerimientos anuales de compras se realizan considerando lo establecido en el Plan Estratégico de la Institución y el Plan Estratégico de TI.
23. Evaluar si existe control sobre el presupuesto de gastos e inversiones asignado a la Unidad de tecnologías.
24. Valorar la estructura de personal de la Unidad de Tecnologías de Información y Comunicación.
25. Valoración de los riesgos existentes en el tema tecnológico en la Dirección Nacional de Notariado y si existe un plan de contingencia de continuidad de la operación.
26. Valoración de todos los demás aspectos relevantes que conforme a la técnica deben ser considerados en un proceso de auditoría de esta naturaleza.
27. Gestión de la seguridad-adminsitración de usuarios, accesos, vulnerabilidades.
28. Gestión de las operaciones
29. Continuidad

PERIODO DE LA AUDITORÍA

El estudio se realizó durante el mes de noviembre-diciembre y corresponde a la auditoría del periodo 2021.

LIMITACIONES DEL ESTUDIO

No se presentaron limitaciones durante el periodo de auditoría.

METODOLOGÍA

Para llevar a cabo este trabajo utilizamos una modalidad de análisis de la información suministrada por la administración de la DNN, se realizaron consultas de control interno relacionados con la administración del departamento, seguridad física y lógica de los sistemas de información, continuidad de las operaciones, planificación de las TI, gestión de riesgo tecnológico, proyectos, respaldos, entre otras áreas.

Además, se formularon preguntas sobre la existencia de controles informáticos y se realizaron entrevistas a algunas áreas usuarias, en todos los casos necesarios solicitamos a los colaboradores las evidencias en documentos escritos o en formato digital que respaldaran sus afirmaciones.

III. HALLAZGOS Y RECOMENDACIONES IDENTIFICADAS EN LA EVALUACIÓN

HALLAZGO 01: DEBILIDADES EN EL MARCO DE GOBIERNO Y GESTIÓN DE TI EN LA DNN. RIESGO MEDIO.

CONDICIÓN:

Dado la derogación de las Normas Técnicas de la Contraloría General de la República para la gestión y el control de las tecnologías de Información (N-2-2007-CO-DFOE), a partir del 1 de enero del 2022 era necesario tener implementado un marco de gobierno y gestión de tecnologías de información. Actualmente en la DNN existe documentación sobre la contratación realizada *"**Servicios profesionales bajo el modelo de Horas por Demanda para el robustecimientos e implementación del marco normativo, prácticas de gestión y gobierno de Tecnologías de Información para la Institución**"*.

En cuanto a este tema, el DNN suministró el documento "DNN - Marco de Gestión de TIC DNN" versión 01, el cual fue elaborado en noviembre del año 2021 por una empresa consultora y según lo indicado fue aprobado por el Consejo Superior Notarial llevándose a cabo el proceso correspondiente y su respectiva comunicación.

CAUSA:

Se indicó por parte de la administración que, se encuentra pendiente el desarrollo de los objetivos del Marco de Gestión de TI para su respectiva implementación, para lo cual cuentan con la contratación 2021CD-000007-0007500001.

EFECTO:

Al presentarse debilidades en el marco de gobierno y gestión de TI, el DNN se podría ver expuesto a los siguientes riesgos:

- Complicaciones para garantizar la correcta gestión de los procesos requeridos para ofrecer de forma oportuna y efectiva los servicios brindados a través del uso y administración de los recursos tecnológicos de forma tal que garanticen la continuidad de las operaciones institucionales, la salvaguarda de la información gestionada, la entrega de valor y el cumplimiento normativo.

CRITERIO:

En la práctica **APO01.01 Diseñar el sistema de gestión para la I&T de la empresa** del proceso **APO01 Gestionar el Marco de Gestión de I&T,** presente en el estándar de Control Objectives for Information and related Technology (COBIT 2019), se menciona*:*

"Diseñar un sistema de gestión adaptado a las necesidades de la empresa. Las necesidades de gestión de la empresa se definen a través del uso de la cascada de metas y por la aplicación de factores de diseño.
Asegurar que los componentes de gobierno están integrados y alineados con el gobierno, la filosofía de gestión y estilo operativo de la empresa".

RECOMENDACIONES:

A la Administración de la DNN en coordinación con la Unidad de Tecnologías de la Información y Comunicación:

1. Continuar con la definición y desarrollo de los objetivos y plan de acción para la implementación del marco de gobierno y gestión de tecnologías de información.

2. Mantener un control o registro de avances y cambios durante la implementación del marco.

3. Revisar el marco de gobierno y gestión de tecnologías de información regularmente (al menos una vez al año) con tal de garantizar que éste se mantenga actualizado de acuerdo con los cambios presentados con el tiempo en la DNN, sus necesidades y procedimientos del negocio.

HALLAZGO 02: DEBILIDADES EN LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. RIESGO ALTO.

CONDICIÓN:

Producto de la revisión efectuada, se verificó que la DNN no cuenta con una política para la seguridad de la información. Además, se indica que, como parte de la concientización sobre seguridad de la información, se realizan envíos de correos al personal con instrucciones generales. Sin embargo, no se han realizado capacitaciones al personal en temas de seguridad.

Por otro lado, se indica que no se han realizado evaluaciones a los esquemas de seguridad de la organización, ni tampoco estudios de vulnerabilidades puesto que la plataforma tecnológica de la DNN es nueva, tienen planeado realizar estos estudios el próximo año.

CAUSA:

Según lo indicado por la administración, no cuentan con políticas ni procedimiento, se va a trabajar en la creación de los documentos y actividades relacionadas a la seguridad mediante la contratación 2021CD-000007-0007500001, la cual corresponde al Marco de Gestión de TI.

EFECTO:

Al no contar con políticas ni actividades para garantizar la seguridad, la DNN se podría ver expuesta a los siguientes riesgos:

- No se garantiza la seguridad de la información, al no presentar políticas de seguridad vigentes.
- Dificultad para medir la eficacia de la política de seguridad en la institución.
- Dificultad para identificar potenciales amenazas que puedan afectar los servicios de la organización y la información que esta maneja.
- Existencia de posibles vulnerabilidades que aún no se han corregido

CRITERIO:

En el proceso **APO13 Gestionar la Seguridad**, presente en el estándar de Control Objectives for Information and related Technology (COBIT 2019), se menciona: *"Definir, operar y monitorear un sistema de gestión de la seguridad de la información."*

RECOMENDACIONES:

A la Administración de la DNN:

1. Gestionar la definición, aprobación y divulgación de una política de seguridad de la información.
2. Aplicar una vez creada la política de seguridad de la información, lo siguiente:
    a. Comunicarla a todos los funcionarios del DNN, con el fin de que estén enterados sobre su existencia y acatamiento.
    b. Realizar capacitaciones sobre seguridad de la información, con el fin de crear una cultura de seguridad, se posea un claro entendimiento de la política de seguridad de la información y así evitar o reducir los incidentes asociados con esta.
    c. Establecer mecanismos de control que ayuden a verificar el cumplimiento de la política tales como actividades de monitoreo de seguridad, pruebas de vulnerabilidades, evaluaciones sobre los esquemas de seguridad e indicar acciones correctivas sobre las debilidades o incidentes de seguridad identificados.
    d. Realizar revisiones periódicas (al menos una vez al año o cuando se requiera) de la política de seguridad de la información, documentando los resultados.
3. Definir responsables de gestionar la política, la frecuencia de la revisión y actualización de este documento.

4. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.

HALLAZGO 03: AUSENCIA DE UN PROCEDIMIENTO PARA LA GESTIÓN DE ACTIVOS. RIESGO MEDIO.

CONDICIÓN:

Producto de la revisión se determinó que el Área de Tecnologías de Información y Comunicación no cuenta con procedimientos para gestión de los activos. No obstante, se suministraron registros con inventarios de los activos de la DNN, esto evidencia que llevan un control sobre sus activos.

CAUSA:

De acuerdo con la respuesta brindada a la solicitud de requerimientos adicionales se mencionó que no se cuenta con estos procedimientos, los mismos se llevarían acaba en la contratación 2021CD-000007-0007500001, la corresponde al Marco de Gestión de TI.

EFECTO

No contar con procedimientos para la gestión de activos aumenta el riesgo de que la organización deba incurrir en costos no programados por reparaciones o pérdidas de equipo y/o sistemas, además, impide determinar si los activos en cuestión siguen aportando valor a los procesos del negocio.

CRITERIO:

En el proceso **BAI09 Gestionar los Activos,** presente en el estándar de Control Objectives for Information and related Technology (COBIT 2019), se menciona: *"Gestionar los activos de I&T a través de su ciclo de vida para asegurarse de que su uso aporta valor a un coste óptimo, continúan operativos (adecuados a su propósito), y se tienen en cuenta y están físicamente protegidos. Asegurar que aquellos activos que son críticos para soportar la capacidad del servicio son confiables y están disponibles. Gestionar las licencias de software para asegurarse de que se adquiere, retiene y despliega la cantidad óptima en relación con el uso que requiere el negocio, y que el software instalado cumpla con los acuerdos de licencia."*

RECOMENDACIÓN:

A la Unidad de Tecnologías de Información y Comunicación:

1. Elaborar una propuesta para el desarrollo de procedimientos para la gestión de activos de información y críticos de TI para posteriormente ser aprobada.

2. Para los procedimientos se recomienda promover acciones para gestionar el mantenimiento preventivo de los activos de TI, tales como establecer una periodicidad para realizar una evaluación de los equipos y/o sistemas, así como de la información.

3. Generar un inventario de activos críticos de TI actualizado e incluir los responsables asociados a cada activo. Para los activos de información se debe elaborar un listado con los respectivos dueños.

HALLAZGO 04: AUSENCIA DE UN PROCEDIMIENTO FORMAL PARA LA GESTIÓN DE ROLES Y PERFILES RIESGO MEDIO.

CONDICIÓN:

Producto de la evaluación no fue posible evidenciar la existencia de un procedimiento documentado y aprobado para la gestión de roles y perfiles de usuarios de los sistemas de información que utiliza el personal de la DNN. No obstante, se suministró evidencia de algunos roles y perfiles que contienen los sistemas de información.

CAUSA:

Según lo indicado, operativamente se administran los usuarios y accesos a los sistemas de información, pero no se cuenta con procedimientos, los mismos se llevarían acaba en la contratación 2021CD-000007-000750000, la cual corresponde al Marco de Gestión de TI.

EFECTO:

Al no contar con un procedimiento para la gestión de roles y perfiles o permisos de usuario, existe el riesgo de que los usuarios no cuente con los privilegios necesarios para el acceso a los sistemas, datos y servicios de información o en caso de que no se elimine los privilegios por salida de un colaborador, existe la posibilidad de que pueda acceder a la información crítica y/o confidencial y realice acciones no autorizadas en los sistemas de información a los que el usuario estaba autorizado.

CRITERIO:

En el proceso **DSS05 Gestionar Servicios de Seguridad**, presente en el estándar de Control Objectives for Information and related Technology (COBIT 2019), se menciona:
"Proteger la información de la empresa para mantener el nivel de riesgo de seguridad de la información aceptable conforme con la política de seguridad. Establecer y mantener roles y privilegiados de acceso de seguridad de la información. Realizar una monitorización de la seguridad.".

RECOMENDACIONES:

A Recursos Humanos:

1. Notificar oportunamente al Departamento de Tecnologías de Información, el cambio en las condiciones laborales de una persona, con el fin de que se proceda con la debida actualización o eliminación de su cuenta de usuario asociada en la plataforma tecnológica (roles y perfiles).

A las áreas usuarias en conjunto con la Unidad de Tecnologías de Información:

2. Definir la periodicidad con la cual se debe realizar el monitoreo de los usuarios y sus permisos, así como los reportes que se deben generar.

A la Unidad de Tecnologías de Información:

3. Elaborar un procedimiento para la gestión de los usuarios y sus perfiles en los sistemas de información, en el cual se contemplen al menos los siguientes aspectos:
    a. Actividades para crear, modificar o eliminar un usuario y sus respectivos permisos en los sistemas de información.
    b. Periodicidad con la cual se debe realizar el monitoreo de los usuarios y sus permisos, así como los reportes que se deben generar, según lo acordado con las áreas usuarias.

4. Presentar el procedimiento ante la gerencia para su respectiva aprobación, y una vez aprobada comunicarla a todas las áreas involucradas.

5. Comunicar y divulgar al personal respectivo sobre la existencia del procedimiento.

6. Definir responsables de gestionar el procedimiento, la frecuencia de la revisión y actualización de este.

7. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.

HALLAZGO 05: AUSENCIA DE UNA METODOLOGÍA PARA LA ADMINISTRACIÓN DE PROYECTOS DE TECNOLOGÍAS DE INFORMACIÓN. RIESGO MEDIO.

CONDICIÓN:

Producto de la evaluación realizada, no fue posible verificar la existencia de una metodología para gestionar proyectos en donde se incluyan todas sus etapas, cabe mencionar que no se suministró información o evidencia de los proyectos realizados.

CAUSA:

De acuerdo con la respuesta brindada en la solicitud de requerimientos iniciales, la Dirección Nacional de Notariado menciona que no se cuenta con un procedimiento para la gestión de programas y proyectos de TI.

EFECTO

El no contar con una metodología formalmente establecida para la gestión de proyectos, podría dificultarle a la organización el seguimiento de cada una de las etapas del ciclo de vida de un proyecto e incurrir en gastos innecesarios.

CRITERIO:

En el proceso **BAI01 Gestionar los Programas**, presente en el estándar de Control Objectives for Information and related Technology 2019 (COBIT 2019), se menciona:
"Gestionar todos los programas del portafolio de inversión, de conformidad con la estrategia de la empresa y de forma coordinada, según un enfoque de gestión de programas estándar. Iniciar, planificar, controlar y ejecutar programas, y monitorizar el valor esperado del programa".

RECOMENDACIONES:

A la Unidad de Tecnologías de Información:

1. Elaborar y documentar una metodología para la gestión de programas y proyectos de TI, considerando los siguientes aspectos:

    a. Acta constitutiva.
    b. Alcance del proyecto.
    c. Entregables a desarrollar en el proyecto.
    d. Recursos no financieros (personal, equipo, materiales, etc.).
    e. Estimación de recursos financieros (costos, presupuesto).
    f. Roles/Responsabilidades de involucrados internos y externos.
    g. Estructura de división de trabajo.
    h. Hitos/Planes de lanzamiento.
    i. Dependencias claves.
    j. Identificación del camino crítico (línea base).
    k. Cronograma del proyecto.
    l. Plan de comunicación del proyecto.
    m. Interesados del proyecto (stakeholders).
    n. Medición del desempeño (desviaciones, impacto, medidas correctivas).
    o. Acta de cierre (aprobación de los entregables, análisis de los beneficios obtenidos, lecciones aprendidas).

2. Incluir en la metodología la identificación de los riesgos que se pueden materializar con el desarrollo del proyecto. Se debe considerar lo siguiente:

    a. Identificación del riesgo.
    b. Análisis del riesgo.
    c. Tratamiento y control del riesgo (evitar, transferir, mitigar, prevenir, asumir).
    d. Supervisión de los riesgos durante el desarrollo del proyecto.
    e. Clasificación del riesgo.

3. Incluir en la metodología el aseguramiento de la calidad del proyecto, incluyendo lo siguiente:

    a. Actividades y prácticas del plan de calidad.
    b. Responsables del aseguramiento de la calidad.
    c. Criterios de éxito/aceptación del proyecto.
    d. Métricas de desempeño de los integrantes del proyecto.

4. Alinear la metodología del proyecto con el procedimiento para la gestión de cambios, incluyendo:

    a. Control de cambios.
    b. Costos que generan los cambios.
    c. Cronograma de implementación del cambio.
    d. Alcance del cambio.

5. Asegurar que la metodología en cada proyecto de TI se contemple:

    a. La comunicación oportuna de los planes y avances del proyecto.
    b. La comunicación de los cambios, principalmente a los interesados que se ven directamente afectados.
    c. La asociación de los entregables e hitos.
    d. La aprobación del proyecto y los planes asociados.
    e. La realización de revisiones post-implementación.
    f. La realización de informes/reportes de avance y estado del proyecto.

6. Establecer un portafolio de proyectos de TI el cual permita mantener una gestión integra para la toma de decisiones, seguimiento y control de los proyectos de TI. Se debe considerar al menos lo siguiente:

    a. Lista de proyectos de TI en proceso y futuros (se debe mantener un registro histórico de proyectos para mantener la trazabilidad de las relaciones con proyectos futuros). Se debe considerar lo siguiente:
        i. Alcance del proyecto.
        ii. Completitud del proyecto en términos de tiempo y costo (proyectado contra el real).
        iii. Estado general de los riesgos del proyecto.
        iv. Dependencias y/o relaciones con otros proyectos.

b. Priorización de proyectos según la planificación estratégica a nivel organizacional.
c. Alineación de los proyectos con los objetivos estratégicos de TI.

7. Realizar para los proyectos que requieran una mayor inversión de recursos económicos, casos de negocio como medio para determinar si los resultados del proyecto obtienen los beneficios esperados. Para ello considerar al menos lo siguiente:

    a. Descripción del proyecto (definición de la actividad, objetivos, requerimientos de negocio y detalle de las características del proyecto).
    b. Estado de la Institución antes de la implementación del proyecto.
    c. Justificación del proyecto.
    d. Análisis financiero de costos (adquisiciones y costos de operación).
    e. Resultado del análisis financiero:
        i. Alineación con los objetivos estratégicos y la arquitectura de información empresarial.
        ii. Beneficios financieros.
        iii. Beneficios no financieros (capacidad técnica, operativa y de negocio).
        iv. Análisis de Riesgos (alineado a la metodología para la gestión de riesgos).

8. Valorar el uso de marcos de referencia como guía para crear o actualizar la metodología para la administración de proyectos. Dichos marcos pueden ser:

    a. PMBOK (Project Management Body of Knowledge) del PMI (Project Management Institute): Estándar que provee guías, reglas y características para la gestión de proyectos, programas y portafolios.
    b. PRINCE2 (Projects IN Controlled Environments, version 2): Procesos basados en métodos para una gestión de proyectos efectiva.
    c. COBIT 2019 (Control Objectives for Information and related Technology): Marco de referencia que consolida aspectos de COBIT 4.1 y COBIT 5, para la formulación de buenas prácticas y la toma de decisiones concernientes a T.I. en soporte de los objetivos organizacionales.

HALLAZGO 06: AUSENCIA DE UN PROCEDIMIENTO PARA LA GESTIÓN DE CAMBIOS DE TI. RIESGO MEDIO.

CONDICIÓN:

Se determinó que la Unidad de TIC no cuenta con un procedimiento que permita un adecuado registro y control de cambios de TI, para gestionarlos en relación con los procesos de negocio, sistemas e infraestructura.

CAUSA

De acuerdo con la respuesta brindada en la solicitud de requerimientos iniciales, la Dirección Nacional de Notariado menciona que no se cuentan con un procedimiento formalmente establecido para la gestión de cambios de TI.

EFECTO

Al no contar con procedimientos para gestionar apropiadamente las solicitudes de cambios, no se puede llevar un control adecuado de los cambios realizados y se dificulta llevar un orden en las versiones de la información y los sistemas. Al no disponer de estos procedimientos, existe el riesgo de afectar los datos y sistemas de la organización, generando un impacto directo para todos los usuarios que utilizan esa información.

CRITERIO:

En el proceso **BAI06 Gestionar los cambios de TI**, presente en el estándar de Control Objectives for Information and related Technology 2019 (COBIT 2019), se menciona: *"Gestionar todos los cambios de una manera controlada, incluidos los cambios estándar y los mantenimientos de emergencia en relación con los procesos de negocio, las aplicaciones y la infraestructura. Esto incluye estándares y procedimientos de cambio, evaluación del impacto, priorización y autorización, cambios de emergencia, seguimiento, informes, cierre y documentación".*

RECOMENDACIONES:

A la Unidad de Tecnologías de Información y Comunicación:

1. Elaborar, aprobar y divulgar procedimientos para la gestión de cambios solicitados a TI. Para ello, se debe considerar:
    a. La descripción del procedimiento de cambios que tome en cuenta:
        i. Registro de la solicitud del cambio.
        ii. Impacto del cambio (según categoría y priorización).
        iii. Proceso de cambios de emergencia.
        iv. Estado del cambio.
        v. Revisión post-implantación.
        vi. Riesgos asociados al cambio.
        vii. Plan de implementación (incluyendo un cronograma).
    b. Un control de cambios que incluya la fecha, la versión, responsable y los involucrados.
    c. Costos relacionados a la implementación del cambio.
    d. Alcance del cambio.
    e. Métricas o indicadores para medir la calidad del cambio.

2. Comunicar los resultados del cambio a todos los usuarios que se ven directamente impactados y brindar la capacitación requerida. En caso de que el cambio impacte o modifique algún sistema de información, se deben actualizar los respectivos manuales de usuario.

HALLAZGO 07: AUSENCIA DE UN PROCEDIMIENTO PARA LA GESTIÓN DE SOLICITUDES, INCIDENTES Y PROBLEMAS DE TI. RIESGO MEDIO.

CONDICIÓN:

Según la revisión efectuada durante el proceso de auditoría, no fue posible determinar si existe un procedimiento formalmente establecido y aprobado para la gestión de solicitudes, incidentes y problemas de TI.

CAUSA:

De acuerdo con la respuesta brindada en la solicitud de requerimientos adicionales, la Dirección Nacional de Notariado menciona que no se cuenta con un procedimiento para la gestión de solicitudes, incidentes y problemas de TI.

EFECTO

Al no contar con un procedimiento formal para atención de incidentes, no se garantiza que se dé una adecuada administración de estos, minimizando el riesgo de recurrencia y procurando la captura del conocimiento y el aprendizaje necesario.

CRITERIO:

En el proceso **DSS02 Gestionar las peticiones y los incidentes de servicio**, presente en el estándar de Control Objectives for Information and related Technology 2019 (COBIT 2019), se menciona: *"Proporcionar una respuesta oportuna y efectiva a las solicitudes de los usuarios y la resolución de todos los tipos de incidentes. Restaurar el servicio normal, registrar y completar las solicitudes de usuario; y registrar, investigar, diagnosticar, escalar y resolver los incidentes".*
Por otra parte, en el proceso **DSS03 Gestionar los problemas**, presente en el estándar de Control Objectives for Information and related Technology 2019 (COBIT 2019), se menciona:
"Identificar y clasificar los problemas y su causa raíz. Ofrecer una solución oportuna para evitar incidentes recurrentes. Ofrecer recomendaciones de mejoras".

RECOMENDACIONES:

A la Unidad de Tecnologías de Información y Comunicación:

1. Elaborar un procedimiento para la gestión y atención de solicitudes de servicio por parte de los usuarios, que permita conocer cuáles son las necesidades de los usuarios de los sistemas o equipos computaciones, y requieran los servicios de TI. Considerar al menos los siguientes aspectos:

a. Registro de solicitudes (Herramienta o formularios de atención de requerimientos).
b. Categorización y priorización para la atención de la solicitud.
c. Estudio de impacto sobre la aplicación de la solicitud.
d. Ejecución de los cambios o inclusión de la nueva solicitud.
e. Cierre de la atención de la solicitud.

2. Elaborar un procedimiento para la gestión de problemas de TI, de tal forma que se le pueda dar seguimiento a los incidentes recurrentes y poder encontrar una solución final a los mismos, evitando que afecten la disponibilidad de los servicios informáticos. Dentro del procedimiento se debe considerar como mínimo lo siguiente.
   a. Identificación de problemas mediante incidentes repetitivos o conocidos.
   b. Clasificación de problemas según categoría, impacto, urgencia y prioridad.
   c. Determinar la causa raíz del problema.
   d. Definir un plan de acción para la resolución de problemas.
   e. Definir el proceso de cierre del problema.

3. Definir responsables de gestionar los procedimientos, la frecuencia de la revisión y actualización de esta (cuando se requiera).

4. Se recomienda tomar en cuenta las buenas prácticas y normativas vigentes que puedan aplicarse en la institución, para realizar el procedimiento de administración de problemas, además de tomar en cuenta Gestión de Solicitudes y Gestión de Incidentes, de tal modo que se considere las diferencias entre estos procedimientos.

HALLAZGO 08: AUSENCIA DE UNA METODOLOGÍA PARA LA EVALUACIÓN DEL CONTROL INTERNO DE TECNOLOGÍAS DE INFORMACIÓN. RIESGO MEDIO.

CONDICIÓN:

No fue posible verificar si la Unidad de Tecnologías de Información y Comunicación cuenta con una metodología para realizar la evaluación de control interno de tecnologías de información. Cabe mencionar que se suministró un informe de auditoría externa del año 2019, sin embargo, no se encontró evidencia de informes de auditoría o control internos.

CAUSA:

En la respuesta a la solicitud de información adicional se menciona que *el seguimiento a las recomendaciones se aplica a través del Sistema de Auditoría ARGOS*, sin embargo, no se suministró documentación que respalde dicho seguimiento. Por otra parte, se menciona que no se cuenta con evidencia del seguimiento realizado a las recomendaciones de auditoría externa.

EFECTO

La Unidad de TI al no poseer una metodología para la evaluación del control interno de tecnologías de información desconocería cuál es su estado actualmente, con respecto a sus deficiencias e ineficiencias, las acciones posibles de mejora, la transparencia de sus labores se vería afectada provocando desconfianza en los principales interesados.

CRITERIO:

En el proceso **MEA02 Gestionar el sistema de control interno**, presente en el estándar de Control Objectives for Information and related Technology 2019 (COBIT 2019), se menciona:
"Supervisar y evaluar continuamente el entorno de control, incluyendo autoevaluaciones y auto concienciación. Habilitar a la gerencia para identificar deficiencias e ineficiencias de control e iniciar acciones de mejora. Planificar, organizar y mantener estándares para la evaluación del control interno y la eficacia del control de procesos".

RECOMENDACIONES:

A las áreas de control interno de la DNN:

1. Elaborar una metodología de evaluación del control interno que permita verificar que se cumpla con las políticas, procedimientos y lineamientos referentes a tecnologías de información. Esta metodología debe considerar las evaluaciones de control sobre los procesos establecidos con los terceros que brinden servicios de TI.

2. Establecer procesos o procedimientos para asegurar que las actividades de control se cumplan y las excepciones son prontamente reportadas, seguidas y analizadas. Se debe asegurar que las acciones correctivas sean escogidas e implementadas apropiadamente.

3. Mantener el sistema de control interno de T.I., considerando cambios continuos en el ambiente de control organizacional, relevante a los procesos de negocio y riesgos de TI. Si las brechas existen, evaluar y recomendar cambios.

4. Evaluar periódicamente el desempeño del marco de trabajo de control interno de T.I.

5. Asegurar que se atiendan oportunamente las recomendaciones realizadas en estudios de auditoría tanto internos como externos, además, dejar evidencia que permita respaldar las acciones ejecutadas.

HALLAZGO 09: AUSENCIA DE UN PROCEDIMIENTO PARA LA GESTIÓN DE LA CONTINUIDAD, CAPACIDAD Y DISPONIBILIDAD DE LA PLATAFORMA TECNOLÓGICA. RIESGO MEDIO.

CONDICIÓN:

Luego de realizar la solicitud de los requerimientos para validar la existencia de un procedimiento para la gestión de la continuidad, capacidad y disponibilidad de la plataforma tecnológica no fue posible identificar un proceso documentado, aprobado y formalizado para dicha gestión.

Sin embargo, fue posible identificar que se realizan actividades de manera automática como pruebas de capacidad al momento de la configuración del activo de TI (Servidores u otros), además, por medio de la consola Avamar, se pueden monitorear el estado de la capacidad de los servidores que componen la plataforma de la organización, así como también el estado de los respaldos realizados.

CAUSA:

Según se comenta por parte de la DNN, *"... aún no se cuentan con ellos, esto debido a que las soluciones que realizan estas actividades están recién instaladas y se está en proceso de medir los RPO y RTO y las reuniones correspondientes*". Además, no se han realizado capacitaciones referentes a los temas de continuidad y capacidad.

EFECTO

Al no contar con dicho(s) procedimiento(s), la organización puede verse expuesta a ver obstaculizada la generación de una respuesta planificada ante un imprevisto que permita minimizar daños y recuperar las actividades o servicios lo antes posible.

CRITERIO:

En el proceso **BAI04 Gestionar la Disponibilidad y la Capacidad**, presente en el estándar de Control Objectives for Information and related Technology 5 (COBIT 5), se menciona: *"Mantener la disponibilidad del servicio, la gestión eficiente y la optimización del rendimiento de los sistemas mediante la predicción del rendimiento y de los requerimientos de capacidad."* Además, el **DSS04 Gestionar la Continuidad**, menciona: *"Establecer y mantener un plan que permita a las organizaciones empresariales y a TI responder a los incidentes y adaptarse rápidamente a las interrupciones. Esto permitirá la operación continua de los procesos críticos de negocio y de los servicios de I&T necesarios, y mantener la disponibilidad de recursos, activos e información en un nivel aceptable para la empresa."*

RECOMENDACIONES:

A la Unidad de Tecnologías de Información y Comunicaciones:

1. Elaborar un procedimiento para gestionar la continuidad, capacidad y disponibilidad de la plataforma tecnológica.

2. Generar un modelo de monitoreo como parte del procedimiento a elaborar considerando al menos los siguientes aspectos:

    a. Periodicidad del monitoreo.
    b. Indicadores de rendimiento.
    c. Herramienta utilizada para el monitoreo.
    d. Umbrales de monitoreo (gestión de alertas).
    e. Reportes periódicos (mensuales o según la periodicidad que se defina) de los siguientes aspectos:

        i. Reportes de disponibilidad.
        ii. Reportes de capacidad.
        iii. Reportes de excepciones (situaciones esporádicas que pueden levantar una alerta sobre capacidad o disponibilidad).

3. Generar un plan de capacidad, desempeño y disponibilidad incluyendo un análisis del comportamiento en el consumo de recursos. En el mismo se debe realizar una proyección de los recursos para determinar cuál va a ser el consumo futuro por parte de la Institución y así generar una estrategia para sustentar la necesidad de esos recursos. Además, se debe incluir un plan de trabajo incluyendo los aspectos a realizar durante el periodo, entre ellos:

    a. Componentes que se deben actualizar en el proceso de monitoreo (nuevo equipo, retiro de ítems de configuración).
    b. Implementación de nuevas herramientas o configuraciones.
    c. Identificación de parámetros a monitorear.
    d. Gestión de acuerdos de nivel de servicio o acuerdos de nivel operativo (en caso de que existan).

4. Revisar periódicamente el procedimiento, los planes y el modelo de monitoreo.

5. Comunicar y divulgar al personal respectivo sobre la existencia del procedimiento.

6. Definir responsables de gestionar el procedimiento, planes y modelo, la frecuencia de la revisión y actualización de estos.

7. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.

HALLAZGO 10: AUSENCIA DE UN CATÁLOGO DE SERVICIOS POR PARTE DE LA UNIDAD DE INFORMÁTICA DE LA DNN. RIESGO BAJO.

CONDICIÓN:

Mediante la revisión efectuada y lo indicado por la administración, la Unidad de Informática de la DNN no cuenta con un catálogo de servicios.

CAUSA

Se notificó por parte de la administración de la DNN que no se cuenta con dicha herramienta, sin embargo, no fue posible identificar una causa específica para esta limitante. Solamente, se puede mencionar que no se han gestionado los recursos necesarios en la unidad de informática como para desarrollar un catálogo de servicios.

EFECTO

Al no contar con un catálogo de servicios, no se tiene conocimiento por parte de las áreas usuarias de cuáles son los servicios de TI que brinda la Unidad de Informática y sus características.

CRITERIO:

En el proceso **APO09 Gestionar los acuerdos de servicio**, presente en el estándar de Control Objectives for Information and related Technology 5 (COBIT 5), se menciona:
"Alinear los servicios basados en TI y los niveles de servicio con las necesidades y expectativas de la entidad, incluyendo identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios TI, niveles de servicio e indicadores de rendimiento.".

RECOMENDACIONES:

A la Unidad de Tecnologías de la Información y Comunicación:

1. Elaborar un catálogo de servicios de TI, identificando los servicios proporcionados por el departamento de informática y documentar cada uno de ellos. Al menos el catálogo de servicios debe contener lo siguiente:
    a. Descripción del servicio.
    b. Horas del servicio.
    c. Contactos.
    d. Disponibilidad.
    e. Características del servicio.

2. Elaborar un procedimiento para la gestión de acuerdos de nivel de servicio, con los siguientes lineamientos:
    a. La estructura que debe cumplir cada SLA.

b. La periodicidad con la cual se deben revisar los SLAs.
c. El responsable que monitorea el cumplimiento de los SLAs.

3. Elaborar los correspondientes acuerdos de nivel de servicio (SLA), tomando en consideración los requerimientos y demandas de cada una de las áreas usuarias. Asegurar que los acuerdos de nivel de servicio cuenten con al menos lo siguiente:
    a. Descripción del servicio.
    b. Alcance del acuerdo (Se incluye lo que abarca el acuerdo y lo que se excluye).
    c. Horas en las cuales el servicio estará disponible, incluyendo condiciones especiales para excepciones (por ejemplo, fines de semana, feriados).
    d. Métricas del servicio tales como:
        i. Disponibilidad (Nivel de disponibilidad del servicio dentro de las horas acordadas, el cual generalmente es expresado en forma de porcentaje).
        ii. Confiabilidad (Número máximo de interrupciones del servicio que pueden tolerarse).
        iii. Rendimiento (Detalles de la capacidad de respuesta esperada del servicio, por ejemplo, número de transacciones a procesar).
    e. Seguridad (Descripción de las políticas de seguridad asociadas).
    f. Soporte al cliente.
    g. Contactos donde el cliente puede llamar o enviar consultas con respecto al servicio.
    h. Responsabilidades de las distintas partes involucradas en el servicio.

4. Revisar periódicamente los acuerdos de nivel de servicio para asegurar que son efectivos, actuales y que los cambios en los requisitos se tienen en cuenta cuando sea apropiado.

5. Comunicar y divulgar al personal respectivo sobre la existencia del catálogo y procedimiento.

6. Definir responsables de gestionar el catálogo de servicios y procedimiento, la frecuencia de la revisión y actualización de estos.

7. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.

HALLAZGO 11: AUSENCIA DE UN CORRECTO SEGUIMIENTO Y COMUNICACIÓN DURANTE LA GESTIÓN DE RIESGOS DE T.I. RIESGO MEDIO.

CONDICIÓN:

Fue posible identificar una herramienta que le facilita a la UTIC las tareas necesarias para realizar la identificación y gestión de los riesgos, denominado “SEVRI 2021-2022 Gestión de las Tecnologías de la Información y Comunicación”, sin embargo, no es posible identificar un plan de comunicación en caso de la materialización de alguno de los riesgos.

Tampoco se identificaron reportes sobre la rendición de cuentas de los avances del plan de acción para la gestión de los riesgos.

CAUSA

Falta de regularidad y detalle en el seguimiento sobre el control de reportes sobre la rendición de cuentan de los avances de planes de acción, lo que también se refleja en la ausencia de un plan de comunicación durante la gestión de riesgos.

EFECTO

Al no realizar un correcto seguimiento y comunicación durante la gestión de riesgos, se podrían materializar inconvenientes dentro de la institución como, por ejemplo:

- Complicaciones en la identificación, análisis, gestión y reporte de los riesgos de TI.
- Ausencia de un perfil de riesgos completo y actualizado.
- Ausencia de acciones definidas para una gestión de riesgo efectivo.

CRITERIO:

En el proceso **APO12 Gestionar el Riesgo**, presente en el estándar de Control Objectives for Information and related Technology 2019 (COBIT 2019), se menciona:*" Identificar, evaluar y reducir continuamente los riesgos relacionados con I&T dentro de los niveles de tolerancia establecidos por la gerencia ejecutiva de la empresa."*

RECOMENDACIONES:

A la Unidad de Tecnologías de Información y Comunicación:

1. Realizar e implementar una metodología formal para la gestión de riesgos de TI, considerando como mínimo el detalle de las actividades necesarias para llevar a cabo los siguientes aspectos:

    a. Identificación de los potenciales riesgos, a partir de los sistemas críticos identificados.
    b. Determinar cuáles procesos, podrían verse impactados por la materialización del riesgo bajo estudio.
    c. Definición de roles y responsabilidades de las áreas involucradas.
    d. Identificación del riesgo.
    e. Análisis de riesgo (análisis cualitativo y cuantitativo, así como un mapa de riesgo).
    f. Evaluación de riesgo (descripción del impacto del riesgo en términos comprensibles al negocio).
    g. Administración del riesgo, estableciendo estrategias de tratamiento del riesgo (evitar, mitigar, transferir o aceptar) y los controles requeridos.
    h. Aceptación del riesgo por parte de las áreas involucradas.

i. Plan o procedimiento de comunicación a nivel de la organización.
j. Revisión y monitoreo.

2. Presentar la metodología de gestión de riesgos de TI ante la gerencia o jefatura correspondiente para su respectiva aprobación, y una vez aprobada comunicarla a todas las unidades involucradas.

3. Realizar un análisis de riesgos periódicamente y actualizar los riesgos según los resultados obtenidos y los avances realizados en el plan de acción, además, de presentar un informe al menos una vez al año de las actualizaciones pertinentes.

4. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.

HALLAZGO 12: AUSENCIA DE ACUERDOS DE NIVEL DE SERVICIO PARA LOS SERVICIOS BRINDADOS A LA DNN. RIESGO BAJO.

CONDICIÓN:

No fue posible identificar evidencia de la definición, documentación, control y/o seguimiento, sobre acuerdos de nivel de servicio relacionado con la respuesta a incidentes que posee la organización.

CAUSA

Como respuesta a los requerimientos solicitados sobre la gestión de SLAs, se comentó por parte de la administración de la DNN que aún "no se cuenta con procedimientos o aplicación de ITIL, los mismos se llevarían acaba en la contratación 2021CD-000007-0007500001".

EFECTO

Al no contar con los acuerdos de nivel de servicio para cada uno de los servicios brindados, no se establecen los acuerdos requeridos para gestionar adecuadamente los servicios de TI ni se tiene un control de los niveles de rendimiento y capacidad de cada uno de los servicios, por lo que existe el riesgo de que alguno no cumpla con los parámetros que necesitan las áreas usuarias.

CRITERIO:

El proceso **APO09 "Gestionar los acuerdos de servicio"** presente en el marco de referencia COBIT 2019 establece que se debe: "*Alinear los productos y servicios habilitados por I&T y los niveles de servicio con las necesidades y expectativas de la empresa, incluidos la identificación, especificación, diseño, publicación, acuerdo y monitorización de los productos y servicios de I&T, niveles de servicio e indicadores de rendimiento.*".

RECOMENDACIONES:

Al Departamento de Tecnologías de Información en conjunto con la Administración del DNN:

1. Elaborar acuerdos de nivel de servicio para los servicios brindados a la DNN, tomando en consideración los requerimientos y necesidades de las áreas usuarias.

2. Asegurar que los acuerdos de nivel de servicio cuenten con al menos lo siguiente:
    a. Compromisos del Cliente.
    b. Requerimientos de soporte para el servicio.
    c. Métricas cuantitativas y cualitativas para la medición del servicio.
        a. Disponibilidad.
        b. Confiabilidad.
        c. Desempeño.
        d. Capacidad de crecimiento.
        e. Niveles de soporte.
        f. Continuidad.
        g. Seguridad.
        h. Restricciones de demanda.
    d. Arreglos comerciales y de financiamiento.
    e. Roles y responsabilidades.
    f. Periodicidad de seguimiento.

3. Dar seguimiento periódico a los SLAs definidos para validar el cumplimiento de los acuerdos tomados.

4. Comunicar a la administración y a los interesados del acuerdo de nivel de servicio, los resultados de la revisión y el análisis de indicadores respectivo.

HALLAZGO 13: DEBILIDADES EN LA SEGURIDAD FÍSICA DEL CUARTO DE COMUNICACIONES DE LA DNN. RIESGO MEDIO.

CONDICIÓN:

Producto de la evidencia suministrada fue posible identificar debilidades en la seguridad física del cuarto de comunicaciones. Además, según se indica, los servidores, almacenamiento y respaldos de producción están el centro de datos ADN.
En el documento **DNN-Tabla cuarto de servidores Auditoria** se indican algunos aspectos que ponen en riesgo la seguridad física del cuarto de comunicaciones:

- No existen detectores de humo para el cuarto de comunicaciones.
- Se menciona que no cuentan con extintores para el cuarto de comunicaciones.
- En el cuarto existe material en desuso u otros materiales no asociados.

CAUSA:

No se cuenta con procedimientos o políticas para la gestión de la seguridad física del cuarto de comunicaciones.

EFECTO

Producto de lo antes expuesto, se evidencia que hay oportunidades de mejora en el cuarto de comunicaciones, el no aplicar medidas correctivas puede implicar la materialización de riesgos en materia de seguridad física y de entorno. Además, la no existencia de políticas impide a los colaboradores de TI y de áreas usuarias hacer un uso efectivo de los recursos de TI.

CRITERIO:

Además, en la práctica de gestión **DSS01.05 Gestionar las instalaciones**, presente en el **DSS01 Gestionar las Operaciones** del estándar de Control Objectives for Information and related Technology (COBIT 2019), se menciona:

"*Gestionar las instalaciones, incluidos los equipos de suministro eléctrico y comunicaciones, alineados con las leyes y reglamentos existentes, los requisitos técnicos y del negocio, las especificaciones del proveedor y las directrices de salud y seguridad*".

RECOMENDACIONES:

<u>Al Departamento de Tecnologías de Información:</u>

1. Elaborar una política de gestión de la seguridad física de las instalaciones de TI, incluyendo el cuarto de comunicaciones.

2. Valorar los riesgos de seguridad física a los que se encuentra expuesto el cuarto de comunicaciones.

3. Elaborar un plan de acción para la implementación de mejoras a nivel de infraestructura que contemplen las medidas de seguridad.

4. Producto de la atención de la *recomendación 1*, comunicar la política en cuestión a nivel institucional.

5. Revisar y actualizar (esto último cuando sea necesario) la política al menos una vez al año, mantener el registro en el control de versiones.

6. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como COBIT e INTE/ISO/IEC.

IV. APÉNDICE

APÉNDICE I: ANÁLISIS DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN.

Departamento de Tecnología de Información
Periodo 2021

Tipos de Riesgo	
ALTO	A
MEDIO	M
BAJO	B

Alto ☑	Requiere una atención inmediata por su impacto en seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. No se han establecido controles en este nivel de riesgo.
Medio ☑	Requiere una atención intermedia ya que su impacto representaría riesgos sobre seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. Se han establecido controles insuficientes en este nivel de riesgo.
Bajo ☑	Requiere una atención no prioritaria ya que su impacto no es directamente sobre seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. Se han establecido controles adecuados en este nivel de riesgo.

V. PLANIFICACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN.

A. PLANIFICACIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
A.1.	Se tiene definido un plan estratégico de TI formalmente aprobado y alineado a los objetivos organizacionales.		✓	Se cumple con la condición.	B
A.2.	Se le da seguimiento al PETI por parte del Comité de TI.		✓	Se cumple con la condición.	B
A.3.	Se define anual un plan anual operativo de TI con los proyectos y actividades que realiza el área de TI y se encuentra alineado a las iniciativas y objetivos del PETI.		✓	Se cumple con la condición.	B
A.4.	Se le da seguimiento periódico al cumplimiento del PAO.		✓	Se cumple con la condición.	B

B. GESTIÓN DEL PRESUPUESTO DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
B.1.	Se genera un plan anual presupuestario de TI formalmente aprobado.		✓	Se cumple con la condición.	B

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
B.2.	El presupuesto se encuentra categorizado y priorizado según las actividades críticas del plan anual operativo de TI.		✓	Se cumple con la condición.	B
B.3.	Se mantiene un control de gastos y ejecuciones presupuestarias de TI y se le brinda informes de ejecución a la administración.		✓	Se cumple con la condición.	B
B.4.	Se mantiene alineado el plan presupuestario de TI con el plan anual operativo.		✓	Se cumple con la condición.	B

C. GESTIÓN DE PROVEEDORES DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
C.1.	Se establecen contratos formales para los servicios que son brindados por terceros.		✓	Se cumple con la condición.	B
C.2.	Para los contratos de servicios de TI, se establecen acuerdos de nivel de servicio con los respectivos indicadores de capacidad, disponibilidad, confiabilidad, etc.		✓	Se cumple con la condición.	B
C.3.	Se realiza un seguimiento al cumplimiento contractual de las responsabilidades de los proveedores.		✓	Se cumple con la condición.	B

D. GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
D.1.	Se tiene una metodología formalmente establecida y aprobada para la gestión de riesgos de TI.		✓	Se cumple con la condición.	B
D.2.	La evaluación de riesgos de TI es periódica y se encuentra revisada y aprobada por la administración (de acuerdo con el nivel de tolerancia al riesgo organizacional).	✗		No se cumple con la condición. Ver el Hallazgo 11 en la página 24.	B

E. GESTIÓN DE ACUERDOS DE NIVEL DE SERVICIO.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
E.1.	Se cuenta con un catálogo de servicios de TI actualizado y aprobado por el Comité de TI.	✗		DNN no cuenta con un catálogo de servicios establecido.	B
E.2.	Se cuenta con una política o procedimiento para la gestión de los acuerdos de nivel de servicio (SLAs) de TI.	✗		No fue posible verificar si se cuenta con un procedimiento o política para gestionar los SLA.	B
E.3.	Se tiene definido acuerdos de nivel de servicio para cada uno de los servicios activos que se encuentran definidos en el catálogo.	✗		No se cumple con la condición.	B

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
E.4.	Cada uno de los SLAs tiene establecido las responsabilidades de las partes, indicadores (disponibilidad, capacidad, confiabilidad, etc.) y requerimientos de soporte.	✗		No se cumple con la condición.	B
E.5.	Se verifica el cumplimiento, validez y actualización de los SLAs establecidos con las áreas usuarias de manera periódica.	✗		No se cumple con la condición.	B

VI. IMPLEMENTACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN.

F. GESTIÓN DE PROYECTOS DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
F.1.	Se cuenta con una metodología para la gestión de proyectos de TI formalmente establecida.	✗		DNN no cuenta con un procedimiento formal para la gestión de proyectos.	M
F.2.	Se documenta cada una de las fases del ciclo de vida del proyecto para cada uno de los proyectos ejecutados por el área de TI (constitución, estimación de recursos, responsabilidades, cronograma, desempeño, riesgos, calidad, cambios y cierre del proyecto.)	✗		No se cumple con la condición.	M

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
F.3.	Los usuarios o clientes de los proyectos aprueban formalmente los entregables de estos.	✗		No se cumple con la condición.	M
F.4.	Se les da seguimiento a los proyectos posterior a la implementación.	✗		No se cumple con la condición.	M

G. GESTIÓN DE LA CAPACIDAD Y DISPONIBILIDAD.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
G.1.	Se cuenta con una política para la gestión de la capacidad y disponibilidad de la plataforma tecnológica.	✗		No se cumple con la condición.	M
G.2.	El equipo de TI es monitoreado periódicamente.		✓	Se cumple con la condición.	B
G.3.	Se realizan proyecciones del uso de recursos de acuerdo con el comportamiento o tendencia del consumo histórico para determinar la necesidad de ampliar la capacidad de la infraestructura.		✓	Se cumple con la condición.	B

H. GESTIÓN DE CAMBIOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
H.1.	Se cuenta con una política y/o procedimiento para la gestión de cambios de TI.	✗		DNN no cuenta con un procedimiento formal para la gestión de cambios de TI.	M
H.2.	Los cambios se realizan a través de solicitudes formales y se documenta todo el proceso realizado (ciclo de vida).	✗		No se cumple con la condición.	M
H.3.	La documentación de los cambios se mantiene de forma centralizada (mesa de servicios).	✗		No se cumple con la condición.	M
H.4.	Se evalúa periódicamente el estado de los cambios para verificar que todas las solicitudes hayan sido atendidas.	✗		No se cumple con la condición.	M

VII. SOPORTE Y SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN.

I. GESTIÓN DE INCIDENTES.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
I.1.	Se cuenta con un procedimiento para la gestión de incidentes de TI.	✗		DNN no posee un procedimiento para la gestión de solicitudes, incidentes y problemas.	M

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
I.2.	La gestión de incidentes se mantiene centralizada (mesa de servicios).	✗		No se cumple con la condición.	M
I.3.	Se verifica periódicamente el estado de los incidentes para determinar si se atienden oportunamente los incidentes registrados.	✗		No se cumple con la condición.	M

J. GESTIÓN DE PROBLEMAS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
J.1.	Se cuenta con un procedimiento para la gestión de problemas de TI.	✗		DNN no posee un procedimiento para la gestión de solicitudes, incidentes y problemas.	M
J.2.	Se identifica, clasifica y analiza la causa raíz de los problemas de TI.	✗		No se cumple con la condición.	M

K. GESTIÓN DE LA CONTINUIDAD DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
K.1.	Se cuenta con un plan de continuidad del negocio (con el componente de TI), formalmente establecido y aprobado por la administración o el Comité de TI.	✗		No se cumple con la condición. Ver Hallazgo 09 en la página 21.	M
K.2.	Se realizan pruebas y capacitaciones sobre el plan de continuidad del negocio.	✗		No se cumple con la condición. Ver Hallazgo 09 en la página 21.	M
K.3.	Se cuenta con una política y/o procedimiento para la realización de respaldos de información.	✗		No se cumple con la condición. Ver Hallazgo 09 en la página 21.	B
K.4.	Se realizan pruebas a los respaldos de información.		✓	Se cumple con la condición.	B
K.5.	Se tienen medidas de seguridad para los respaldos de información (acceso restringido, traslado de respaldos a un sitio externo).		✓	Se cumple con la condición.	B
K.6.	Se cuenta con redundancia de equipos que soportan los servicios críticos (servidores, equipo de comunicación, enlaces a redes externas).		✓	Se cumple con la condición.	B
K.7.	Se cuenta con un sitio alterno para el procesamiento de datos en una posición geográfica distinta a la ubicación del cuarto de servidores principal.		✓	Se cumple con la condición.	B

L. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
L.1.	Se cuenta con una política de seguridad de la información formalmente aprobado por la administración y divulgado a nivel organizacional.	✗		No se cumple con la condición.	A
L.2.	Se le brinda seguimiento al cumplimiento de la política de seguridad de la información (se aplican medidas correctivas) y se le comunica los resultados a la administración.	✗		No se cumple con la condición.	A
L.3.	Se cuenta con una política de uso de recursos de TI (correo electrónico, equipos, red).	✗		No se cumple con la condición.	A
L.4.	Se cuenta con una política y/o procedimiento para la gestión de cuentas de usuario.	✗		No se cumple con la condición.	M
L.5.	Se revisan periódicamente los perfiles de los usuarios para determinar si estos poseen la cantidad de accesos mínimos necesarios.	✗		No se cumple con la condición	M

M. GESTIÓN DE LA SEGURIDAD FÍSICA Y AMBIENTAL.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
M.1.	Se tienen definidos mecanismos de autorización y/o autenticación para el ingreso a sitios restringidos (por ejemplo, cuarto de servidores, cuartos de comunicaciones, etc.).		✓	Se cumple con la condición.	B
M.2.	Se mantiene una bitácora de acceso para el personal interno y externo que ingresa al cuarto de servidores.		✓	Se cuenta con una bitácora digital que registra los ingresos de personal.	B
M.3.	Se tiene definido formalmente el personal que posee autorización para ingresar al cuarto de servidores y/o comunicaciones.		✓	Se cumple con la condición.	B
M.4.	El personal externo que accede a sitios restringidos siempre está acompaño por personal interno autorizado.		✓	Se cumple con la condición.	B
M.5.	La puerta de acceso al cuarto de servidores y comunicaciones se encuentra asegurada contra accesos no autorizados y hecha de un material resistente.		✓	Se cuenta con tarjeta electrónica e imán en la puerta.	B
M.6.	Las paredes del cuarto de servidores y comunicaciones están hechas de un material resistente y se encuentra completamente cerrado (por ejemplo, concreto).		✓	Se cumple con la condición.	B
M.7.	El cuarto de servidores se encuentra en un sitio seguro (lugares no propensos a desastres como inundaciones, incendios, etc.).		✓	Se cumple con la condición.	B

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
M.8.	Los equipos se encuentran ubicados en racks y asegurados en el suelo.		✓	Se cumple con la condición.	B
M.9.	El cableado de datos se encuentra aislado del cableado eléctrico.		✓	Se cumple con la condición.	B
M.10.	El cableado de red se encuentra debidamente rotulado.		✓	Se cumple con la condición.	B
M.11.	Se tiene instalado un pararrayos u otras medidas para la prevención de picos de corriente.		✓	Se cuenta con una UPS para todo el piso.	B
M.12.	El cuarto de servidores cuenta con aires acondicionados exclusivos para esta área (A/C principal y respaldo).		✓	Se cumple con la condición.	B
M.13.	Se cuenta con medios para detectar incendios e inundaciones.	✗		Se cuenta con detectores de humedad, sin embargo, no existen detectores de humo para el cuarto de comunicaciones.	M
M.14.	Se cuenta con extintores y/o aspersores en el cuarto de servidores.	✗		En la información solicitada se menciona que no cuentan con extintores para el cuarto de comunicaciones.	M

VIII. EVALUACIÓN DE TECNOLOGÍAS DE INFORMACIÓN.

N. VALORAR EL CONTROL INTERNO.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
N.1.	Se han establecido normas para la evaluación del control interno de TI.	✗		No fue posible verificar si se cuentan con evaluaciones para el control interno de TI.	M
N.2.	Se realizan autoevaluaciones periódicas para que TI identifique de manera proactiva las debilidades de control.	✗		No se cumple con la condición.	M
N.3.	Se ejecutan estudios de auditoría periódicos (internos o externos) para identificar debilidades en el cumplimiento de obligaciones con normativas relativas a TI.	✗		Solo se verificaron estudios de auditoría externos.	B

IX. RECOMENDACIONES GENERALES PARA LA CIBERSEGURIDAD

Controles	Familia de control / Dominio de práctica CMMC[1]	Práctica
Conozca sus activos	Gestión de la configuración	Establecer y mantener configuraciones de referencia e inventarios de sistemas organizacionales (incluidos hardware, software, firmware y documentación) a lo largo de los respectivos ciclos de vida de desarrollo del sistema.
	Gestión de la configuración	Seguimiento, revisión, aprobación o desaprobación y registro de cambios en los sistemas organizacionales.
	Gestión de la configuración	Restrinja, deshabilite o impida el uso de programas, funciones, puertos, protocolos y servicios no esenciales.
	Gestión de la configuración	Controle y supervise el software instalado por el usuario.
Capacite a sus usuarios	Concienciación y Formación	Asegúrese de que los gerentes, administradores de sistemas y usuarios de los sistemas organizacionales sean conscientes de los riesgos de seguridad asociados con sus actividades y de las políticas, normas y procedimientos aplicables relacionados con la seguridad de esos sistemas.

[1] Certificación del Modelo de Madurez de Ciberseguridad

Controles	Familia de control / Dominio de práctica CMMC[1]	Práctica
	Concienciación y Formación	Asegúrese de que el personal esté capacitado para llevar a cabo las funciones y responsabilidades relacionadas con la seguridad de la información que se le asignen.
	Concienciación y Formación	Proporcione capacitación de concientización sobre seguridad para reconocer y reportar indicadores potenciales de amenazas internas.
Software de lista blanca	Gestión de la configuración	Aplique la política de denegación por excepción (lista negra) para evitar el uso de software no autorizado o la política de denegación total, permiso por excepción (lista blanca) para permitir la ejecución de software autorizado.
Software de parches y sistemas operativos	Gestión de riesgos	Remediar las vulnerabilidades de acuerdo con las evaluaciones de riesgo.
	Sistema e Integridad de la Información	Identificar, reportar y corregir fallas en el sistema de información de manera oportuna.
Restringir privilegios administrativos	Control de acceso	Emplear el principio de privilegio mínimo, incluso para funciones de seguridad específicas y cuentas privilegiadas.

Controles	Familia de control / Dominio de práctica CMMC[1]	Práctica
	Control de acceso	Utilice cuentas o roles sin privilegios cuando acceda a funciones que no sean de seguridad.
	Control de acceso	Evite que los usuarios sin privilegios ejecuten funciones privilegiadas y capture la ejecución de dichas funciones en los registros de auditoría.
	Control de acceso	Autorice la ejecución remota de comandos privilegiados y el acceso remoto a información relevante para la seguridad.
Componentes del sistema de endurecimiento	Gestión de la configuración	Establecer y hacer cumplir los ajustes de configuración de seguridad para los productos de tecnología de la información empleados en los sistemas organizacionales.
Segmente su red	Control de acceso	Autorice el acceso inalámbrico antes de permitir dichas conexiones.
	Control de acceso	Controlar el flujo de CUI de acuerdo con las autorizaciones aprobadas.
	Sistema y Comunicación	Supervisar, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los sistemas de información de la organización) en los límites externos y los límites internos clave de los sistemas de información.

Controles	Familia de control / Dominio de práctica CMMC[1]	Práctica
	Sistema y Comunicación	Implemente subredes para los componentes del sistema de acceso público que estén física o lógicamente separados de las redes internas.
Copia de seguridad de sus datos y restauración de prueba	Recuperación	Realice y pruebe regularmente copias de seguridad de datos.
	Recuperación	Proteja la confidencialidad de la CUI de respaldo en las ubicaciones de almacenamiento.
	Recuperación	Realice periódicamente copias de seguridad de datos completas, completas y resistentes, según lo definido por la organización.
Habilitar autenticación multifactor	Identificación y autenticación	Utilice la autenticación multifactor para el acceso local y de red a cuentas privilegiadas y para el acceso de red a cuentas no privilegiadas.
	Mantenimiento	Requiera autenticación multifactor para establecer sesiones de mantenimiento no local a través de conexiones de red externas y finalice dichas conexiones cuando finalice el mantenimiento no local.
Recopilar y analizar registros de eventos	Auditoría y rendición de cuentas	Asegúrese de que las acciones de los usuarios individuales del sistema se puedan rastrear de manera única hasta esos usuarios para que puedan ser responsables de sus acciones.

Controles	Familia de control / Dominio de práctica CMMC[1]	Práctica
	Auditoría y rendición de cuentas	Revise los registros de auditoría.
	Auditoría y rendición de cuentas	Revisar y actualizar los eventos registrados.
	Auditoría y rendición de cuentas	Alerta en caso de falla del proceso de registro de auditoría.
	Auditoría y rendición de cuentas	Recopile información de auditoría (p. ej., registros) en uno o más repositorios centrales.
	Auditoría y rendición de cuentas	Proteja la información de auditoría y las herramientas de registro de auditoría contra el acceso, la modificación y la eliminación no autorizados.
	Auditoría y rendición de cuentas	Limite la gestión de la funcionalidad de registro de auditoría a un subconjunto de usuarios privilegiados.
	Auditoría y rendición de cuentas	Correlacione los procesos de revisión, análisis e informe de registros de auditoría para investigar y

Controles	Familia de control / Dominio de práctica CMMC[1]	Práctica
		responder a indicios de actividades ilegales, no autorizadas, sospechosas o inusuales.
	Auditoría y rendición de cuentas	Proporcione reducción de registros de auditoría y generación de informes para respaldar análisis e informes a pedido.

--Fin del documento--