CONTADURÍA GENERAL DE LA NACIÓN
Cuentas Claras, Estado Transparente

INFORME DE AUDITORÍA INTERNA DE GESTIÓN AL PROCESO GESTIÓN TICs

26 DE AGOSTO DEL 2024

Dirección: Calle 26 # 69 - 76 | Edificio Elemento
Torre 1 (Aire) - Piso 15
Código Postal: 111071, Bogotá, Colombia
www.contaduria.gov.co | contactenos@contaduria.gov.co
PBX: +57 (601) 492 64 00

Bogotá D.C.,

Ingeniero:
JAMIR MOSQUERA RUBIO
Coordinador GIT de Apoyo Informático
Doctor(a):
FREDDY ARMANDO CASTAÑO PINEDA
Secretario General
CARLOS ANDRÉS RODRÍGUEZ RAMÍREZ
Subcontaduría General y de Investigación
JUAN CAMILO SANTAMARÍA HERRERA
Subcontaduría de Centralización de la Información
ELIZABETH SOLER CASTILLO
Subcontaduría de Consolidación de la Información
VILMA YOLANDA NARVÁEZ NARVÁEZ
GIT de Planeación
KATHERINE DE LOS ANGELES GONZALEZ BARRERA
GIT Jurídica (E)
ÁLLISON CRISTINA MARÍN FLÓREZ
GIT Logístico de Capacitación y Prensa

Asunto: Informe de Auditoría Interna de Gestión al Proceso Gestión TICs.

Respetados doctores,

El Grupo Interno de Trabajo (GIT) de Control Interno, en ejercicio de las facultades legales otorgadas por la Ley 87 de 1993, Ley 1474 de 2011, el Decreto 1083 de 2015 y sus modificaciones; así como los lineamientos establecidos en la Guía de Auditoria para Entidades Públicas del DAFP, y las Resoluciones 364 de 2017 y 456 de 2018 emitidas por la CGN, tiene como función realizar la evaluación independiente al Sistema de Control Interno, los riesgos y los procesos, contemplando como mínimo los procedimientos, actividades y actuaciones de la administración; con el fin de determinar la efectividad del Control Interno, el cumplimiento de la gestión y los objetivos de la entidad, produciendo recomendaciones para asesorar a la alta dirección en busca del mejoramiento continuo. Es de aclarar, que las recomendaciones realizadas por el GIT no son de obligatorio cumplimiento, solo son una guía de asesoramiento; el líder del proceso debe a través de un análisis de causas establecer las acciones más apropiadas frente a las observaciones realizadas en el presente informe.

En cumplimiento al Programa General de Auditorías aprobado para la vigencia 2023 por el Comité Institucional de Coordinación de Control Interno CICCI, este GIT adelantó la evaluación al proceso "Gestión TICs ", cuyo objetivo fue: "Verificar el avance y cumplimiento de la gestión integral del proceso de Gestión TICs de la UAE Contaduría General de la Nación respecto a la eficacia, eficiencia y seguridad de su infraestructura tecnológica, sistemas de información, servicios de gestión de información y procesos institucionales, así como el cumplimiento

de estándares y regulaciones; mediante un enfoque que abarque desde la gestión del talento en tecnología hasta la administración de operaciones y desarrollo de software, con énfasis en la seguridad informática, la continuidad del negocio y la capacitación de usuarios".

A continuación, se informan las fortalezas y los hallazgos, producto del desarrollo del proceso de auditoría, las cuales son socializadas con los lideres de los procesos o unidades auditables con la finalidad de concertar el plan de mejoramiento en el formato "CYE05-FR02".

Los procedimientos de auditoría se realizaron sobre la base de pruebas selectivas; un procedimiento de esta naturaleza no puede identificar todas las desviaciones de control, sino solamente aquellas que estén presentes dentro de la muestra evaluada.

Cordialmente,

DEISY HERNÁNDEZ SOTTO
Coordinador GIT de Control Interno (E)

C.C.: Mauricio Gómez Villegas, contador general de la nación
Elaboró: Juan José Tafur Castro
Revisó: Deisy Hernández Sotto

CONTENIDO

1. RESUMEN EJECUTIVO 5
1.1 OBJETIVO GENERAL 5
1.2 OBJETIVOS ESPECÍFICOS 6
1.3 ALCANCE 7
1.4 METODOLOGÍA 7
1.5 PORCENTAJE DE CUMPLIMIENTO DE LA GESTIÓN INTEGRAL DEL PROCESO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES 11
1.6 FORTALEZAS 12
1.7 HALLAZGOS 14
1.7.1 ESTRATEGIA DE TECNOLOGÍAS DE LA INFORMACIÓN (TI) 14
1.7.2 COMPONENTES FUNDAMENTALES DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI) 25
1.7.3 ASPECTOS OPERACIONALES Y DE GESTIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN 36
1.7.4 PLANIFICACIÓN Y SEGUIMIENTO A LA GESTIÓN TIC 46
1.7.5 MEJORA CONTINUA DE LA GESTIÓN TIC 54
1.8 CONCLUSIONES 55
2. INFORME DETALLADO 57

1. RESUMEN EJECUTIVO

El Decreto 1008 de 2018 establece los lineamientos de la política de Gobierno Digital en Colombia, marcando un avance significativo en la transformación digital del Estado; cuya aplicación propende por el aprovechamiento de las tecnologías de la información y las comunicaciones (TIC) para modernizar la administración pública, mejorar la calidad de vida de los ciudadanos y promover el desarrollo económico y social del país. Entre sus objetivos, destacan la eficiencia administrativa, la transparencia, la participación ciudadana y la innovación en la prestación de servicios públicos.

En este marco, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) ha establecido el Modelo de Seguridad y Privacidad de la Información (MSPI), orientado a garantizar la confidencialidad, integridad y disponibilidad de la información en entidades públicas y privadas. Este modelo se basa en estándares internacionales como ISO/IEC 27001 y en la normativa nacional de protección de datos, brindando un enfoque integral para la gestión de la seguridad y privacidad de la información.

En cumplimiento de lo dispuesto en la Ley 87 de 1993 y el Decreto 648 de 2017, el GIT de Control Interno de la Unidad Administrativa Especial Contaduría General de la Nación llevo a cabo un proceso de auditoría para evaluar la eficacia, eficiencia y seguridad en la gestión de las TIC dentro de la entidad. Esta evaluación abarcó desde la gestión del talento en tecnología, administración de operaciones y desarrollo de software, hasta la seguridad informática y la continuidad del negocio, teniendo en cuenta las necesidades específicas de la entidad y el cumplimiento de estándares y regulaciones pertinentes.

La metodología de auditoría incluyó la planificación del alcance, la recopilación de información relevante, el análisis de riesgos, la evaluación de controles, la realización de 5 mesas de trabajo llevadas a cabo en 12 sesiones, pruebas de cumplimiento, y la identificación de acciones de mejora. Para ello, se utilizó una Matriz de Evaluación adaptada a las características de la UAE Contaduría General de la Nación, en línea con los estándares normativos y mejores prácticas internacionales.

El resultado de esta auditoría proporcionó un diagnóstico sobre el estado actual de la gestión TIC en la entidad, identificando oportunidades de mejora y recomendaciones para fortalecer la infraestructura tecnológica y los procesos institucionales, alineados con la política de Gobierno Digital.

1.1 OBJETIVO GENERAL

Verificar el avance y cumplimiento de la gestión integral del proceso de Gestión TICs de la UAE Contaduría General de la Nación respecto a la eficacia, eficiencia y seguridad de su infraestructura tecnológica, sistemas de información, servicios de gestión de información y procesos institucionales, así como el cumplimiento de estándares y regulaciones; mediante un enfoque que abarque desde la gestión del talento en tecnología hasta la administración de operaciones y desarrollo de software, con énfasis en la seguridad informática, la continuidad del negocio y la capacitación de usuarios.

1.2 OBJETIVOS ESPECÍFICOS

- Evaluar el nivel de cumplimiento de la estrategia de gestión del talento en tecnología, incluyendo la identificación de habilidades críticas, el reclutamiento y retención de personal calificado, y la implementación de programas de capacitación y desarrollo profesional en especial los relacionados con la seguridad informática y el uso de apropiación de las Tecnologías de la Información y las Comunicaciones (TIC).

- Revisar el diseño e implementación del plan estratégico de tecnología, así como la adecuación y mantenimiento de la Infraestructura Tecnológica (IT), Sistemas de Información (SI) y Servicios de Gestión de Información (SGI) para asegurar la alineación con los objetivos institucionales, las mejores prácticas del sector TIC y de Seguridad Informática.

- Verificar la efectividad de las relaciones con proveedores, evaluando la selección, contratación y supervisión de proveedores de servicios y productos tecnológicos, así como el cumplimiento de los acuerdos contractuales y la gestión de riesgos asociados.

- Analizar la gestión de proyectos tecnológicos, incluyendo la planificación, ejecución y seguimiento de proyectos, así como la gestión de riesgos, calidad y recursos involucrados en cada fase del ciclo de vida del proyecto.

- Evaluar los procesos de adquisición y mantenimiento de software de aplicación, asegurando la selección adecuada, licenciamiento, actualización, y seguridad de las aplicaciones utilizadas en la organización.

- Verificar la correcta instalación y acreditación de sistemas, asegurando la integridad y disponibilidad de estos, así como el cumplimiento de estándares de seguridad informática y regulaciones vigentes.

- Evaluar la gestión de cambios en los sistemas y procesos tecnológicos, incluyendo la planificación, autorización, implementación y seguimiento de cambios para minimizar riesgos y mantener la estabilidad del entorno tecnológico.

- Revisar la administración de servicios con terceros, asegurando la efectividad de los Acuerdos de Nivel de Servicio (ANS), la supervisión de la calidad del servicio y la gestión de incidentes y problemas.

- Analizar el desempeño, capacidad y disponibilidad de la infraestructura tecnológica, sistemas de información y servicios de gestión de información, identificando posibles cuellos de botella, puntos de fallo y oportunidades de mejora en la capacidad y rendimiento de estos.

- Evaluar la implementación de planes de continuidad del negocio (COB), incluyendo la identificación de riesgos, la elaboración de planes de contingencia y la realización de pruebas periódicas para asegurar la capacidad de recuperación frente a eventos adversos.

- Verificar las medidas de seguridad informática implementadas, incluyendo controles de acceso, monitoreo de actividad, gestión de vulnerabilidades, y respuesta ante incidentes, entre otros, para proteger la confidencialidad, integridad y disponibilidad de la información institucional.

- Revisar los programas de formación y entrenamiento de usuarios, asegurando que el personal esté adecuadamente capacitado para utilizar la infraestructura tecnológica, los sistemas de información y los servicios de gestión de información de manera segura y eficiente.

- Analizar la administración de operaciones de tecnología, incluyendo la supervisión de procesos diarios, la gestión de incidentes y problemas, y la generación de informes de rendimiento y cumplimiento para la toma de decisiones informadas.

- Revisar la gestión de desarrollo y mantenimiento de software, asegurando la aplicación de prácticas de desarrollo o compra de aplicaciones, la revisión de código o versionamiento de componentes tecnológicos, la gestión de versiones de parcheo y la implementación de actualizaciones para mantener la integridad y seguridad de los sistemas de información.

1.3 ALCANCE

El alcance de la auditoría abarca todos los aspectos relacionados con la gestión integral del área de tecnología de la información en la UAE Contaduría General de la Nación, es el de evaluar la gestión del talento en tecnología, el diseño y mantenimiento del plan estratégico de tecnología, así como las relaciones con proveedores. Analizar la gestión de proyectos tecnológicos, la adquisición y mantenimiento de software, y la instalación y acreditación de sistemas, garantizando la integridad y seguridad. Revisar la gestión de cambios y la administración de servicios con terceros. Evaluar el desempeño de la infraestructura tecnológica y la implementación de planes de continuidad del negocio. Verificar las medidas de seguridad informática y los programas de formación de usuarios. Analizar la administración de operaciones tecnológicas y el mantenimiento de software para mantener la integridad y seguridad de los sistemas de información.

1.4 METODOLOGÍA

Para efectos de determinar el nivel de avance y cumplimiento de los lineamientos y alcances establecidos en diferentes documentos normativos relevantes, tales como el Decreto 1078 de 2015; el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones; el CONPES 3854, que establece la Política Nacional de Seguridad Digital; el CONPES 3701, que define los Lineamientos de Política para Ciberseguridad y Ciberdefensa; y la Norma Técnica Colombiana NTC-ISO/IEC 27001 sobre Tecnología de la Información, Técnicas de Seguridad y Sistemas de Gestión de la Seguridad de la Información (SGSI) y sus requisitos; el GIT de Control Interno diseñó y aplicó un instrumento para determinar el nivel de avance y cumplimiento de los lineamientos emitidos por MinTIC y las especificaciones de la NTC ISO 27001, adaptado a

las características propias de la CGN.

De manera más detallada, el instrumento es un documento en Excel, el cual se denominó "Matriz de Evaluación" mediante el cual se realizó la evaluación de criterios que están relacionados con los distintos componentes del Ecosistema Digital, incluyendo Aplicaciones, Servicios, Infraestructura y Usuarios. Asimismo, abarcó los principios fundamentales de seguridad informática, como la Disponibilidad, Confidencialidad e Integridad de la información. Además, considera los componentes esenciales del Gobierno Digital, tales como el Gobierno de Tecnologías de la Información, la Infraestructura Tecnológica (IT), los Sistemas de Información (SI), los Servicios de Gestión de Información (SGI), los Servicios Tecnológicos (ST), la Estrategia de Tecnologías de la Información (TI), y la promoción del uso y apropiación de la información por parte de los usuarios.

El instrumento consta de 3 hojas. En la primera se consigna la información relacionada con la evaluación, en la segunda la calificación producto de la evaluación y en la tercera el resultado o conclusiones del ejercicio.

Con respecto a la hoja de evaluación se establecieron 6 columnas, a saber:

1. Criterio / Lineamiento
2. Evidencia
3. Criterios de Calidad
4. Observaciones Auditados
5. Evaluación
6. Observaciones GIT de Control Interno

A continuación, se describe cada una:

1) Criterio / Lineamiento. Se refiere a los estándares, directrices, normativas o criterios específicos que se utilizan como referencia para evaluar el avance y cumplimiento de la gestión integral del proceso de Gestión de Tecnologías de la Información y Comunicación (TICs). Estos criterios pueden abarcar aspectos como la seguridad de la información, la disponibilidad de los sistemas, la eficiencia operativa, la alineación con los objetivos estratégicos, el cumplimiento normativo, entre otros. Los criterios evaluados en la matriz de evaluación se agruparon en 5 componentes:

Tabla 1. Componentes de la Matriz de Evaluación

Componente	Número de Criterios
1. Estrategia de Tecnologías de la Información (TI)	18
2. Componentes Fundamentales del Modelo de Seguridad Y Privacidad de la Información (MSPI)	60
3. Aspectos Operacionales y de Gestión en Tecnologías de la Información	56
4. Planificación y Seguimiento a la Gestión TICS	27
5. Mejora Continua de la Gestión TIC	15
Total Criterios	**176**

Fuente: Elaboración propia.

2) Evidencia. Se refiere a los documentos, registros, datos o información que como mínimo debería tener la entidad para demostrar el cumplimiento del Criterio/Lineamiento.

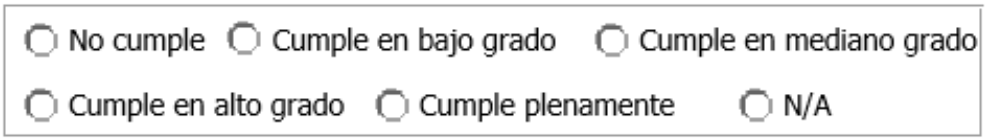
3) Criterios de Calidad. Se refiere a los estándares o parámetros establecidos que deben cumplir las evidencias, que aporta el auditado y que dan cuenta del cumplimiento del Criterio / Lineamiento. Este ítem se centra en la calidad de la evidencia que deberán entregar los auditados para respaldar el cumplimiento del criterio o lineamiento establecido en la evaluación. La calidad de la evidencia está en función de su relevancia, fiabilidad, precisión y completitud para demostrar que se están cumpliendo los criterios de calidad definidos.

4) Observaciones Auditados. Se refiere a los comentarios, explicaciones o aclaraciones proporcionadas por los auditados respecto a la evidencia entregada y el cumplimiento del criterio o lineamiento establecido en la evaluación de la gestión integral del proceso de Gestión de Tecnologías de la Información y Comunicación (TICs). Estas observaciones pueden surgir como resultado de la revisión de la evidencia presentada por el proceso y pueden abordar aspectos como la interpretación de los requisitos del criterio, los detalles específicos sobre las acciones realizadas para cumplir con el criterio, las limitaciones o restricciones encontradas durante el proceso de cumplimiento, las medidas correctivas implementadas para abordar las deficiencias identificadas, entre otros.

5) Evaluación. Se refiere al proceso mediante el cual se revisan, analizan y evalúan las evidencias entregadas por el proceso respecto al cumplimiento del criterio o lineamiento establecido en la evaluación de la gestión integral del proceso de Gestión de Tecnologías de la Información y Comunicación (TICs). Para este ítem, se examinan detalladamente la evidencia proporcionada por el proceso, se compara con los requisitos establecidos en el criterio o lineamiento y se determina el grado de cumplimiento con base a un sistema de calificación predefinida. Este sistema de calificación presenta las categorías de "no cumple", "cumple en bajo grado", "cumple en mediano grado", "cumple en alto grado" y "cumple plenamente".

Es de precisar que las tres primeras opciones (No cumple, Cumple en bajo grado y Cumplen en mediano grado), dentro del ejercicio de auditoría se configuran como hallazgos; las demás, en oportunidades de mejora.

Imagen 1. Calificaciones de evaluación



Fuente: Elaboración propia.

Cada ítem de la calificación representa un valor cuando es seleccionado, así:

Tabla 2. Valores de las calificaciones de evaluación

Calificación	Valor	Descripción
No cumple	0	El criterio evaluado no alcanza el cumplimiento esperado, ya sea por la ausencia de evidencias suficientes o porque las evidencias aportadas por el proceso auditado no demuestran la implementación o efectividad del criterio. Además, en caso de que se haya proporcionado información verbal o documental durante la auditoría, esta no resulta suficiente o relevante para satisfacer los requerimientos establecidos.
Cumple en bajo grado	1	El criterio evaluado muestra un nivel mínimo de implementación o desarrollo. Las evidencias aportadas o las actividades realizadas son insuficientes o dispersas, lo que indica una falta de consistencia o integración en el proceso. Aunque existen algunos esfuerzos aislados para cumplir con el criterio, estos no son suficientes para garantizar su efectividad o alineación con los estándares requeridos.
Cumple en mediano grado	2	El criterio evaluado evidencia un cumplimiento moderado, basado en las evidencias aportadas o en la ejecución de actividades parciales que, aunque contribuyen al cumplimiento del criterio, no están completamente integradas o desarrolladas de manera consistente. Si bien se han implementado acciones relevantes, estas carecen de cohesión o sistematicidad, lo que limita su eficacia. El cumplimiento del criterio se encuentra en un nivel intermedio, reflejando avances importantes, pero aún con temas de mejora para alcanzar el estándar óptimo.
Cumple en alto grado	3	El criterio evaluado presenta un nivel de cumplimiento significativo, evidenciado por la implementación de la mayoría de las acciones esperadas según las evidencias aportadas. Las actividades realizadas son coherentes y están alineadas con el criterio evaluado, demostrando un enfoque sistemático en la gestión. Sin embargo, aunque se ha alcanzado un alto grado de cumplimiento, todavía existen mejoras necesarias para alcanzar el estándar óptimo. La gestión es efectiva, pero requiere refinamientos adicionales para maximizar su eficacia y alinearse completamente con el criterio.
Cumple plenamente	5	El criterio evaluado alcanza el cumplimiento esperado, respaldado por las evidencias aportadas y la ejecución de las actividades planificadas. La gestión demuestra una alineación con los estándares establecidos, reflejando una implementación integral y efectiva del criterio. Las acciones realizadas cubren todas las expectativas sin desviaciones, garantizando el logro de los objetivos estratégicos y normativos.
N/A	No se tiene en cuenta en la evaluación.	

Fuente: Elaboración propia.

Es importante tener presente que las calificaciones "No cumple", "Cumple en bajo grado" y "Cumple en mediano grado", son catalogadas como Hallazgos, mientras que las calificaciones "Cumple en alto grado" y "Cumple plenamente" se catalogan como oportunidades de mejora.

La evaluación proporciona una visión del grado de cumplimiento del criterio o lineamiento, lo que permite identificar áreas de mejora, fortalezas y posibles riesgos en la gestión de TICs de la entidad.

6) Observaciones GIT de Control Interno. Se refiere a los comentarios, observaciones o recomendaciones proporcionadas por el proceso respecto a la evaluación asignada sobre el cumplimiento del criterio o lineamiento establecido en la Matriz de Evaluación. Estas observaciones se basan en el análisis y la revisión realizada de la evidencia, así como el grado de cumplimiento del criterio o lineamiento. Las observaciones pueden abordar aspectos como deficiencias identificadas en el cumplimiento, áreas de mejora, riesgos potenciales, fortalezas destacadas, recomendaciones para la implementación de mejores prácticas, entre otros.

RESULTADOS DE LA EVALUACIÓN.

Para obtener los resultados de la evaluación final, se estableció un sistema de puntuación donde a cada criterio se le puede asignar una calificación máxima de 5 puntos. Posteriormente, se suman los puntos correspondientes a cada criterio dentro de cada componente, es decir, se multiplica el total de criterios por la calificación máxima. De esta manera, se obtienen los valores ideales de la evaluación de cada componente, así.

Tabla 3. Valores ideales de los componentes de la Matriz de Evaluación

Componente		Valor Ideal Componente
18	1. Estrategia de Tecnologías de la Información (TI)	90
60	2. Componentes Fundamentales del Modelo de Seguridad Y Privacidad de la Información (MSPI)	300
56	3. Aspectos Operacionales y de Gestión en Tecnologías de la Información	280
27	4. Planificación y Seguimiento a la Gestión TICS	135
15	5. Mejora Continua de la Gestión TIC	75
176	**Valor Total Ideal de la Evaluación**	**880**

Fuente: Elaboración propia.

En el proceso de evaluación, se revisaron, analizaron y evaluaron las evidencias proporcionadas por los auditados, en relación con el cumplimiento de los criterios y lineamientos establecidos en la Matriz de Evaluación. A partir de esta revisión, se asignó un valor de evaluación a cada criterio. Luego, se sumaron los puntos correspondientes a cada criterio dentro de cada componente, obteniendo así los valores de evaluación para cada uno.

Posteriormente, se realizó una comparación porcentual entre los valores ideales y los obtenidos en la evaluación de cada criterio, lo que permitió medir el grado de cumplimiento.

1.5 PORCENTAJE DE CUMPLIMIENTO DE LA GESTIÓN INTEGRAL DEL PROCESO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Como resultado de la aplicación de la Matriz de Evaluación, se obtuvo el avance y cumplimiento en la Gestión Integral del proceso de TICs de la UAE Contaduría General de la Nación, por componente (agrupación de los lineamientos establecidos por MinTIC y la ISO 27001), observando que alcanzó un porcentaje de nivel de cumplimiento del 30% a nivel general. En la Tabla 4 se desglosa el resultado.

Tabla 4. Resultados de la Matriz de Evaluación

Componente		Valor Ideal Componente	Valor Evaluación obtenida por la CGN	% Nivel de Cumplimiento
18	1. Estrategia de Tecnologías de la Información (TI)	90	31	34
60	2. Componentes Fundamentales del Modelo de Seguridad Y Privacidad de la Información (MSPI)	300	98	33
56	3. Aspectos Operacionales y de Gestión en Tecnologías de la Información	280	90	32
27	4. Planificación y Seguimiento a la Gestión TICS	135	28	21
15	5. Mejora Continua de la Gestión TIC	75	14	19
176	**Valor Total Evaluación**	**880**	**261**	**30**

Fuente: Elaboración propia.

1.6 FORTALEZAS

En la auditoría al proceso de Gestión TICs, se identificaron fortalezas que reflejan el compromiso de la entidad con la modernización tecnológica, el cumplimiento normativo y la seguridad informática. Entre ellas:

- ✓ Se observó un firme compromiso de la alta y media gerencia con la implementación y sostenimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad. Este compromiso se evidencia en la Resolución 193 de 2019, que asigna al Comité Institucional de Gestión y Desempeño funciones para la gestión de la seguridad de la información, tales como la revisión y aprobación de los lineamientos técnicos y operativos para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), conforme al Manual y la Política de Gobierno Digital. Además, se designan roles esenciales, como el responsable de seguridad digital y el Oficial de Seguridad de la Información, en cumplimiento con la norma ISO-IEC 27001:2013.

  Igualmente se evidenció un apoyo a las iniciativas de seguridad de la información, asegurando la disponibilidad de recursos y promoviendo la formulación, actualización y divulgación de políticas de seguridad dentro de la entidad.

- ✓ Mediante Resolución No. 383 del 15 de noviembre de 2023, se designó al Oficial de Seguridad y Privacidad de la Información en la Contaduría General de la Nación (CGN) y define claramente sus responsabilidades.

- ✓ Se observó que los documentos revisados proporcionan una visión detallada y organizada de la transición de IPv4 a IPv6. Estos documentos establecen el marco para la planificación y transición a IPv6, incluyendo la revisión de configuraciones en la red de datos y servidores, y la aplicación del mecanismo de Doble Pila (Dual Stack).

  El análisis de los documentos aportados muestra que la CGN ha avanzado significativamente en la ejecución del proyecto de adopción de IPv6. La

documentación incluye un cronograma detallado de actividades, que abarca desde la planeación y diagnóstico inicial hasta la implementación y pruebas de funcionalidad. Entre los documentos destacados están el "Diagnóstico para la Adopción de IPv6", elaborado en diciembre de 2017, y el "Modelamiento de la Aplicación para la Transición de IPv4 a IPv6", que detalla el proceso de configuración de la red y servidores para soportar el nuevo protocolo.

Además, se observaron evidencias de la fase de implementación, incluyendo la habilitación de direccionamiento IPv6 en hardware y software, la configuración de servicios como DNS y DHCP, y la coordinación con proveedores de servicios de Internet para asegurar la conectividad externa. Los documentos como el "Plan de Implementación Seguridad y Redes" y el "Cronograma Detallado" reflejan un enfoque metódico en la ejecución del proyecto, incluyendo pruebas de funcionalidad para verificar la correcta implementación del protocolo.

Las evidencias documentales, como los informes de pruebas de funcionalidad y las actas de ejecución, confirman que la CGN ha realizado una transición ordenada y planificada hacia IPv6, asegurando la funcionalidad y seguridad de los sistemas de información de la entidad. Este enfoque integral y sistemático garantiza la adecuación de la infraestructura tecnológica a las necesidades actuales y futuras de la CGN.

- ✓ El proceso proporcionó documentación de la gestión de incidentes de seguridad informática, estos documentos registran de manera exhaustiva la información sobre eventos e incidentes de seguridad.

  El análisis de estos documentos demostró una gestión estructurada de los incidentes de seguridad. La información contenida en ellos refleja un registro minucioso de acciones y eventos que podrían impactar la eficacia y el desempeño de la seguridad y privacidad de la información en la entidad. La calidad en la documentación y el seguimiento de estos incidentes resalta el compromiso de la entidad con la mejora continua en la gestión de la seguridad de la información, facilitando una respuesta oportuna y una evaluación efectiva de los riesgos asociados. Esta práctica refuerza la capacidad de la entidad para mantener una postura proactiva y resiliente frente a posibles amenazas de seguridad.

- ✓ El proceso proporcionó el documento titulado "Planes de Mejoramiento_2022-2023.xls", que incluye cinco secciones detalladas: SGA, Auditoría Int Primer Ciclo, PM_Riesgos, Auditoría Int 2do Ciclo, e Icontec_2022. Este documento, denominado "PLAN DE MEJORAMIENTO SIGI", presenta información crítica sobre el procedimiento de "No Conformidades, Acción Correctiva, Preventiva y Planes de Mejoramiento".

  La revisión y análisis de la información revelan un registro detallado de las acciones emprendidas para abordar hallazgos y observaciones relacionadas con el proceso TICs, así como con la evaluación de riesgos en gestión, corrupción, proyectos y seguridad digital. Se identificó un enfoque sistemático en la documentación y seguimiento de las acciones correctivas y preventivas, evidenciando un compromiso con la mejora continua.

- ✓ El proceso proporcionó el documento titulado "PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN - PETI 2023-2026" (PETI-2023-2026V1.3.pdf). Este documento abarca diversos apartados cruciales, tales como: Glosario de Términos, Introducción, Objetivo, Alcance, Contexto Normativo, Motivadores Estratégicos de TI, Modelo Operativo, Situación Actual, Políticas y Estándares para la Gestión de la Gobernabilidad de TI, Situación Objetivo, Identificación de Hallazgos y Brechas, Portafolio de Iniciativas, Proyectos y Mapa de Ruta, Plan de Comunicaciones, y Estrategia de Actualización del PETI.

  En particular, el numeral 11.1 CONFORMACIÓN DE INICIATIVAS O PROYECTOS del documento detalla los siguientes proyectos clave:

  PRY01: Fortalecimiento de los servicios de TI.
  PRY02: Fortalecimiento de las capacidades en Gestión de Gobierno de TI.
  PRY03: Mejora de las capacidades de Gestión de TI.
  PRY04: Fortalecimiento del aseguramiento de la seguridad y privacidad de la información.
  PRY05: Soporte y mejora de la plataforma de administración de datos.
  PRY06: Fortalecimiento de los sistemas de información de la CGN.
  PRY07: Fortalecimiento de la arquitectura de información.

  La revisión y análisis de la información proporcionada evidenció un enfoque integral y estratégico para la mejora de los procesos de TI. Los proyectos e iniciativas delineados en el PETI están orientados a apoyar el cumplimiento de las metas institucionales y mejorar los indicadores de desempeño relacionados con la gestión del Modelo de Seguridad y Privacidad de la Información (MSPI). Este enfoque proactivo y documentado en el PETI refuerza el compromiso de la entidad con la optimización de sus recursos tecnológicos y el fortalecimiento de la seguridad de la información.

- ✓ Se destaca el apoyo del coordinador del GIT y su equipo, quienes mostraron la disposición para atender los requerimientos y brindar la información necesaria, permitiendo así un proceso de auditoría adecuado y efectivo.

1.7 HALLAZGOS

1.7.1 ESTRATEGIA DE TECNOLOGÍAS DE LA INFORMACIÓN (TI)

Los resultados de la evaluación realizada a los criterios del componente "1. ESTRATEGIA DE TECNOLOGÍAS DE LA INFORMACIÓN (TI)", presentan un nivel de cumplimiento del 34%, lo que denota deficiencias en los aspectos evaluados, así:

HALLAZGO 1. El Plan Estratégico de Tecnologías de la Información PETI no involucra la totalidad de aspectos definidos por el MinTIC para este.

Revisado el documento del Plan Estratégico de Tecnologías de la Información (PETI) frente a los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones

(MinTIC), se observó deficiencia en los siguientes aspectos:

a. La introducción debe contener una descripción del ejercicio de planeación estratégica realizado por la entidad.
b. El alcance del PETI debe indicar lo que espera lograr la entidad durante la vigencia de este (4 años), y dar cubrimiento a todos los dominios del Marco de Referencia de Arquitectura Empresarial (AE).
c. La adaptación de los lineamiento y conceptos emitidos por MinTIC (por ejemplo 6.1 Alineación estratégica, 6.2 Política de Gobierno Digital, 6.3 Tendencias tecnológicas y 10. Dominios, entre otras), a las características de la entidad.
d. Que el resultado del ejercicio de AE al plasmarlo en el PETI se realice de forma integrada y holística, abarcando los temas de estrategia, procesos institucionales, información, aplicaciones y tecnologías, y no de manera atomizada mediante el uso y evaluación de lineamientos aislados, así estén agrupados por categoría.

El PETI se encuentra en un nivel intermedio de desarrollo, con áreas que requieren mejora para cumplir plenamente con el estándar establecido por MinTIC.

RECOMENDACIÓN

Es pertinente que se realice una actualización del PETI teniendo en cuenta un ejercicio de planeación estratégica de TI, el cual debe abordar las necesidades específicas de la entidad en términos de objetivos institucionales, procesos, infraestructura tecnológica, y servicios de gestión de información, conforme a la guía G.ES.06 del MinTIC. Así mismo, integrar y contextualizar los conceptos de MinTIC, reflejando la misión y visión institucionales.

Finalmente, se recomienda tener en cuenta aplicar las buenas prácticas del PROYECT MANAGEMET INSTITUTE (PMI) y el lineamiento LI.ES.09 de MinTIC para realizar un seguimiento y control periódico del presupuesto y plan de compras asociados a los proyectos estratégicos del PETI, asegurando que estos controles estén documentados y disponibles para revisión, ajustes y seguimiento.

HALLAZGO 2. Debilidades en el diseño del modelo de Arquitectura Empresarial (AE).

Tras la revisión del diseño del modelo de Arquitectura Empresarial (AE), con base en los lineamientos establecidos por el MinTIC, se observó avances significativos, lo que conllevó a determinar qué la AE se encuentra en un estado intermedio de desarrollo, pero aún con áreas que requieren mejoras para alcanzar el estándar. Los aspectos más relevantes para mejorar son:

- ✓ Detallar, en la sección introductoria del documento, cómo se llevó a cabo el proceso de Arquitectura Empresarial y su contribución a la estrategia de TI, acorde con elementos clave establecidos por las guías del MinTIC.

- ✓ Incorporar en los apartados de *Introducción, Alcance y Objetivo* los conceptos

fundamentales del Marco de Referencia de Arquitectura Empresarial, como lo exige el MinTIC. Esta adaptación es esencial para asegurar que el proceso de AE esté alineado con las directrices institucionales y sectoriales.

- ✓ Adaptar Las secciones dedicadas a la estrategia de adopción y otros modelos conceptuales presentan una reproducción de los lineamientos del MinTIC, a las particularidades de la entidad.

RECOMENDACIÓN

Fortalecer el documento de Arquitectura Empresarial (AE) de la entidad, teniendo en cuenta la realización de un ajuste integral, de los elementos clave definidos por MinTIC, adaptados a las particularidades de la entidad.

HALLAZGO 3. Debilidades en la implementación de las Políticas y estándares para la gestión y gobernabilidad de Tecnologías de la Información (TI).

Tras la revisión y análisis de la implementación de las Políticas y Estándares para la Gestión y Gobernabilidad de Tecnologías de la Información (TI), se observó que, si bien se han adoptado acciones relevantes en este ámbito, estas no están completamente desarrolladas ni integradas. Las evidencias presentadas y las actividades ejecutadas reflejaron avances parciales, por lo que es pertinente fortalecer la cohesión y sistematicidad en la implementación.

De otra parte, en la implementación de las Políticas y Estándares para la Gestión y Gobernabilidad de Tecnologías de la Información (TI), se observaron algunos aspectos que requieren atención, los cuales se enuncian a continuación:

- ✓ Documentar las políticas operativas y las políticas de seguridad informática. Actualmente, estas están incluidas de manera general en el Manual de Seguridad de la Información y Seguridad Digital. Es necesario desarrollar documentos que definan los objetivos, alcances y la alineación de cada política con la estrategia y objetivos de la entidad.

- ✓ Implementar la política general de seguridad de la información que establezca formalmente los principios clave, incluyendo la asignación de responsabilidades, el concepto de seguridad de la información, y los procesos para gestionar desviaciones o excepciones.

- ✓ Designar formalmente a los responsables de desarrollar, actualizar y realizar revisiones periódicas de las Políticas y Estándares para la Gestión y Gobernabilidad de TI.

- ✓ Establecer un sistema formal para el registro de cambios en las Políticas y Estándares para la Gestión y Gobernabilidad de TI. Contar con un registro documentado de actualizaciones es fundamental para asegurar la trazabilidad de las modificaciones y garantizar que las políticas se mantengan actualizadas y alineadas con las necesidades

institucionales.

RECOMENDACIÓN

Acorde a lo establecido en el MSPI es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar las políticas operativas y de seguridad informática, asegurando que cada una contenga todos los componentes necesarios para su implementación. Esto no solo facilita la comprensión y aplicación de estas, sino que también garantiza que todos los aspectos críticos de la seguridad informática y operativa sean abordados y conforme a las mejores prácticas establecidas, de tal manera que, para cada una de ellas se desarrollen los conceptos de: claridad y especificidad, focalización en temas específicos, facilidad de actualización, responsabilidad y cumplimiento, facilidad de evaluación y el seguimiento del cumplimiento, mitigación de riesgos y adaptabilidad a cambios normativos, entre otros, según lo establecido en la normatividad vigente.

HALLAZGO 4. Falta documentar y fortalecer las acciones relacionadas con el del Modelo de Gobierno de Tecnologías de la Información (TI).

Tras la revisión y análisis del Modelo de Gobierno de Tecnologías de la Información (TI), se identificó que la entidad carece de un documento maestro que consolide dicho modelo. Sin embargo, las evidencias reflejan un cumplimiento moderado de los lineamientos establecidos por MinTIC con relación a este.

Los principales puntos de mejora identificados son los siguientes:

- ✓ Es necesario asegurar que la gestión de TI esté alineada con los objetivos institucionales y estratégicos de la entidad, integrando la tecnología con el cumplimiento de la misión organizacional y del proceso de Arquitectura Empresarial (AE).

- ✓ Definir los roles y responsabilidades en la gestión de TI.

- ✓ Fortalecer la matriz de riesgo relacionados con seguridad informática, continuidad del negocio y protección de datos.

- ✓ Implementar un sistema de seguimiento y control continuo que permita evaluar el desempeño de los servicios de TI mediante indicadores que midan eficiencia, eficacia y efectividad.

- ✓ Promover de manera continua el uso de buenas prácticas para la gestión de servicios de TI, alineadas con estándares como ITIL, que mejoren la calidad, disponibilidad y seguridad de los servicios tecnológicos.

- ✓ Fortalecer la promoción de la innovación y la adopción de nuevas tecnologías que aporten valor a la entidad, así como fomentar la mejora continua de los procesos y servicios de TI para asegurar la sostenibilidad tecnológica y competitividad a largo plazo.

RECOMENDACIÓN

Es procedente que la entidad cuente con un documento maestro del Modelo de Gobierno de Tecnologías de la Información (TI), aprobado por la instancia de decisión correspondiente. Este documento debe detallar procesos de gobernanza de TI, roles y responsabilidades, gestión de riesgos y estructura organizacional, asegurando una gobernanza efectiva y alineada con los objetivos estratégicos de la entidad.

HALLAZGO 5. Debilidades en la caracterización del proceso de gestión de TI.

La revisión y análisis de la caracterización del Proceso de Gestión TICs en el Sistema Integrado de Gestión Institucional de la entidad, reveló la necesidad de incorporar los elementos clave del gobierno de TI basados en las cinco dimensiones fundamentales de las Tecnologías de la Información y las Comunicaciones (TIC):

- ✓ Gobierno TIC
- ✓ Sistemas de Información
- ✓ Infraestructura Tecnológica
- ✓ Soporte y Apoyo
- ✓ Seguimiento y Control

Las principales oportunidades de mejora identificadas incluyen:

- ✓ Se requiere integrar de manera estructurada las cinco dimensiones fundamentales de las TIC, garantizando una visión holística del proceso que permita su alineación con los objetivos estratégicos de la entidad.

- ✓ Es necesario ajustar la caracterización a los lineamientos establecidos por el MinTIC, en particular el LI.GO.04, asegurando que el proceso de Gestión TIC refleje una gobernanza adecuada y conforme a las mejores prácticas.

- ✓ Se observan actividades dispersas y no articuladas dentro del proceso de caracterización, lo que dificulta su eficacia y coherencia. Es fundamental fortalecer la sistematización de los procesos y asegurar su integración.

RECOMENDACIÓN

Para cumplir con los lineamientos establecidos en el lineamiento LI.GO.04 del Macro-proceso de Gestión de TI del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y las mejores prácticas recomendadas por la Biblioteca de Infraestructura de Tecnologías de la Información (ITIL), es pertinente integrar en la caracterización del proceso de Gestión TICs, los lineamientos de los subprocesos o elementos de TI. Es importante abarcar las cinco dimensiones fundamentales de las Tecnologías de la Información y las Comunicaciones (TIC): Gobierno TIC, Sistemas de Información, Infraestructura Tecnológica, Soporte y Apoyo, y Seguimiento y Control.

HALLAZGO 6. Debilidades en la Capacidades y recursos de TI.

La revisión y análisis del Plan de Capacidad de los Servicios de TI reveló que, si bien existe un plan, este no contempla un enfoque integral que abarque todas las capacidades de TI requeridas para la prestación efectiva de los servicios. Además, resulta pertinente que el plan incluya proyecciones de capacidad a futuro que garanticen el adecuado funcionamiento de la entidad en el marco de una estrategia de TI establecida.

El análisis evidenció que el plan no cubre todos los aspectos y requerimientos del Marco de Referencia de la Arquitectura Empresarial (MRAE) definido por el MinTIC, lo cual genera las siguientes brechas:

- ✓ No se incluyen directrices sobre la gestión de la información, los sistemas de información, ni sobre el uso y la apropiación de los servicios TIC por parte de los usuarios.

- ✓ El plan no contempla una proyección de las capacidades de TI necesarias para garantizar la continuidad y crecimiento de la entidad, de acuerdo con una estrategia de TI alineada con los objetivos institucionales.

- ✓ La formulación y revisión del plan no evidencia una participación transversal de la alta y media gerencia, ni de los líderes de procesos o responsables de los activos de información en la elaboración. Esta participación contribuye a ampliar la visión estratégica y operativa del mismo.

El cumplimiento observado es moderado, sustentado en las evidencias aportadas y en la ejecución de actividades parciales que, aunque han contribuido a la implementación de algunos aspectos del plan, no están completamente integradas ni desarrolladas de manera consistente y cohesionada. Aunque se han realizado avances significativos, estos no logran un impacto estructural que garantice la adecuada gestión de las capacidades de TI.

El Plan de Capacidad de los Servicios de TI se encuentra en un nivel intermedio, reflejando avances importantes, pero con áreas clave de mejora que deben ser abordadas para alcanzar el estándar deseado.

RECOMENDACIÓN

Es pertinente realizar un ajuste integral al Plan de Capacidad de Tecnologías de Información (TI) para alinearlo con el lineamiento LI-GO.05 - Capacidades y recursos de TI del "Modelo de Gestión y Gobierno TI (MGGTI)" del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Este ajuste debe garantizar que el plan incluya la participación de todas las partes interesadas relevantes, como la alta y media gerencia, líderes de procesos y dueños de activos de información, para asegurar que se aborden de manera integral las necesidades institucionales y se logre una alineación efectiva con los objetivos estratégicos de la entidad.

El plan debe considerar la capacidad y gestión de la información, los sistemas de información, y el uso y apropiación de los servicios TIC, integrando proyecciones de capacidad de TI necesarias para el funcionamiento futuro de la entidad. Estas proyecciones deben basarse en una estrategia de TI definida y contextualizada, que refleje la evolución tecnológica y las necesidades específicas de la entidad. Además, es esencial que el plan contemple un enfoque participativo y transversal que permita la adaptación continua a los cambios institucionales y tecnológicos, asegurando que el crecimiento y la capacidad de TI estén en consonancia con la misión y visión de la entidad.

HALLAZGO 7. Debilidades en el Liderazgo de proyectos de TI y Gestión de proyectos de TI.

La revisión y análisis de las actividades realizadas por el GIT de Apoyo Informático en la implementación de proyectos de TI reveló áreas de mejora clave que requieren atención para optimizar la gestión y liderazgo de proyectos tecnológicos en la entidad.

Deficiencias Detectadas:

- ✓ Falta de metodologías y guías estructuradas para la gestión de proyectos de TI, lo cual genera inconsistencias en la planificación y ejecución.

- ✓ No se evidenció solicitudes de incorporación en el PIC, de formación en gestión de proyectos y tecnologías de la información, lo que limita el desarrollo de competencias clave para la gestión efectiva". El desarrollo de estas habilidades permitirá corregir deficiencias en el monitoreo, evaluación, mecanismos de comunicación, mitigación de riesgos asociados a los proyectos y evaluación formal del retorno de la inversión (ROI)

- ✓ Deficiencias en el plan detallado de cada proyecto, lo que impide un seguimiento adecuado de los hitos, tiempos y recursos asignados.

El lineamiento LI.GO.09 - "Liderazgo de proyectos de TI" indica que se debe ir más allá de seguir las directrices establecidas por Colombia Compra Eficiente, implicando una gestión estructurada, participativa y alineada con estándares de buenas prácticas.

Se observó un nivel mínimo de implementación o desarrollo en el liderazgo y gestión de proyectos de TI. Aunque se han hecho esfuerzos aislados para cumplir con los requerimientos, estos no son suficientes para garantizar la efectividad ni la alineación con los estándares necesarios para una gestión de proyectos de TI exitosa.

RECOMENDACIÓN

Es pertinente desarrollar e implementar un marco integral para la gestión de proyectos de TI que incluya metodologías estándar como PMP, ITIL y PRINCE2, junto con guías, manuales y un programa de capacitación continua para los líderes de proyectos. Este marco debe establecer un plan de proyectos detallado con mecanismos de monitoreo y evaluación del progreso, así como una metodología para la gestión de riesgos.

Además, se debe implementar un Plan de Calidad que incluya actas de comités (o equipos de trabajo) de seguimiento y/o gerenciales, formalizar todos los documentos con información crítica, y reforzar el proceso de aprobación para asegurar validez y respaldo formal. Finalmente, integrar la seguridad de la información en todas las fases del proyecto para proteger eficazmente la información institucional y mitigar vulnerabilidades.

HALLAZGO 8. Debilidades en el Análisis de riesgos de TI.

El Grupo de Apoyo Informático (GIT) desarrolló acciones para establecer un Plan de Tratamiento de Riesgos de Seguridad de la Información, el cual incluye la identificación de cuatro (4) activos y un total de 24 riesgos. Sin embargo, se observó que en esta tipificación no se identifican riesgos asociados a componentes críticos de la infraestructura tecnológica (IT) de la entidad, tales como:

- ✓ Servidores físicos y virtuales
- ✓ Servidores de aplicaciones y bases de datos
- ✓ Routers, switches, firewalls, access points
- ✓ Controladores de red, VPN (Red Privada Virtual)
- ✓ Servicios de DNS y DHCP
- ✓ Sistemas de almacenamiento en red (NAS) y redes de almacenamiento (SAN)
- ✓ Unidades de almacenamiento locales
- ✓ Sistemas de suministro de energía ininterrumpida (UPS)
- ✓ Generadores y sistemas de climatización y refrigeración del centro de datos

De otra parte, la revisión y análisis del plan reveló que no se han identificado riesgos específicos relacionados con la infraestructura tecnológica crítica, ni se han considerado amenazas claves como:

- ✓ Ciberataques e intrusiones
- ✓ Fallas en aplicaciones o hardware
- ✓ Interrupciones en la operatividad de routers, firewalls y otros equipos esenciales
- ✓ Riesgos asociados a sistemas de climatización y refrigeración del centro de datos, que son vitales para la continuidad del servicio.

Además, no se ha desarrollado un plan de tratamiento de riesgos que aborde de manera integral estos aspectos, lo que pone en riesgo la seguridad y la continuidad operativa de la infraestructura tecnológica de la entidad.

La identificación, valoración y control de estos riesgos en la gestión de la seguridad de TI redunda en la capacidad de la entidad para responder adecuadamente a incidentes que afecten sus componentes tecnológicos críticos, mitigando riesgos que pueden traducirse en fallos que impactan la continuidad de los servicios, vulnerabilidad ante ciberamenazas, y una respuesta insuficiente frente a interrupciones o fallos de infraestructura.

Si bien se han realizado esfuerzos relevantes en la identificación de algunos riesgos, estos no cubren de manera adecuada la totalidad de los componentes tecnológicos críticos, lo que limita la efectividad del plan y lo deja incompleto para abordar la gestión integral de

la seguridad de TI.

RECOMENDACIÓN

Llevar a cabo un análisis exhaustivo y gestionar los riesgos asociados a la infraestructura tecnológica de la entidad. Este análisis debe centrarse en identificar riesgos que puedan comprometer la seguridad de la información o afectar la continuidad de los servicios de TI. Para ello, es importante implementar las siguientes acciones:

- ✓ Desarrollar un plan integral de pruebas de seguridad de la información, que incluya evaluaciones de vulnerabilidades para garantizar una protección adecuada de los sistemas tecnológicos.

- ✓ Establecer una matriz de riesgos de seguridad de la información que permita identificar, clasificar y priorizar los riesgos en función de su impacto y probabilidad, facilitando así una gestión más efectiva.

- ✓ Generar informes sobre el análisis de vulnerabilidades, los cuales deben ser revisados y actualizados regularmente para monitorear y abordar las debilidades detectadas en la infraestructura tecnológica institucional.

HALLAZGO 9. Debilidades en la implementación de estrategias de capacitación y adherencia a las Políticas de Seguridad Informática.

La revisión y análisis realizados sobre la implementación de estrategias de capacitación y adherencia a las políticas de seguridad informática reveló elementos que requieren atención:

- ✓ Implementación de una estrategia integral de capacitación y adherencia que garantice que todos los servidores públicos, colaboradores y proveedores comprendan y adopten de manera efectiva las políticas de seguridad informática antes de recibir acceso a los sistemas e información de la entidad.

- ✓ Programas de capacitación específicos en seguridad operativa y privacidad de la información, dirigidos a todos los actores involucrados.

- ✓ Programas de concientización y formación continua en temas críticos como la seguridad operativa, manejo de información confidencial, prevención de ciberataques y protección de la privacidad.

- ✓ Evidenciar que los servidores públicos, colaboradores y proveedores comprenden a cabalidad las políticas, procedimientos, protocolos y responsabilidades en materia de seguridad de la información.

La ausencia de estrategias de capacitación integral y la falta de programas específicos de formación en seguridad informática exponen a la entidad a riesgos significativos, tales

como:

- ✓ Vulneraciones a la seguridad de la información debido al desconocimiento de las políticas y mejores prácticas por parte de los usuarios.

- ✓ Exposición a ciberataques y brechas de seguridad que podrían comprometer información sensible.

- ✓ Falta de adherencia a los estándares internacionales de seguridad y lineamientos normativos, lo que podría afectar el cumplimiento de las obligaciones legales de la entidad.

Se observa un nivel mínimo de implementación en las estrategias de capacitación y adherencia a las políticas de seguridad informática. A pesar de algunos esfuerzos aislados, como la creación de cursos básicos en el Aula Virtual, las actividades y evidencias aportadas deben articularse en la implementación de una estrategia que garantice la formación adecuada y el cumplimiento de las políticas de seguridad informática.

RECOMENDACIÓN

Es pertinente desarrollar e implementar estrategias integrales para asegurar que todos los servidores públicos, colaboradores y proveedores comprendan y se adhieran a las políticas de seguridad informática antes de otorgarles acceso a información o sistemas. Estas estrategias deben incluir formación en seguridad operativa y privacidad de la información, asegurando que todos los involucrados conozcan en detalle las políticas, procedimientos, protocolos y responsabilidades relacionadas con la seguridad de la información de la entidad.

Para mitigar el riesgo de vulneraciones en la seguridad de la información, se debe establecer programas de capacitación y concientización específicos en seguridad informática, dirigidos a todos los servidores, colaboradores y proveedores. Estos programas deben abordar en profundidad temas de seguridad operativa, privacidad y protección de la información.

HALLAZGO 10. Debilidades en la Responsabilidad y Gestión de Componentes de Información.

Como resultado de la revisión documental y el análisis efectuado a la Gestión de Componentes de Información, se identificó la ausencia de documentación clave para la gestión de componentes de información y el gobierno de la información en la entidad. Los siguientes aspectos requieren atención:

- ✓ Implementar una política formal de Tecnologías de la Información (TI) que incorpore directrices para la gestión integral del ciclo de vida de los componentes de información. Esto incluye la creación, almacenamiento, uso, archivo y disposición final de los datos, lo cual es fundamental para una adecuada administración de los activos de información de la entidad.

- ✓ Documentar el modelo o esquema de gobierno de la información, el cual debe seguir los lineamientos establecidos en la Guía G.INF.06 - Guía Técnica del Gobierno del Dato. Este documento es esencial para asegurar una gobernanza efectiva y debe incluir aspectos como:

  - Gobernanza de la información (con la asignación de custodios y responsables de los datos).
  - Calidad de los datos (mecanismos para garantizar la precisión, integridad y consistencia de la información).
  - Migración de datos (proceso de traslado seguro y eficiente de datos entre sistemas).
  - Ciclo de vida de los datos (gestión de datos desde su creación hasta su eliminación).
  - Datos maestros (información crítica para los procesos de la entidad).

La existencia de un marco formal y documentado para la gestión del ciclo de vida de los componentes de información y para el gobierno de los datos contribuye a mitigar riesgos importantes para la entidad. La materialización de estos riesgos puede conllevar a:

- ✓ Inconsistencias en la gestión de datos, lo que puede generar errores en la información utilizada para la toma de decisiones.
- ✓ Riesgos de cumplimiento normativo, dado que la entidad pude no estar alineada con los lineamientos relacionados con la gestión de datos y la protección de la información.
- ✓ Dificultades en la gobernanza de la información, al no haber claridad en las responsabilidades y roles asignados para la gestión de los datos.
- ✓ Falta de control sobre la calidad y seguridad de los datos, lo que incrementa las probabilidades de pérdida de información o acceso no autorizado.

A pesar de algunos esfuerzos puntuales para abordar este tema, estos no son suficientes para garantizar una gestión efectiva y alineada con los estándares requeridos.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar una política integral de Tecnologías de la Información (TI) que establezca directrices para la gestión del ciclo de vida de los componentes de información. Esta política debe alinearse con las mejores prácticas e incluir procedimientos detallados para la adquisición, uso, mantenimiento y disposición final de los activos de información. Adicionalmente, se debe elaborar un documento que defina el modelo o esquema de gobierno de la información, conforme a los requisitos y lineamientos especificados en la "Guía G.INF.06 - Guía Técnica del Gobierno del Dato".

1.7.2 COMPONENTES FUNDAMENTALES DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

Los resultados de la evaluación realizada a los criterios del componente "2. COMPONENTES FUNDAMENTALES DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)", presentan un nivel de cumplimiento del 33%, lo que denota deficiencias en los aspectos evaluados, los cuales se exponen a continuación

HALLAZGO 11. Inexistencia de la Política de Seguridad de la Información (Marco de Referencia).

Como resultado de la revisión documental y el análisis efectuado a la Política de Seguridad de la Información, se identificó la ausencia de un documento formal que establezca la Política de Seguridad y Privacidad de la Información en la entidad. Este documento es de carácter fundamental, ya que debe definir las acciones y decisiones clave para gestionar de manera eficaz la seguridad de la información, protegiendo los activos tecnológicos y garantizando la confidencialidad, integridad y disponibilidad de la información.

Deficiencias Identificadas:

- ✓ No se ha formalizado un marco de referencia que contemple los aspectos esenciales de la seguridad de la información. En particular, se identifican las siguientes deficiencias:

- ✓ Política de Seguridad de la Información: No existe un documento formal que establezca los lineamientos generales para proteger los activos de información de la entidad.

- ✓ Falta de definición de políticas específicas, que son cruciales para garantizar una gestión integral de la seguridad de la información. Estas incluyen, entre otras:

  Política de Organización de la Seguridad de la Información: Definición clara de roles y responsabilidades.

  Política de Gestión de Activos: Gestión del ciclo de vida de los activos de información.

  Política de Control de Acceso: Garantizar que solo el personal autorizado tenga acceso a la información sensible.

  Política de No Repudio: Establecer medidas para garantizar la autenticidad de la información y las transacciones.

  Política de Privacidad y Confidencialidad: Protección de los datos sensibles.

  Política de Disponibilidad del Servicio e Información: Asegurar la disponibilidad

continua de los servicios y sistemas críticos.

Política de Registro y Auditoría: Implementación de mecanismos para monitorear y auditar el uso de los sistemas de información.

Política de Gestión de Incidentes de Seguridad: Procedimientos para responder y mitigar incidentes de seguridad.

Política de Capacitación y Sensibilización en Seguridad de la Información: Capacitación continua del personal sobre buenas prácticas y cumplimiento de las normativas de seguridad.

Contar con una Política de Seguridad y Privacidad de la Información formalizada contribuye a mitigar riesgos para la entidad, tales como:

- ✓ Inseguridad en la protección de los activos tecnológicos: Sin una política, los mecanismos de protección pueden ser inconsistentes o inadecuados, exponiendo a la entidad a vulnerabilidades y ciberataques.

- ✓ Falta de capacidad para responder adecuadamente a incidentes de seguridad: Sin lineamientos formales, la respuesta ante incidentes de seguridad puede ser reactiva, poco eficiente y no alineada con los estándares regulatorios.

- ✓ Riesgo de incumplimiento normativo: La entidad podría no estar cumpliendo con los requisitos legales y regulatorios establecidos en materia de seguridad de la información.

- ✓ Pérdida de confianza: La falta de políticas estructuradas puede comprometer la confianza de clientes, socios, contratistas y proveedores en la capacidad de la entidad para proteger sus datos y garantizar la continuidad de sus servicios.

Las evidencias aportadas y las actividades realizadas son insuficientes, dispersas y carecen de cohesión, lo que refleja una falta de integración en la gestión de la seguridad de la información. Aunque se han observado algunos esfuerzos puntuales para cumplir con ciertos criterios, estos no son suficientes para garantizar la efectividad y alineación con los estándares requeridos en materia de seguridad de la información.

RECOMENDACIÓN

Es pertinente implementar la Política de Seguridad y Privacidad de la Información que sirva como marco de referencia para el desarrollo de la seguridad informática en la entidad y con los siguientes ítems:

- ✓ Desarrollo, revisión, contextualización, aprobación, implementación y apropiación de mínimo las siguientes políticas:

  - Política de la Organización de la Seguridad de la Información.

- Política de Gestión de Activos.
- Política de Control De Acceso.
- Política de No Repudio.
- Política de seguridad para la Privacidad y Confidencialidad.
- Política de Integridad de la Información.
- Política de Disponibilidad del Servicio e Información.
- Política de Registro y Auditoría.
- Política de Gestión de Incidentes de Seguridad de la Información.
- Política de Capacitación y Sensibilización en Seguridad de La Información.

✓ Definición de los controles que disminuirán el impacto generado en los activos, por los riesgos identificados para mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de estos, acorde con las necesidades de los diferentes grupos de interés identificados.

✓ Definición de las acciones o toma de decisiones para las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes.
- Garantizar la continuidad del negocio frente a incidentes.
- Implementar y gestionar el Sistema de Gestión de Seguridad de la Información, bajo lineamientos claros, acorde a las necesidades del negocio y a los requerimientos regulatorios.

✓ Definición de los siguientes principios:

- Responsabilidades frente a la seguridad de la información definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
- Protección de la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- Protección de la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta, junto con la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- Protección de la información frente a las amenazas originadas por parte del personal.
- Protección de las instalaciones de procesamiento y la infraestructura tecnológica que

soporta los procesos críticos.
- Control de la operación de los procesos de negocio, garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Implementación del control de acceso a la información, sistemas y recursos de red.
- Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- Garantizar que, a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información, una mejora efectiva de su modelo de seguridad.
- Garantizar la disponibilidad de los procesos de negocio y la continuidad de operación basada en el impacto que pueden generar los eventos.
- Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

✓ Establecer las fases de implementación de las políticas de seguridad de información:

1. Desarrollo de las políticas.
2. Cumplimiento.
3. Comunicación.
4. Monitoreo.
5. Mantenimiento."

HALLAZGO 12. Falta de Implementación de los Procedimientos Seguridad de la Información

La revisión documental y análisis realizados sobre la implementación de los Procedimientos de Seguridad de la Información revelaron que varios procedimientos fundamentales no han sido formalmente implementados, aprobados por la alta dirección ni socializados al interior de la entidad. Entre los procedimientos pendientes se destacan:

- Capacitación y sensibilización del personal.
- Ingreso y desvinculación del personal.
- Identificación y clasificación de activos.
- Ingreso seguro a los sistemas de información.
- Gestión de usuarios y contraseñas.
- Controles criptográficos.
- Gestión de llaves criptográficas.
- Control de acceso físico.
- Protección de activos.
- Retiro de activos.
- Mantenimiento de equipos.
- Gestión de cambios.
- Gestión de capacidad.
- Separación de ambientes.
- Protección contra códigos maliciosos.
- Aseguramiento de servicios en la red.
- Transferencia de información.

- Seguridad en acuerdos con proveedores.
- Adquisición, desarrollo y mantenimiento de software.
- Control de software.
- Gestión de incidentes de seguridad de la información.
- Gestión de la continuidad de negocio.

La ausencia de estos procedimientos afecta la seguridad de la información de la entidad y compromete la integridad, confidencialidad y disponibilidad de sus activos tecnológicos. Además, se incrementa el riesgo de:

- ✓ Accesos no autorizados a sistemas y datos sensibles.
- ✓ Fugas de información debido a la falta de controles sobre el ingreso y retiro de personal.
- ✓ Vulnerabilidades criptográficas por falta de gestión adecuada de llaves y controles criptográficos.
- ✓ Exposición a amenazas informáticas, como malware y ataques cibernéticos, por la ausencia de procedimientos preventivos.
- ✓ Incapacidad para gestionar incidentes de seguridad de manera efectiva y rápida.
- ✓ Pérdida de confianza de clientes, proveedores y entidades reguladoras debido a una gestión inconsistente de la seguridad de la información.

Aunque se han realizado esfuerzos en algunos frentes, estos son insuficientes para garantizar la efectividad y alineación con los estándares normativos y buenas prácticas en materia de seguridad de la información.

RECOMENDACIÓN

Desarrollar, revisar, contextualizar, aprobar, implementar y apropiar, como mínimo, los siguientes procedimientos:

- ✓ Procedimiento para Capacitación y Sensibilización del Persona.
- ✓ Procedimiento de Ingreso y Desvinculación del Personal.
- ✓ Procedimiento de Identificación y Clasificación de Activos.
- ✓ Procedimiento para Ingreso Seguro a los Sistemas de Información.
- ✓ Procedimiento de Gestión de Usuarios y Contraseñas.
- ✓ Procedimiento de Controles Criptográficos.
- ✓ Procedimiento de Gestión de Llaves Criptográficas.
- ✓ Procedimiento de Control de Acceso Físico.
- ✓ Procedimiento de Protección de Activos.
- ✓ Procedimiento de Retiro de Activos.
- ✓ Procedimiento de Mantenimiento de Equipos.
- ✓ Procedimiento de Gestión de Cambios.

- ✓ Procedimiento de Gestión de Capacidad.
- ✓ Procedimiento de Separación de Ambientes.
- ✓ Procedimiento de Protección Contra Códigos Maliciosos.
- ✓ Procedimiento de Aseguramiento de Servicios en la Red.
- ✓ Procedimiento de Transferencia de Información.
- ✓ Procedimiento para el Tratamiento de la Seguridad en los Acuerdos con los Proveedores.
- ✓ Procedimiento Adquisición, Desarrollo y Mantenimiento de Software.
- ✓ Procedimiento de Control Software.
- ✓ Procedimiento de Gestión de Incidentes de Seguridad de la Información.
- ✓ Procedimiento de Gestión de la Continuidad de Negocio.

La implementación de los Procedimientos Seguridad de la Información, deben atender los requisitos establecidos en la NTC ISO 27001 y las Guías MSPI de MinTIC.

HALLAZGO 13. Debilidades en la implementación de las funciones de seguridad de la información.

La revisión documental y análisis realizados sobre la implementación de las funciones de seguridad de la información en la entidad reveló que estas no se han desarrollado conforme a los lineamientos establecidos en la NTC ISO 27001 ni se han adoptado las directrices definidas en la Guía de Roles y Responsabilidades del Modelo de Seguridad y Privacidad de la Información (MSPI) emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Asimismo, se identificó la ausencia de un equipo de gestión específico encargado de la implementación del modelo MSPI, lo que genera una brecha significativa en la alineación con los principios de la norma ISO 27001 y el cumplimiento de las responsabilidades clave contempladas en la guía del MSPI. Esta situación impacta la capacidad de la entidad para asegurar una gestión integral y efectiva de la seguridad y privacidad de la información.

La falta de un equipo especializado y la no adopción de las directrices del MSPI pueden comprometer varios aspectos críticos de la seguridad de la información, tales como:

- ✓ **Cumplimiento normativo y regulatorio:** La no implementación de la norma ISO 27001 y la guía del MSPI puede derivar en incumplimientos frente a las regulaciones que rigen la gestión de la seguridad de la información.

- ✓ **Responsabilidad clara en roles de seguridad:** La ausencia de un equipo específico y de roles bien definidos puede llevar a confusiones en la asignación de responsabilidades, afectando la eficiencia en la toma de decisiones y gestión de incidentes.

- ✓ **Riesgo operacional:** Sin un equipo de gestión y directrices, la entidad está expuesta a posibles vulnerabilidades de seguridad que pueden comprometer la confidencialidad, integridad y disponibilidad de los activos de información.

- ✓ **Falta de cohesión en las acciones:** Las actividades que se han realizado hasta la fecha, aunque valiosas, carecen de una estructura integrada y sistemática, lo que limita su efectividad para garantizar una gestión robusta de la seguridad.

RECOMENDACIÓN

Es pertinente implementar las funciones de seguridad de la información conforme a la NTC ISO 27001 y siguiendo las directrices establecidas en la Guía de Roles y Responsabilidades del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Además, Conformar un equipo de gestión específico para la implementación del modelo MSPI, asegurando que este equipo esté alineado con los principios de la norma técnica y que cumpla con las responsabilidades detalladas en la Guía de Roles y Responsabilidades del MSPI de MinTIC.

HALLAZGO 14. Debilidades en la Implementación del Inventario de activos de información

La revisión documental y el análisis a la implementación del Inventario de Activos de Información en la entidad revelaron deficiencias que impactan la gestión integral de los activos de información. Si bien se han proporcionado evidencias documentales que incluyen el Procedimiento para la Gestión de Activos de TIC y el Instructivo para la Gestión de Activos de Información, se han identificado aspectos que requieren atención para asegurar una implementación alineada con los estándares de seguridad de la información, tales como:

- ✓ **Ausencia de un documento formal de metodología:** Aunque se han desarrollado procedimientos, no se identificó un documento formal que describa la metodología para la identificación, clasificación y valoración de los activos de información. Este documento es esencial para garantizar un proceso homogéneo y consistente, validado y aprobado por la alta dirección.

- ✓ **Deficiencias en la implementación transversal:** Se evidenció que la metodología no ha sido implementada de forma transversal por los líderes de procesos, responsables de activos de información y las áreas correspondientes dentro de la entidad. Esto limita la cobertura y eficacia del inventario.

- ✓ **Revisión del inventario de activos no documentada:** No se aportó evidencia documental que respalde la revisión periódica del inventario de activos de información, lo que puede generar riesgos de desactualización y falta de control sobre los activos de información.

- ✓ **Falta de información crítica en el inventario:** El inventario actual omite varios tipos de activos esenciales para la entidad, como activos físicos (edificios, vehículos), humanos (competencias técnicas, conocimientos), financieros, y otros activos como la propiedad intelectual y sistemas de seguridad. Esta falta de información compromete la capacidad de la entidad para gestionar eficazmente sus activos de

información.

- ✓ **Cobertura limitada del inventario:** Se observó que la lista de activos de información está enfocada en el proceso de "Gestión TICs", sin incluir otros procesos clave como Gestión Jurídica, Gestión de Recursos Financieros, Gestión Administrativa, entre otros. Esto refleja una visión parcial de los activos de información, lo que pude generar riesgos de gestión inadecuada.

- ✓ **Caracterización incompleta de activos:** La caracterización actual de los activos de información es insuficiente para identificar riesgos asociados y gestionar adecuadamente su ciclo de vida.

Estas deficiencias en la gestión del inventario de activos de información generan un riesgo significativo para la entidad, al no contar con un control adecuado y actualizado de sus activos. Esto puede comprometer la confidencialidad, integridad y disponibilidad de la información, aumentar la exposición a riesgos de seguridad, y dificultar la toma de decisiones informadas respecto a la gestión y protección de los activos.

Los esfuerzos actuales, aunque valiosos, no son suficientes para garantizar una gestión de activos consistente y efectiva, alineada con los estándares internacionales y las buenas prácticas de seguridad de la información.

RECOMENDACIÓN

Es pertinente llevar a cabo una revisión del inventario de activos de información, detallando las razones que motivan dicha revisión o validación, teniendo presente:

- ✓ Realizar una revisión del inventario de activos que considere: modificaciones recientes en procesos, inclusión de nuevas actividades y registros, catalogación de nuevos activos, ajustes por cambios organizacionales, documentación de migraciones en sistemas de información, y actualización de cambios físicos en la ubicación de los activos.

- ✓ Revisar, contextualizar, aprobar, implementar y apropiarse del inventario de activos de información de la entidad, abarcando no solo la "Gestión TICs", sino también todos los procesos críticos como Gestión Jurídica, Gestión de Recursos Financieros y Gestión Administrativa.

- ✓ Los activos de información deben estar alineados con los objetivos estratégicos de la entidad, integrando la seguridad de la información en las operaciones diarias para proteger los activos, optimizar la asignación de recursos, y establecer planes de contingencia y procedimientos robustos de gestión de incidentes.

- ✓ La información del inventario de activos de información debe ser actualizada y mantenida constantemente por los líderes de procesos, dueños de activos y responsables de cada área, garantizando una visión completa y exacta del estado de los activos.

- ✓ Desarrollar, revisar, contextualizar, aprobar, implementar y apropiarse de una caracterización de los activos de información que contengan datos personales, para identificar, clasificar y documentar los activos que almacenen, procesen o transmitan este tipo de datos.

- ✓ Establecer y formalizar una metodología para la identificación, clasificación y valoración de activos de información, que sea validada, revisada y aprobada por la alta dirección.

HALLAZGO 15. Deficiencias en la Gestión de los Documentos Electrónicos y Digitales.

En la revisión del portal web de la Contaduría General de la Nación (CGN) y de la documentación aportada en relación con la gestión documental, se identificaron los siguientes puntos clave que merecen atención para fortalecer la administración de documentos electrónicos y digitales, conforme a la normatividad vigente:

Política Institucional de Gestión Documental: Se evidenció la versión 2 de la "Política Institucional de Gestión Documental", actualizada en noviembre de 2023, la cual define lineamientos generales sobre la creación, manejo y disposición final de documentos. Respecto a la gestión de documentos electrónicos, el desarrollo en esta política se limita a la planificación de un sistema de gestión documental electrónico, sin detalles específicos sobre su implementación o el ciclo de vida de los documentos electrónicos.

Programa de Gestión Documental (PGD): Se revisó la versión 7.1 del PGD, que incluye apartados sobre normalización de formularios electrónicos y un subprograma para la gestión de documentos y expedientes electrónicos. Si bien estos subprogramas establecen directrices y actividades planificadas hasta 2027, falta evidencia que respalde la implementación actual y operativa de estas estrategias en toda la entidad.

Sistema Integrado de Conservación (SIC): En cuanto a la preservación de documentos digitales, la SIC versión 2 establece un marco para la conservación y preservación de documentos electrónicos. No obstante, no se encontraron evidencias de la implementación de procesos para la evaluación y gestión de recursos digitales en la práctica diaria de la entidad.

A pesar de los avances mencionados en la normatividad y la planificación estratégica, se identificaron elementos de mejora en la gestión de documentos electrónicos y digitales:

- ✓ Falta de Implementación Integral: No se encontró evidencia documental que demuestre la implementación efectiva de los procesos para la planificación, producción, gestión, organización, transferencia, disposición, preservación y valoración de los documentos electrónicos y digitales en la CGN.

- ✓ Políticas y Procedimientos: Existe una ausencia de políticas y procedimientos específicos que regulen la administración de documentos electrónicos, bases de datos

y registros digitales, lo cual compromete la integridad, fiabilidad y disponibilidad de estos activos documentales.

- ✓ Protección de Documentos: No se observan medidas para prevenir la pérdida o corrupción de documentos electrónicos ni esquemas de mantenimiento y verificación de errores en las bases de datos.

- ✓ Segregación de Funciones: No se han implementado mecanismos que asignen y supervisen los permisos de acceso a los documentos electrónicos, lo que puede comprometer la seguridad y confidencialidad de la información.

- ✓ Integridad y Disponibilidad: La integridad de las bases de datos no está garantizada por reglas estándar desde su diseño, y no se han implementado mecanismos para asegurar la futura disponibilidad de expedientes digitales, independientemente del sistema en el que se encuentren.

- ✓ Vinculación de Metadatos: Falta un procedimiento que asegure el vínculo permanente entre los documentos electrónicos y sus metadatos, lo que es fundamental para garantizar su trazabilidad y autenticidad.

La Gestión de los Documentos Electrónicos y Digitales se encuentra en un nivel intermedio, reflejando avances importantes.

RECOMENDACION

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y consolidar un Programa Integral de Gestión de Documentos y Expedientes Digitales. Este programa debe incluir el diseño, implementación y supervisión de estrategias que aseguren la administración y control adecuados en la producción de documentos electrónicos, en plena conformidad con la normatividad vigente. El programa debe garantizar la integridad, confiabilidad, disponibilidad y autenticidad de los documentos electrónicos a lo largo de su ciclo de vida, mediante procesos de identificación, estandarización, mantenimiento y sostenibilidad de estos documentos, respaldados por el uso eficaz de Tecnologías de la Información y Comunicaciones (TIC).

HALLAZGO 16. Deficiencias en la identificación, valoración y tratamiento del Riesgo de seguridad de la información o seguridad digital, registrados en la matriz de riesgos.

Se revisó y analizó la siguiente evidencia documental:

Política de Administración del Riesgo: Documento versionado en mayo de 2023 por el Grupo Interno de Trabajo (GIT) de Planeación. El documento cubre aspectos como introducción, alcance, metodología aplicada, riesgos institucionales y de proyectos, niveles de responsabilidad, entre otros.

Riesgos Digitales: El documento describe el actuar de la primera y segunda línea de

defensa ante incidentes de seguridad digital. Para la primera línea (líderes de proceso, equipo operativo y colaboradores), se establece la obligación de informar al GIT de Apoyo Informático, aplicar controles de mitigación, ejecutar el plan de contingencia y documentar los incidentes. La segunda línea (GIT de Apoyo Informático y GIT de Planeación) es responsable de supervisar la implementación de los planes de mejoramiento, evaluar su efectividad, y actualizar los Mapas de Riesgo, entre otras actividades.

Matriz de Riesgos de Seguridad de la Información: Documento en formato Excel, con dos secciones: "Descripción del Riesgo" y "Mapa y Plan de Tratamiento de Riesgo de Seguridad de la Información - Seguridad Digital", que incluye 23 registros sobre activos de hardware, software, servicios, información y talento humano. Se analizan tanto el riesgo inherente como el residual, tras la implementación de controles.

Según la revisión y análisis de las evidencias documentales, se identificaron elementos de mejora, así:

- ✓ Documentar los criterios para la evaluación y tratamiento del riesgo en la seguridad de la información, el cual es clave para garantizar un enfoque sistemático y alineado con los marcos normativos aplicables.

- ✓ Aunque se cuenta con una matriz de riesgos, no se ha desarrollado un documento integral que precise los procesos para identificar, evaluar y mitigar los riesgos de seguridad de la información. Este documento debe cubrir, entre otros, el valor estratégico del proceso de información para la entidad, la criticidad de los activos de información involucrados, los requisitos legales y reglamentarios, y las expectativas de las partes interesadas.

- ✓ Las acciones implementadas para la identificación, valoración y tratamiento de riesgos digitales no están completamente integradas ni desarrolladas de manera sistemática, lo que puede limitar la efectividad global de la gestión del riesgo.

- ✓ La gestión de riesgos en la seguridad de la información no se encuentra alineada con las directrices del Departamento Administrativo de la Función Pública, el Archivo General de la Nación (AGN) y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). En particular, se identifican vacíos en el cumplimiento de criterios de evaluación y aceptación del riesgo, así como en la implementación de controles y medidas correctivas.

RECOMENDACIÓN

Es pertinente establecer las especificaciones para la gestión de riesgos en seguridad de la información o riesgos digitales a lo largo de las cuatro fases del proceso del Modelo de Seguridad y Privacidad de la Información (MSPI), alineados con los lineamientos del DAFP y el AGN.

1.7.3 ASPECTOS OPERACIONALES Y DE GESTIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Los resultados de la evaluación realizada a los criterios del componente "3. ASPECTOS OPERACIONALES Y DE GESTIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN", presentan un nivel de cumplimiento del 32%, lo que denota deficiencias en los aspectos evaluados.

HALLAZGO 17. Debilidades en la Planificación y Control Operacional.

La revisión y análisis a la Planificación y Control Operacional de la entidad reveló deficiencias como:

- ✓ El plan de tratamiento de riesgos digitales o de seguridad de la información, no contemplaban el desarrollo mínimo de los temas como.

  - Objetivos.
  - Alcance.
  - Marco referencial.
  - Metodología que contemple la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos,
  - Definición de las medidas de seguridad identificadas para desarrollar e implementar.
  - Plan de tratamiento para los riesgos de Seguridad y Privacidad de la Información.
  - Plan de implementación de la Seguridad Digital.
  - Plan de la implementación de la Continuidad de la Operación.
  - Plan de Tratamiento de Riesgos que mitigan los riesgos presentes en el análisis de riesgos Perdida de la Confidencialidad de los activos, Perdida de Integridad de los activos y Perdida de Disponibilidad de los activos).
  - Oportunidades de mejora.
  - En el marco de la gestión de riesgos de seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, disposición de los recursos Humanos, Técnicos, Logísticos y Financieros.
  - Estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la información identificados en la entidad.
  - Especificaciones de la medición del modelo de seguridad y privacidad de la información.

- ✓ Falta de la implementación de las políticas de: la Política de Control de Acceso, Política de Seguridad de los Activos de Información, Política de Criptografía y Política de Antivirus y Antimalware, que deben ser aprobadas por la alta dirección y debidamente documentadas. Como tampoco un acto administrativo que confirme la revisión y aprobación de la Declaración de aplicabilidad por parte de la alta dirección; acorde a lo indicado en el control establecido por la norma NTC ISO/IEC 27001, en el control A.5.1.1.

- ✓ Falta de la implementación, ejecución y apropiación de los siguientes planes:

  - Plan de tratamiento para los riesgos de Seguridad y Privacidad de la Información.

- Plan de implementación de la Seguridad Digital.
- Plan de la implementación de la Continuidad de la Operación.
- Plan de Tratamiento de Riesgos que mitigan los riesgos digitales.
- Plan de atención a las oportunidades de mejora.

✓ Falta de implementación de la estrategia de planificación y control operacional, revisada y aprobada por la alta Dirección de acuerdo con lo establecido por la norma NTC ISO/IEC 27001 y las guías de MinTIC.

RECOMENDACIÓN

Es pertinente que la entidad desarrolle y formalice un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación que sea integral y alineado con las normas NTC ISO/IEC 27001 y las directrices del MinTIC. Se debe incluir, como mínimo, los siguientes elementos:

✓ Establecer para el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, los objetivos específicos, el alcance de su aplicación, y un marco referencial que guíe su implementación y monitoreo.

✓ Incluir una metodología que defina las actividades necesarias para mitigar los riesgos sobre los activos de información, así como la identificación y desarrollo de medidas de seguridad.

✓ Desarrollar planes detallados para la implementación de la Seguridad Digital, la Continuidad de la Operación y el tratamiento de los riesgos identificados. Estos planes deben ser coherentes, viables y contar con la aprobación de la alta dirección.

✓ Estimar y asignar los recursos humanos, técnicos, logísticos y financieros necesarios para la ejecución efectiva de los planes, asegurando que estos recursos sean suficientes para cubrir todas las áreas críticas identificadas.

✓ Desarrollar, revisar, contextualizar, aprobar, implementar y apropiar políticas como la Política de Control de Acceso, la Política de Seguridad de los Activos de Información, la Política de Criptografía y la Política de Antivirus y Antimalware. Además, formalizar la Declaración de Aplicabilidad mediante un acto administrativo aprobado por la alta dirección.

✓ Desarrollar y aprobar una estrategia integral de planificación y control operacional, revisada por la alta dirección, que garantice el cumplimiento de las normativas de seguridad de la información y que sea coherente con las guías del MinTIC.

HALLAZGO 18. Inaplicabilidad de los indicadores de gestión diseñados por MinTIC.

Se revisaron y analizaron 2 documentos en formato Excel, denominados "TIC-GES-IND-

2022-ConsolidadoIndicador2022" y "TIC-GES-IND-2023-ConsolidadoIndicador2023". Estos documentos contienen información relevante en dos secciones principales:

Sección Seguridad: Bajo el título "INDICADOR CALIDAD SGSI: PÉRDIDA DE DISPONIBILIDAD, INTEGRIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN", se presenta la medición del cumplimiento de lineamientos de la Política de Seguridad Informática de la CGN. Esta sección incluye 15 lineamientos clave, tales como:

- Autorización e identificación de usuarios para acceso a sistemas.
- Restricciones para el uso de módems o dispositivos similares sin VPN y firewall.
- Procedimientos para autorización de accesos remotos.

La fórmula utilizada para evaluar estos lineamientos mide el porcentaje de políticas satisfactorias en relación con las políticas medibles.

Sección Proceso de Gestión TICs: Aquí se abordan indicadores relacionados con la disponibilidad de servicios tecnológicos, tales como internet, red LAN, plataformas misionales y de gestión, así como indicadores de efectividad de soporte, pérdida de confidencialidad y disponibilidad de información, entre otros. En esta sección, se evidencian descripciones detalladas de la disponibilidad de los servicios y la gestión de incidentes tecnológicos.

Adicionalmente, en el archivo correspondiente a 2023, se incluye una sección denominada "HOJA DE VIDA", en la cual se especifican indicadores de proyectos de inversión tecnológica, como la disponibilidad de la infraestructura tecnológica y el avance del Plan Estratégico de TI.

Si bien los documentos aportados reflejan avances importantes en la medición de indicadores relacionados con la gestión de infraestructura tecnológica y seguridad de la información, se evidenció la ausencia de un documento específico que contemple de manera integral los indicadores de gestión de seguridad y privacidad de la información recomendados por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Este documento debe incluir indicadores clave, tales como:

- Organización de la seguridad de la información.
- Cobertura del Sistema de Gestión de Seguridad de la Información (SGSI) en activos críticos.
- Tratamiento de eventos de seguridad y privacidad de la información.
- Plan de sensibilización y concientización sobre seguridad.
- Cumplimiento de políticas de seguridad en la entidad.
- Control de acceso y su verificación.
- Adquisición segura y mantenimiento de software.
- Implementación de procesos de registro y auditoría.
- Políticas de privacidad, confidencialidad e integridad de la información.
- Disponibilidad del servicio y protección ante ataques informáticos.
- Porcentaje de implementación de controles y disponibilidad de servicios digitales (gobierno en línea).

La revisión documental y los análisis realizados permitió establecer que, aunque se ha avanzado en la implementación de indicadores relacionados con la gestión de TIC y seguridad, estos no se encuentran alineados con los lineamientos y mejores prácticas recomendadas por MinTIC. Específicamente, no se ha evidenciado la aprobación, implementación ni socialización interna de los indicadores de gestión en seguridad y privacidad de la información establecidos por dicho organismo.

RECOMENDACIÓN

Adoptar y adaptar los indicadores de gestión establecidos por el MinTIC, en el marco de la implementación del MSPI.

HALLAZGO 19. Debilidad en la aplicabilidad de los requisitos del control de acceso en la entidad.

La revisión y análisis a la implementación de los requisitos de la entidad para el control de acceso reveló deficiencias como:

- ✓ Falta de las especificaciones de un proceso/procedimiento de gestión de derechos de acceso privilegiado para que estos sean gestionados de manera controlada y alineados con las políticas de seguridad de la entidad. Este proceso debe comenzar con la identificación de los derechos de acceso privilegiado necesarios para cada sistema o proceso y los usuarios correspondientes, garantizando que solo aquellos con una necesidad justificada reciban dichos privilegios.

- ✓ Falta de las especificaciones de un proceso/procedimiento para la gestión y el uso de información de autenticación secreta de usuarios que garantice la confidencialidad y protección de las credenciales. Este proceso debe incluir la firma de una declaración por parte de los usuarios, comprometiéndose a mantener la confidencialidad de su información de autenticación secreta personal y, en caso de credenciales compartidas, a restringir su conocimiento únicamente a los miembros autorizados del grupo.

- ✓ Falta de las especificaciones de un proceso/procedimiento para restringir el acceso a la información en la aplicación individual de la entidad, según la política de control de acceso definida. Este proceso debería incluir el control de acceso a funciones y datos, gestión de derechos de acceso para usuarios y aplicaciones, limitación de información en elementos de salida, y la implementación de controles de acceso físico o lógico para proteger aplicaciones y sistemas críticos.

- ✓ Falta de las especificaciones de un proceso/procedimiento para el acceso a sistemas y aplicaciones, el cual debe incluir medidas como la protección de identificadores hasta el ingreso exitoso, advertencias de acceso solo para usuarios autorizados, evitar mensajes de ayuda en el ingreso, validación de información solo al completar todos los datos, protección contra intentos de ingreso por fuerza bruta, registro de intentos de acceso, declaración de eventos de seguridad en caso de intentos sospechosos, y medidas de seguridad adicionales como la finalización de sesiones inactivas y

restricción de tiempos de conexión.

- ✓ Falta de las especificaciones de un Sistema de Gestión de Contraseñas que cubra aspectos esenciales como el uso de identificaciones y contraseñas individuales, la capacidad de los usuarios para seleccionar y cambiar contraseñas, la exigencia de contraseñas de calidad, el cambio obligatorio de contraseñas en el primer ingreso y de forma regular, la prevención del reuso de contraseñas, la protección de contraseñas durante la entrada, y el almacenamiento seguro de las contraseñas separadas de los datos del sistema y protegidas durante la transmisión.

- ✓ Falta de la implementación de la Política para el Uso de programas utilitarios privilegiados, debidamente aprobada por la alta dirección y socializado al interior de la entidad.

- ✓ Falta de la implementación del Procedimiento de Control de acceso a códigos fuente de programas o componentes tecnológicos, debidamente aprobado por la alta dirección y socializado al interior de la entidad.

RECOMENDACIÓN

Para la implementación de los requisitos del control de acceso en la entidad es pertinente desarrollar lo siguiente:

- ✓ Establecer e implementar un proceso para la asignación de derechos de acceso privilegiado, que incluya directrices de autorización y un registro detallado de todos los privilegios concedidos.

- ✓ Desarrollar, revisar, contextualizar, aprobar, implementar y apropiar procedimientos para prevenir el uso no autorizado de identificaciones de administración genérica y garantizar la confidencialidad de la información de autenticación, especialmente durante la rotación de personal.

- ✓ Es pertinente implementar un proceso integral y seguro para la gestión de la información de autenticación secreta de usuarios, que garantice la confidencialidad y protección de las credenciales.

- ✓ Desarrollar, revisar, contextualizar, aprobar, implementar y apropiar procedimientos que verifiquen la identidad del usuario antes de proporcionarle nuevas credenciales temporales o de reemplazo, asegurando que este proceso se realice de manera segura y evitando el uso de canales inseguros como correos electrónicos no protegidos.

- ✓ Desarrollar, revisar, contextualizar, aprobar, implementar y apropiar una política para el uso de programas utilitarios privilegiados, con directrices que incluyan procedimientos de identificación, autenticación y autorización; la separación de estos programas del software de aplicaciones; la limitación de su uso a un mínimo de usuarios confiables y autorizados; y la autorización del uso ad hoc. Además, se debe registrar su uso, definir niveles de autorización, deshabilitar programas innecesarios

y evitar que estén disponibles para usuarios con acceso a aplicaciones en sistemas que requieran separación de deberes.

- ✓ Desarrollar, revisar, contextualizar, aprobar, implementar y apropiar el Procedimiento de Control de Acceso a Códigos Fuente, el cual debe incluir la ubicación segura de las librerías de códigos fuente, una gestión conforme a procedimientos establecidos, acceso restringido para el personal de soporte, actualizaciones y entregas solo con autorización, almacenamiento seguro de listados de programas, un registro de auditoría de accesos, y un estricto control de cambios para las copias y mantenimiento de las librerías.

HALLAZGO 20. Falta de uso de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

Tras revisar el contenido del Manual de Seguridad de la Información 2022 y la evidencia presentada, se constató que aunque se ha abordado el tema de herramientas criptográficas y protocolos autorizados, eliminando cifrados débiles y gestionando adecuadamente las llaves criptográficas y los certificados SSL, no existe un documento específico que desarrolle de manera integral y específica la Política sobre el uso de controles criptográficos, aprobado por la alta dirección y socializado al interior de la entidad. Esta política es fundamental para definir las directrices que deben guiar el uso de la criptografía en la protección de la confidencialidad, autenticidad e integridad de la información.

La ausencia de un documento que incluya elementos esenciales como la introducción, objetivos, alcance, condiciones de implementación, y roles y responsabilidades específicos, limita la efectividad de los controles criptográficos implementados. Una política formal y debidamente aprobada debería abarcar, entre otros aspectos:

- ✓ El enfoque de la entidad respecto al uso de controles criptográficos para la protección de la información del negocio.

- ✓ Valoraciones de riesgos que determinen el nivel de protección necesario, considerando la fortaleza y calidad de los algoritmos de encriptación utilizados.

- ✓ El uso de encriptación para proteger información transmitida a través de dispositivos móviles o líneas de comunicación.

- ✓ La gestión adecuada de las llaves criptográficas, incluyendo su protección, recuperación y el manejo de llaves comprometidas o dañadas.

- ✓ Definición de roles y responsabilidades claras para la implementación de la política y la gestión de las llaves criptográficas.

- ✓ Normas y procedimientos que aseguren la implementación efectiva y coherente en toda la organización.

- ✓ Impacto de la encriptación en los controles que dependen de la inspección del contenido de la información.

El análisis realizado revela que actualmente la CGN carece de una política formal sobre el uso de controles criptográficos y la gestión de llaves criptográficas, debidamente aprobada y socializada. Esto se traduce en un nivel mínimo de implementación de mecanismos criptográficos que protejan la confidencialidad, autenticidad e integridad de la información. Las evidencias aportadas reflejan actividades dispersas y aisladas que, aunque valiosas, no garantizan una protección integral ni una alineación con los estándares requeridos.

RECOMENDACIÓN

Implementación de manera integral y formal, el uso de la criptografía para garantizar la protección efectiva de la confidencialidad, autenticidad e integridad de la información. Esto debe incluir no solo el uso de tecnologías y herramientas criptográficas, sino también la aprobación y socialización de una Política de Controles Criptográficos que establezca las directrices necesarias para su correcta aplicación en la entidad.

Esta política deberá contemplar, como mínimo, los siguientes elementos clave:

- ✓ Establecer los principios y directrices que aseguren la protección de la información sensible y de misión crítica.

- ✓ Incluir un proceso de valoración de riesgos que determine los niveles de protección requeridos, identificando los algoritmos criptográficos más adecuados según la sensibilidad de la información.

- ✓ Utilizar la criptografía para proteger la información que se transporta a través de dispositivos móviles, medios removibles o redes de comunicación, asegurando la seguridad en todo el ciclo de vida de los datos.

- ✓ Establecer procedimientos para la gestión segura de llaves, incluyendo su generación, almacenamiento, distribución y renovación, así como mecanismos para la recuperación de información en casos de pérdida o compromisos de seguridad.

- ✓ Definir quién será responsable de implementar, supervisar y gestionar los controles criptográficos, asegurando que cada área o dependencia involucrada comprenda sus funciones y obligaciones.

- ✓ Garantizar que el uso de la criptografía cumpla con las normativas aplicables y los mejores estándares de seguridad de la información.

La aprobación de esta política por la alta dirección y su debida socialización dentro de la entidad son factores esenciales para asegurar una correcta implementación y un uso consistente de los controles criptográficos en todos los procesos que involucren información sensible.

HALLAZGO 21. Deficiencias en la protección física y control de acceso a instalaciones de procesamiento de información.

Tras una revisión y análisis de las evidencias presentadas y del estado de las políticas de seguridad física y control de acceso, se identificó la ausencia de un documento específico que contenga los lineamientos detallados de la Política de Control de Acceso, debidamente aprobada por la alta dirección y socializada en toda la entidad. Este documento es fundamental para garantizar la implementación adecuada y uniforme de las directrices sobre la gestión de acceso a instalaciones y sistemas críticos.

Además, se identifica la necesidad de avanzar en el desarrollo de acciones tendientes a corregir las siguientes debilidades:

- ✓ Falta de directrices para la definición y uso de perímetros de seguridad de tal manera que no se han definido los perímetros de seguridad necesarios para proteger áreas con información sensible o crítica. La implementación de estas directrices es esencial para asegurar que solo el personal autorizado tenga acceso a dichas áreas.

- ✓ Ausencia de especificaciones para áreas seguras en cuanto a que no se han establecido controles de acceso físico para proteger áreas seguras dentro de las instalaciones, lo que representa un riesgo significativo para la seguridad de la información sensible que allí se maneja.

- ✓ Inexistencia de especificaciones sobre seguridad física en oficinas y recintos de tal manera que no se cuenta con un diseño ni implementación formalizados de medidas de seguridad física para oficinas, recintos o instalaciones clave. La falta de estas especificaciones puede comprometer la integridad de la información y de los sistemas que allí se resguardan.

- ✓ Falta de un Plan de Continuidad del Negocio basado en los estándares del National Institute of Standards and Technology (NIST), que garantice la operatividad en situaciones adversas o emergencias que puedan comprometer la seguridad física y tecnológica de la CGN.

- ✓ Ausencia de un procedimiento formal para trabajo en áreas seguras aprobado por la alta dirección y socializado internamente para regular el trabajo en áreas seguras, lo que deja expuestas estas áreas a riesgos de la información.

RECOMENDACIÓN

Desarrollar, revisar, contextualizar, aprobar, implementar, apropiar e implementar estrategias para la Protección Física y Control de Acceso a Instalaciones de Procesamiento de Información acorde a lo establecidos en las NIST SP 800-34 Rev. 1.

HALLAZGO 22. Deficiencias para prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones.

La revisión y análisis realizado para prevenir la pérdida, daño, robo o compromiso de activos, así como la interrupción de las operaciones, reveló que es necesario definir lo siguiente:

- ✓ Lineamientos específicos para que los equipos deban estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado. Además, no se identificó especificaciones detalladas de la Política de protección de los equipos, debidamente aprobado por la alta dirección y socializado al interior de la entidad.

- ✓ Descripción de los servicios de suministro (electricidad, telecomunicaciones, suministro de agua, alcantarillado, ventilación y aire acondicionado) para proteger los equipos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro con el fin de garantizar la continuidad operativa y la integridad de los sistemas críticos de la entidad.

- ✓ Especificaciones detalladas de la política de protección del cableado de potencia y telecomunicaciones que transporta datos o soporta servicios de información, debidamente aprobado por la alta dirección y socializado al interior de la entidad.

- ✓ Especificaciones detalladas de una política de mantenimiento para equipos informáticos, debidamente aprobado por la alta dirección y socializado al interior de la entidad.

- ✓ Especificaciones detalladas de una política para el retiro de activos, debidamente aprobado por la alta dirección y socializado al interior de la entidad.

- ✓ Especificaciones detalladas de una política de seguridad a los activos que se encuentran fuera de las instalaciones de la entidad, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones, debidamente aprobada por la alta dirección y socializado al interior de la entidad.

- ✓ Detalle de la Política de Seguridad para el Borrado y Encriptación de Discos, debidamente aprobada por la alta dirección y socializado al interior de la entidad.

- ✓ Ausencia de la Política para equipos de usuarios desatendidos, debidamente aprobado por la alta dirección y socializado al interior de la entidad.

- ✓ Especificaciones de la política de escritorio limpio para los papeles y medios de almacenamiento removibles, debidamente aprobado por la alta dirección y socializado al interior de la entidad.

RECOMENDACIÓN

Para prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar las siguientes políticas:

- ✓ Política de Protección de Equipos
- ✓ Política de Protección del Cableado de Potencia y Telecomunicaciones
- ✓ Política de Mantenimiento para Equipos Informáticos
- ✓ Política para el Retiro de Activos
- ✓ Política de Seguridad para Activos Fuera de las Instalaciones debe incluir directrices basadas en la NIST para proteger los equipos y medios en ubicaciones externas.
- ✓ Política de Seguridad para el Borrado y Encriptación de Discos
- ✓ Política para equipos de usuarios desatendidos
- ✓ Política de escritorio limpio para papeles y medios de almacenamiento removibles

HALLAZGO 23. Deficiencias en la adquisición, desarrollo y mantenimiento de Sistemas.

La revisión y análisis realizado a la adquisición, desarrollo y mantenimiento de Sistemas, reveló:

- ✓ Que no se han documentado las siguientes políticas:

  - Política de seguridad de la información para nuevos sistemas de información o para mejoras a los sistemas de información existentes
  - Política de desarrollo seguro para establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la entidad.
  - Política de protección de las transacciones de los servicios de las aplicaciones
  - Política de desarrollo seguro para establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la entidad.
  - No ha documentado un procedimiento control de cambio en los sistemas de información para establecer y aplicar los cambios a los desarrollos dentro del ciclo de vida de desarrollo de software con el fin de controlar mediante el uso de procedimientos formales de control de cambios a los desarrollos de software.
  - No ha documentado la política de revisión técnica de las aplicaciones después de cambios en la plataforma de operación.
  - Política de Restricciones en los cambios a los paquetes de software.
  - Política protección de datos de prueba.

- ✓ Ausencia de las políticas, procedimientos, metodologías y principios para la construcción o implementación de sistemas seguros, y su aplicación en cualquier actividad de implementación de sistemas de información más allá del sistema CHIP, de tal manera que, se establezcan, documenten y mantengan principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información de la entidad.

- ✓ Inexistencia de las políticas, procedimientos, y metodologías para proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas para establecer un marco integral que garantice la seguridad y la integridad en todas las fases del ciclo de vida del desarrollo de sistemas. Esto incluye desde la concepción y planificación inicial, pasando por el diseño, desarrollo, pruebas, integración, despliegue, y hasta el mantenimiento continuo de los sistemas. La documentación debe asegurar que todos los procesos y actividades se realicen bajo estándares de seguridad robustos, protegiendo los datos y activos de información contra accesos no autorizados, alteraciones, pérdidas y otros riesgos.

- ✓ Falta de supervisión y seguimiento a las actividades de desarrollo de sistemas contratados externamente.

- ✓ Ausencia de documentación y evidencias de las pruebas de aceptación de sistemas. Esta deficiencia se presenta tanto para los sistemas de información nuevos como para las actualizaciones y nuevas versiones. Adicionalmente, no se encontraron programas de prueba para aceptación ni criterios de aceptación relacionados. La ausencia de esta documentación crítica compromete la capacidad de la entidad para garantizar que los sistemas implementados cumplan con los estándares de calidad y seguridad requeridos, y limita la posibilidad de realizar un seguimiento efectivo y una evaluación objetiva del cumplimiento de los requisitos.

- ✓ No se han especificado los servicios de aplicaciones que pasan sobre redes públicas para proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.

RECOMENDACIÓN

Para la adquisición, desarrollo y mantenimiento de sistemas es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar las políticas en mención, acorde a los lineamientos de la NTC ISO 27001 y MinTIC.

1.7.4 PLANIFICACIÓN Y SEGUIMIENTO A LA GESTIÓN TIC

Los resultados de la evaluación realizada a los criterios del componente "4. PLANIFICACIÓN Y SEGUIMIENTO A LA GESTIÓN TICS", presentan un nivel de cumplimiento del 21%, lo que denota deficiencias en los aspectos evaluados.

HALLAZGO 24. Debilidades en la revisión y seguimiento a la implementación de la Gestión TIC.

La revisión y análisis realizado a la revisión y seguimiento a la implementación de la Gestión TIC, reveló:

- ✓ Inexistencia del Procedimiento de Evaluación del Desempeño del MSPI.

- ✓ Ausencia de la realización de actividades de revisión y evaluación de la eficacia del Modelo de Seguridad de la Información (MSPI) en la entidad. La falta de evidencias documentales impide verificar si se están llevando a cabo las evaluaciones necesarias para asegurar que los controles de seguridad implementados son efectivos y se alinean con las políticas y normativas establecidas.

- ✓ Inexistencia de la realización de actividades para medir la efectividad de los controles implementados frente a los riesgos digitales. Esta falta de evidencia impide verificar si los controles establecidos son adecuados y eficaces para mitigar los riesgos digitales identificados, comprometiendo la capacidad de la entidad para asegurar la protección integral de su información y sistema.

- ✓ Inexistencia de la revisión de las valoraciones de riesgos. La ausencia de estas evidencias documentales impide verificar la realización adecuada de las evaluaciones y el seguimiento de los riesgos identificados.

- ✓ Falta de la realización de la actividad de medición de los indicadores de Gestión del Modelo de Seguridad y Privacidad de la Información (MSPI). La falta de evidencias documentales impide verificar la correcta ejecución y monitoreo de estos indicadores, lo cual es fundamental para evaluar la eficacia y eficiencia del MSPI.

- ✓ Ausencia de la realización de la actividad de revisión y actualización de los planes de seguridad. La ausencia de estas evidencias documentales impide verificar que los planes de seguridad se revisen y actualicen de manera sistemática y en conformidad con los procedimientos establecidos.

- ✓ Inexistencia de la realización de la actividad de revisión del Modelo de Seguridad y Privacidad de la Información (MSPI) por parte de la dirección. La falta de evidencias documentales impide verificar que las revisiones del MSPI, realizadas por la dirección, se efectúan de manera sistemática y conforme a los procedimientos establecidos.

- ✓ Falta de la realización de la actividad del registro de las actividades relacionadas con el Modelo de Seguridad y Privacidad de la Información (MSPI). La falta de estas evidencias documentales impide validar que las actividades del MSPI se registren de manera adecuada y sistemática, lo cual es esencial para garantizar la trazabilidad, el seguimiento y la efectividad de las medidas de seguridad implementadas.

- ✓ Ausencia de la realización de las actividades de revisión de acciones o planes de mejora (respuesta a no conformidades) relacionadas con el Modelo de Seguridad y Privacidad de la Información (MSPI). La falta de estas evidencias documentales dificulta verificar que se estén tomando medidas correctivas adecuadas y oportunas para abordar las no conformidades identificadas, lo cual es esencial para mantener la integridad y efectividad del MSPI.

- ✓ Inexistencia de la realización de actividades de programación y ejecución de las revisiones por parte del encargado de seguridad y privacidad de la información para garantizar que los controles implementados para proteger la integridad,

confidencialidad y disponibilidad de los datos estén operando de manera efectiva y conforme a las políticas establecidas por la entidad.

RECOMENDACIÓN

Para la revisión y seguimiento a la implementación de la Gestión TIC es pertinente lo siguiente:

- ✓ Desarrollar, revisar, contextualizar, aprobar, implementar y apropiar el Procedimiento de Evaluación del Desempeño del MSPI con las actividades para establecer una metodología sistemática que permita medir y analizar el rendimiento del MSPI dentro de la entidad. Este procedimiento tiene como finalidad asegurar que los controles y políticas de seguridad implementadas sean efectivos, identificar áreas de mejora y garantizar el cumplimiento de las normativas y estándares de seguridad establecidos. Además, busca proporcionar información precisa y oportuna para la toma de decisiones estratégicas, fomentando la mejora continua y la robustez del MSPI en la protección de la información crítica de la entidad.

- ✓ Para asegurar un monitoreo continuo y una mejora constante en la seguridad de la información dentro de la entidad, es importante establecer y mantener registros detallados y sistemáticos de las revisiones de desempeño del MSPI. Estos registros deben documentar de manera exhaustiva cada evaluación realizada, incluyendo los hallazgos, recomendaciones y acciones correctivas implementadas. La información debe ser organizada de forma que facilite el seguimiento y análisis de las tendencias a lo largo del tiempo, permitiendo así la identificación oportuna de áreas que requieran ajustes. Además, se debe garantizar que estos registros estén accesibles para auditorías internas y externas, y que se utilicen para informar el desarrollo de estrategias de mejora y la optimización continua de los controles de seguridad.

- ✓ Para garantizar la efectividad de los controles establecidos en la implementación del MSPI, se debe llevar a cabo un proceso estructurado de medición y evaluación. Esto incluye la realización de actividades sistemáticas para evaluar cómo estos controles están operando en la práctica y si están cumpliendo con los objetivos de seguridad establecidos. Se deben definir claramente los indicadores clave de rendimiento y los criterios de éxito, así como realizar auditorías periódicas y revisiones de los controles implementados. Además, se debe asegurar la recopilación y análisis de datos relevantes para identificar áreas de mejora y ajustar los controles según sea necesario para optimizar su efectividad y garantizar la protección adecuada de la información.

- ✓ Establecer y mantener registros detallados que documenten de manera sistemática la revisión y actualización periódica de las valoraciones de riesgos del MSPI. Estos registros deben incluir información sobre la frecuencia de las revisiones, los criterios utilizados para la evaluación de riesgos, los cambios implementados en respuesta a las valoraciones, y las razones detrás de cada ajuste. Deben capturar todas las fases del proceso, desde la identificación de riesgos hasta la implementación de controles y la evaluación de su efectividad. Además, es importante que los registros sean accesibles y auditables, permitiendo así una evaluación transparente y rigurosa del

proceso de gestión de riesgos del MSPI.

- ✓ Implementar un sistema de registro y seguimiento detallado para las mediciones de los indicadores establecidos en la implementación del MSPI, a fin de asegurar la transparencia y efectividad en la gestión de seguridad y privacidad de la información.

- ✓ Documentar y archivar de manera detallada todas las actividades de revisión realizadas por la dirección para asegurar una supervisión efectiva y una mejora continua del Modelo de Seguridad de la Información (MSPI). Esta documentación debe incluir los criterios de evaluación utilizados, los hallazgos de cada revisión, las acciones correctivas implementadas, y las decisiones tomadas durante el proceso.

- ✓ Es importante que se documenten exhaustivamente todas las actividades relacionadas con la revisión y actualización de los planes de seguridad informática. Esta documentación debe incluir detalles sobre las revisiones realizadas, los criterios de evaluación utilizados, las modificaciones implementadas y las razones detrás de cada cambio. Mantener registros detallados garantiza que los planes de seguridad informática permanezcan actualizados, efectivos y alineados con las necesidades y riesgos actuales de la entidad.

- ✓ Establecer e implementar actividades para centrarse en evaluar y gestionar los riesgos relacionados con la seguridad de la información y la privacidad de los datos, asegurando que se alineen con los objetivos organizacionales. Es importante verificar el cumplimiento de normativas y regulaciones aplicables en protección de datos y privacidad. Además, se debe analizar la efectividad de los controles implementados, tanto técnicos como administrativos, para proteger la información sensible y reducir brechas de seguridad. Es importante identificar vulnerabilidades en los sistemas y procesos de la entidad, y recomendar mejoras para mitigarlas.

HALLAZGO 25. Debilidades en la implementación del plan de ejecución de auditorías y seguimiento a la gestión TIC.

La revisión y análisis realizado a la implementación del plan de ejecución de auditorías y seguimiento a la gestión TIC, acorde a lo establecido en la Guía No. 15 de Seguridad y Privacidad de la Información emitida por MinTIC, reveló:

- ✓ No se cuenta con las especificaciones de las métricas, que permiten medir los procesos técnicos que se está aplicando en la entidad, respecto a sus productos, con el fin de poder identificar como mejorar su calidad, de tal manera que se obtenga un resultado de calidad que pueda llegar al ciudadano.

- ✓ Ausencia de especificaciones de las métricas de seguridad donde se defina las mediciones de los procesos que determinan que tan bien se cumplen los procesos de seguridad en la entidad, si los procesos cumplen con los requisitos definidos por las políticas de seguridad y las normas técnicas seguidas por la entidad. Además de medir el grado de riesgo de daño que pueden recibir objetos, recursos y personas; salud y seguridad tanto del usuario como de los afectados por dicho uso, al igual que

consecuencias económicas o físicas no intencionadas.

- ✓ Inexistencia de la realización de acciones derivadas producto del seguimiento a los indicadores asociados al cumplimiento de la estrategia de Seguridad de la Información.

- ✓ Falta de un tablero de control con los indicadores asociados al cumplimiento de la Estrategia de Seguridad de la Información.

- ✓ Ausencia de la realización de actividades del seguimiento al cumplimiento de los Acuerdos de Nivel de Servicio (ANS) establecidos con las dependencias o entidades externas para el intercambio de la información de calidad, los cuales contemplan las características de oportunidad, disponibilidad y seguridad que requieran los componentes de información. El seguimiento al cumplimiento de los Acuerdos de Nivel de Servicio (ANS) establecidos con las dependencias o entidades externas para el intercambio de información de calidad debe garantizar que las partes involucradas cumplan con los estándares acordados en términos de oportunidad, disponibilidad y seguridad de la información.

- ✓ Inexistencia de evidencia que respalde el seguimiento y gestión de los hallazgos detectados durante el uso de los servicios de información y en los reportes de solicitudes gestionadas a través de la mesa de ayuda. Esta carencia se extiende más allá de la simple atención y resolución de solicitudes de servicio y de la gestión de problemas reportados por la herramienta ZABBIX. Además, No se cuenta con soportes documentales que demuestren la realización de auditorías, evaluaciones y seguimientos que resulten en la formulación de planes de mejoramiento.

- ✓ Inaplicabilidad de actividades de seguimiento y gestión de los responsables (custodio y dueño) de la protección y privacidad de la información conforme con la normativa de protección de datos de tipo personal y de acceso a la información pública, según el catálogo de componentes de información de la Entidad.

- ✓ Ausencia de la realización de actividades de seguimiento y gestión de los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de todos los sistemas de información de la CGN, según los lineamientos de trazabilidad y auditoría definidos para los componentes de los sistemas de información.

- ✓ Inexistencia de la realización de actividades de seguimiento y gestión de los mecanismos que aseguran el registro histórico de las acciones realizadas por los usuarios sobre los sistemas de Información, los cuales mantienen la trazabilidad y apoyan los procesos de auditoría, según los Log de trazas sobre las acciones realizadas por los usuarios.

- ✓ Falta de la realización de actividades de monitoreo, seguimiento y evaluación del modelo de continuidad y seguridad, supervisión de los niveles de seguridad, análisis de tendencias, identificación de nuevos riesgos y vulnerabilidades. El monitoreo,

seguimiento y evaluación del modelo de continuidad y seguridad, así como la supervisión de los niveles de seguridad, análisis de tendencias, e identificación de nuevos riesgos y vulnerabilidades, debe garantizar que la entidad está preparada para enfrentar y mitigar cualquier incidente que pueda comprometer la continuidad operativa y la seguridad de la información. Esto implica asegurar que los controles de seguridad sean efectivos, que se anticipen y respondan adecuadamente a los cambios en el entorno de riesgos, y que se protejan los activos críticos de la organización.

- ✓ Ausencia de la realización de actividades de monitoreo, seguimiento y evaluación de las capacidades de alta disponibilidad de las infraestructuras críticas y los Servicios Tecnológicos que afecten la continuidad del servicio de la Entidad. El monitoreo, seguimiento y evaluación de las capacidades de alta disponibilidad de las infraestructuras críticas y los Servicios Tecnológicos que afectan la continuidad del servicio de la entidad debe garantizar que estos componentes estén siempre operativos y disponibles, minimizando el riesgo de interrupciones que puedan afectar la continuidad de las operaciones. Esto es fundamental para asegurar que la entidad pueda cumplir con sus funciones sin interrupciones, incluso en situaciones de alta demanda o bajo condiciones adversas.

- ✓ Inexistencia de la realización de actividades de monitoreo, seguimiento y evaluación a los controles de seguridad informática, los cuales gestionan los riesgos que atentan contra la disponibilidad, integridad y confidencialidad de la Información; según el Inventario de servicios tecnológicos (donde se detallan los controles de seguridad informática asociados al acceso, trazabilidad, modificación o pérdida de información) y la Matriz de riesgos (la cual detalla los aspectos que atentan contra la disponibilidad, integridad y confidencialidad de la información, junto con los controles requeridos).

- ✓ Falta de realización de actividades de monitoreo, seguimiento y evaluación de los Indicadores de Uso y Apropiación del nivel de adopción tecnológica y la satisfacción en su uso. Esta carencia de documentación también se extiende a las acciones de mejora y transformación, la medición de los indicadores de adopción tecnológica, la satisfacción en su uso, y la evolución del plan de formación y gestión del cambio.

- ✓ Ausencia de la realización de actividades de monitoreo, seguimiento y evaluación de los efectos derivados de la implantación de los proyectos de TIC y del plan de gestión de impactos de los proyectos de TIC. El monitoreo, seguimiento y evaluación de los efectos derivados de la implantación de los proyectos de TIC y del plan de gestión de impactos de los proyectos de TIC debe asegurar que estos proyectos cumplan con sus objetivos, generen los beneficios esperados y minimicen cualquier impacto negativo en la entidad. Esto implica evaluar tanto los resultados inmediatos como los efectos a largo plazo de la implantación, garantizando que los proyectos contribuyan positivamente a la eficiencia, productividad y transformación digital de la organización.

RECOMENDACIÓN

Para la revisión y seguimiento a la implementación del plan de ejecución de auditorías y

seguimiento a la gestión TIC es pertinente lo siguiente:

- ✓ Documentar e implementar las métricas para evaluar los procesos técnicos en la entidad, con el objetivo de mejorar la calidad de los productos y asegurar que los resultados sean óptimos para el ciudadano. Este documento debe detallar dos tipos de métricas: las métricas indirectas, que incluyen aspectos como calidad, complejidad, fiabilidad, eficiencia, funcionalidad y facilidad de mantenimiento, y las métricas directas, que abarcan factores como velocidad de ejecución, defectos encontrados en un periodo determinado, costo, tamaño de memoria utilizada y número de líneas de código.

- ✓ Documentar e implementar las Métricas de Seguridad para evaluar la efectividad de los procesos de seguridad en la entidad. Este documento debe medir la alineación de los procesos con las políticas internas y normativas técnicas, así como el riesgo asociado a daños físicos, económicos u otros. Las métricas deben cubrir el cumplimiento de políticas y normas, evaluación del riesgo, efectividad en salud y seguridad, identificación de vulnerabilidades, análisis de consecuencias económicas y físicas, monitoreo continuo, eficacia en la mitigación de riesgos, toma de decisiones basada en datos e identificación de áreas para mejora continua. Estas métricas asegurarán un entorno seguro y fortalecerán la resiliencia organizacional frente a incidentes imprevistos.

- ✓ Realizar acciones basadas en el seguimiento de los indicadores de la estrategia de Seguridad de la Información, incluyendo la mejora de controles, adaptación a nuevas amenazas, y realineación con los objetivos estratégicos. Esto implica aplicar medidas correctivas y preventivas, asegurar el uso eficiente de recursos, mantener el cumplimiento normativo, y evaluar la efectividad de las acciones. Además, es esencial desarrollar programas de capacitación para el personal, garantizando que la estrategia de seguridad se fortalezca continuamente y que la entidad proteja efectivamente la información crítica.

- ✓ Implementar un tablero de control con indicadores clave que permita realizar un seguimiento y evaluación periódica de la Estrategia de Seguridad de la Información. Este tablero debe ofrecer una visión integral de los avances y resultados, facilitando el análisis, el seguimiento y la toma de decisiones a nivel de objetivos estratégicos e iniciativas de seguridad, contribuyendo así al cumplimiento efectivo de la estrategia de seguridad de la entidad.

- ✓ Implementar un seguimiento riguroso de los Acuerdos de Nivel de Servicio (ANS) para el intercambio de información, garantizando el cumplimiento de estándares de calidad, oportunidad, disponibilidad y seguridad. Esto incluye verificar que la información cumpla con los requisitos de seguridad, esté disponible y sea entregada a tiempo, identificar y mitigar riesgos de incumplimiento, y mejorar los acuerdos según los resultados del seguimiento. Además, se debe asegurar el cumplimiento de normativas vigentes y establecer un mecanismo claro para la rendición de cuentas y la resolución de incumplimientos, fortaleciendo la confianza en el intercambio de información con socios externos.

- ✓ Implementar un seguimiento y gestión a los reportes de los hallazgos encontrados durante el uso de los servicios de información o reportes de incidentes a través de la Mesa de Ayuda.

- ✓ Implementar un seguimiento a los responsables de la protección y privacidad de la información, asegurando el cumplimiento de la normativa de protección de datos personales y acceso a la información pública. Esto incluye verificar que custodios y dueños cumplan con las leyes vigentes, implementen medidas adecuadas para la integridad y confidencialidad de los datos, y gestionen la información de manera transparente. Establecer mecanismos de seguimiento y evaluación continua para identificar y corregir riesgos, garantizar la capacitación de los responsables, y ajustar políticas y prácticas conforme a los desafíos regulatorios y tecnológicos. El objetivo es asegurar una gestión conforme a la ley, protegiendo derechos y garantizando un acceso adecuado a la información.

- ✓ Implementar un seguimiento y gestión de los criterios necesarios para asegurar la trazabilidad y auditoría de todas las acciones en los sistemas de información, como la creación, actualización, modificación o borrado de datos. Esto incluye garantizar que todas las acciones sean registradas y accesibles, cumpliendo con las políticas y regulaciones aplicables. Además, se debe asegurar la integridad y seguridad de los datos, facilitar auditorías, promover la rendición de cuentas, y usar la trazabilidad para identificar mejoras y fortalecer los controles.

- ✓ Implementar un seguimiento a los mecanismos que registran automáticamente todas las acciones de los usuarios en los sistemas de información. Este proceso debe asegurar que los registros sean detallados, precisos, inalterables y protegidos, facilitando auditorías y promoviendo la rendición de cuentas. Debe cumplir con normativas, detectar actividades sospechosas y utilizar los logs para mejorar la seguridad y los controles operativos, garantizando la integridad y conformidad en la gestión de la información.

- ✓ Implementar un monitoreo y evaluación exhaustivos del modelo de continuidad y seguridad para asegurar que la entidad pueda mantener operaciones esenciales durante y después de incidentes. Este proceso debe supervisar los niveles de seguridad, detectar nuevos riesgos y vulnerabilidades, y analizar tendencias en amenazas. Además, debe evaluar regularmente la efectividad de los controles, cumplir con normativas vigentes, y promover mejoras continuas en el modelo. La capacitación del personal y la documentación precisa son esenciales para asegurar la resiliencia y operatividad continua de la entidad.

- ✓ Implementar un monitoreo y evaluación constantes de las capacidades de alta disponibilidad de las infraestructuras críticas y los servicios tecnológicos, asegurando que estos se mantengan operativos y accesibles en todo momento. Este proceso debe identificar y mitigar puntos de falla, verificar la efectividad de los mecanismos de redundancia, y garantizar el cumplimiento de los Acuerdos de Nivel de Servicio (ANS). Además, debe implementar sistemas de monitoreo continuo, evaluar el impacto en la

continuidad del negocio, capacitar al personal, y mantener registros detallados para asegurar la resiliencia y minimizar el riesgo de interrupciones en los servicios esenciales.

- ✓ Implementar un monitoreo y evaluación continuos de los controles de seguridad informática para garantizar la disponibilidad, integridad y confidencialidad de la información. Este proceso debe asegurar que los controles prevengan interrupciones y accesos no autorizados, protejan la integridad de los datos, y mantengan registros detallados de todas las acciones. Además, debe verificar la eficacia de los controles frente a riesgos identificados, cumplir con normativas y políticas, y utilizar los resultados para mejorar continuamente la seguridad. Mantener documentación completa facilita auditorías y asegura un entorno seguro para la gestión de la información.

- ✓ Monitorear, seguir y evaluar los indicadores de uso y adopción tecnológica para asegurar una efectiva integración y satisfacción con las nuevas tecnologías. Esto incluye evaluar la competencia de los usuarios, identificar y abordar insatisfacciones, y ajustar estrategias de adopción y formación según las necesidades. El análisis de los indicadores debe informar mejoras en la tecnología y en el plan de gestión del cambio, garantizando que estas acciones estén alineadas con los objetivos estratégicos de la entidad. Mantener una documentación detallada asegura trazabilidad y apoya la toma de decisiones, contribuyendo a una adopción tecnológica eficiente y una mejora continua.

- ✓ Monitorear, seguir y evaluar los efectos de la implantación de proyectos de TIC y su plan de gestión de impactos. Esto incluye verificar que los proyectos cumplan con los objetivos y beneficios esperados, medir mejoras en eficiencia y calidad, y gestionar impactos negativos como interrupciones o resistencia al cambio. Asegurar la ejecución efectiva del plan de gestión de impactos, evaluar la sostenibilidad de los proyectos y registrar lecciones aprendidas para futuras iniciativas. Garantizar la conformidad con normativas y políticas, comunicar resultados a las partes interesadas, y asegurar que los proyectos contribuyan positivamente a los objetivos estratégicos y a la misión institucional.

1.7.5 MEJORA CONTINUA DE LA GESTIÓN TIC

Los resultados de la evaluación realizada a los criterios del componente "5. MEJORA CONTINUA DE LA GESTIÓN TIC", presentan un nivel de cumplimiento del 19%, lo que denota deficiencias en los aspectos evaluados, así:

HALLAZGO 26. Debilidad en la implementación del plan de mejora continua de la Gestión TIC y del Modelo de Seguridad y Privacidad de la Información (MSPI).

La revisión y análisis realizado a la implementación del plan de mejora continua de la Gestión TIC y del Modelo de Seguridad y Privacidad de la Información (MSPI), reveló que es necesario avanzar en los siguientes aspectos:

- ✓ La implementación del Plan de acción producto de la evaluación de las mediciones de los indicadores o impacto de las soluciones de TI a partir del plan de mejora continua.

- ✓ Definir el plan de acción para abordar y ajustar aquellos procesos identificados como no conformes que interactúan con la gestión de TIC y el MSPI, según las auditorías de control interno y externo realizadas.

RECOMENDACIÓN

Fortalecer la implementación del plan de mejora continua, para lo cual es pertinente Implementar el Plan de Acción basado en la evaluación de las soluciones de TI para corregir desviaciones, mejorar la eficiencia y mitigar riesgos. Alinear las mejoras con la estrategia institucional y asegurar un seguimiento continuo del progreso, evaluando el impacto en los indicadores clave. Comunicar los avances a las partes interesadas, mantener una documentación detallada, y garantizar la conformidad con normativas y mejores prácticas para maximizar el impacto positivo y la sostenibilidad de las soluciones de TI y del MSPI.

1.8 CONCLUSIONES

Como resultado de la aplicación de instrumentos de auditoría para verificar el avance y cumplimiento en la Gestión Integral del proceso de TICs de la UAE Contaduría General de la Nación, en la que se evaluó la eficacia, eficiencia y seguridad de su infraestructura tecnológica, sistemas de información, servicios de gestión de datos y procesos institucionales, se evidenció que la entidad ha venido ejecutando acciones para la implementación y gestión TIC, acorde a los lineamientos establecidos por el MinTIC, la NTC ISO 27001 y el MIPG.

Con corte a julio de 2024, se estableció que la entidad alcanzó un nivel de cumplimiento general del desarrollo de los componentes del 30%, del Modelo de Seguridad y Privacidad de la Información MSPI. Lo anterior implica que la entidad presenta oportunidades de mejora en los aspectos evaluados, los cuales se relacionaron como hallazgos en el presente informe.

Particularizando el resultado de cada uno de los 5 componentes, se observó: Para primer componente **Estrategia de Tecnologías de la Información (TI),** se obtuvo un puntaje de 34% indicando que se requieren abordar aspectos relacionados con mejoras en la infraestructura tecnológica y sistemas de información, asegurar el cumplimiento de normativas y estándares, y verificar que la Estrategia de TI optimice procesos, garantice la seguridad de la información y desarrolle el talento tecnológico, en aras de fortalecer la capacidad organizacional.

El segundo componente, denominado **Componentes Fundamentales del Modelo de Seguridad y Privacidad de la Información (MSPI)**, arrojó un puntaje de 33%. Lo anterior implica que se debe establecer la efectividad de las políticas y controles de seguridad de la información, cumpliendo con normativas y estándares, identificando riesgos, y garantizando la protección, continuidad, y capacidad de respuesta de la entidad

ante incidentes.

El tercer componente, **Aspectos Operacionales y de Gestión en Tecnologías de la Información,** presentó un nivel de avance del 32%, lo que indica que la entidad requiere impulsar acciones para mejorar la eficiencia y efectividad de los procesos operativos, la administración de recursos tecnológicos, y la gestión de servicios de TI. Esto incluye la evaluación de la capacidad para mantener la continuidad del negocio, garantizar la seguridad informática, optimizar la utilización de la infraestructura tecnológica, y asegurar que las prácticas de gestión estén alineadas con los objetivos estratégicos de la entidad.

El cuarto componente, **Planificación y Seguimiento a la Gestión TICs, registró un nivel de cumplimiento del 21%,** indicando que la entidad debería revisar y analizar que las estrategias y planes tecnológicos estén alineados con los objetivos institucionales, verificar el cumplimiento de los cronogramas y recursos asignados, y asegurar que se realice un seguimiento efectivo para medir el avance e identificar desviaciones.

Finalmente, el quinto componente, **Mejora Continua de la Gestión TICs**, **presentó un avance del 19%, lo que implica que la entidad debería** identificar oportunidades para optimizar los procesos tecnológicos, garantizar que se implementen acciones correctivas y preventivas de manera efectiva, y asegurar que las prácticas de gestión de TICs evolucionen en respuesta a los cambios en el entorno y las necesidades institucionales.

En la tabla 1, se presenta el Resultado de la verificación al avance y cumplimiento en la Gestión Integral del proceso de TICs de la CGN.

Tabla 1. Resultado de la verificación al avance y cumplimiento en la Gestión Integral del proceso de TICs de la CGN.

Componente	Nivel de Cumplimiento por Componente (%)	Nivel de Cumplimiento General (%)
1. Estrategia de Tecnologías de la Información (TI)	34	30
2. Componentes Fundamentales del Modelo de Seguridad Y Privacidad de la Información (MSPI)	33	
3. Aspectos Operacionales y de Gestión en Tecnologías de la Información	32	
4. Planificación y Seguimiento a la Gestión TICS	21	
5. Mejora Continua de la Gestión TIC	19	

Nivel de Cumplimiento	Descripción	Rango
	Deficiencias en los aspectos evaluados respecto a los riesgos de incumplimiento en la Gestión Integral del Proceso de Gestión TICs en la Entidad, los cuales no se encuentran controlados y con probabilidad de materialización alta.	<=60%
	Se identifican deficiencias en aspectos evaluados que requieren acciones o actividades dirigidas a fortalecerlas y mejorarlas; además, los riesgos de incumplimiento en la Gestión Integral del Proceso de Gestión TICs en la Entidad no se encuentran controlados y con probabilidad de materialización.	>60% - <=90%
	Cumplimiento de los aspectos evaluados por lo que se requiere acciones o actividades de mejoramiento dirigidas al mantenimiento; además, los riesgos de incumplimiento en la Gestión Integral del Proceso de Gestión TICs en la Entidad se encuentran gestionados y controlados con baja probabilidad de materialización.	>90%

Fuente: Elaboración propia.

2. INFORME DETALLADO

El enfoque de la auditoría abarcó diversos aspectos críticos, desde la gestión del talento en tecnología hasta la administración de operaciones y desarrollo de software, poniendo especial énfasis en la seguridad informática, la continuidad del negocio y la capacitación de los usuarios. A continuación, se expone en detalle el resultado.

2.1 ASPECTOS OPERACIONALES Y DE GESTIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Como resultado del ejercicio de arquitectura empresarial, la entidad debe establecer la estrategia de tecnología de la información respecto a sus servicios tecnológicos (infraestructura tecnológica), sistemas de información, servicios de gestión de información y procesos institucionales; lo anterior implica, la gestión del talento humano el cual debe partir de una línea base, respecto a las capacidades y recursos de tecnologías de la información disponibles en la entidad. Teniendo en cuenta está línea se debe proyectar a mediano y largo plazo, las necesidades de talento humano y recursos requeridos para dar cumplimiento de la estrategia.

2.1.1 Criterio evaluado Capacidades y recursos de TI - LI.GO.05

La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe generar, direccionar, evaluar y monitorear las capacidades de TI, asegurando el adecuado aprovisionamiento del talento humano y los recursos necesarios para ofrecer los servicios de TI de la institución.

Resultado:

Para evaluar el nivel de cumplimiento de la estrategia de gestión del talento en tecnología, incluyendo la identificación de habilidades críticas, el reclutamiento y retención de personal calificado, y la implementación de programas de capacitación y desarrollo profesional en especial los relacionados con la seguridad informática y el uso de apropiación de las Tecnologías de la Información y las Comunicaciones (TIC), se realizaron mesas de trabajo, con el equipo designado por el líder del proceso, y se analizaron los soportes documentales presentados por los auditados (“MediciónCapacidad-032024.xls” y “PLAN DE CAPACIDAD DE LOS SERVICIOS DE TI”), el resultado se expone a continuación:

- ✓ Revisado el archivo “MediciónCapacidad-032024.xls”, se observó una serie de mediciones para los servicios de Red, Plataforma de comunicaciones, Internet, Servidores de Gestión, Servidores Misionales, Portátiles, Computadores Personales (PC), Escritorio Virtual, Telefonía IP, Ofimática, Orfeo, Chip, Portal Web, Repositorio, Correo electrónico, Soporte técnico HW, Soporte Desarrollo SW, Mesa de servicio, Plataforma de capacitación, SISCON y Soporte teletrabajo.

  Para cada uno de los servicios, se presentan mediciones en términos de Capacidad del Servicio, Capacidad de la Infraestructura y Nivel de Importancia. Además, se detallan

los elementos que conforman y afectan cada servicio. Asimismo, se observó un diagrama a manera de grafos para cada servicio y sus componentes, donde se establecen las relaciones e interacciones de cada uno de los componentes del servicio.

Según lo indicado por los auditados, las mediciones se establecen basándose en los resultados obtenidos en cortes específicos, de acuerdo con el servicio prestado. Estas mediciones consideran tanto los tiempos y esfuerzo de operación ejecutados por los proveedores y por los profesionales del GIT de Apoyo Informático.

Como resultado del análisis a los documentos "MediciónCapacidad-032024.xls" y "PLAN DE CAPACIDAD DE LOS SERVICIOS DE TI", se evidenció:

HALLAZGO

Al revisar y analizar el documento "PLAN DE CAPACIDAD DE LOS SERVICIOS DE TI", cuyo objetivo es: "***Elaborar un plan de acción que facilite la gestión de las capacidades de los servicios*** *clave de TI proporcionados por el GIT de Apoyo Informático para toda la CGN*" (negrilla fuera de texto), se observó que no cubre todos los aspectos y requerimientos del Marco de Referencia de la Arquitectura Empresarial (MRAE) de MinTIC, dejando fuera de su gestión aspectos importantes relacionados con la capacidad y gestión de la Información, los Sistemas de Información y el Uso y apropiación de los servicios TIC.

El documento, en su forma actual, corresponde a un plan de acción para la gestión de capacidades y no a un plan integral de las capacidades de TI requeridas para la prestación de los servicios de TI. Además, no incluye las proyecciones de capacidad de TI necesarias para el futuro funcionamiento de la entidad, según una estrategia de TI establecida por esta. Además, el objetivo descrito en el documento es una iniciativa propia del GIT de Apoyo Informático que fue elaborado sin la participación transversal de la alta y media gerencia, líderes de procesos o dueños de activos de información.

RECOMENDACIÓN

La entidad debe establecer e implementar el Plan de Capacidad de Tecnologías de Información (TI) teniendo en cuenta los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en su lineamiento LI-GO.05 - Capacidades y recursos de TI del "Modelo de Gestión y Gobierno TI (MGGTI)", de tal manera que involucre a todas las partes interesadas relevantes para asegurar que se aborden las necesidades institucionales y el plan se alinee a los objetivos estratégicos de la entidad.

2.1.2 Criterio evaluado: Seguridad informática – LI.ST.15

La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar controles de seguridad informática para gestionar los riesgos que atenten contra la disponibilidad, integridad y confidencialidad de la Información.

RESULTADO

Para efectos de verificación de cumplimiento del criterio se revisaron tres documentos entregados por el auditado, a saber: "Acuerdo de confidencialidad_MAN01-FOR31.pdf", "GTI010-FOR02 - Solicitud de cuentas de usuario institucional.pdf" y "Induccion_Aula Virtaul.png".

Revisados los documentos mencionados en el párrafo anterior se evidenció que:

a. El "Acuerdo de confidencialidad_MAN01-FOR31" es un documento donde se establecen los términos y condiciones bajo los cuales las partes (Contratante y Contratista) mantendrán la confidencialidad de los datos e información intercambiados con la U.A.E. Contaduría General de la Nación (CGN). El contratista se compromete a no revelar, divulgar, exhibir, mostrar, comunicar, utilizar y/o emplear la información recibida de la CGN en beneficio propio o de terceros, garantizando su confidencialidad y privacidad. Asimismo, el contratista debe proteger dicha información para evitar su divulgación no autorizada, ejerciendo el mismo grado de diligencia que utiliza para proteger su propia información confidencial.

   HALLAZGO

   El acuerdo de confidencialidad no proporciona las directrices en relación con los roles de cada individuo, como parte activa de la entidad; toda vez que excluye la entrega de políticas, procedimientos, protocolos y guías; entre otros, que definan de manera detallada las responsabilidades y prácticas recomendadas para garantizar la protección de la información institucional.

   Si bien el acuerdo de confidencialidad es crucial para asegurar que los contratistas gestionen adecuadamente la información sensible, es importante aclarar que este documento, por su naturaleza física y conceptual, no informa a los servidores públicos, colaboradores y proveedores sobre sus roles y responsabilidades específicas en materia de seguridad informática.

   RECOMENDACIÓN

   Establecer estrategias para que los servidores públicos, colaboradores y proveedores conozcan e interioricen la seguridad informática antes de que se les otorgue acceso a información o sistemas de información. Estas deben abarcar aspectos de seguridad operativa y privacidad de la información, asegurando que los involucrados comprendan plenamente las políticas, procedimientos, protocolos, y responsabilidades sobre seguridad informática de la entidad.

b. GTI010-FOR02 - Solicitud de cuentas de usuario institucional. Se observó que el contenido del formato se utiliza para solicitar la creación de una Cuenta de usuario; Buzón de correo; Acceso a ORFEO, Intranet, SIGI, GLPI, Impresora, IBM COGNOS, servidor de archivos y la creación de otros usuarios.

c. Inducción_Aula Virtual: Documento en formato imagen, en el cual se observó que para la inducción de los funcionarios se disponen dos (2) cursos en formato virtual: Uso, beneficios y acceso a la Intranet; y Uso adecuado de la VPN en la CGN.

De acuerdo a lo comentado por los auditados, el Aula Virtual es el aplicativo utilizado por la entidad para proveer capacitaciones en formato virtual para los funcionarios de la entidad. También indicaron que la capacitación de inducción o reinducción solo se realiza para los funcionarios de la entidad, excluyendo a los contratistas y proveedores.

HALLAZGO

a. No se evidenció que en las presentaciones de los cursos de inducción y reinducción se incluyeran módulos específicos sobre seguridad informática. Adicionalmente, según las evidencias aportadas por los auditados y a lo comentado por ellos, la entidad no ha establecido un programa de capacitaciones en seguridad informática en el aula virtual u otros medios de capacitación al respecto.

RECOMENDACIÓN

Con el ánimo de mitigar el riesgo vulneración a la seguridad de la información a entidad debería implementar programas de capacitación y concientización específicos en seguridad informática dirigidos a todos los servidores, colaboradores y proveedores (según aplique). Estos programas deben abarcar aspectos de seguridad operativa, privacidad y seguridad de la información.

b. Revisados los documentos **"**Acuerdo de confidencialidad_MAN01-FOR31.pdf", "GTI010-FOR02 - Solicitud de cuentas de usuario institucional.pdf" y "Induccion_Aula Virtaul.png", se evidenció que estos no constituían por sí mismos un control de seguridad informática para gestionar los riesgos que atenten contra la disponibilidad, integridad y confidencialidad de la Información. Es de recordar que por definición el control "es el proceso que consiste en supervisar las actividades para garantizar que se realicen según lo planeado y corregir cualquier desviación significativa" En Robbins y Coulter (2014).

RECOMENDACIÓN

Implementar controles de seguridad informática para gestionar los riesgos que atenten contra la disponibilidad, integridad y confidencialidad de la Información.

2.1.3 Criterio evaluado: Procedimiento de Gestión de Usuarios y Contraseñas

Documento con las especificaciones de creación de usuarios y la asignación de contraseñas (las cuales deberán tener un nivel de seguridad aceptable, con base a una política de contraseñas seguras definidas previamente), prohibiendo su reutilización posterior, permitiendo a los usuarios cambiarla regularmente, llevando un registro de las mismas. Este procedimiento debe aplicar a todos los sistemas de información, también se debe tener en cuenta el rol que cada usuario requiera en los determinados sistemas, para

brindar el acceso necesario.

RESULTADO

Para efectos de la prueba el auditado entregó los siguientes documentos: GTI010-FOR02 - Solicitud de cuentas de usuario institucional_V.04: Formato titulado SOLICITUD DE CUENTASS DE USUARIO INSTITUCIONAL" y "GTI-PRC10 Seguridad de la Información.pdf"

a. GTI010-FOR02 - Solicitud de cuentas de usuario institucional_V.04: Formato titulado SOLICITUD DE CUENTASS DE USUARIO INSTITUCIONAL", este formato fua analizado en el ítem anterior.

b. GTI-PRC10 Seguridad de la Información: Procedimiento que establece las actividades de seguridad de la información, privacidad y seguridad digital para asegurar, salvaguardar y mantener la integridad, disponibilidad, confidencialidad y privacidad de la información, de la infraestructura tecnológica, servicios de TI y sistemas de información, acorde a las políticas y lineamientos de seguridad y ciberseguridad aplicables a la Contaduría General de la Nación.

HALLAZGO

Verificado el cumplimiento del criterio con las evidencias presentadas por el auditado se evidenció que no se dispone de un documento específico que contenga las especificaciones detalladas del Procedimiento de Gestión de Usuarios y Contraseñas, debidamente aprobado por la alta dirección y socializado al interior de la entidad.

RECOMENDACIÓN

Implementar el procedimiento de Gestión de Usuarios y Contraseñas teniendo en cuenta los requisitos establecidos en la NTC ISO 27001 y en las Guías MSPI de MinTIC.

2.1.4 Criterio evaluado: procedimiento de gestión de capacidad

Documento con las especificaciones de cómo la entidad realiza una gestión de la capacidad para los sistemas de información críticos, en especial si los recursos requeridos son escasos, demorados en su arribo o costosos. La entidad puede realizar acciones como la eliminación de datos obsoletos, cierre de aplicaciones, ambientes y sistemas en desuso, restricción de ancho de banda etc.

RESULTADO

Evidencia aportada: GTI-PRC10 Seguridad de la Información. Su descripción se realizo en el ítem anterior.

HALLAZGO

Analizado el contenido del procedimiento "GTI-PRC10 Seguridad de la Información" se

evidenció que este no correspondía al procedimiento de Gestión de la Capacidad, acorde a lo establecido en el criterio que se evaluó.

RECOMENDACIÓN

Implementar el procedimiento de Gestión de la Capacidad, teniendo en cuenta los requisitos establecidos en la NTC ISO 27001 y en las Guías MSPI de MinTIC.

2.1.5 Criterio evaluado: Estrategia de planificación y control operacional, revisada y aprobada por la alta Dirección

Documento con el plan de tratamiento de riesgos, donde se identifique el desarrollo mínimo de los siguientes temas.

- Objetivos.
- Alcance.
- Marco referencial.
- Metodología que contemple la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos,
- Definición de las medidas de seguridad identificadas para desarrollar e implementar.
- Plan de tratamiento para los riesgos de Seguridad y Privacidad de la Información.
- Plan de implementación de la Seguridad Digital.
- Plan de la implementación de la Continuidad de la Operación.
- Plan de Tratamiento de Riesgos que mitigan los riesgos presentes en el análisis de riesgos (Perdida de la Confidencialidad de los activos, Perdida de Integridad de los activos y Perdida de Disponibilidad de los activos).
- Oportunidades de mejora.
- En el marco de la gestión de riesgos de seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, disposición de los recursos Humanos, Técnicos, Logísticos y Financieros.
- Estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la información identificados en la entidad.
- Especificaciones de la medición del modelo de seguridad y privacidad de la información.

Acto administrativo mediante el cual fue revisado y aprobado por la alta Dirección el plan de tratamiento de riesgos.

RESULTADO

Documentos aportados:

- ACTA No. 1 CIGD 2024: Acta No. 1 del Comité Institucional de Gestión y Desempeño de la CGN, con fecha del 17 de enero del 2024.
- Acta No. 15 CIGD - diciembre 15 de 2022: Acta No. 15 del Comité Institucional de Gestión y Desempeño de la CGN, con fecha del 15 de diciembre del 2022.
- Matriz Riesgos Seguridad de la Información: Archivo en formato Excel de Microsoft

denominado "Matriz Riesgos Seguridad de la Información".
- PlanDeTratamientoDeRiesgos: Documento titulado "PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN".
- POLITICA DE ADMINISTRACION RIESGO: Documento titulado "POLÍTICA DE ADMINISTRACIÓN DEL RIESGO". El documento esta versionado en mayo del 2023 por el GIT de Planeación.

HALLAZGO

Revisados los documentos aportados por el auditado y verificado su contenido frente a los lineamientos del criterio, en relación con el plan de tratamiento de riesgos digitales o de seguridad de la información, se observó que éstos no contemplaban el desarrollo mínimo de los temas que especifica el criterio.

RECOMENDACIÓN

En el momento de diseñar la Estrategia de Planificación y Control Operacional tener en cuenta que el plan de tratamiento de riesgos hace parte integral de la misma; por lo tanto, es procedente tener presente los lineamientos establecidos por el criterio.

2.1.6 Criterio evaluado: Plan Integral de Gestión de Riesgos, Plan Mejora Continua en Seguridad de la Información y Plan Continuidad Operacional

Verificación de la existencia, implementación, ejecución y apropiación de los planes estratégicos, asegurando que estén debidamente documentados, implementados, integrados y alineados con los lineamientos del MSPI y MIPG y lo establecido en la Estrategia de planificación y control operacional; cobija los planes relacionados a continuación:

- Plan de Tratamiento para los Riesgos de Seguridad y Privacidad de la Información.
- Plan de Implementación de la Seguridad Digital.
- Plan de Implementación de la Continuidad de la Operación.
- Plan de Tratamiento de Riesgos Mitigadores.
- Plan de Atención a las Oportunidades de Mejora.

RESULTADO

Documentos aportados:

- Matriz Riesgos Seguridad de la Información.xls: El documento contiene dos secciones: una que describe 23 riesgos asociados a activos, amenazas, vulnerabilidades y sus consecuencias, y otra que detalla el tratamiento de estos riesgos, incluyendo opciones de control, evaluación del riesgo residual y medidas de seguimiento. Los riesgos abordan aspectos relacionados con hardware, software, servicios, información y talento humano, evaluando tanto el riesgo inherente como el residual después de implementar controles.

- PlanContinuidadNegocio-2022: Documento con el plan de continuidad de negocio de TI de la UEA Contaduría General de la Nación (CGN).

- POLITICA DE ADMINISTRACION RIESGO: Documento titulado "POLÍTICA DE ADMINISTRACIÓN DEL RIESGO". El documento establece lineamientos para la administración de riesgos en la Unidad Administrativa Especial (UEA) Contaduría General de la Nación (CGN.

HALLAZGO

Revisados los documentos Matriz Riesgos Seguridad de la Información, el Plan de continuidad del negocio y el Plan de continuidad del negocio y, verificado su contenido frente a los lineamientos del criterio, en relación con la existencia, implementación, ejecución y apropiación del plan Integral de Gestión de Riesgos, Plan Mejora Continua en Seguridad de la Información y Plan Continuidad Operacional, debidamente documentados, implementados, integrados y alineados con el MSPI y MIPG, se observó que no contemplan los planes establecidos en el criterio.

RECOMENDACIÓN

Implementar, ejecutar y apropiar los planes indicados en el criterio, teniendo en cuenta los requisitos establecidos en la NTC ISO 27001, las Guías MSPI de MinTIC y las guías del MIPG del DAFP.

2.1.7 Criterio evaluado: Ejecución Presupuestal y Financiera en la Gestión de Recursos y Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Verificación de la existencia y suficiencia de la ejecución presupuestal y financiera relacionada con:

- Disposición y asignación de recursos humanos, técnicos, logísticos y financieros.
- Implementación y seguimiento del presupuesto destinado al plan de tratamiento de riesgos de Seguridad y Privacidad de la Información.

Evaluar si los recursos han sido gestionados conforme a los planes y presupuestos establecidos por la entidad.

RESULTADO

Documentos aportados:

- ✓ Proyecto FORTALECIMIENTO DE LA PLATAFORMA TECNOLÓGICA PARA LA PRESTACIÓN DE LOS SERVICIOS DE LA CGN NACIONAL.

- ✓ Plan Anual de Adquisiciones versión 12, publicado en SECOP II.

Como resultado de la revisión de los documentos y las mesas de trabajo realizadas con el

equipo designado por el GIT de Apoyo Informático, se evidenció que la entidad ha venido gestionando los recursos, orientados en su mayoría al fortalecimiento del Sistema CHIP.

OPORTUNIDAD DE MEJORA

Proyectar la gestión de los recursos de tal manera que se evidencie, el cumplimiento a cabalidad del criterio *Ejecución Presupuestal y Financiera en la Gestión de Recursos y Tratamiento de Riesgos de Seguridad y Privacidad de la Información*, acorde a los lineamientos establecidos en la NTC ISO 27001, MinTIC y MIPG.

2.1.8 Criterio evaluado: Evaluación sobre la Implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) y su Alineación con la Estrategia de Planificación y Control Operacional

Verificación de la existencia y calidad de la evidencia documental que respalde las mediciones realizadas sobre la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), asegurando su alineación con la estrategia de planificación y control operacional de la entidad.

RESULTADO

Documentos aportados:

InstrumentoDeclaracionSGSI 2023.xls, InstrumentoDeclaracionSGSI 2023_V6.xls, TIC-SEG-SGS-HDG-Instrumentodeevaluación 2022.xls y TIC-SEG-SGS-HDG-Instrumentodeevaluación 2022_v01.xls: Documentos titulados "INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD".

Revisados los soportes documentales y comparados frente al criterio se evidenció que la entidad realizó el diagnóstico haciendo uso de las herramientas dispuestas por MinTIC.

HALLAZGO

Como resultado de la revisión a los soportes documentales se evidenció que la entidad no ha realizado una adecuada medición del estado de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), toda vez que ha llevado a cabo es la actualización del diagnóstico lo que no se constituye en una medición de implementación del modelo.

La herramienta de diagnóstico de seguridad y privacidad de la información de MinTIC, está dirigida a entidades públicas de orden nacional y territorial, así como a proveedores de servicios de Gobierno Digital y terceros interesados en adoptar el Modelo de Seguridad y Privacidad de la Información (MSPI) dentro del Programa Gobierno Digital, con el fin de realizar un diagnóstico para comprender el estado actual de seguridad y privacidad de la información. A partir de este diagnóstico, cada entidad puede generar un plan de seguridad de la información específico, que debe ser implementado internamente.

RECOMENDACIÓN

Para evaluar adecuadamente el estado y los avances en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) y su alineación con la estrategia de planificación y control operacional, se deben utilizar indicadores específicos diseñados para este propósito. Es esencial que las mediciones de efectividad y progreso del MSPI se realicen utilizando herramientas y métricas que reflejen claramente el cumplimiento de los objetivos y estándares de seguridad establecidos en el MSPI y en la estrategia de planificación y control operacional.

2.1.9 Criterio evaluado: Documento de Declaración de Aplicabilidad del Anexo A de la Norma NTC: ISO/IEC 27001: Objetivos de Control, Controles Seleccionados, Justificación de Exclusiones y Aprobación por la Alta Dirección.

Documento donde en su contenido se especifique los objetivos de control y controles seleccionados del estándar de controles correspondientes al Anexo A de la norma NTC: ISO/IEC 27001, las razones por las cuales han sido seleccionados y medidas de seguridad adicionales si es el caso.

También, debe indicar si los objetivos de control y controles se encuentran implementados y operando, los que hayan sido descartados, así como una justificación del porqué algunas medidas han sido excluidas (las que son innecesarias y la razón del porqué no son requeridas en una organización).

Acto administrativo mediante el cual fue revisado y aprobado por la alta Dirección la Declaración de aplicabilidad.

RESULTADO

Documentos aportados:

InstrumentoDeclaracionSGSI 2023.xls y TIC-SEG-SGS-HDG-Instrumentodeevaluación 2022_v01.xls: Documentos titulados “INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD”. La descripción del contenido de estos documentos se realizó en el punto anterior.

HALLAZGO

Revisadas las evidencias no se observaron documentos que demuestren la implementación política independientes, tales como: la Política de Control de Acceso, Política de Seguridad de los Activos de Información, Política de Criptografía y Política de Antivirus y Antimalware, que deben ser aprobadas por la alta dirección y debidamente documentadas. Como tampoco un acto administrativo que confirme la revisión y aprobación de la Declaración de aplicabilidad por parte de la alta dirección; acorde a lo indicado en el control establecido por la norma NTC ISO/IEC 27001, en el control A.5.1.1.

RECOMENDACIÓN

En aras de mitigar el riesgo de riesgo de pérdida o daño de activos es procedente que la entidad diseñe e implemente políticas independientes de seguridad de la información, incluyendo la Política de Control de Acceso, Política de Seguridad de los Activos de Información, Política de Criptografía, y Política de Antivirus y Antimalware; las cuales deben ser aprobadas por la alta dirección y contar con elementos esenciales como Introducción, Objetivo, Alcance, Condiciones de Implementación, Roles y Responsabilidades. Esto garantizará la alineación con los estándares establecidos y fortalecerá el control interno sobre la seguridad de la información y cumpliría con los requisitos de la norma NTC: ISO/IEC 27001.

2.1.10 Criterio evaluado: Documento detallado con el plan de transición e implementación del protocolo IPv6 en la entidad

Documento con el plan de transición e implementación del protocolo IPv6 en la entidad, en donde se especifique:

- Introducción y Objetivos.
- Alcance del Plan.
- Análisis de Impacto.
- Estrategia de Implementación.
- Recursos y Responsabilidades.
- Procedimientos de Configuración y Pruebas.
- Plan de Formación y Capacitación.
- Plan de Comunicación.
- Gestión de Riesgos.
- Revisión y Evaluación.
- Documentación y Reportes.

RESULTADO

Documentos aportados:

- Diagnostico Para La Adopción de IPv6 - Contaduría General de la Nación.pdf. Documento titulado "DIAGNÓSTICO PAR A LA ADOPCIÓN DE IPv6". El documento describe el diagnóstico del estado, en su momento, de la Infraestructura de TI de Contaduría General de la Nación, para preparar el proceso de adopción del nuevo protocolo IPv6.

- Modelamiento - Transición protocolo IPv6.pdf: Documento titulado "MODELAMIENTO DE LA APLICACIÓN PARA LA TRANSICION DE IPV4 A IPV6". El documento describe los aspectos esenciales para la implementación del protocolo IPv6 en la red de datos de la Contaduría General de la Nación (CGN). Se detalla el proceso de modelamiento de configuraciones en la plataforma de red de datos y servidores. Estas configuraciones se aplican exclusivamente al entorno local de la red y, en el momento de la revisión, no incluyeron capacidades de enrutamiento hacia los servicios de internet; esto se

debió a la falta del pool de direcciones IPv6 globales que la CGN debía adquirir.

Asimismo, el documento expone el mecanismo de transición a utilizar, basado en Doble Pila (Dual Stack). Este mecanismo requiere que tanto los nodos como los enrutadores de nivel 3 estén habilitados para enviar y recibir paquetes de ambos protocolos, IPv4 e IPv6. Cada nodo configurado en esta modalidad posee direcciones para ambos protocolos y obtiene su direccionamiento mediante un servidor DHCP configurado para IPv4 e IPv6.

- Plan Proyecto Contaduría.pdf: Documento titulado "Cronograma detallado". El documento presenta la planeación de actividades relacionadas con la implementación del IPv6 en la CGN como: Formalización acta de inicio de contrato; Kick Off; Plan para la Dirección de Desarrollo y Ejecución del Proyecto; y Levantamiento activos información, entre otras.

De acuerdo con las evidencias aportadas por los auditados, y verificado su contenido frente a los lineamientos del criterio, en relación con el plan de transición e implementación del protocolo IPv6 en la entidad, se observó la disposición del plan de transición e implementación del protocolo IPv6 en la CGN según lo establecido en el criterio.

2.1.11 Criterio evaluado: Ejecución de la Fase de Planeación de IPv6

Ejecución de la Fase de Planeación de IPv6, con respecto a las actividades de:

- Construcción del plan de Diagnóstico.
- Inventario de TI (Hardware, Software)
- Análisis de la nueva topología de la infraestructura actual y su funcionamiento.
- Protocolo de pruebas de validación de aplicativos, comunicaciones, plan de seguridad y coexistencia de los protocolos.
- Planeación de la transición de los servicios tecnológicos de la Entidad.
- Validación de estado actual de los sistemas de información, los sistemas de comunicaciones, las interfaces y revisión de los RFC correspondientes.
- Identificación de esquemas de seguridad de la información y las comunicaciones.

RESULTADO

Documentos aportados:

Diagnostico Para La Adopción de IPv6 - Contaduría General de la Nación.pdf: La descripción del contenido del documento se realizó en el punto anterior.

De acuerdo con las evidencias aportadas por los auditados, y verificado su contenido frente a los lineamientos del criterio, en relación con la ejecución de la Fase I, Planeación de IPv6, se observó el cumplimiento de lo indicado en el criterio.

2.1.12 Criterio evaluado: Fase de Pruebas de funcionalidad de IPv6

Ejecución de la Fase de Pruebas de funcionalidad de IPv6, con respecto a las actividades de:

- Pruebas de funcionalidad y monitoreo de IPv6 en los servicios de la Entidad.
- Análisis de información y pruebas de funcionalidad frente a las políticas de seguridad perimetral de la infraestructura de TI.
- Afinamiento de las configuraciones de hardware, software y servicios de la Entidad.

RESULTADO

Documentos aportados:

- 1 – AIX.xls y Actividades de configuración.xls y pruebas.xls: Documentos titulados "DOCUMENTO DE CONFIGURACIÓN, Recursos Técnicos Involucrados, Cronograma de Actividades para Ejecución, respectivamente. Los documentos contienen información detallada sobre la ejecución de actividades, incluyendo datos como número, ejecutor, área responsable, equipos involucrados, tiempo de ejecución, fechas de inicio y finalización, y un checklist. Entre las actividades descritas se encuentran validaciones y configuraciones de cadenas de conexión a bases de datos y APIs externas utilizando nombres de dominio, pruebas de conectividad en IPv4, y la preparación de un plan de pruebas para verificar el funcionamiento de los sistemas de información.

- actahorasipv6_11302021_042914.pdf: Documento correspondiente al acta de ejecución suscrita con MCOglobal y la CGN para certificar las horas ejecutadas respecto al apoyo especializado IPV6 asociada a la orden No. 16 del 2021. En esta acta se observó la descripción de horas que fueron ejecutadas como parte del contrato.

- PRUEBAS DE FUNCIONALIDAD.pdf: Documento titulado "PRUEBAS DE FUNCIONALIDAD – SERVICIOS DNS Y DHCP". El documento registra las actividades desarrolladas para comprobar la configuración de IPv6 sobre los servidores de AD BESTLA y GALILEO. Además, de actividades para realizar pruebas a las configuraciones faltantes de: DHCPv6, DNS, Servicios de Internet, Funcionalidad página WEB, y Funcionalidad ORFEO.

De acuerdo con las evidencias aportadas por los auditados, y verificado su contenido frente a lo establecido por el criterio, en relación con la ejecución de la Fase de Pruebas de funcionalidad de IPv6, se observó el cumplimiento de lo establecido en el criterio.

2.1.13 Criterio evaluado: Implementación del protocolo IPv6

Evidencia documental de la ejecución de la implementación del protocolo IPv6, con respecto a las actividades de:

- Habilitación direccionamiento IPv6 para cada uno de los componentes de hardware y

software de acuerdo al plan de diagnóstico de la Primera Fase.
- Configuración de servicios de DNS, DHCP, Seguridad, VPN, servicios WEB, entre otros.
- Configuración del protocolo IPv6 en aplicativos, sistemas de Comunicaciones, sistemas de almacenamiento y en general de los equipos susceptibles a emplear direccionamiento IP.
- Activación de políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea cada entidad de acuerdo con los RFC de seguridad en IPv6.
- Coordinación con el (los) proveedor (es) de servicios de Internet ISP, para establecer el enrutamiento y la conectividad integral en IPv6 hacia el exterior.

RESULTADO

Documentos aportados:

- Direccionamiento IPV6 Segmentado V2.xls. El documento incluye varias secciones y hojas de trabajo tales como "Segmentación", "RED 42 ->48", "RED 48 ->49", "Red Usuario", "64 Internet Usuarios", "64 Vlan 10" y "64 Vlan 35". La sección "Segmentación" presenta un diagrama jerárquico que ilustra la distribución de direcciones IPv6 y segmentos de la red de la CGN. Otras secciones contienen información detallada sobre direcciones IP, redes, host menor y mayor, tipo de asignación de prefijo, IPv4, último octeto, hexadecimal, IPv6, y la asignación a diferentes componentes o usuarios.

- Diseño Logico de Red Implemetar V1.pdf: El documento incluye diagramas del diseño lógico de la red, detallando las direcciones IPv6 de la Contaduría General de la Nación (CGN). Los documentos titulados "Diseño Lógico Red-IPV6_LACNIC" y "Diseño Red Implementación V2" tienen una fecha de versión del 1 de septiembre de 2020. Estos documentos muestran la segmentación de la red para diferentes áreas, como Secretaría General, Financiera, VozIP, y Jurídica, entre otras.

- LoA ISP.pdf. El documento presenta la descripción de un correo electrónico dirigido a Media Commerce, confirmando la adquisición ante LACNIC, un bloque de direcciones IPv6, con las direcciones: 2801:1e6::/44. Además, se confirma que, dentro del proceso, se adquirió el sistema autónomo (AS271826).

- Membresía LACNIC.pdf: Documento titulado "Membresía LACNIC", con fecha de versionamiento del 24 de noviembre del 2020 y elaborado por RealTime Consulting & Services, el cual contiene las evidencias generadas del proceso de adquisición del prefijo IPv6 y el ASN para la Contaduría General de la Nación, en el marco del contrato GTI04-FOR02.

- Monitoreo Seguridad -redes-Servidor.pdf: Documento titulado "Plan de Implementación Seguridad y redes", elaborado por RealTime Consulting & Services, el cual contiene las evidencias de las configuraciones realizadas en los equipos de red, seguridad y servidores de la red de la Contaduría General de la Nación. Además, el documento describe la información de las actividades que se llevaron a cabo en cada uno de los equipos computacionales para configurar su respectivo direccionamiento

según lo indicado en el plan de direccionamiento IPv6.

- Plan de Implementación Seguridad -redes-Servidor.pdf: Documento titulado "Plan de Implementación Seguridad y redes", con fecha de versionamiento del 5 de octubre del 2020 y elaborado por RealTime Consulting & Services, el cual describe el avance que se realizó en cuanto a la ejecución del proyecto de Diagnóstico de la red de seguridad de la entidad CGN en el marco de la consultoría de diagnóstico y realización de un plan para la implementación del protocolo de internet IPV6 en la entidad.

De acuerdo con las evidencias aportadas por los auditados, y verificado su contenido frente a lo establecido por el criterio, en relación con la ejecución de la implementación del protocolo IPv6, se observó el cumplimiento de lo establecido en el criterio.

2.1.14 Criterio evaluado: Política del uso de redes y de servicios de red.

Disponer de la política relacionada con el uso de redes y de servicios de red, la cual como mínimo debe incluir:

- Las redes y servicios de red a los que se permite el acceso.
- Los procedimientos de autorización para determinar a quién se permite el acceso a qué redes y servicios de red.
- Los controles y procedimientos de gestión para proteger el acceso a las conexiones de red y a los servicios de red.
- Los medios usados para acceder a las redes y servicios de red (uso de VPN o redes inalámbricas).
- Los requisitos de autenticación de usuarios para acceder a diversos servicios de red.
- El seguimiento del uso de servicios de red.

RESULTADO

Documentos aportados:

- GTI010-FOR02- Natali Rios.pdf: Formato titulado "SOLICITUD DE CUENTAS DE USUARIO INSTITUCIONAL", el cual se utiliza para solicitar la creación de una Cuenta de usuario; Buzón de correo; Acceso a ORFEO, Intranet, SIGI, GLPI, Impresora, IBM COGNOS, y servidor de archivos; y la creación de otros usuarios.

- GTI010-FOR04 - Solicitud de cuentas de usuario institucional - VPN Juan Sebastian Olaya Perdomo-.pdf: Formato titulado "SOLICITUD DE CUENTAS DE USUARIO INSTITUCIONAL - VPN", el cual se utiliza para solicitar la habilitación del servicio de Red Privada Virtual (VPN, por sus siglas en inglés) como una conexión que se establece entre los recursos informáticos de la entidad y el recurso utilizado por las personas autorizadas para realizar dicho enlace del Internet de la entidad.

- GTI10-POL01 - Política de Acceso a la Red Privada Virtual de la CGN.pdf: El documento establece lineamientos para guiar a los funcionarios, contratistas y colaboradores en el uso correcto del servicio de VPN institucional y otros

mecanismos de acceso remoto a los servicios proporcionados por la Contaduría General de la Nación. Detalla las características y requerimientos mínimos que deben cumplirse y las implicaciones asociadas al mal uso de estos servicios.

- GTI10-POL03 - Política para el uso de la red inalámbrica pública en la CGN.pdf: El documento establece lineamientos a seguir para el acceso y uso apropiado de las zonas establecidas de internet inalámbrico, aplicables a todos los usuarios que utilicen el servicio proporcionado por la Contaduría General de la Nación.

- GTI-PRC10 Seguridad de la Información.pdf: Procedimiento que establece las actividades de seguridad de la información, privacidad y seguridad digital para asegurar, salvaguardar y mantener la integridad, disponibilidad, confidencialidad y privacidad de la información, de la infraestructura tecnológica, servicios de TI y sistemas de información, acorde a las políticas y lineamientos de seguridad y ciberseguridad aplicables a la Contaduría General de la Nación.

HALLAZGO

Como resultado de la revisión de las evidencias y contrastadas frente al criterio, no se identificó un documento que contenga las especificaciones detalladas de la Política de Acceso a redes y a servicios en red, debidamente aprobado por la alta dirección y socializado al interior de la entidad. Esta política debe incluir elementos esenciales como Introducción, Objetivo, Objetivos específicos, Alcance, Condiciones de implementación, Roles y Responsabilidades, entre otros aspectos. La Política como mínimo debe establecer lineamientos para los ítems indicados en el criterio.

RECOMENDACIÓN

Desarrollar, revisar, contextualizar, aprobar, implementar y apropiar la Política del Uso de Redes y de Servicios de Red, teniendo en cuenta los requisitos establecidos en la NTC ISO 27001, las Guías MSPI de MinTIC y las guías del MIPG del DAFP.

2.1.15 Criterio evaluado: Política Relaciona con los Perímetros de Seguridad Física

Disponer de la política relacionada con los perímetros de seguridad física, la cual como mínimo debe incluir:

- Definir los perímetros de seguridad, y el emplazamiento y fortaleza de cada uno de los perímetros deben depender de los requisitos de seguridad de los activos dentro del perímetro y de los resultados de una valoración de riesgos.
- Establecer los perímetros de una edificación o sitio que contenga instalaciones de procesamiento de la información debe ser físicamente seguros; el techo exterior, las paredes y el material de los pisos del sitio deben ser de construcción sólida, y todas las paredes externas deben estar protegidas adecuadamente contra acceso no autorizado con mecanismos de control (barras, alarmas, cerraduras); las puertas y ventanas deben estar cerradas con llave cuando no hay supervisión, y se debe

considerar protección externa para ventanas, particularmente al nivel del suelo.

- Definir un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o edificación; el acceso a los sitios y edificaciones debe estar restringido únicamente para personal autorizado.
- Establecer cuando sea aplicable y construir barreras físicas para impedir el acceso físico no autorizado y la contaminación ambiental.
- Establecer que todas las puertas contra incendio en un perímetro de seguridad deben tener alarmas, estar monitoreadas y probadas junto con las paredes, para establecer el nivel requerido de resistencia de acuerdo con normas regionales, nacionales e internacionales adecuadas; deben funcionar de manera segura de acuerdo con el código local de incendios.
- Instalar sistemas adecuados para detección de intrusos de acuerdo con normas nacionales, regionales o internacionales y se deben probar regularmente para abarcar todas las puertas externas y ventanas accesibles; las áreas no ocupadas deben tener alarmas en todo momento; también deben abarcar otras áreas, tales como las salas de cómputo o las salas de comunicaciones.
- Establecer que las instalaciones de procesamiento de información gestionadas por la organización deben estar separadas físicamente de las gestionadas por partes externas.

RESULTADO

Documentos aportados:

- GTH-PLN001 Plan de prevencionPreparacionyRespuestasEmergencias.pdf: Documento titulado "PLAN DE PREVENCIÓN, PREPARACIÓN Y RESPUESTA A EMERGENCIAS". El documento hace referencia a que la Contaduría General de la Nación debe enfrentar emergencias provocadas por el hombre o fenómenos naturales que pueden causar pérdidas económicas y afectar la vida y salud de las personas.

HALLAZGO

De acuerdo con las evidencias aportadas por los auditados, no se identificó un documento que contenga las especificaciones detalladas de la Política Relaciona con los Perímetros de Seguridad Física, debidamente aprobada por la alta dirección y socializado al interior de la entidad. Esta política debe incluir elementos esenciales como Introducción, Objetivo, Objetivos específicos, Alcance, Condiciones de implementación, Roles y Responsabilidades, entre otros aspectos. La Política como mínimo debe establecer lineamientos para los ítems indicados en el criterio.

RECOMENDACIÓN

Desarrollar, revisar, contextualizar, aprobar, implementar y apropiar la Política Relaciona con los Perímetros de Seguridad Física, teniendo en cuenta los requisitos establecidos en la NTC ISO 27001, las Guías MSPI de MinTIC y las guías del MIPG del DAFP.

2.1.16 Criterio evaluado: Disponer de Lineamientos y Controles de Acceso Físico

Disponer de documentación donde especifique los lineamiento y controles de acceso físico:

- Tener un registro de la fecha y hora de entrada y salida de los visitantes, y todos los visitantes deben ser supervisados a menos que su acceso haya sido aprobado previamente; solo se les debe otorgar acceso para propósitos específicos autorizados y se deben emitir instrucciones sobre los requisitos de seguridad del área y de los propósitos de emergencia. La identidad de los visitantes se debe autenticar por los medios apropiados.
- Establecer que el acceso a las áreas en las que se procesa o almacena información confidencial se debería restringir a los individuos autorizados solamente mediante la implementación de controles de acceso apropiados, (mediante la implementación de un mecanismo de autenticación de dos factores, tales como una tarjeta de acceso y un PIN secreto).
- Mantener y hacer seguimiento de un libro de registro (physical log book) físico o un rastro de auditoría electrónica de todos los accesos.
- Definir que todos los empleados, contratistas y partes externas deben portar algún tipo de identificación visible, y se deben notificar de inmediato al personal de seguridad si se encuentran visitantes no acompañados, y sin la identificación visible.
- Establecer que el personal de servicio de soporte de la parte externa se le debería otorgar acceso restringido a áreas seguras o a instalaciones de procesamiento de información confidencial solo cuando se requiera; este acceso se debe autorizar y se le debe hacer seguimiento.
- Definir los derechos de acceso a áreas seguras, revisados y actualizados regularmente, y revocar cuando sea necesario.

RESULTADO

Documentos aportados:

- GTI-PRC10 Seguridad de la Información.pdf: Documento descrito en el numeral 2.1.14.

- Planilla de acceso al piso.pdf y Bitácora Acceso Centro de datos.pdf: Estos documentos presentan información con los datos de Nombre y firma de la persona autorizada a ingresar, fecha del registro, hora del registro, quien autoriza, Actividad, hora de salida y firmas.

HALLAZGO

Revisadas las evidencias aportadas por los auditados, no se identificó un documento específico que contenga las descripciones detalladas sobre las áreas seguras que se deben proteger mediante controles de entrada para asegurar que solamente se permite el acceso a personal autorizado, respecto a los controles de acceso físico, en concordancia con lo mínimo exigido en el criterio.

RECOMENDACIÓN

Desarrollar y documentar un plan detallado de seguridad física que describa las áreas críticas de la entidad que requieren protección, especificando los controles de acceso necesarios para garantizar que solo el personal autorizado pueda ingresar. Este documento debe incluir un mapa de las áreas seguras, los procedimientos de control de entrada y salida, los roles y responsabilidades del personal encargado de la seguridad, y las medidas adicionales para asegurar el cumplimiento de los estándares mínimos exigidos por la normativa aplicable. Además, este documento debe ser revisado y aprobado por la alta dirección para asegurar su alineación con las políticas de seguridad de la entidad.

2.1.17 Criterio evaluado: Seguridad a oficinas, recintos e instalaciones.

Diseñar, documentar y aplicar seguridad física a oficinas, recintos e instalaciones con las siguientes directrices:

- Establecer que las instalaciones clave deben estar ubicadas de manera que se impida el acceso del público.
- Definir donde sea aplicable, las edificaciones deben ser discretas y dar un indicio mínimo de su propósito, sin señales obvias externas o internas, que identifiquen la presencia de actividades de procesamiento de información.
- Definir los directorios y guías telefónicas internas que identifican los lugares de las instalaciones de procesamiento de información confidencial no deben ser accesibles a ninguna persona no autorizada.

RESULTADO

El auditado no aportó documentación para este criterio e indicó que la entidad no ha desarrollado un diseño y estrategia para realizar el aseguramiento de oficinas, recintos e instalaciones.

HALLAZGO

Se constató la ausencia de un documento que contenga las especificaciones detalladas del diseño y su implementación en relación con la seguridad física de oficinas, recintos e instalaciones de acuerdo con lo establecido en el criterio.

RECOMENDACIÓN

Documentar la implementación de las medidas de seguridad física para oficinas, recintos e instalaciones, teniendo en cuenta las condiciones de uso del bien (contrato de arrendamiento). Este documento debe incluir especificaciones sobre los controles de acceso, sistemas de vigilancia, medidas contra incendios, protección de equipos críticos, y cualquier otra medida necesaria para garantizar la seguridad física según los criterios establecidos. Además, es esencial que este documento sea revisado y aprobado por la alta dirección para asegurar su alineación con las políticas de seguridad y normativas

vigentes, y que se implemente de manera efectiva en todas las áreas de la entidad.

2.1.18 Criterio evaluado: Protección Física y Resiliencia ante Desastres y Amenazas para Servicios Críticos

Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes, identificándose los elementos de resiliencia para soportar la entrega de los servicios críticos de la entidad según las indicaciones de la NIST (National Institute of Standards and Technology).

RESULTADO

Documento aportado:

PlanContinuidadNegocio-2022.pdf: Documento con el plan de continuidad de negocio de TI de la UEA Contaduría General de la Nación (CGN), el cual se centra en los procesos misionales de normalización y culturización contable, centralización y consolidación de la información, y en el proceso de apoyo de gestión TIC, considerados críticos en el mapa institucional de procesos. Este plan de continuidad se aborda desde un enfoque tecnológico, ya que cada proceso de la entidad necesita soporte tecnológico para su correcto funcionamiento.

HALLAZGO

Revisado y analizado el contenido de la evidencia, se constató que no existe un documento específico que detalle un Plan de Continuidad de Negocio conforme a los lineamientos del NIST (National Institute of Standards and Technology).

RECOMENDACIÓN

Identificar y documentar los elementos de resiliencia necesarios para asegurar la entrega continua de los servicios críticos de la entidad, según se describen en el NIST SP 800-34, "Contingency Planning Guide for Federal Information Systems".

2.1.19 Criterio evaluado: Diseñar y aplicar procedimientos para trabajo en áreas seguras.

Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras y establecer las siguientes directrices:

- Establecer que el personal solo debe conocer de la existencia de un área segura o de actividades dentro de un área segura, con base en lo que necesita conocer.
- Definir que el trabajo no supervisado en áreas seguras se debe evitar tanto por razones de seguridad como para evitar oportunidades para actividades malintencionadas.
- Establecer que las áreas seguras vacías deben estar cerradas con llave y se revisan periódicamente.

- No se permite el ingreso y uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello.

RESULTADO

Documento aportado:

Manual de Seguridad de la Información 2022.pdf: El documento abarca diversos aspectos de seguridad de la CGN, incluyendo su propósito, alcance, principios, políticas y roles. Además, se describe la gestión de las áreas comunes del edificio donde se ubica la CGN, adoptando lineamientos para mantener la seguridad de la información, como el control de acceso y tránsito, y la vigilancia de equipos y señalización de emergencia, de acuerdo con el Manual de Seguridad Física SF-MA-01.

HALLAZGO

Revisado el contenido de la evidencia, no se identificó un documento específico que contenga las actividades detalladas de un procedimiento para trabajo en áreas seguras, aprobado por la alta dirección y socializado al interior de la entidad. Este procedimiento debe incluir elementos esenciales como Introducción, Objetivo, Objetivos específicos, Alcance, Condiciones de implementación, Roles y Responsabilidades, entre otros aspectos necesarios para su adecuada comprensión y aplicación en línea con lo indicado por el criterio.

RECOMENDACIÓN

Desarrollar, revisar, contextualizar, aprobar, implementar y apropiar procedimientos para trabajo en áreas seguras, teniendo en cuenta los requisitos establecidos en la NTC ISO 27001 y las Guías MSPI de MinTIC.

2.1.20 Criterio evaluado: Implementación de la política para el mantenimiento de equipos.

Implementación de la política para el mantenimiento de equipos con el fin de asegurar su disponibilidad e integridad continua, con las siguientes directrices:

- Mantener los equipos de acuerdo con los intervalos y especificaciones de servicio recomendados por el proveedor.
- Establecer que solo el personal de mantenimiento autorizado debería llevar a cabo las reparaciones y el servicio a los equipos.
- Llevar registros de todas las fallas reales o sospechadas, y de todo el mantenimiento preventivo y correctivo.
- Implementar los controles apropiados cuando el equipo está programado para mantenimiento, teniendo en cuenta si éste lo lleva a cabo el personal en el sitio o personal externo a la organización; en donde sea necesario, la información confidencial se debe borrar del equipo, o el personal de mantenimiento debería

retirarse (cleared) lo suficientemente de la información.
- Cumplir todos los requisitos de mantenimiento impuestos por las políticas de seguros.
- Establecer que antes de volver a poner el equipo en operación después de mantenimiento, se debería inspeccionar para asegurarse de que no ha sido alterado y que su funcionamiento es adecuado.

RESULTADO

Documentos aportados:

- CronogramasManteniento.pdf: El contenido del documento corresponde a un Cronograma de Actividades. La información del cronograma presenta los datos de: N°, Proyecto, Mantenimientos ejecutados, Fechas ejecutados, Mantenimientos pendientes, Fechas Pendientes, Vigencia garantía, Actividades, Elemento Afectado, Especificación de actividad, Cronograma Mantenimientos (Data Center), Meses de enero a diciembre por semanas.

- Manual de Seguridad de la Información 2022: Documento descrito en el numeral 2.1.19.

HALLAZGO

Revisado el contenido de las evidencias aportadas, no se identificó un documento que contenga las especificaciones detalladas de una Política de mantenimiento para equipos informáticos, debidamente aprobado por la alta dirección y socializado al interior de la entidad. Esta política debe incluir elementos esenciales como Introducción, Objetivo, Objetivos específicos, Alcance, Condiciones de implementación, Roles y Responsabilidades, entre otros aspectos necesarios para su adecuada comprensión y aplicación.

RECOMENDACIÓN

Desarrollar, revisar, contextualizar, aprobar, implementar y apropiar una Política de mantenimiento para equipos informáticos, teniendo en cuenta los requisitos establecidos en la NTC ISO 27001 y las Guías MSPI de MinTIC.

2.1.21 Criterio evaluado: Implementación de la Política para el retiro de activos.

Implementación de la Política para el retiro de activos, en donde se indique que los equipos, información o software no se deben retirar de su sitio sin autorización previa y con las siguientes directrices para el retiro de activos:

- Identificar a los empleados y usuarios de partes externas que tienen autoridad para permitir el retiro de activos del sitio.
- Establecer los límites de tiempo para el retiro de activos y verificar que se cumplen las devoluciones.
- Definir cuando sea necesario y apropiado, registrar los activos se retiran del sitio y

cuando se hace su devolución.
- Documentar la identidad, el rol y la filiación de cualquiera que maneje o use activos, y devolver esta documentación con el equipo, la información y el software.

RESULTADO

Documentos aportados:

- GAD-PRC19 Baja de bienes inservibles.pdf: Procedimiento denominado "BAJA DE BIENES INSERVIBLES Y OBSOLETOS Y O RESPONSABILIDAD POR PÉRDIDA", el cual establece los lineamientos y actividades para el reintegro de bienes que se encuentran en desuso por su estado de obsolescencia o inservibles, con el fin de darles de baja, donarlos o destruirlos y rendir oportuno y completo informe sobre faltantes y sobrantes en los Inventarios de elementos y bienes para de esta manera iniciar las investigaciones pertinentes.

- GAD-PRC22 Administracion de bienes.pdf: Procedimiento denominado "ADMINISTRACIÓN DE BIENES", el cual establece los lineamientos relacionados con la administración de bienes desde el ingreso a la entidad hasta el uso por parte de la unidad consumidora en la U.A.E Contaduría General de la Nación. El procedimiento para el ingreso de bienes presenta actividades de: Recibir documentación y revisar los bienes; Clasificar e ingreso al sistema SOA; Identificar los bienes; Asignar el bien adquirido; Entregar de bienes de consumo; Solicitar de reintegro; Actualizar el inventario en SOA; Consultar de inventario; y Diligenciar el Paz y Salvo de inventario.

- GTI-PRC11 Gestión de activos de información.pdf: Procedimiento para la administración de activos de TIC con el fin de garantizar la administración del inventario de activos de TIC, mediante la custodia, seguimiento y control en su ciclo de vida. El procedimiento presenta actividades de: Identificación de activos TIC; Administración activos de TIC; Recepción, verificación y registro del activo en almacén; Retirar activo de las instalaciones de la Contaduría; Ingreso al inventario de activos TICs; Instalación o implementación del activo de TI, Servicio de soporte y registro en Sistema (SDM); Asignar equipos de cómputo a funcionarios o contratistas (Registro en Sistema SDM); Disponer de forma segura o reutilizar equipos; Verificación del funcionamiento del Activo TIC; Evaluación de los activos; Mantenimiento preventivo o correctivo; y Plan de mejoramiento.

HALLAZGO

Revisado el contenido de las evidencias aportadas, no se identificó un documento que contenga las especificaciones detalladas de una Política para el retiro de activos, debidamente aprobado por la alta dirección y socializado al interior de la entidad. Esta política debe incluir elementos esenciales como Introducción, Objetivo, Objetivos específicos, Alcance, Condiciones de implementación, Roles y Responsabilidades, entre otros aspectos necesarios para su adecuada comprensión y aplicación.

RECOMENDACIÓN

Desarrollar, revisar, contextualizar, aprobar, implementar y apropiar una Política para el retiro de activos, teniendo en cuenta los requisitos establecidos en la NTC ISO 27001 y las Guías MSPI de MinTIC.

2.1.22 Criterio evaluado: Implementación de la Política de Seguridad para el Borrado y Encriptación de Discos

Implementación de la Política de Seguridad para el borrado y encriptación de discos, con las siguientes directrices del proceso de borrado y de encriptación de medio discos (para evitar la divulgación de la información confidencial cuando se dispone del equipo o se le da un destino diferente, siempre y cuando):

- Establecer que el proceso de encriptación sea suficientemente fuerte y abarque todo el disco (incluido el espacio perdido, archivos temporales de intercambio, etc.).
- Definir que las llaves de encriptación sean lo suficientemente largas para resistir ataques de fuerza bruta.
- Establecer que las llaves de encriptación se mantengan confidenciales.

RESULTADO

Documentos aportados:

- GTI010-INS01 Instructivo de borrado seguro.pdf: Documento titulado "INSTRUCTIVO DE BORRADO SEGURO", el cual define los pasos para eliminar de forma segura la información de la Contaduría General de la Nación, garantizando los niveles de seguridad de esta y poder eliminar el riesgo de recuperar información confidencial que se hubiere podido almacenar en los activos. El instructivo presenta tareas de Identificación y gestión del activo; Solicitar Autorización; Respuesta a la solicitud; Ejecutar borrado seguro o destrucción; Recuperación de Datos; Actualizar información del Activo; e Informar resultado del procedimiento.

- GTI010-POL04 - Política para el uso de medios removibles, borrado seguro y disposición de medios: Documento titulado "POLÍTICA PARA EL USO DE MEDIOS REMOVIBLES, BORRADO SEGURO Y DISPOSICIÓN DE MEDIOS", el cual describe los lineamientos para la protección de datos en diferentes medios de almacenamiento removible, así como del manejo de borrado seguro y disposición de medios, con el fin de evitar la divulgación no autorizada, modificación, borrado y destrucción de activos de información e interrupción de las actividades del negocio.

HALLAZGO

Revisado el contenido de las evidencias aportadas, se identificó que no existe un documento que detalle una Política de Seguridad para el Borrado y Encriptación de Discos, debidamente aprobada por la alta dirección y socializado al interior de la entidad. Esta

política debe incluir elementos esenciales como Introducción, Objetivo, Objetivos específicos, Alcance, Condiciones de implementación, Roles y Responsabilidades, entre otros aspectos necesarios para su adecuada comprensión y aplicación.

RECOMENDACIÓN

Desarrollar, revisar, contextualizar, aprobar, implementar y apropiar una Política de Seguridad para el Borrado y Encriptación de Discos, teniendo en cuenta los requisitos establecidos en la NTC ISO 27001 y las Guías MSPI de MinTIC.

2.1.23 Criterio evaluado: Implementación de la Política para equipos de usuarios desatendidos

Implementación de la Política para equipos de usuarios desatendidos, con las siguientes directrices:

- Establecer que se cierren las sesiones activas cuando hayan terminado, a menos que se puedan asegurar mediante un mecanismo de bloqueo apropiado (un protector de pantalla protegido con contraseña).
- Establecer que es obligatorio salir de las aplicaciones o servicios de red cuando ya no los necesiten.
- Hay que asegurar que los computadores o dispositivos móviles contra uso no autorizado mediante el bloqueo de teclas o un control equivalente (acceso con contraseña, cuando no están en uso).

RESULTADO

Documentos aportados:

- ConfiguracionDirectiva.png: El documento contienen imagen de una lista de opciones de configuración de Windows entre las que se encuentra resaltada la de "Tiempo de espera del protector de pantalla", la cual se encuentra en estado "Habilitada" y "comentario" en "No".

- Manual de Seguridad de la Información 2022: Documento descrito en el numeral 2.1.19.

HALLAZGO

Revisado el contenido de las evidencias aportadas, se identificó que no existe un documento que detalle las especificaciones de la Política para equipos de usuarios desatendidos, debidamente aprobado por la alta dirección y socializado al interior de la entidad. Este procedimiento debe incluir elementos esenciales como Introducción, Objetivo, Objetivos específicos, Alcance, Condiciones de implementación, Roles y Responsabilidades, entre otros aspectos necesarios para su adecuada comprensión y aplicación.

RECOMENDACIÓN

Desarrollar, revisar, contextualizar, aprobar, implementar y apropiar una Política para equipos de usuarios desatendidos, teniendo en cuenta los requisitos establecidos en la NTC ISO 27001 y las Guías MSPI de MinTIC.

2.1.24 Criterio evaluado: Implementación de la Política de escritorio limpio

Implementación de la política de escritorio limpio con las siguientes directrices:

- Establecer que la información sensible o crítica del negocio, (sobre papel o en un medio de almacenamiento electrónico), se guarda bajo llave (idealmente, en una caja fuerte o en un gabinete u otro mueble de seguridad) cuando no se requiera, especialmente cuando la oficina esté desocupada.
- Definir un procedimiento para la gestión de equipos desatendidos; los computadores y terminales deben estar fuera del sistema y estar protegidos con un sistema de bloqueo de la pantalla y el teclado, controlado por una contraseña, token o mecanismo similar de autenticación de usuario, y deben estar protegidos por bloqueo de teclas u otros controles, cuando no están en uso.
- Evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción (escáneres, cámaras digitales);
- Establecer que los medios que contienen información sensible o clasificada se deben retirar de las impresoras inmediatamente.

RESULTADO

Documentos aportados:

- ConfiguracionDirectiva.png: Documento descrito en el numeral 2.1.22.

- Manual de Seguridad de la Información 2022.pdf: Documento descrito en el numeral 2.1.19.

HALLAZGO

Revisado el contenido de las evidencias aportadas, se identificó que no existe un documento que detalle las especificaciones de la Política de escritorio limpio para los papeles y medios de almacenamiento removibles, debidamente aprobado por la alta dirección y socializado al interior de la entidad. Este procedimiento debe incluir elementos esenciales como Introducción, Objetivo, Objetivos específicos, Alcance, Condiciones de implementación, Roles y Responsabilidades, entre otros aspectos necesarios para su adecuada comprensión y aplicación.

RECOMENDACIÓN

Desarrollar, revisar, contextualizar, aprobar, implementar y apropiar una Política de escritorio limpio, teniendo en cuenta los requisitos establecidos en la NTC ISO 27001 y

las Guías MSPI de MinTIC.

2.1.25 Criterio evaluado: Implementación del Procedimiento de Evaluación del Desempeño del MSPI

Implementación, publicación y apropiación del procedimiento de Evaluación del Desempeño del MSPI y aprobado por la alta Dirección, en el cual se especifique los siguientes ítems:

- Objetivo.
- Alcance.
- Descripción.
- Entradas.
- Salidas.
- Actividades.
- Frecuencia.
- Indicadores.
- Roles y Responsabilidades.
- Relaciones con procedimientos.
- Observaciones.

RESULTADO

Documentos aportados:

- 12 PlanDeSeguridadPrivacidadInformación (1).pdf: Documento titulado "PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN", el cual establece las medidas, actividades y controles necesarios para adelantar la gestión de la seguridad y privacidad de la información (SPI) de acuerdo con los lineamientos del Modelo de Seguridad y Privacidad de la Información, la norma ISO NTC/IEC ISO 27001:2013, la estrategia de Seguridad Digital y Continuidad de la operación de la U.A.E Contaduría General de la Nación – CGN para asegurar la confidencialidad, integridad y disponibilidad de la información para mitigar riesgos de seguridad y cumplir con regulaciones relacionadas.

- Declaración Aplicabilidad 27001-2013.xls: Documento titulado "DECLARACION DE APLICABILIDAD ISO 27001:2013, GTI010-PRC10 SEGURIDAD DE LA INFORMACIÓN, GESTION TICS", en el cual se establecen las medidas, actividades y controles necesarios para adelantar la gestión de la seguridad y privacidad de la información (SPI) de acuerdo con los lineamientos del Modelo de Seguridad y Privacidad de la Información, la norma ISO NTC/IEC ISO 27001:2013, la estrategia de Seguridad Digital y Continuidad de la operación de la U.A.E Contaduría General de la Nación – CGN para asegurar la confidencialidad, integridad y disponibilidad de la información para mitigar riesgos de seguridad y cumplir con regulaciones relacionadas.

- TIC-SEG-SD-2023_ESTRATEGIA DE SEGURIDAD DIGITAL_13122022-1 (3).pdf: Documento titulado "ESTRATEGIA DE SEGURIDAD DIGITAL", en el cual se describe la

estrategia de Seguridad Digital que aplica a todos los niveles de la U.A.E Contaduría General de la Nación - CGN, sus funcionarios, contratistas, proveedores y aquellas personas o terceros que debido al cumplimiento de sus funciones compartan, utilicen, recolecten, procesen, intercambien o consulten cualquier tipo de información, ya sea interna o externa independientemente de su ubicación.

- TIC-SEG-SGS-HDG-Instrumentodeevaluación 2022_v01.pdf: Documento titulado "INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD". Este documento corresponde a la herramienta de diagnóstico de seguridad y privacidad de la información, dirigida a entidades públicas de orden nacional y territorial, así como a proveedores de servicios de Gobierno Digital y terceros interesados en adoptar el Modelo de Seguridad y Privacidad de la Información (MSPI) dentro del Programa Gobierno Digital.

HALLAZGO

Revisado el contenido de las evidencias aportadas, se identificó que no existe un documento específico que detalle las actividades del Procedimiento de Evaluación del Desempeño del MSPI. Este procedimiento debe incluir elementos esenciales como Introducción, Objetivo, Objetivos específicos, Alcance, Condiciones de implementación, Roles y Responsabilidades, entre otros aspectos necesarios para su adecuada comprensión y aplicación.

RECOMENDACIÓN

Desarrollar, revisar, contextualizar, aprobar, implementar y apropiar un Procedimiento de Evaluación del Desempeño del MSPI, teniendo en cuenta los requisitos establecidos en la NTC ISO 27001 y las Guías MSPI de MinTIC.

2.1.26 Criterio evaluado: Plan de Seguimiento y Revisión de la Eficacia del MSPI.

Disposición de un documento con el plan de seguimiento y revisión del MSPI, revisado y aprobado por la alta Dirección y la realización de la actividad de revisión de la eficacia del MSPI.

Los auditados aportaron la siguiente evidencia documental:

- Declaración Aplicabilidad 27001-2013.xls: Documento descrito en el numeral 2.1.24.

- TIC-SEG-SGS-HDG-Instrumentodeevaluación 2022.xls: Documento descrito en el numeral 2.1.24.

- InstrumentoDeclaracionSGSI_2023.xls: Documento titulado "INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD". Este documento corresponde a una herramienta de diagnóstico de seguridad y privacidad de la información, la cual está dirigida a entidades públicas de orden nacional y territorial, así como a proveedores de servicios de Gobierno Digital y terceros interesados en adoptar el

Modelo de Seguridad y Privacidad de la Información (MSPI) dentro del Programa Gobierno Digital.

HALLAZGO

Revisado el contenido de las evidencias aportadas, se identificó la ausencia de documentación que respalde la realización de actividades de revisión y evaluación de la eficacia del Modelo de Seguridad de la Información (MSPI) y de medición de los indicadores del modelo en mención.

RECOMENDACIONES

- Desarrollar e implementar un procedimiento formal para la revisión y evaluación periódica de la eficacia del Modelo de Seguridad de la Información (MSPI). Este procedimiento debe ser documentado y aprobado por la alta dirección, y debe incluir criterios claros de evaluación, responsables designados, frecuencia de las revisiones, y mecanismos de registro y seguimiento de los hallazgos. Además, se sugiere que se establezca un proceso de mejora continua basado en los resultados de estas evaluaciones, garantizando que el MSPI se mantenga alineado con los objetivos de seguridad y las mejores prácticas de seguridad informática. Así mismo, para los indicadores de gestión del modelo.

Criterio: Plan de seguimiento y medición de indicadores de gestión TIC

Evidencias documentales que respaldan la programación y ejecución de las revisiones realizadas por el encargado de seguridad y privacidad de la información.

Evidencias documentales que soportan la realización de las actividades establecidas en los planes de seguridad tanto para el establecimiento como la ejecución y actualización de estos, como respuesta a los aspectos identificados a nivel de las revisiones y seguimientos realizados, en las dos (2) ultimas vigencias.

Evidencias documentales que permitan constatar el monitoreo, seguimiento y evaluación a los Indicadores de Uso y Apropiación del nivel de adopción de la tecnología y la satisfacción en su uso, y a las acciones de mejora y transformación.

Reporte de la medición de los indicadores de adopción de la tecnología y la satisfacción de su uso.

Evidencias de la evolución del plan de formación y gestión del cambio.

RESULTADO

Documentos aportados:

- InstrumentoDeclaracionSGSI_2023.xls: Documento titulado "INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD". Este documento corresponde a una herramienta de diagnóstico de seguridad y privacidad de la información. Esta

herramienta está dirigida a entidades públicas de orden nacional y territorial, así como a proveedores de servicios de Gobierno Digital y terceros interesados en adoptar el Modelo de Seguridad y Privacidad de la Información (MSPI) dentro del Programa Gobierno Digital.

- Declaración Aplicabilidad 27001-2013.xls: Documento titulado "DECLARACION DE APLICABILIDAD ISO 27001:2013, GTI010-PRC10 SEGURIDAD DE LA INFORMACIÓN, GESTION TICS", describe las medidas y controles necesarios para gestionar la seguridad y privacidad de la información en la U.A.E Contaduría General de la Nación (CGN). Siguiendo el Modelo de Seguridad y Privacidad de la Información, la norma ISO 27001:2013 y la estrategia de Seguridad Digital y Continuidad de la operación de la CGN, se asegura la confidencialidad, integridad y disponibilidad de la información, mitigando riesgos y cumpliendo regulaciones. El documento incluye una sección denominada "27001-2013" que detalla la implementación de los 114 controles del Anexo A de la norma ISO 27001, indicando que ninguno fue excluido y que se aplicó al menos un control para cada uno.

- TIC-SEG-SGS-HDG-Instrumentodeevaluación 2022.xls: Documento titulado "INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD". Este documento corresponde a la herramienta de diagnóstico de seguridad y privacidad de la información, dirigida a entidades públicas de orden nacional y territorial, así como a proveedores de servicios de Gobierno Digital y terceros interesados en adoptar el Modelo de Seguridad y Privacidad de la Información (MSPI) dentro del Programa Gobierno Digital.

- Declaración Aplicabilidad 27001-2013.xls: Documento titulado "DECLARACION DE APLICABILIDAD ISO 27001:2013, GTI010-PRC10 SEGURIDAD DE LA INFORMACIÓN, GESTION TICS", describe las medidas y controles necesarios para gestionar la seguridad y privacidad de la información en la U.A.E Contaduría General de la Nación (CGN). Siguiendo el Modelo de Seguridad y Privacidad de la Información, la norma ISO 27001:2013 y la estrategia de Seguridad Digital y Continuidad de la operación de la CGN, se asegura la confidencialidad, integridad y disponibilidad de la información, mitigando riesgos y cumpliendo regulaciones. El documento incluye una sección denominada "27001-2013" que detalla la implementación de los 114 controles del Anexo A de la norma ISO 27001, indicando que ninguno fue excluido y que se aplicó al menos un control para cada uno.

- TIC-SEG-SGS-HDG-Instrumentodeevaluación 2022.xls: Documento titulado "INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD". Este documento corresponde a la herramienta de diagnóstico de seguridad y privacidad de la información, dirigida a entidades públicas de orden nacional y territorial, así como a proveedores de servicios de Gobierno Digital y terceros interesados en adoptar el Modelo de Seguridad y Privacidad de la Información (MSPI) dentro del Programa Gobierno Digital.

- Uso y apropiación.pdf: Documento titulado "ESTRATEGIA DE USO Y APROPIACIÓN DE LA ARQUITECTURA EMPRESARIAL DE TI", mediante el cual se define la Estrategia de

Uso y Apropiación de TI en la Contaduría General de la Nación para aumentar las capacidades laborales de los servidores y colaboradores, fortalecer la cultura organizacional de la entidad, alcanzar los resultados en la implementación de los proyectos de TI y ofrecer un mejor servicio a los usuarios estratégicos y partes interesadas.

HALLAZGO

Revisando y analizando la información proporcionada, se identificó la ausencia de documentación que respalde la realización de actividades de programación y ejecución de las revisiones por parte del encargado de seguridad y privacidad de la información para garantizar que los controles implementados para proteger la integridad, confidencialidad y disponibilidad de los datos estén operando de manera efectiva y conforme a las políticas establecidas por la entidad.

De igual manera, se identificó la ausencia de evidencias documentales que respalden la actividad de medición de los indicadores de MSPI. La falta de evidencias documentales impide verificar la correcta ejecución y monitoreo de estos indicadores, lo cual es fundamental para evaluar la eficacia y eficiencia del MSPI.

De otra parte, se identificó la ausencia de documentación que respalde la realización de las actividades establecidas en los planes de seguridad tanto para el establecimiento como la ejecución y actualización de estos, como respuesta a los aspectos identificados a nivel de las revisiones y seguimientos realizados con el fin de asegurar la protección continua y efectiva de los activos de información de la entidad frente a los riesgos identificados. Estas actividades son esenciales para responder proactivamente a las vulnerabilidades y debilidades detectadas en las revisiones y seguimientos, garantizando que los controles de seguridad se mantengan robustos y adaptativos.

Finalmente, se identificó la ausencia de evidencias documentales que permitan constatar el monitoreo, seguimiento y evaluación de los Indicadores de Uso y Apropiación del nivel de adopción tecnológica y la satisfacción en su uso. Esta carencia de documentación también se extiende a las acciones de mejora y transformación, la medición de los indicadores de adopción tecnológica, la satisfacción en su uso, y la evolución del plan de formación y gestión del cambio.

RECOMENDACIÓN

Es procedente que el proceso implemente un sistema de registro y seguimiento detallado para las mediciones de los indicadores de la Gestión TIC y la realización de evaluaciones de seguimiento a la implementación del MSPI, a fin de asegurar la efectividad en la gestión TIC y de seguridad y privacidad de la información.

Criterio: Seguimiento y evaluación a los indicadores de uso y apropiación de la adopción de la tecnología y plan de acción

Evidencias documentales que permitan constatar el monitoreo, seguimiento y evaluación

a los Indicadores de Uso y Apropiación del nivel de adopción de la tecnología y la satisfacción en su uso, y a las acciones de mejora y transformación.

Reporte de la medición de los indicadores de adopción de la tecnología y la satisfacción de su uso.

Evidencias de la evolución del plan de formación y gestión del cambio.

RESULTADO

Documentos aportados:

- Uso y apropiación.pdf: Documento titulado "ESTRATEGIA DE USO Y APROPIACIÓN DE LA ARQUITECTURA EMPRESARIAL DE TI", mediante el cual se define la Estrategia de Uso y Apropiación de TI en la Contaduría General de la Nación para aumentar las capacidades laborales de los servidores y colaboradores, fortalecer la cultura organizacional de la entidad, alcanzar los resultados en la implementación de los proyectos de TI y ofrecer un mejor servicio a los usuarios estratégicos y partes interesadas.

- TIC-GES-RPA-2023-PI19_FOR02_DetalledeactividadPlanesAcción_4trim_ Gestión TICs.xls: Documento titulado "DETALLE DE ACTIVIDADES DE PLANES DE ACCIÓN 2023", el cual registra el Plan de Acción Operativo 2023, atendiendo los objetivos institucionales: 12. Preservar la confidencialidad, integridad y disponibilidad de la información de la CGN. (Objetivo SGSI) y 14. Disponer de la infraestructura tecnológica que asegure la sostenibilidad de los sistemas de información de la CGN.

Las actividades registradas en el plan son:

- Soportar, administrar y mantener la plataforma tecnológica de la Contaduría General de Nación
- Fortalecer, Desarrollar e integrar los productos y servicios en la Contaduría General de la Nación
- Elaborar, divulgar e implementar políticas de seguridad
- Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI
- Plan de tratamiento de riesgos de seguridad y privacidad de la información
- Plan de seguridad y privacidad de la información

- TIC-GES-RPA-2023-PI19_FOR04_REPORTE DE INDICADORES_4trim_Gestión TICs.xls: Documento titulado "REPORTE DE INDICADORES 2023", asociado al procedimiento "SISTEMA INTEGRADO DE MEDICION PLAN ESTRATEGICO INSTITUCIONAL (SIMPEI)", el cual presenta el registro de información con los datos de: Nombre del Líder del proceso, No del Objetivo Estratégico al que apunta según H.V en el aplicativo SIGI, Nombre del Indicador, Tipo según H.V. del Aplicativo SIGI, No. Trimestre del reporte, Promedio del indicador (suma / No. de trimestres), Promedio de todos los indicadores (suma /No. De indicadores) y Reporte de la gestión adelantada respecto al indicador en el trimestre.

En el documento se encontró el registro de los siguientes indicadores:

- DISPONIBILIDAD DE LAN
- DISPONIBILIDAD DE PLATAFORMA MISIONAL
- DISPONIBILIDAD DE PLATAFORMA GESTION
- DISPONIBILIDAD DE INTERNET
- EFECTIVIDAD EN RESPUESTA DE SOLICITUDES
- EFECTIVIDAD DESARROLLO Y SOPORTE
- PRESTACIÓN DE SERVICIOS INFORMÁTICOS CONTRATADOS
- PERDIDA DE DISPONIBILIDAD, INTEGRIDAD Y CONFIDENCIALIDAD DE LA INFORMACION.

- Correo_Avance Plan de Accion II_Trimestre_GESTIÓN TICs.pdf: Documento correspondiente a un correo electrónico, con referencia "SEGUIMIENTO PLAN DE ACCIÓN Y PEI TRIMESTRE 2 – GESTIÓN TICs", con el fin de "De acuerdo con lo solicitado adjunto envío los formatos diligenciados con la información correspondiente al avance del segundo semestre de 2024.".

HALLAZGO

Revisando y analizando la información proporcionada, y de acuerdo con las evidencias aportadas por los auditados, se identificó la ausencia de evidencias documentales que permitan constatar el monitoreo, seguimiento y evaluación de los Indicadores de Uso y Apropiación del nivel de adopción tecnológica y la satisfacción en su uso, como también de los planes de acción aplicados, y la correspondiente socialización. Esta carencia de documentación también se extiende a las acciones de mejora y transformación, la medición de los indicadores de adopción tecnológica, la satisfacción en su uso, y la evolución del plan de formación y gestión del cambio.

RECOMENDACIÓN

Establecer los indicadores alineados con la arquitectura empresarial, NTC ISO 27001, el MSPI y EL MIPG para realizar seguimiento y evaluación, insumo requerido para la toma de decisiones acertadas.

2.2 ESTRATÉGIA DE TECNOLOGÍA DE LA INFORMACIÓN

La estrategia de tecnología de la información es un plan integral que describe cómo se debe utilizar la tecnología para cumplir con los objetivos estratégicos. Está compuesto por planes los cuales deben incluir y determinar los fines de la estrategia que se busca cumplir, la manera en la que se van a hacer realidad incluyendo actividades, el uso de talento humano, físicos, tecnológicos y de conocimientos para desplegar la tecnología; y los mecanismos para hacer monitoreo, seguimiento y evaluación de cumplimiento; de tal manera, que se esté generando valor público mediante la tecnología. Lo anterior, se refleja en el documento denominado Plan Estratégico de Tecnología de la Información (PETI).

2.2.1. Criterio: Entendimiento estratégico - LI.ES.01.

La planeación integral de las tecnologías de la Información se refleja en el documento denominado Plan Estratégico de Tecnologías de la Información (PETI), el cual debe estar alineado con las estrategias sectoriales, el Plan Nacional de Desarrollo, los planes sectoriales, los planes decenales (cuando existan), los objetivos estratégicos de la entidad, los planes institucionales y el Modelo Integrado de Planeación y Gestión (MIPG).

RESULTADO

Para revisar el diseño e implementación del plan estratégico de tecnología, así como la adecuación y mantenimiento de la Infraestructura Tecnológica (IT), Sistemas de Información (SI) y Servicios de Gestión de Información (SGI) y asegurar la alineación con los objetivos institucionales, las mejores prácticas del sector TIC y de Seguridad Informática, se revisó documento denominado "PETI-2023-2026V1.3", el cual se encontró disponible en el portal institucional web de la UAE General de la Nación bajo el siguiente enlace:
https://www.contaduria.gov.co/productos/-document_library/SNUXvXyrbcKS/view_file/6483648.

Revisado y analizado el contenido del PETI se observó:

a. El control de cambios indica que la versión inicial es del 29 de noviembre del 2022, la última actualización del documento se realizó el 30 de noviembre del 2023 y la última publicación en el sitio web institucional corresponde al 19 de enero del 2024.

b. El documento presenta contenidos que abarcan principalmente los siguientes apartados: Glosario de Términos, Introducción, Objetivo, Alcance, Contexto Normativo, Motivadores Estratégicos de TI, Modelo Operativo, Situación Actual, Políticas y Estándares para la Gestión de la Gobernabilidad de TI, Situación Objetivo, Identificación de Hallazgos y Brechas, Portafolio de Iniciativas, Proyectos y Mapa de Ruta, Plan de Comunicaciones, y Estrategia de Actualización del PETI.

c. El Plan Estratégico de Tecnologías de la Información (PETI) está proyectado para un periodo de tres (3) años, desde la vigencia 2023 hasta 2026. Según lo indicado por los auditados, esta proyección se debió a varios factores, como el cambio de gobierno, el nombramiento de nuevas directivas y la demora en la aprobación del Plan Nacional de Desarrollo por parte del actual gobierno.

HALLAZGO

Comparado el PETI frente a los criterios establecidos el lineamiento LI.ES.05 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), se evidenció:

a) Que este no contiene "*la proyección de la estrategia para 4 años y deberá ser actualizado anualmente en respuesta a los cambios en la estrategia del sector o de la institución, la normatividad y las tendencias tecnológ*icas**"**

b) En la introducción, no se identificó una descripción que indique que el Plan Estratégico de Tecnologías de la Información (PETI) forma parte integral de la estrategia de la institución. Además, no se especificó que su resultado correspondió a un ejercicio de planeación estratégica de Tecnologías de la Información (TI) y que dichos resultados fueron integrados al PETI. Los auditados señalaron que la elaboración del PETI se llevó a cabo por iniciativa del GIT Apoyo Informático, sin la participación transversal de la alta y media gerencia de la entidad.

c) En la revisión y análisis del documento, se observó que algunos apartados no se adaptaron al contexto institucional toda vez que presentan descripciones que corresponden al texto literal de los lineamientos establecidos por MinTIC para la elaboración del PETI. Esto se evidenció en secciones como "6.1 ALINEACIÓN ESTRATÉGICA", "Política de Gobierno Digital" y "6.3 TENDENCIAS TECNOLÓGICAS", entre otras.

d) En la sección "8.1.2 MISIÓN Y VISIÓN DE TI" del documento, la Misión y Visión de Tecnologías de la Información (TI) se describen bajo los conceptos de "*Somos el órgano rector de la contabilidad pública en Colombia, con autoridad doctrinaria en la materia, que normaliza, centraliza y consolida la contabilidad del sector público (…)*" y "*Seremos reconocidos como una entidad pilar del Sistema de Gestión Financiera Pública (…)*" respectivamente.

   Al revisar y analizar lo descrito en la visión y misión, no se identificó una relación directa y vinculante con una Estrategia de TI según lo indicado en G.ES.01 Guía del dominio de estrategia de TI de MinTIC. Además, de acuerdo a lo manifestado por los auditados, el planteamiento de la misión y visión se estableció por iniciativa propia, sin la participación de la alta y media gerencia de la entidad y sin un ejercicio de planeación estratégica vinculante.

e) En el documento PETI, apartado "11 PORTAFOLIO DE INICIATIVAS, PROYECTOS Y MAPA DE RUTA", se observó la descripción de la información de las iniciativas o proyectos que se plantearon en el desarrollo del Plan Estratégico de TI por parte del GIT de Apoyo Informático, con datos tales como: Id del proyecto, objetivos del proyecto, procesos de la entidad impactados con el proyecto, brechas a cerrar con el proyecto y estimación del costo de inversión por año. En el punto "11.2 EVALUACIÓN DE PROYECTOS", se incluyó información sobre los costos de inversión y operación de los proyectos registrados en el PETI. Asimismo, en el punto "11.3 HOJA DE RUTA", se presentó información respecto a la hoja de ruta para los costos de inversión de los proyectos y su distribución por vigencias.

   Es de indicar, que según los documentos aportados y a lo revisado en la Mesa No. 1 con los auditados, no se identificaron reportes, informes o actas de seguimiento y

control de la ejecución del presupuesto asociado a los proyectos del PETI, ni documentación relacionada con la ejecución de las fases de gestión de proyectos.

RECOMENDACIÓN

Es pertinente que se realice una actualización del PETI teniendo en cuenta un ejercicio de planeación estratégica de TI que incluya la participación de la alta y media gerencia de la entidad. Este proceso debe abordar las necesidades específicas de la entidad en términos de objetivos institucionales, procesos, infraestructura tecnológica, y servicios de gestión de información, conforme a la guía G.ES.06 del MinTIC. Así mismo, integrar y contextualizar los conceptos de MinTIC, reflejando la misión y visión institucionales. Además, el desarrollo de la estrategia de TI debería ser participativo, involucrando todos los niveles gerenciales y alineándose con el Plan Nacional de Desarrollo y la modernización de la entidad. Finalmente, tener en cuenta aplicar las buenas prácticas del PROYECT MANAGEMET INSTITUTE (PMI) y el lineamiento LI.ES.09 de MinTIC para realizar un seguimiento y control periódico del presupuesto y plan de compras asociados a los proyectos estratégicos del PETI, asegurando que estos controles estén documentados y disponibles para revisión, ajustes y seguimiento.

Acorde a lo anterior, se concluye que el nivel de cumplimiento de las especificaciones del PETI frente a los criterios establecidos el lineamiento LI.ES.05 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) presenta deficiencias en los aspectos evaluados, lo que implica una mayor exposición a la materialización de riesgos asociados a la Gestión Integral del Proceso de Gestión TICs.

2.2.2 Criterio: Definición de la Arquitectura Empresarial - LI.ES.02.

El MinTIC, a través de la política de Gobierno Digital, impulsa la adopción del enfoque de Arquitectura Empresarial (AE) con el Marco de Referencia de Arquitectura Empresarial (MRAE) para fortalecer la gestión y gobierno de TI, desarrollando proyectos y maximizando el valor público. Esta práctica estratégica facilita la transformación y alineación de la gestión institucional con los objetivos estratégicos y necesidades de los grupos de interés, promoviendo una gestión efectiva y sostenible. Por ende, la entidad debe definir una Arquitectura Empresarial que incluya una arquitectura de negocio y de TI, aplicando el MRAE.

RESULTADO

Para revisar la definición de la Arquitectura Empresarial se tuvo en cuenta los artefactos propuestos para cada uno de los dominios del Marco de Referencia en la guía G.GEN.03 Guía General de un Proceso de Arquitectura Empresarial y G.ES.01 Guía del dominio de estrategia de TI, para lo cual se revisó y analizó el documento denominado “Modelo de Arquitectura Empresarial de TI - 2021 - 2024”.

Analizado el contenido del documento se observó:

a. El control de cambios del documento indica que la versión inicial es del 31 de agosto del 2021 y la última actualización se realizó el 30 de septiembre del 2022.

b. El documento presenta contenidos que abarcan principalmente los siguientes apartados: Introducción, Alcance, Normatividad, Glosario de términos, Objetivo, Estrategia de adopción, Modelo conceptual de la arquitectura empresarial, Estructura del marco de referencia de arquitectura empresarial, Principios del marco de referencia, Dominios, Base de conocimiento, Planeación del ejercicio de AE, y Estrategia de actualización documento AE.

c. El apartado "12 PLANEACIÓN DEL EJERCICIO DE AE" describe que el ejercicio de Arquitectura Empresarial en la CGN reconoce el modelo conceptual propuesto por MinTIC, y destaca la importancia de abordar integralmente los seis (6) dominios del modelo, junto con sus ámbitos y lineamientos. Este enfoque permite realizar un diagnóstico para evaluar el cumplimiento actual de los lineamientos y establecer la arquitectura actual (AS-IS), que será la base para futuros ejercicios de AE.

d. En el apartado "12.1 DEFINICIÓN DE LA ARQUITECTURA EMPRESARIAL ACTUAL (AS – IS)" indica: "*El diagnóstico del modelo actual de AE se realiza calificando el estado de cumplimiento de cada uno de los lineamientos de marco de referencia de arquitectura de MinTic, adoptado por la CGN, (…)".*

e. A partir de una tabla de criterios, se realizó una calificación detallada de cada uno de los lineamientos establecidos por MinTIC para los seis dominios clave del proceso de AE: Estrategia TI, Gobierno TI, Información, Sistemas de Información, Servicios Tecnológicos, y Uso y Apropiación.

HALLAZGO

a) En la INTRODUCCIÓN no describe cómo se realizó el proceso de Arquitectura Empresarial (AE), el propósito de dicho proceso y cómo este contribuyó a establecer la estrategia institucional de Tecnologías de la Información (TI), lo cual está establecido en las guías G.GEN.03 Guía General de un Proceso de Arquitectura Empresarial y G.ES.01 Guía del dominio de estrategia de TI.

b) Los apartados de Introducción, Alcance y Objetivo presentan una descripción enfocada en la implementación del documento, pero no reflejan la adopción y adaptación de los conceptos establecidos en el documento G.GEN.01, Generalidades del Marco de Referencia de Arquitectura Empresarial (AE) para la gestión de TI.

c) El apartado "6 ESTRATEGIA DE ADOPCIÓN", describe textualmente los conceptos establecidos en la G.GEN.02 "Guía general de adopción del Marco de Referencia de Arquitectura Empresarial" de MinTIC, que orienta a las entidades públicas en la adopción del Marco de Referencia de Arquitectura Empresarial (AE) para la gestión de TI de Colombia, pero no desarrolla su adopción y adaptación a las características propias de la entidad. Igual sucede con los apartados "7 MODELO CONCEPTUAL DE LA ARQUITECTURA EMPRESARIAL", "8 ESTRUCTURA DEL MARCO DE REFERENCIA DE

ARQUITECTURA EMPRESARIAL", "9 PRINCIPIOS DEL MARCO DE REFERENCIA" y "10 DOMINIOS".

d) Los auditados indicaron que la información registrada bajo el apartado "12.1 DEFINICIÓN DE LA ARQUITECTURA EMPRESARIAL ACTUAL (AS-IS)" respecto al uso y la evaluación de los lineamientos de MinTIC, fueron realizados por iniciativa propia del GIT de Apoyo Informático, sin la participación transversal de la alta y media gerencia, acorde a lo estipulado en las guías de AE emitidas por MinTIC.

RECOMENDACIÓN

Es importante que se realice el ajuste del documento de Arquitectura Empresarial (AE), de la entidad, describa en detalle:

1. Cómo el proceso ha alineado las Tecnologías de la Información con los procesos, objetivos y metas institucionales.

2. Cómo este proceso ha guiado la transformación de la entidad, asegurando el cumplimiento de su misión y estrategia institucional, siguiendo la Guía General de un Proceso de Arquitectura Empresarial de MinTIC (G.GEN.03).

3. Cómo la entidad ha integrado buenas prácticas de gestión y cómo la AE contribuye a la eficiencia operativa, reduciendo costos, transformando sistemas y reconfigurando procesos institucionales.

4. Aborde sistemáticamente el diseño, implementación y evolución de la AE y sea un constructo participativo de la alta y media gerencia, líderes de procesos, equipos de TIC y cualquier otro grupo con un interés directo en la implementación y los resultados de la AE.

En resumen, el documento debe mostrar cómo se han adoptado y adaptado los conceptos del MinTIC a las características específicas de la entidad, asegurando que la estrategia de TI sea contextualizada y relevante para las necesidades y objetivos institucionales.

2.2.3 Criterio: Alineación del gobierno de TI - LI.GO.01

La Dirección de Tecnologías y Sistemas de la Información, o la instancia que la sustituya, debe definir e implementar un esquema de Gobierno de TI alineado con la estrategia misional de la entidad y el Modelo Integrado de Planeación y Gestión, que estructure y direccione adecuadamente el flujo de decisiones de TI.

Es fundamental que la entidad cuente con una política de TI actualizada, debidamente aprobada y comunicada, que esté en consonancia con la estrategia institucional y el sistema integrado de gestión.

Debe disponerse de documentación e información detallada sobre el Modelo de Gobierno de TI, así como evidencias que demuestren su efectiva implementación.

RESULTADO

Documentos aportados:

- ManualSeguridadInformaciónDigitalV7.0.pdf: El documento describe las políticas y objetivos para proteger los activos de información, tanto físicos como digitales con el objetivo de reducir riesgos de divulgación, modificación o uso indebido de estos activos, mejorar la administración de su seguridad, detectar amenazas y fomentar una cultura de control y responsabilidad. Además, indica que la CGN se compromete a mantener políticas efectivas para asegurar la integridad, confidencialidad y disponibilidad de la información, garantizando la seguridad y continuidad de sus operaciones.

- PETI-2023-2026V1.3.pdf: Este documento se describió en el numeral 2.2.1.

- Sistema Integrado de Gestión Institucional de la UEA Contaduría General de la Nación (CGN): En este sistema se identificaron los siguientes procedimientos de la Gestión TICs:

  GTI-PRC10 - SEGURIDAD DE LA INFORMACIÓN
  GTI-PRC04 - PLANEACIÓN Y GESTIÓN TICs_V0.2
  GTI-PRC03 - OPERACIÓN CENTRO DE COMPUTO_V.10
  GTI-PRC09 - MANTENIMIENTO DE SOFTWARE_V.07
  GTI-PRC08 - GENERACIÓN DE VERSIÓN_ V.07
  GTI-PRC07 - PROCEDIMIENTO DESARROLLO DE SOFTWARE_ V.10
  GTI-PRC06 - CERTIFICACIÓN DE SOFTWARE_V.08
  GTI-PRC02 - ADMINISTRACIÓN DE LA PLATAFORMA TECNOLÓGICA_ V.09
  GTI-PRC11 - ADMINISTRACIÓN DE ACTIVOS TIC

  También se identificaron los siguientes documentos:

  FLUJOGRAMA -OPERACIÓNCENTRODATOS.xls
  FLUJOGRAMA -SEGURIDADREDESCOMUNIC.xls
  FLUJOGRAMA -SEGURIDADDESARROLLOMTOSW.xls
  FLUJOGRAMA -PROPIEDAD INTELECTUAL.xls
  FLUJOGRAMA -GESTIÓNINCIDENTESAMENDEBSEG.xls
  FLUJOGRAMA -GESTIONCAPACIDAD.xls
  FLUJOGRAMA -GESTIONCAMBIOSTECNOLOGICOS.xlsx
  FLUJOGRAMA -CONTROLACCESOSISTEMASINFO.xls
  FLUJOGRAMA -CONTINUIDADSEGURIDAD.xls
  FLUJOGRAMA -ACTUALIZACIÓNSOFTWAREHARDWARE.xls
  GTI02-FOR04 ADMINISTRACIÓN DE CAMBIOS A TI - Actualización.docx
  TIC-GES-SGC-POL-2019-PoliticasCopiasRespaLdoGTI03-POL01.doc
  TIC-SEG-SGS-MAN-2019-ManualDeSeguridadAprobado.doc
  POLÍTICA_DE_ACCESO_A_LA_RED_PRIVADA_VIRTUAL_DE_LA_CGN.doc
  CAMBIO 7.1 POLÍTICA_ADMINISTRACIÓN_DE_USUARIOS_Y-O_CONTRASEÑAS.doc
  FLUJOGRAMA -SEGURIDADFÍSICAYENTORNO.xls

FLUJOGRAMAGESTIONMEDIOSREMOVIBLES.xls
Formato seguimiento y control SI.xls
FLUJOGRAMA -COPIASRESPALDOINFO.xls

La revisión de los anteriores documentos permitió establecer que existe una caracterización del proceso de gestión de TIC y el desarrollo de procedimientos y formatos. Lo anterior, establece un estándar y un marco de actuación en la gestión de TIC en la entidad, facilitado por el GIT Apoyo Tecnológico, quien atiende sus responsabilidades como la de administrar y asegurar el funcionamiento de las redes de computadores y el correo electrónico; el diseñar, implementar y documentar el portal web institucional; el estructurar y ejecutar desarrollos informáticos y el definir procesos y procedimientos relacionados con el desarrollo informático de la entidad.

HALLAZGO

Como resultado de la revisión y análisis de las evidencias, se identificó la ausencia de un documento maestro del Modelo de Gobierno de Tecnologías de la Información (TI) que describa detalladamente los procesos de gobierno de TI, la definición de roles y responsabilidades de TI, la metodología de Gestión de Riesgos de TI, la estructura organizacional del área de TI y la estructura de decisiones de TI, alineado con el modelo conceptual definido en el dominio de Gobierno de TI del Marco de Referencia de Arquitectura Empresarial.

RECOMENDACIÓN

Es procedente que la entidad cuente con un documento maestro del Modelo de Gobierno de Tecnologías de la Información (TI) aprobado por la instancia de decisión correspondiente. Este documento debe detallar procesos de gobernanza de TI, roles y responsabilidades, gestión de riesgos y estructura organizacional, asegurando una gobernanza efectiva y alineada con los objetivos estratégicos de la entidad.

2.2.4 Criterio: Implementación de la Política de seguridad de la información

Implementación de la política de seguridad de la información, aprobada por la alta Dirección y debidamente socializada dentro de la Entidad, que incluye la definición de acciones y toma de decisiones bajo las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes.

- Garantizar la continuidad del negocio frente a incidentes.
- Implementar y gestionar el Sistema de Gestión de Seguridad de la Información, bajo lineamientos claros, acorde a las necesidades del negocio y a los requerimientos regulatorios.

RESULTADO

Documentos aportados:

- Acta No. 11 CIGD - 13 de octubre de 2022.pdf: Acta No. 11 del Comité Institucional de Gestión y Desempeño en donde se trataron temas del proceso de gestión TIC como Plan Estratégico de Tecnologías de la Información -PETI- para aprobación, Actualización arquitectura empresarial de TI para aprobación y actualización manual de seguridad de la información para aprobación, entre otros.

- Manual de Seguridad de la Información 2022.pdf: Documento descrito en el numeral 2.1.19.

- ManualSeguridadInformaciónDigitalV7.0 2023.pdf: Documento descrito en el numeral 2.2.2.

HALLAZGO

Revisando y analizando la información proporcionada por los auditados, no se evidenció un documento con la Política de Seguridad y Privacidad de la Información, acorde a lo establecido en el criterio.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar una Política de seguridad de la información, teniendo en cuenta los requisitos establecidos en la NTC ISO 27001 y las Guías MSPI de MinTIC.

2.2.5 Criterio: Implementación de la Política Organización de la Seguridad de la Información

Implementación de la Política Organización de la Seguridad de la Información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad, con las especificaciones de cómo establecer el comité directivo de la seguridad de la información y los siguientes elementos:

- ¿Quiénes conforman el comité directivo de seguridad de la información?

- Objetivos: Se deben especificar los objetivos del comité como por ejemplo el mejoramiento continuo de los programas o las distintas actividades que se realizarán en dichos comités, verificación de avance de los distintos proyectos, la revisión del documento de la política de seguridad etc.

- Cumplimiento: Debe establecerse que dicho comité verifique el cumplimiento de las políticas.

RESULTADO

Documento aportado:

Res_193_2019.pdf. El contenido del documento corresponde a la Resolución 193 del 2019 por la cual se crea el Sistema de Gestión y Desempeño de la Unidad Administrativa Especial (UEA) Contaduría General de la Nación (CGN) y se dictan otras disposiciones.

Para los temas de seguridad informática, el Comité Institucional de Gestión y Desempeño tiene las funciones de revisar lineamientos técnicos y operativos, designar responsables de seguridad, asignar roles conforme a la norma ISO 27001, apoyar el desarrollo de iniciativas de seguridad, generar recomendaciones para políticas y controles, mejorar la gestión de incidentes, revisar planes de mitigación de riesgos, realizar revisiones periódicas al SGSI, consultar aspectos jurídicos, y asegurar el cumplimiento de todas las políticas y normas relacionadas con la seguridad de la información.

Estas acciones incluyen revisar lineamientos técnicos y operativos, designar responsables de seguridad, asignar roles conforme a la norma ISO 27001, apoyar el desarrollo de iniciativas de seguridad, generar recomendaciones para políticas y controles, mejorar la gestión de incidentes, revisar planes de mitigación de riesgos, realizar revisiones periódicas al SGSI, consultar aspectos jurídicos, y asegurar el cumplimiento de todas las políticas y normas relacionadas con la seguridad de la información.

HALLAZGO

Revisada y analizada la información proporcionada, se observó la ausencia de la Política Organización de la Seguridad de la Información, debidamente aprobada por la alta dirección y socializada al interior de la entidad, con los elementos esenciales de Introducción, Objetivo, Objetivos específicos, Alcance, Condiciones de implementación, Roles y Responsabilidades, entre otros.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar una Política Organización de la Seguridad de la Información, de acuerdo con especificado en la Guía de Roles y Responsabilidades del Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), versión 4 del 28 de octubre de 2021. Esta guía puede ubicarse en el enlace: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

La guía destaca la necesidad de vincular de forma efectiva al personal de alto nivel asociado al proceso de desarrollo del MSPI en la entidad, para garantizar el apoyo en la

planeación del proyecto de implementación del MSPI y asegurar el éxito del modelo de gestión de seguridad de la información propuesto para la entidad.

Los representantes de alto nivel de la entidad deben identificar y establecer, sin perjuicio de lo establecido en la Ley 489 de 1998, en el menor tiempo posible, la organización del grupo de trabajo responsable de implementar el Modelo de Seguridad de la Información (MSPI). Este grupo debe definir el perfil y rol de sus miembros de conformidad con lo establecido en la política. Al final del ejercicio, el equipo directivo que lidera la implementación del MSPI debe comunicar claramente el perfil y las responsabilidades de los responsables.

2.2.6 Criterio: Implementación de las Funciones de Seguridad de la Información

Acto administrativo a través del cual se crea o se modifica las funciones del Comité Gestión Institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, junto con la designación de quien será el encargado de seguridad de la información dentro de la entidad. El acto administrativo debe especificar lo siguiente:

- Conformación del Comité de Seguridad de la Información.
- Objetivo del Comité de Seguridad de la Información.
- Funciones del comité.
- Secretaria Técnica.
- Funciones de la Secretaría Técnica.
- Reuniones del Comité de Seguridad de la Información.
- Sesiones Extraordinarias.
- Vigencia y Derogatoria.

RESULTADO

Documento aportado:

Resolución 193 de 2019.pdf: Documento descrito en el numeral 2.2.6.

HALLAZGO

Revisada y analizada la información proporcionada, y de acuerdo con las evidencias aportadas por los auditados, se identificó que en la Resolución 193 de 2019 no se especificaron los siguientes aspectos del criterio:

- Conformación del Comité de Seguridad de la Información.
- Objetivo del Comité de Seguridad de la Información.
- Funciones del comité.
- Secretaria Técnica.
- Funciones de la Secretaría Técnica.
- Reuniones del Comité de Seguridad de la Información.
- Sesiones Extraordinarias.

- Vigencia y Derogatoria.

RECOMENDACIÓN

Implementar las Funciones de Seguridad de la Información conforme a la norma ISO 27001 y a lo especificado en la Guía de Roles y Responsabilidades del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)

2.2.7 Criterio: Implementación de los roles y responsabilidades de seguridad y privacidad de la información

La alta Gerencia de la entidad identifica, establece y organiza, sin perjuicio de lo establecido en la Ley 489 de 1998, (cada entidad establecerá los términos en los cuales se puede cumplir con esta obligación) el grupo de trabajo responsable de implementar el Modelo de Seguridad de la Información, definiendo el perfil y rol de conformidad con lo establecido en la Política Organización de la Seguridad de la Información.

Evidenciar que el personal de alto nivel se encuentra vinculado de forma efectiva al proceso de desarrollo del MSPI en la entidad, para que el apoyo se vaya garantizando desde el principio de la planeación del proyecto e ir marcando un punto de partida de éxito con la implementación del modelo de Gestión de Seguridad de la Información planteado para la entidad.

RESULTADO

De acuerdo con las evidencias aportadas, se observó el compromiso de la alta y media gerencia con la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad. Este compromiso se refleja en la Resolución 193 de 2019, mediante la cual se asignan al Comité Institucional de Gestión y Desempeño las funciones de revisar los lineamientos técnicos y operativos para implementar el MSPI según el Manual y la Política de gobierno digital, designar al responsable de seguridad digital y del SGSI de la CGN, y asignar el rol de Oficial de seguridad de la información conforme a la norma ISO-IEC 27001:2013.

2.2.8 Criterio: Conformación de un equipo de gestión del proyecto para la implementación del MSPI

Conformación de un equipo de gestión del proyecto implementación del modelo MSPI en la entidad, junto con la asignación mediante acto administrativo de las funciones y responsabilidades de tomar las medidas necesarias para planear, implementar y hacer seguimiento a todas las actividades necesarias para adoptar el Modelo de Seguridad de la Información (MSPI) al interior de la entidad, así como planear las actividades necesarias para una adecuada administración y sostenibilidad del mismo.

RESULTADO

Los auditados no aportaron evidencia documental para el criterio; pero comentaron que se están llevando a cabo actividades para la gestión e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) al interior de la entidad. En particular, se observó una preocupación y un esfuerzo significativo por parte del Grupo Interno de Trabajo (GIT) de Apoyo Tecnológico para desarrollar actividades que permitan avanzar en la implementación del MSPI. También, se identificó que estas actividades y esfuerzos se están desarrollando de manera aislada, sin una participación integral de los líderes de procesos, propietarios de activos de información, y demás dependencias o áreas de la entidad, lo que puede limitar la efectividad y el alcance en la implementación del MSPI.

HALLAZGO

De acuerdo con las evidencias aportadas y a lo comentado por los auditados, se observó que la entidad no ha conformado un equipo de gestión del proyecto para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI). Además, no se ha realizado la asignación de funciones y responsabilidades mediante acto administrativo para tomar las medidas necesarias que permitan planificar, implementar y hacer seguimiento a todas las actividades requeridas para adoptar el MSPI al interior de la entidad. Asimismo, se observó debilidades en la planificación estructurada de las actividades necesarias para una adecuada administración y sostenibilidad del modelo.

RECOMENDACIÓN

Conformación de un equipo de gestión del proyecto implementación del modelo MSPI de acuerdo con la norma ISO 27001 y a lo especificado en la Guía de Roles y Responsabilidades del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)

2.2.9 Criterio: Nombramiento del responsable de Seguridad de la Información

Nombramiento del responsable de Seguridad de la Información para la entidad, mediante acto administrativo, en donde se identifique las siguientes responsabilidades:

- Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias del proyecto, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo.
- Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad.
- Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información.
- Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido.
- Gestionar el equipo de proyecto de la entidad, definiendo roles, responsabilidades, entregables y tiempos.
- Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo

- Encarrilar el proyecto hacia el cumplimiento de la implementación del Modelo de Seguridad y privacidad de la Información para la entidad.
- Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y escalar al Comité de seguridad en caso de ser necesario.
- Monitorear el estado del proyecto en términos de calidad de los productos, tiempo y los costos.
- Trabajar de manera integrada con el grupo o áreas asignadas.
- Asegurar la calidad de los entregables y del proyecto en su totalidad.
- Velar por el mantenimiento de la documentación del proyecto, su custodia y protección.
- Contribuir al enriquecimiento del esquema de gestión del conocimiento sobre el proyecto en cuanto a la documentación de las lecciones aprendidas.
- Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del proyecto

RESULTADO

Documento aportado:

Resolución No. 383 del 15 de noviembre del 2023.pdf. Documento en el cual se especifica la designación del Oficial de Seguridad y Privacidad de la Información en la Contaduría General de la Nación y se asignan sus funciones de acuerdo con lo establecido en el Artículo 3 de la citada resolución. En conclusión, la entidad da cumplimiento a lo establecido en el criterio.

2.2.10 Criterio: Ejecución del Plan de Seguimiento y Revisión del MSPI

Implementación del plan de seguimiento y revisión del MSPI, revisado y aprobado por la alta Dirección, junto con la ejecución de las revisiones del Modelo MSPI por parte de la Dirección.

RESULTADO

Documento aportado:

InstrumentoDeclaracionSGSI_2023.xls: Documento descrito en el numeral 2.1.26.

HALLAZGO

En los soportes documentales aportados por los auditados no se identificó la realización de la actividad de revisión del Modelo de Seguridad y Privacidad de la Información (MSPI) por parte de la dirección. La falta de evidencias documentales impide verificar que las revisiones del MSPI, realizadas por la dirección, se efectúan de manera sistemática y conforme a los procedimientos establecidos.

RECOMENDACIÓN

Es importante que la dirección implemente un sistema formalizado para documentar las revisiones del Modelo de Seguridad y Privacidad de la Información (MSPI). Este sistema debe incluir un registro detallado de cada revisión realizada, destacando los puntos analizados, las decisiones tomadas, y las acciones correctivas o preventivas acordadas. Adicionalmente, se recomienda establecer un calendario de revisiones periódicas, asegurar la aprobación de estos documentos por parte de la alta dirección, y garantizar su adecuada conservación y disponibilidad para auditorías futuras. Esto asegurará que las revisiones del MSPI se realicen de manera sistemática y en conformidad con los procedimientos establecidos, fortaleciendo así la gestión de la seguridad y privacidad de la información en la entidad.

2.2.11 Criterio: Documentación y Seguimiento de Acciones Derivadas de Indicadores de Seguridad de la Información

Documentación de las acciones derivadas producto del seguimiento a los indicadores asociados al cumplimiento de la estrategia de Seguridad de la Información. Las acciones derivadas deben contar con una asignación de fechas de cumplimiento y responsables.

RESULTADO

Documento aportado:

TIC-SEG-SD-2023_ESTRATEGIA DE SEGURIDAD DIGITAL_13122022-1 (4).pdf: Documento descrito en el numeral 2.1.25.

HALLAZGO

De acuerdo con las evidencias aportadas por los auditados, no se identificó documentación que respalde la realización de seguimiento a las acciones derivadas de indicadores de seguridad de la Información.

RECOMENDACIÓN

Establecer y ejecutar acciones derivadas del seguimiento de los indicadores de seguridad de la información para fortalecer la protección de los activos de información y asegurar que la estrategia de seguridad esté alineada con los objetivos de la entidad. Estas acciones deben enfocarse en mejorar controles de seguridad, abordar desviaciones, aplicar medidas correctivas y preventivas, optimizar el uso de recursos, garantizar el cumplimiento normativo, y mejorar la resiliencia ante incidentes, además de desarrollar programas de capacitación que refuercen la cultura de seguridad dentro de la organización. Las acciones deben garantizar que la entidad no solo cumpla con su estrategia de Seguridad de la Información, sino que también la fortalezca continuamente, mejorando su capacidad para proteger sus activos de información, reducir riesgos y asegurar la confianza de sus grupos de interés en su capacidad para gestionar de manera segura y eficiente la información crítica.

2.2.12 Criterio: Desarrollo e Implementación del Tablero de Control para Monitoreo de la Estrategia de Seguridad de la Información

Implementación del Tablero de control con los indicadores asociados al cumplimiento de la Estrategia de Seguridad de la Información.

El tablero de control debe contar con un conjunto de indicadores cuyo seguimiento y evaluación periódica permita tener una visión integral de los avances y resultados en el desarrollo de la Estrategia de Seguridad de la Información definida para la entidad.

El tablero de control debe facilitar el análisis, seguimiento y toma de decisiones a nivel de objetivos estratégicos o iniciativas de seguridad de la información, que en su conjunto contribuyan al cumplimiento de toda la Estrategia de Seguridad de la Información de la entidad.

RESULTADO

Los auditados no aportaron evidencia documental para el cumplimiento del criterio e indicaron que no se dispone de un Tablero de Control para Monitoreo de la Estrategia de Seguridad de la Información.

HALLAZGO

Revisada y analizada la información proporcionada, y de acuerdo con las evidencias aportadas por los auditados, se identificó la ausencia de un tablero de control con los indicadores asociados al cumplimiento de la Estrategia de Seguridad de la Información.

RECOMENDACIÓN

Es importante implementar y apropiar un tablero de control que integre los indicadores clave asociados al cumplimiento de la Estrategia de Seguridad de la Información de la entidad. Este tablero debe ser diseñado para facilitar el monitoreo continuo, el análisis y la toma de decisiones informadas, permitiendo una visión integral del estado y avance de la estrategia. Además, el tablero debe incluir mecanismos de actualización regular y asignación de responsabilidades para asegurar que se realicen los seguimientos necesarios y que se adopten las medidas correctivas o preventivas en caso de desviaciones o riesgos emergentes.

2.3 RELACIÓN CON PROVEEDORES

Verificar la efectividad de las relaciones con proveedores, evaluando la selección, contratación y supervisión de proveedores de servicios y productos tecnológicos, así como el cumplimiento de los acuerdos contractuales y la gestión de riesgos asociados.

Criterio: Implementación de la Política y Procedimiento para el Tratamiento de la Seguridad en los Acuerdos con los Proveedores.

Implementación de la Política y Procedimiento para el Tratamiento de la Seguridad en los Acuerdos con los Proveedores, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional, con las especificaciones de cómo la entidad establece, acuerda, aprueba y divulga los requerimientos y obligaciones relacionados con la seguridad de la información, tanto con los proveedores como con la cadena de suministros que estos tengan (es decir algún intermediario).

RESULTADO

Documentos aportados:

- GAD-MAN01 MANUAL DE CONTRATACIÓN.pdf: El manual establece el funcionamiento de la gestión contractual en la U.A.E. Contaduría General de la Nación (CGN) y proporciona a los participantes del Sistema de Compra Pública una comprensión clara de cómo se lleva a cabo dicha gestión. Asimismo, garantiza que los procesos de contratación en la entidad se alineen con los objetivos del Sistema de Compra Pública, asegurando eficacia, eficiencia, economía, promoción de la competencia, rendición de cuentas, gestión de riesgos, publicidad y transparencia.

  El documento en el numeral 3.1 de las Buenas Prácticas en la Gestión Contractual, exige el cumplimiento de varias normas certificadas por la entidad, como ISO 9001:2015, ISO 14001:2015, ISO 18001:2018, y ISO 27001:2013, en todos los procesos de selección. Además, establece que los miembros del comité evaluador deben firmar y cumplir con el Compromiso de Transparencia y Confidencialidad.

- MAN01-FOR21 - COMPLEMENTO AL CONTRATO (1).pdf: Contrato CS-001-2024, en el cual se observó la disposición de la cláusula referente a ANEXO: ACUERDO DE CONFIDENCIALIDAD, ANEXO: COMPROMISO DE INTEGRIDAD y ANEXO: COMPROMISO ANTICORRUPCIÓN.

- TIC-PLG-CJU-2024-REFI-EJEC-ACUERDO DE CONFIDENCIALIDAD CS-001 (1).pdf: Formato titulado "MAN01-FOR31 ACUERDO DE CONFIDENCIALIDAD Y ACEPTACIÓN DE LAS POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN", en el cual se describen los términos y condiciones bajo los cuales las partes mantendrán la confidencialidad de los datos e información intercambiados entre la U.A.E. CGN y el Contratista o proveedor, en donde este último, se obliga a no revelar, divulgar, exhibir, mostrar, comunicar, utilizar y/o emplear la información con persona natural o jurídica, en su favor o en el de terceros, que reciban de la otra parte y en consecuencia a mantenerla de manera confidencial y privada y a proteger dicha información para evitar su divulgación no autorizada, ejerciendo sobre esta el mismo grado de diligencia que utiliza para proteger información confidencial de su propiedad.

HALLAZGO

De acuerdo con las evidencias aportadas por los auditados, no se identificó que la entidad contara con de la Política y el Procedimiento para el Tratamiento de la Seguridad en los

Acuerdos con los Proveedores, debidamente aprobados por la alta dirección y socializados al interior de la entidad. La Política y el procedimiento deben incluir elementos esenciales como Introducción, Objetivo, Objetivos específicos, Alcance, Condiciones de implementación, Roles y Responsabilidades, entre otros aspectos necesarios para su adecuada comprensión y aplicación.

RECOMENDACIÓN

Implementar la Política y el Procedimiento para el Tratamiento de la Seguridad en los Acuerdos con los Proveedores teniendo en cuenta los requisitos establecidos en la NTC ISO 27001, las Guías MSPI de MinTIC y los lineamientos de Colombia Compra Eficiente.

2.4 GESTIÓN DE PROYECTOS DE TECNOLOGÍAS DE LA INFORMACIÓN

Analizar la gestión de proyectos tecnológicos, incluyendo la planificación, ejecución y seguimiento de proyectos, así como la gestión de riesgos, calidad y recursos involucrados en cada fase del ciclo de vida del proyecto.

2.4.1 Criterio: Capacidades y recursos de TI - LI.GO.05.

La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe generar, direccionar, evaluar y monitorear las capacidades de TI, asegurando el adecuado aprovisionamiento del talento humano y los recursos necesarios para ofrecer los servicios de TI de la institución, para lo cual se debe tener en cuenta:

- Implementación del Plan de capacidad de TI para cada uno de los servicios de TI establecidos en el catálogo de Servicios de TI.

- Definición de las capacidades de TI requeridas para la prestación de los servicios de TI, así como las proyecciones de capacidad de TI requeridas para su funcionamiento en el futuro, junto con las mediciones de capacidades de TI.

- Proyección de dos años del plan de capacidad TI y realizar la evaluación de la capacidad de acuerdo con las necesidades de la entidad (mensual, trimestral o anual).

- Resultados y/o reportes de las mediciones de capacidades existentes para la provisión de los servicios de TI.

- Monitorización del rendimiento y talento humano de los servicios TI y de los componentes que lo soportan.

RESULTADO

Documentos aportados:

- MediciónCapacidad-032024.pdf: En el documento se describe una serie de mediciones para los servicios de Red, Plataforma de comunicaciones, Internet, Servidores de

Gestión, Servidores Misionales, Portátiles, Computadores Personales (PC), Escritorio Virtual, Telefonía IP, Ofimática, Orfeo, Chip, Portal Web, Repositorio, Correo electrónico, Soporte técnico HW, Soporte Desarrollo SW, Mesa de servicio, Plataforma de capacitación, SISCON y Soporte teletrabajo.

Para cada uno de los servicios, se presentan mediciones en términos de Capacidad del Servicio, Capacidad de la Infraestructura y Nivel de Importancia. Además, se detallan los elementos que conforman y afectan cada servicio. Por ejemplo, para el servicio de red, se asignaron componentes como Personal (RH), Acuerdos de Nivel de Servicio (Disponibilidad LAN), Redes Lógicas (Subredes VLANs), Red Física, Red Eléctrica, UPS y Cableado, entre otros.

Asimismo, se observó un diagrama a manera de grafos para cada servicio y sus componentes, donde se establecen las relaciones e interacciones de cada uno de los componentes del servicio. Estos diagramas permiten identificar las relaciones críticas que conforman el servicio y que lo afectan de manera directa y principal, lo cual es esencial para garantizar que el servicio esté activo y en producción. A continuación, se presenta un ejemplo del diagrama para el servicio de repositorios:

Según lo indicado por los auditados, las mediciones se establecen basándose en los resultados obtenidos en cortes específicos, de acuerdo con el servicio prestado. Estas mediciones consideran tanto los tiempos y esfuerzo de operación ejecutados por los proveedores como el tiempo y esfuerzo dedicado por los profesionales del GIT de Apoyo Tecnológico.

- PlanCapacidadServiciosTI-V1-Nov2023.doc: Documento titulado "PLAN DE CAPACIDAD DE LOS SERVICIOS DE TI", en el cual se describe un plan de acción para facilitar la gestión de las capacidades de los servicios clave de TI proporcionados por el GIT de Apoyo Tecnológico para toda la CGN.

HALLAZGO

Revisada y analizada la información proporcionada por el proceso auditado, se identificó que los documentos presentados no cubren todos los aspectos y requerimientos establecidos por el Marco de Referencia de la Arquitectura Empresarial (MRAE) del MinTIC. En particular, se excluyen aspectos cruciales relacionados con la capacidad y gestión de la información, los sistemas de información, y el uso y apropiación de los servicios TIC. Como resultado, el plan presentado no puede considerarse un plan integral de las capacidades de TI necesarias para la prestación de servicios de TI. Además, el documento carece de proyecciones a futuro sobre la capacidad de TI que la entidad requerirá, conforme a una estrategia de TI alineada con los objetivos de institucionales. Cabe destacar que este plan fue desarrollado de manera independiente por el GIT de Apoyo Tecnológico, sin la participación de la alta y media gerencia, líderes de procesos y responsables de activos de información, lo que limita su alcance y efectividad.

RECOMENDACIÓN

Realizar una revisión integral del plan de capacidades de TI para asegurar que cumpla con todos los aspectos y requerimientos establecidos por el Marco de Referencia de la Arquitectura Empresarial (MRAE) del MinTIC. Es importante que el plan incluya la capacidad y gestión de la información, los sistemas de información, y el uso y apropiación de los servicios TIC. Además, se deben incorporar proyecciones futuras sobre la capacidad de TI necesaria, alineadas con la estrategia institucional de TI. Para mejorar la efectividad del plan, se recomienda involucrar a la alta y media gerencia, líderes de procesos y responsables de activos de información en su desarrollo y actualización, garantizando así una planificación integral y coordinada que responda a las necesidades estratégicas de la entidad.

2.4.2 Criterio: Liderazgo de proyectos de TI - LI.GO.09.

La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe liderar la planeación, ejecución y seguimiento a los proyectos de TI. En aquellos casos en que los proyectos estratégicos de la institución incluyan componentes de TI y sean liderados por otras áreas, la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, deberá supervisar el trabajo sobre el componente de TI conforme con los lineamientos de la Arquitectura Empresarial de la institución, teniendo en cuenta.

- Cartas de proyecto, actas de seguimiento y cronogramas de los proyectos donde apoya TI o lidera.

- Contratos firmados donde se verifica la supervisión compartida entre TI y las áreas funcionales en los proyectos que tienen componentes tecnológicos, que implican el liderazgo de TI.

- En las cartas de proyecto, se debe identificar el rol y responsabilidad del área de TI, con relación al proyecto, dichas cartas deben estar firmadas.

- Para verificar el liderazgo de TI en los proyectos que tienen componentes de TI, puede existir la supervisión compartida por lo cual se debe verificar los contratos asociados a proveedores que estén desarrollando proyectos en la entidad.

RESULTADO

Los auditados aportaron evidencia documental relacionada con la ficha de viabilidad técnica del proceso para la prestación de servicios de soporte, mantenimiento, actualización, apoyo, formulación y capacitación funcional del Sistema de Gestión Humana "SARA". Además, se presentaron estudios previos de contratación directa para estos servicios, así como para el programa de almacén e inventarios de activos fijos "SOA" de la U.A.E. Contaduría General de la Nación. También se incluyeron fichas de viabilidad técnica para la adquisición de licencias Suite Adobe completa y estudios previos de mínima cuantía para la adquisición de cuatro (4) licencias Adobe Creative Cloud for Teams All Apps All Multiple Platforms Multi Languages Level 1 por 12 meses.

En estos documentos se evidenciaron acciones realizadas por el GIT de Apoyo Informático para definir los estudios previos y las fichas de viabilidad de proyectos con componentes tecnológicos, así como en los estudios de mercado realizados para la adquisición de servicios o bienes de Tecnologías de la Información (TI). Estas acciones cumplen con las directrices establecidas por Colombia Compra Eficiente para la contratación y compras estatales, especialmente en lo referente a TI.

HALLAZGO

Revisada y analizada la información, se identificó la ausencia de metodologías de gestión de proyectos de TI; guías y manuales para la gestión de proyectos de TI; programa de capacitación continua para los líderes de proyectos de TI; formación o capacitación en gestión de proyectos y TI (PMP, ITIL, y PRINCE2, entre otros); plan de proyecto detallado; monitoreo y evaluación del progreso de los proyectos; participación transversal de la alta y media gerencia, líderes de procesos y dueños de activos de información en la planificación y ejecución de proyectos de TI; mecanismos de comunicación; sistema de gestión de riesgos de los proyectos de TI; evaluación del retorno de la inversión, y metodología para evaluar el retorno de la inversión (ROI) de los proyectos de TI, entre otras.

RECOMENDACIÓN

Desarrollar e implementar un marco integral para la gestión de proyectos de TI que incluya metodologías estándar reconocidas como PMP, ITIL, y PRINCE2. Este marco debe abarcar guías y manuales específicos para la gestión de proyectos de TI, así como un programa de capacitación continua para los líderes de proyectos y demás personal involucrado. Además, se debe establecer un plan de proyectos detallado que incluya mecanismos de monitoreo y evaluación del progreso, y una metodología para la gestión de riesgos de los proyectos de TI.

Es crucial asegurar la participación transversal de la alta y media gerencia, líderes de procesos y responsables de activos de información en la planificación y ejecución de los proyectos. Asimismo, deben implementarse mecanismos eficaces de comunicación y una metodología para evaluar el retorno de la inversión (ROI) de los proyectos de TI, garantizando que las inversiones en tecnología se alineen con los objetivos estratégicos de la entidad y generen el valor esperado.

2.4.3 Gestión de proyectos de TI - LI.GO.10.

La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe gestionar todas las iniciativas y proyectos de TI, utilizando una metodología formal de gestión de proyectos que incorpore el uso de lecciones aprendidas y un esquema de gestión de cambios, mediante:

Planes de proyectos que incluyan lo solicitado por la metodología de gestión de proyectos definida para la entidad, por ejemplo:

- Matriz de interesados (stakeholders)
- Acta de constitución.
- Definición de Alcance.
- Cronograma.
- Matriz RACI.
- Matriz de Comunicaciones.
- Matriz de Riesgos.
- Plan de calidad.
- Gestión de adquisiciones, contratos.
- Actas de aceptación de entregables.
- Actas de comités de seguimiento y/o ejecutivos.
- Formatos de solicitudes de cambios.
- Informes de avance y estado del proyecto.
- Documento de lecciones aprendidas.
- Documento de cierre del proyecto.

Para demostrar gestión sobre los planes, se deben verificar las evidencias generadas con relación a las matrices de riesgos: Acciones y planes de mitigación.

Actas de aceptación de entregables firmadas. Cronograma inicial y ajustes al cronograma. Formatos de solicitud de cambios en el proyecto.

Actas de seguimiento al proyecto firmadas y archivadas en las carpetas de los contratos.

Las carpetas de los proyectos deben estar actualizadas y evidenciar gestión en los tiempos y costos, si se evidencian cambios en los estimadas iniciales, se deben verificar los formatos de solicitud de control de cambios aprobados por la entidad o comité pertinente.

Revisar como la Entidad integra la seguridad de la información en el ciclo de vida de los proyectos para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto. Tener en cuenta que esto no solamente aplica para proyectos de TI, por ejemplo, puede aplicar en proyectos de traslado de activos de información, gestión de instalaciones, personal en outsourcing que soporta procesos de la organización.

Las mejores prácticas sugieren:

- Que los objetivos de la seguridad de la información se incluyan en los objetivos del proyecto.

- Que la valoración de los riesgos de seguridad de la información se lleve a cabo en una etapa temprana del proyecto, para identificar los controles necesarios.

- Que la seguridad de la información sea parte de todas las fases de la metodología del proyecto aplicada.

RESULTADO

Documentos aportados:

- TIC-GDP-MPY-DOCS-Metodologia-MGPTI.pdf. Documento titulado "METODOLOGÍA PARA GESTIÓN DE PROYECTOS DE TECNOLOGÍAS DE INFORMACIÓN". El control de cambios indica que la versión inicial es del 10 de septiembre del 2018, la última actualización del documento se realizó el 20 de mayo del 2022.

  El documento presenta contenidos que abarcan principalmente los siguientes apartados: Introducción, Alcance, Metodología de gestión de proyectos de tecnologías de información, Organización y responsabilidades, Roles y responsabilidades, Fase de factibilidad, Fase de inicio de proyecto, Fase de planificación de proyecto, Fase de ejecución y control de proyecto, Fase de cierre de proyecto y Bibliografía, entre otros.

- Carpeta TIC-GDP-MPY-2023-GLPI-FASE0: En esta carpeta se ubican documentos como el Estudio preliminar y factibilidad de proyecto, Matriz de riesgos precontractual, Matriz de riesgos del proyecto, Matriz de roles y funciones del proyecto, Matriz de talento humano y Solicitud de proyectos.

- Carpeta TIC-GDP-MPY-2023-GLPI-FASE1: En esta carpeta ubicaron documentos como: Acta de constitución del proyecto, Matriz de comunicaciones del proyecto, Matriz poder/interés del proyecto, Matriz de registro de interesados del proyecto, y Matriz de riesgos del proyecto.

- Carpeta TIC-GDP-MPY-2023-GLPI-FASE2: Carpeta que contiene Grabaciones Reuniones, Correo con situación Soporte GLPI 19122024, Correo reporte riesgo, Presentación Estatus Contrato GLPI, Acta de reunión (Realizar reunión de seguimiento para revisar el cronograma enviado por el proveedor, así mismo revisar los compromisos adquiridos en reunión anterior), Acta de reunión (Implementación, soporte y transferencia de conocimiento de la solución GLPI para la gestión de servicios de la CGN), Acta de reunión (Realizar reunión de apertura para presentar el proveedor aprobado, las personas que participan en el proyecto, los requerimientos y las diferentes actividades con las tareas que se trabajaran en el proyecto), Formato definición de eventos (formato sin diligenciar), cronograma del proyecto, plan migración nueva versión, Plan de trabajo proyecto adquisición servicio GLPI (diligenciado parcialmente), Pruebas funcionales, y Pruebas técnicas - LDAP sobre GLPI.

- Carpeta TIC-GDP-MPY-2023-GLPI-FASE3: Seguimiento de proyectos.

HALLAZGOS

- Con base en las evidencias aportadas, se identificó la ausencia de un Plan de Calidad y de actas de comités de seguimiento y/o ejecutivos. Esta falta de documentación dificulta la trazabilidad y el control efectivo de la calidad en la gestión de proyectos.

- Los documentos aportados no presentan información crítica de control de calidad, como

la fecha de aprobación, el código, y la versión. Esto sugiere que los formatos utilizados para la gestión del proyecto no han sido formalmente incorporados al Sistema Integrado de Gestión Institucional de la UEA Contaduría General de la Nación (CGN), lo que puede afectar la coherencia y la consistencia en la gestión documental.

- Se identificó que algunos documentos carecen del registro de firmas requerido, como es el caso del formato de "ACTA DE CONSTITUCIÓN DEL PROYECTO," que no presenta ninguna firma. Además, otros documentos, como el "ESTUDIO PRELIMINAR Y FACTIBILIDAD DE PROYECTO," presentan firmas parciales, lo que compromete la validez y el respaldo formal de estos documentos.

- Se constató que la seguridad de la información no está integrada en el ciclo de vida del proyecto. Además, los riesgos relacionados con la seguridad de la información no se identifican ni se gestionan como parte integral del proyecto, y no se contemplan en todas las fases de la metodología aplicada. Esto genera vulnerabilidades significativas en la gestión de los proyectos y compromete la protección de la información institucional.

RECOMENDACIÓN

Es pertinente desarrollar e implementar un Plan de Calidad para la gestión de proyectos, que incluya la creación de actas de comités de seguimiento y/o ejecutivos, garantizando la trazabilidad y el control efectivo de la calidad en cada fase del proyecto. Asimismo, es importante formalizar todos los documentos y formatos utilizados en la gestión de proyectos, asegurando que contengan información crítica como fecha de aprobación, código, y versión, y que estén debidamente incorporados al Sistema Integrado de Gestión Institucional de la UEA Contaduría General de la Nación (CGN). Además, reforzar el proceso de aprobación documental para que todos los documentos clave cuenten con las firmas requeridas, garantizando así su validez y respaldo formal. Finalmente, se debe integrar la seguridad de la información en todas las fases del ciclo de vida de los proyectos, asegurando la identificación y gestión adecuada de los riesgos asociados a la seguridad de la información, a fin de proteger eficazmente la información institucional y mitigar vulnerabilidades significativas.

2.4.4 Responsabilidad y gestión de Componentes de información - LI.INF.01

La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir las directrices y liderar la gestión de los componentes de información durante su ciclo de vida. Así mismo, debe trabajar en conjunto con las dependencias para establecer acuerdos que garanticen la calidad de la información, para lo cual debe implementar:

- Política de Tecnologías de la Información (TI), actualizada, aprobada, publicada y apropiada en la entidad. Además, debe incorporar políticas de gestión del ciclo de vida de los componentes de información, estar actualizada

- Modelo o esquema de gobierno de Información, aprobado, publicado y apropiado en la entidad, el cual debe contener como mínimo los aspectos definidos en la guía G.INF.06

Guía técnica del gobierno del Dato, con relación a gobernanza (custodios y responsables), calidad de datos, migración de datos, ciclo de vida de los datos y datos maestros. El modelo debe estar acompañado de un plan de implementación del mismo.

- Proceso de gestión del ciclo de vida de los componentes de información.
- Roles y perfiles que desempeñen las funciones de gestión de los componentes de información.
- Acuerdos entre áreas que establezcan criterios de calidad para la producción, intercambio y consumo de componentes de información.

RESULTADO

Documentos aportados:

- Activos de información.pdf: El documento presenta información relacionada con el inventario de activos de tipo información; inventario de activos de tipo hardware, software y servicios; e inventario de activos de tipo talento humano.
- PAA_Ver_10_May_16_2024: El documento presenta información relacionada con el plan de adquisiciones de la entidad.
- PETI-2023-2026V1.3.pdf: Este documento se describió en el numeral 2.2.1.
- POLADMRIESGO.pdf: El documento establece los parámetros necesarios para una administración efectiva de riesgos que incluya: el contexto estratégico, la identificación, análisis, y valoración de riesgos, así como la formulación de políticas de administración del riesgo, su trazabilidad, registro y monitoreo. Orientar la toma de decisiones informadas y fomentar el pensamiento basado en riesgos dentro de la entidad. Promover la mejora continua en todos los procesos. Realizar un seguimiento exhaustivo de los riesgos asociados a los proyectos de inversión de la CGN, con el objetivo de reducir el nivel de riesgo en las etapas de inversión y operación de los proyectos. Implementar una gestión adecuada mediante la identificación de acciones de control, respuestas oportunas y estrategias institucionales para enfrentar situaciones que puedan comprometer el cumplimiento de la misión y el logro de los objetivos.
- Res_193_2019.pdf: Este documento se describió en el numeral 2.2.6.
- Resolución 383 del 2023.pdf: Resolución por la cual se designa al Oficial de Seguridad y Privacidad de la Información en la CGN y se asignan sus funciones.
- TIC-SEG-SGS-ACT-2018-ActaSIGIVariosSEG1.pdf: Acta número 9 de septiembre del 2018 del comité SIGI, en la cual se observó que uno de los temas es el de la socialización temas tecnológicos de interés del GIT de Apoyo Informático.

HALLAZGO

Una vez analizadas las evidencias aportadas por el proceso, se constató la ausencia de una política de Tecnologías de la Información (TI), la cual debe incorporar directrices para la gestión del ciclo de vida de los componentes de información. Así mismo, no se evidenció la existencia de un documento que describa el modelo o esquema de gobierno de la información, conforme a los aspectos definidos en la "Guía G.INF.06 - Guía Técnica del Gobierno del Dato".

RECOMENDACIÓN

Es pertinente desarrollar y formalizar una política de Tecnologías de la Información (TI) que incluya directrices para la gestión del ciclo de vida de los componentes de información. Esta política debe alinearse con las mejores prácticas y contemplar aspectos como la adquisición, uso, mantenimiento, y disposición final de los activos de información. Además, elaborar un documento que describa el modelo o esquema de gobierno de la información, en cumplimiento con los lineamientos establecidos en la "Guía G.INF.06 - Guía Técnica del Gobierno del Dato". Lo anterior en línea con lo establecido en el criterio.

2.4.5 Implementación de la Política de Gestión de Activos

Implementación de la Política de Gestión de Activos, aprobada por la alta Dirección y socializada al interior de la Entidad, mediante la cual se indica los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de Información. Las políticas relacionadas con gestión de activos deben contemplar como mínimo:

- Identificación de Activos.
- Clasificación de Activos.
- Etiquetado de la Información.
- Devolución de los Activos.
- Gestión de medios removibles.
- Disposición de los activos.
- Dispositivos móviles.

RESULTADO

Documentos aportados:

- Acta No. 11 CIGD - 13 de octubre de 2022.pdf: Documento descrito en el numeral 2.2.3.

- GTI-PRC11.pdf: Documento descrito en el numeral 2.1.21.

- Manual de Seguridad de la Información 2022.pdf: Documento descrito en el numeral 2.1.19.

- PI-PRC28.pdf: Documento titulado "GESTIÓN DE ACTIVOS DE INFORMACIÓN" correspondiente a un procedimiento, mediante el cual se establecen las acciones necesarias para garantizar la administración del inventario de activos de información, mediante la custodia, seguimiento y control en su ciclo de vida.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó la Política de Gestión de Activos de información, debidamente aprobado por la alta dirección y socializado al interior de la entidad. Esta política debe incluir elementos esenciales como Introducción, Objetivo, Objetivos específicos, Alcance, Condiciones de implementación, Roles y Responsabilidades, entre otros aspectos necesarios para su adecuada comprensión y aplicación.

RECOMENDACIÓN

Desarrollar, revisar, contextualizar, aprobar, implementar y apropiar una Política Integral de Gestión de Activos que establezca directrices claras y precisas para la identificación, uso, administración y responsabilidad de los activos de información. Esta política debe ser comunicada de manera efectiva a todos los servidores públicos, contratistas y proveedores, asegurando su entendimiento y cumplimiento. Además, la política debe incluir la implementación de procedimientos específicos relacionados con la gestión de activos, tales como: Identificación de Activos, Clasificación de Activos, Etiquetado de la Información, Devolución de los Activos, Gestión de Medios Removibles, Disposición de los Activos, y Gestión de Dispositivos Móviles

2.4.6 Implementación del Procedimiento de Controles Criptográficos.

Implementación del Procedimiento de Controles Criptográficos, debidamente documentado, socializado y aprobado por el comité que integre los sistemas de gestión institucional, mediante el cual se establezcan las especificaciones de cómo se utilizará la criptografía dentro de los sistemas de información de la organización para garantizar su integridad, disponibilidad y confidencialidad, además, de las especificaciones de la complejidad de los controles criptográficos a emplear, dependiendo de la criticidad de la información que circulará a través de la red o se encontrará alojada en un sistema determinado.

RESULTADO

Documentos aportados:

- Estado de TOKENS 22_02_2024 Area.pdf: Documento que presenta información en una tabla con los siguientes campos: Tipo de Documento, Identificación, Nombre, SIIN, GIT SGAF, Centralización, Planeación, Control Interno, CHIP y Apoyo Informático.

- Estado de TOKENS 22_02_2024.pdf: Documento que registra información en una tabla con los siguientes campos: Documento, Número de Documento, Nombre, Unidad,

Fecha de Solicitud, Número, Estado, Estado Actual, Serial, Fecha de Emisión y Fecha de Vencimiento.

HALLAZGO

Como resultado del análisis de las evidencias aportadas, se identificó la ausencia del Procedimiento de Controles Criptográficos, debidamente aprobado por la alta dirección y socializado al interior de la entidad. Este procedimiento debe incluir elementos esenciales como Introducción, Objetivo, Objetivos específicos, Alcance, Condiciones de implementación, Roles y Responsabilidades, entre otros aspectos necesarios para su adecuada comprensión y aplicación.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar un Procedimiento de Controles Criptográficos mediante el cual se defina las actividades para proteger la confidencialidad, integridad y autenticidad de la información mediante técnicas criptográficas avanzadas. Este procedimiento debe abarca la selección, implementación y gestión de algoritmos y claves criptográficas, y detallar los procesos para su generación, distribución, almacenamiento, renovación y destrucción. Además, establecer roles y responsabilidades, medidas de monitoreo y auditoría, y promueve la formación del personal para prevenir accesos no autorizados y asegurar el cumplimiento de normativas y políticas de seguridad de la información.

2.4.7 Implementación del Procedimiento de Gestión de Llaves Criptográficas.

Implementación del Procedimiento de Gestión de Llaves Criptográficas, debidamente documentado, socializado y aprobado por el comité que integre los sistemas de gestión institucional, el cual establece las especificaciones del ciclo de vida de las llaves criptográficas dentro de la entidad, desde que se crean hasta que se distribuyen a cada usuario o aplicación de manera segura, junto con las especificaciones de los aspectos como la creación de las llaves, obtención de certificados, almacenamiento seguro de las llaves, actualización o cambio, revocación y recuperación de llaves.

RESULTADO

El proceso no presentó evidencia documental que respaldara el cumplimiento de este criterio. Adicionalmente, los auditados manifestaron que consideran que este criterio no es aplicable para su implementación.

Es fundamental resaltar la importancia de proporcionar la documentación necesaria y justificaciones adecuadas para cualquier criterio, incluso aquellos que se consideran no aplicables, para asegurar la transparencia y la coherencia en los procesos de auditoría. La ausencia de evidencia y justificación puede implicar un riesgo para el cumplimiento de las políticas y normativas establecidas, así como para la mejora continua de los procesos institucionales.

La implementación de políticas y procedimientos de seguridad informática es crucial para garantizar la protección integral de la información dentro de la entidad. Estos elementos son fundamentales no solo para proteger los datos sensibles contra accesos no autorizados, alteraciones o pérdidas, sino también para cumplir con las normativas legales y regulatorias que exigen salvaguardas específicas. Al establecer controles robustos, las entidades pueden mitigar riesgos asociados con amenazas de seguridad informática y mantener la continuidad operativa frente a posibles incidentes de seguridad.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó un Procedimiento o actividades para la Gestión de Llaves Criptográficas, debidamente aprobado por la alta dirección y socializado al interior de la entidad; acorde a lo establecido en la NTC ISO 27001 y los lineamientos de control del MSPI de MINTIC.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar el Procedimiento de Gestión de Llaves Criptográficas para establecer las actividades para la generación, almacenamiento, distribución, uso, mantenimiento y revocación de las llaves criptográficas utilizadas en los sistemas de información de la entidad. Este procedimiento tiene como finalidad garantizar la seguridad y confidencialidad de la información protegida mediante cifrado, asegurando que las llaves criptográficas sean gestionadas de manera segura a lo largo de su ciclo de vida. Además, busca minimizar los riesgos asociados con el uso inadecuado o la pérdida de llaves, asegurando que solo personal autorizado tenga acceso a ellas y que se cumplan las políticas de seguridad establecidas. Asimismo, el procedimiento define responsabilidades claras y roles dentro de la organización para la gestión efectiva de las llaves criptográficas, asegurando la integridad y disponibilidad de los datos protegidos mediante cifrado.

2.4.8 Implementación del Política de Control De Acceso

La política establece los lineamientos para delimitar el acceso y uso aceptable de la Infraestructura Tecnológica – IT, equipamiento computacional, servicios tecnológicos, sistemas de información y servicios de gestión de la información, así como de las redes de datos de la entidad y que estén debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico y físico; debe contener lo siguiente:

- Los requisitos de seguridad para las aplicaciones del negocio.
- Las políticas para la divulgación y autorización de la información, y los niveles de seguridad de la información y de clasificación de la información.
- La coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes.
- la legislación pertinente y cualquier obligación contractual concerniente a la limitación del acceso a datos o servicios.
- la gestión de los derechos de acceso en un entorno distribuido y en red, que reconoce todos los tipos de conexiones disponibles.

- La separación de los roles de control de acceso, (solicitud de acceso, autorización de acceso, administración del acceso);
- Los requisitos para la autorización formal de las solicitudes de acceso.
- Los requisitos para la revisión periódica de los derechos de acceso.
- El retiro de los derechos de acceso.
- El ingreso de los registros de todos los eventos significativos concernientes al uso y gestión de identificación de los usuarios, e información de autenticación secreta, en el archivo permanente.
- Los roles de acceso privilegiado.

RESULTADO

Documento aportado:

Manual de Seguridad de la Información.pdf: Documento descrito en el numeral 2.1.19.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó la Política de Control de Acceso, debidamente aprobado por la alta dirección y socializado al interior de la entidad.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar la Política de Control de Acceso.

2.4.9 Implementación de la Política de desarrollo seguro

Implementar la Política de desarrollo seguro para establecer y aplicar reglas para el desarrollo de software y de sistemas de información, a los desarrollos que se dan dentro de la entidad, la cual se debe enmarcar en los siguientes lineamientos:

- Definir la seguridad del ambiente de desarrollo.
- Orientar la seguridad en el ciclo de vida de desarrollo del software: Definir la seguridad en la metodología de desarrollo de software y establecer las directrices de codificación seguras para cada lenguaje de programación usado.
- Definir los requisitos de seguridad en la fase diseño.
- Definir los puntos de chequeo de seguridad dentro de los hitos del proyecto.
- Establecer los depósitos seguros.
- Definir la seguridad en el control de la versión.
- Establecer el conocimiento requerido sobre seguridad de la aplicación.
- Definir la capacidad de los desarrolladores para evitar, encontrar y resolver las vulnerabilidades.

RESULTADO

Documentos aportados:

- GTI07-FOR03 Documento Guiones de prueba de seguridad.xls: Formato titulado "DOCUMENTOS GUIONES DE PRUEBA" utilizado para el registro de las pruebas realizadas a una funcionalidad especifica según la información de los datos de: No. Evento, Descripción del Evento, Resultado Esperado, Medio de Verificación, Primera Iteración (Estado, Observación, Ejecutor y Fecha), y Segunda Iteración (Estado, Observación, Ejecutor y Fecha).

- GTI07-POL01- Política de Desarrollo y Mantenimiento de Software.pdf: Documento titulado "POLÍTICAS DE DESARROLLO Y MANTENIMIENTO DE SOFTWARE DE LA CONTADURÍA GENERAL DE LA NACIÓN", el cual describe los lineamientos para el mantenimiento y la construcción de software que se aplican en la Contaduría General de la Nación. El documento presenta los apartes de: Introducción, Alcance, Actores y funciones, Ciclo de desarrollo, y Detalle de las políticas.

- GTI-PRC07 Desarrollo de software.pdf: Procedimiento que establece las actividades para la producción de un producto de software que reúna los requisitos de los usuarios, tanto internos como externos de la Contaduría General de la Nación.

- MetodologiaDeDesarrolloyMMtoDeSoftware.pdf: Documento titulado "METODOLOGÍA DE DESARROLLO Y MANTENIMIENTO DE SOFTWARE", el cual describe la metodología de desarrollo y mantenimiento de software a implementar por el grupo de Desarrollo de Software en el procedimiento de Desarrollo y Mantenimiento de Software. En el documento se describen las actividades a realizar por los integrantes del grupo de desarrollo al implementar un nuevo proyecto. Desde la obtención de requerimientos hasta estar en estado de producción, incluyendo reuniones de SCRUM, documentación, roles de los integrantes, Iteraciones, y planeaciones de Sprint, entre otros.

HALLAZGO

Como resultado del análisis de las evidencias aportadas, se identificó la ausencia de la Política de desarrollo seguro para establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la entidad.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar la Política de desarrollo seguro con directrices para garantizar que todos los desarrollos tecnológicos realizados se adhieran a estándares de seguridad, minimizando las vulnerabilidades y riesgos asociados a amenazas de seguridad digital. La política debe asegurar que las prácticas de desarrollo incluyan la implementación de controles de seguridad desde las etapas iniciales del diseño hasta la implementación y el mantenimiento de los sistemas.

2.4.10 Supervisión y Evaluación de Alta Disponibilidad en Infraestructuras Críticas y Servicios Tecnológicos

Monitoreo, seguimiento y evaluación de las capacidades de alta disponibilidad de las infraestructuras críticas y los servicios tecnológicos que impactan la continuidad operativa de la entidad, complementado con pruebas periódicas para asegurar la efectividad de estas capacidades.

RESULTADO

Documentos aportados:

- Informe Análisis vulnerabilidades CGN V2 correccion 2024.pdf: Documento titulado "ANÁLISIS DE VULNERABILIDADES", elaborado por KAVANTIC S.A.S en noviembre del 2023.

  El documento incluye una introducción, alcance, objetivo, metodología de clasificación, y reportes técnicos y ejecutivos sobre las vulnerabilidades identificadas. La empresa KAVANTIC fue contratada para realizar un re-test de vulnerabilidades en las IP internas y externas de la entidad, identificando problemas de seguridad y emitiendo recomendaciones para su corrección.

- TIC-SEG-PCO-GUIA-PCH-CHIP-FormatoPruebaCHP-RT_OCT-2023.pdf: Documento titulado "FORMATO DE PRUEBAS DEL PLAN DE CONTINGENCIA TECNOLÓGICA", el cual fue diligenciado para garantizar el funcionamiento del Sistemas de Información CHIP en ambiente productivo de la Entidad del Centro Alterno localizado en la ciudad de Medellín, restableciendo el servicio en el menor tiempo posible, conforme a las disposiciones de los procedimientos, actividades y elementos requeridos para afrontar una contingencia basado en la Guía de Implementación No 21 Contingencia Plataforma AIX – CHIP, CHIP producción.

- TIC-SEG-PCO-GUIA-PCH-CHIP-RT_v21.pdf: Documento titulado "ANEXO N° 21 - GUÍA DE IMPLEMENTACIÓN - CONTINGENCIA PLATAFORMA AIX – CHIP", el cual establece las características de los requerimientos físicos, de base de datos, lógicos; junto con las actividades de verificación de ambiente y fallos, recuperación de contingencia y recuperación de desastres, entre otras para ejecutar el plan de contingencia de la plataforma AIX del sistema CHIP.

- TIC-SEG-PCO-GUIA-PCH-ORFEO-FormatoPruebaOrfeo5.5-RT.PDF: Documento titulado "FORMATO DE PRUEBAS DEL PLAN DE CONTINGENCIA TECNOLÓGICA", el cual fue diligenciado para garantizar el funcionamiento del sistemas de gestión documental Orfeo 5.5 en ambiente de producción de la entidad en el centro de datos de la entidad, restableciendo el servicio en el menor tiempo posible, a través de la puesta en marcha de procedimientos, actividades y elementos requeridos para afrontar la contingencia basado en la guía de implementación Contingencia Orfeo.

- TIC-SEG-PCO-GUIA-PCH-ORFEO-GuiaContingenciaOrfeo5.5.pdf: Documento titulado

"ANEXO N° 12 - GUÍA DE IMPLEMENTACIÓN - CONTINGENCIA GESTIÓN DOCUMENTAL ORFEO 5.5", el cual establece las características de los requerimientos físicos, de base de datos, lógicos; junto con las actividades de verificación de ambiente y fallos, y contingencia, entre otras para ejecutar el plan de contingencia de la plataforma de gestión documental ORFEO 5.5.

HALLAZGO

Revisada y analizada la información proporcionada, se identificó la ausencia de evidencias documentales que permitan constatar el monitoreo, seguimiento y evaluación del modelo de continuidad y seguridad, supervisión de los niveles de seguridad, análisis de tendencias, identificación de nuevos riesgos y vulnerabilidades.

RECOMENDACIÓN

Implementar un proceso continuo de monitoreo, seguimiento y evaluación del modelo de continuidad y seguridad de la entidad, con el fin de garantizar una adecuada preparación ante incidentes que puedan comprometer tanto las operaciones como la seguridad de la información. Este proceso debe incluir la verificación de la eficacia de los niveles de seguridad, la identificación temprana de nuevos riesgos y vulnerabilidades, y la realización de análisis de tendencias para anticipar posibles amenazas. Además, se debe asegurar el cumplimiento de normativas vigentes, proporcionar capacitación regular al personal involucrado, y mantener una documentación completa y precisa de todas las actividades relacionadas.

2.4.11 Monitoreo y Evaluación de Impactos en Proyectos de TIC

Realización del monitoreo, seguimiento y evaluación de los efectos derivados de la implantación de los proyectos de TIC y de la ejecución del plan de gestión de impactos de los proyectos de TIC como medidas, responsables y nivel de progreso.

RESULTADO

Documento aportado:

TIC-GDP-MPY-2023-GLPI-FASE2-CronogramaProyecto.xls: Documento titulado "CRONOGRAMA DEL PROYECTO", el cual registra la planeación y ejecución de las actividades del proyecto de adquisición de servicios para mantener actualizada la herramienta GLPI. La información registrada en el documento presenta los datos de: No., Tareas del Proyecto, Responsable, Ticket, Dependencia entre Tareas, Fecha Inicio, Fecha cierre, Fecha Final, Días Retraso y meses (de septiembre a marzo).

HALLAZGO

Revisada y analizada la información proporcionada, se identificó la ausencia de evidencias documentales que permitan constatar el monitoreo, seguimiento y evaluación de los

efectos derivados de la implantación de los proyectos de TIC y del plan de gestión de impactos de los proyectos de TIC.

RECOMENDACIÓN

Es pertinente establecer un sistema de monitoreo y evaluación para los proyectos de TIC, asegurando que estos cumplan con los objetivos establecidos, generen beneficios tangibles y minimicen cualquier impacto negativo en la entidad. Este proceso debe incluir la verificación de la alineación de los proyectos con la estrategia institucional, la medición de los beneficios obtenidos, y la mitigación de impactos adversos. Además, es importante garantizar la sostenibilidad de los proyectos a largo plazo y el cumplimiento con todas las normativas vigentes. Se debe registrar las lecciones aprendidas, confirmar la alineación con los objetivos estratégicos y mantener una comunicación transparente con las partes interesadas sobre los resultados y efectos de los proyectos.

2.4.12 Identificación y Optimización de Oportunidades de Mejora en los Procesos de TI

Identificación de oportunidades de mejora en los procesos de TI, de modo que la entidad pueda focalizar esfuerzos en la optimización de estos a través de las TI para contribuir con el cumplimiento de los objetivos y metas institucionales; y los indicadores de desempeño de la gestión del MSPI.

RESULTADO

Documento aportado:

PETI-2023-2026V1.3.pdf: Este documento se describió en el numeral 2.2.1.

De acuerdo con las evidencias aportadas por el proceso, se identificaron proyectos o iniciativas de mejoramiento de los procesos de TI para contribuir al cumplimiento de las metas institucionales y los indicadores de desempeño de la gestión del MSPI.

2.5 ADQUISICIÓN Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

- Evaluar los procesos de adquisición y mantenimiento de software de aplicación, asegurando la selección adecuada, licenciamiento, actualización, y seguridad de las aplicaciones utilizadas en la organización.

2.5.1 Identificación y Optimización de Oportunidades de Mejora en los Procesos de TI

Para asegurar una adecuada gestión de TI, es fundamental implementar el proceso de gestión de TI en el mapa de procesos de la entidad. Este proceso debe estar debidamente documentado y actualizado, y su implementación debe ser formalmente publicada. Además, es necesario establecer y medir indicadores de desempeño que evidencien la efectividad y eficiencia del proceso de gestión de TI. Estos indicadores deben evaluar si el

proceso cumple con los objetivos establecidos y si contribuye al cumplimiento de los estándares y políticas de la entidad.

RESULTADO

Documento aportado:

FICHA CARACTERIZACIÓN GESTIÓN TICS.xls: Documento que registra la ficha de caracterización del Proceso de Gestión de TICs. Esta ficha presenta información relevante, como los proveedores internos y externos, las entradas necesarias para el proceso, las actividades específicas a realizar, las salidas o resultados esperados, los responsables de cada tarea y los clientes internos y externos que se benefician de dichos resultados.

En el Sistema Integrado de Gestión Institucional de la UEA Contaduría General de la Nación (CGN), se identificó un macroproceso denominado "Gestión TICs" en el mapa de procesos. Dentro de este macroproceso, se detallaron los siguientes procedimientos específicos para la gestión de las tecnologías de la información:

GTI-PRC10 - SEGURIDAD DE LA INFORMACIÓN
GTI-PRC04 - PLANEACIÓN Y GESTIÓN TICs_V0.2
GTI-PRC03 - OPERACIÓN CENTRO DE COMPUTO_V.10
GTI-PRC09 - MANTENIMIENTO DE SOFTWARE_V.07
GTI-PRC08 - GENERACIÓN DE VERSIÓN_ V.07
GTI-PRC07 - PROCEDIMIENTO DESARROLLO DE SOFTWARE_ V.10
GTI-PRC06 - CERTIFICACIÓN DE SOFTWARE_V.08
GTI-PRC02 - ADMINISTRACIÓN DE LA PLATAFORMA TECNOLÓGICA_ V.09
GTI-PRC11 - ADMINISTRACIÓN DE ACTIVOS TIC

HALLAZGO

La caracterización del proceso de Gestión TICs no incorpora un subproceso de gobierno de TI basado en las cinco (5) dimensiones de Tecnologías de la Información y las Comunicaciones (TIC): Gobierno TIC, Sistemas de Información, Infraestructura Tecnológica, Soporte y Apoyo, y Seguimiento y Control. Esto va en contra de lo establecido en el lineamiento LI.GO.04 del Macro-proceso de gestión de TI del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y las mejores prácticas recomendadas por la Biblioteca de Infraestructura de Tecnologías de la Información (ITIL).

RECOMENDACIÓN

Para cumplir con los lineamientos establecidos en el lineamiento LI.GO.04 del Macro-proceso de Gestión de TI del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y las mejores prácticas recomendadas por la Biblioteca de Infraestructura de Tecnologías de la Información (ITIL), se recomienda integrar un la caracterización del proceso de Gestión TICs, los lineamientos de los subprocesos de TI. Es necesario abarcar las cinco dimensiones fundamentales de las Tecnologías de la

Información y las Comunicaciones (TIC): Gobierno TIC, Sistemas de Información, Infraestructura Tecnológica, Soporte y Apoyo, y Seguimiento y Control. Incorporar estas dimensiones garantizará una gestión integral y efectiva, alineada con los estándares nacionales e internacionales, y mejorará la capacidad de la entidad para gestionar sus recursos tecnológicos de manera eficiente.

2.5.2 Implementación del Procedimiento de Separación de Ambientes

Implementar un Procedimiento de Separación de Ambientes, documentado, socializado y aprobado, con las especificaciones de cómo la entidad permite realizar una transición de los diferentes sistemas, desde el ambiente de desarrollo hacia el de producción. Dentro de los aspectos más importantes a considerar se encuentran la implementación de un ambiente de pruebas para las aplicaciones, definición de los requerimientos para la transición entre ambientes, la compatibilidad de los desarrollos con diferentes sistemas entre otros.

RESULTADO

Documentos aportados:

- Ambiente – RT.ppt: Documento con la disposición de la estructuración y diagramación de los servicios para los sistemas CHIP, BDME, SARA, y Portal CGN.

- Ambientes - Previos.ppt: Documento en el cual se observó la disposición de la estructuración y diagramación de los servicios para los ambientes de desarrollo, pruebas y producción de los sistemas SARA, CHIP, CELA, BDME, y MEFP.

- Inventario Servidores AIX -2024.pdf: Documento en el cual se registra la disposición de una tabla con la información de servicios tecnológicas con datos de: LPARs VIOS, Equipo, NOMBRE, IP, Core, Memoria RAM (GB), Cant. Almacenamiento, Sistema Operativo, Aplicaciones/BD/Sist. De Información, (U)nico/(A)lta Disponibilidad y Ambiente.

- Metodologia Desarrolloy Software.pdf: Documento titulado “METODOLOGÍA DE DESARROLLO Y MANTENIMIENTO DE SOFTWARE”, el cual detalla la metodología de desarrollo y mantenimiento de software a implementar por el grupo de Desarrollo de Software en el procedimiento de Desarrollo y Mantenimiento de Software.

HALLAZGO

De acuerdo con las evidencias aportadas por el proceso, no se identificó el Procedimiento de Separación de Ambientes, aprobado por la alta dirección y socializado al interior de la entidad.

RECOMENDACIÓN

Es procedente implementar el Procedimiento de Separación de Ambientes para asegurar la seguridad y la integridad de los sistemas de información. Este procedimiento debe garantizar la adecuada segregación de los entornos de desarrollo, pruebas y producción para minimizar riesgos como accesos no autorizados y cambios no controlados. Es fundamental que se asegure una implementación segura y controlada de cambios y actualizaciones, facilite una transición efectiva entre ambientes y mantenga la compatibilidad y estabilidad operativa, cumpliendo con los estándares y normativas vigentes.

2.5.3 Implementación de la Política de Integridad (manejo de información)

Implementar la Política de Integridad, aprobada por la alta Dirección y socializada al interior de la entidad, con las especificaciones para la información verbal, física o electrónica, a ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información. En el caso de vinculación contractual, el compromiso de administración y manejo integro e integral de la información interna y externa hará parte de las cláusulas del respectivo contrato, bajo la denominación de Cláusula de Integridad de la Información, además de establecer la vigencia de la política según el tipo de vinculación del personal al cual aplica el cumplimiento.

RESULTADO

Documento aportado:

POLITICA DE INTEGRIDAD: Documento que tiene como objetivo fortalecer una cultura organizacional basada en valores éticos. Aplicable a todos los servidores públicos, colaboradores, contratistas y usuarios, promueve comportamientos éticos y responsables en la administración pública. Los servidores y colaboradores deben cumplir con los principios establecidos, difundir los valores institucionales y garantizar su aplicación en todas las actividades. La política se evaluará continuamente para mejorarla, fomentando la participación, compromiso y adaptación de todos los involucrados.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó que la Política de Integridad, aprobada por la alta dirección y socializada al interior de la entidad, contemple el compromiso de administración y manejo integro e integral de la información interna y externa.

RECOMENDACIÓN

Es pertinente implementar la Política de Integridad la cual debe establecer las directrices para garantizar que todas las operaciones, procesos y sistemas de la entidad se desarrollen de manera íntegra y confiable. Esto implica proteger la información contra modificaciones no autorizadas, asegurar la precisión y confiabilidad de los datos, y promover prácticas que preserven la integridad de los activos y la información institucional frente a amenazas internas y externas. La política debe establecer directrices y procedimientos para asegurar que todos los aspectos operativos y administrativos se lleven a cabo de acuerdo con estándares éticos y legales, promoviendo una cultura organizacional basada en la integridad y la confianza. Además, la política debe establecer especificaciones para la información verbal, física o electrónica, de ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información.

2.5.4 Implementación del Procedimiento Ingreso Seguro a los Sistemas de Información

Implementación del Procedimiento Ingreso Seguro a los Sistemas de Información, documentado, socializado y aprobado con las especificaciones de cómo gestionar el acceso a los sistemas de información de manera segura, empleando métodos preventivos contra ataques de fuerza bruta, validando los datos completos para ingreso a los sistemas, empleando métodos para cifrar la información de acceso a través de la red entre otros.

RESULTADO

Documentos aportados:

- GTI010-FOR03 - Creación de usuarios aplicativo CHIP.pdf: Formato titulado “CREACIÓN DE USUARIOS APLICATIVO CHIP”.

- GTI-PRC10 Seguridad de la Información: Documento descrito en el numeral 2.1.14.

HALLAZGO

De acuerdo con las evidencias aportadas, no se identificó el Procedimiento para Ingreso Seguro a los Sistemas de Información, aprobado por la alta dirección y socializado al interior de la entidad.

RECOMENDACIÓN

Es importante implementar el Procedimiento para Ingreso Seguro a los Sistemas de Información para garantizar un acceso autorizado y seguro a los sistemas de información de la entidad. Este procedimiento debe incluir medidas rigurosas de autenticación y autorización, verificación continua de privilegios, detección de accesos no autorizados, y

auditorías regulares. Estas acciones protegerán la integridad, confidencialidad y disponibilidad de la información, minimizando riesgos de seguridad y asegurando el cumplimiento de las normativas y políticas internas.

2.5.5 Implementación del Procedimiento Adquisición, Desarrollo y Mantenimiento de Software

Implementación del Procedimiento Adquisición, Desarrollo y Mantenimiento de Software, documentado, socializado y aprobado con las especificaciones de cómo la entidad realiza la gestión de la seguridad de la información en los sistemas desarrollados internamente (inhouse) o adquiridos a un tercero, verificando que cada uno de ellos preserve la confidencialidad, integridad y disponibilidad de la información de la entidad. Dicha gestión y control también debe ser especificada para los sistemas ya existentes que son actualizados o modificados en la entidad. Se deben tener en cuenta el uso de ambientes de desarrollo, pruebas y producción para los sistemas de información.

RESULTADO

Documentos aportados:

- GTI-PRC07 Desarrollo de Software.pdf: Documento descrito en el numeral 2.4.9.

- GTI-PRC09 Mantenimiento de Software.pdf: Procedimiento que establece las actividades para garantizar el proceso de mejora y optimización del software después de su entrega al usuario final, así como también la corrección y prevención de los defectos de los productos de software de la Contaduría General de la Nación.

- TIC-CDS-GDPR-CHIP – AutenticacionChip.xls: Formato titulado "DOCUMENTOS GUIONES DE PRUEBA". La información registrada en el formato presenta los datos de: No. Evento, Descripción del Evento, Resultado Esperado, Medio de Verificación, Primera Iteración Versión: <24.11.0> (Estado, Observación, Ejecutor y Fecha), y Segunda Iteración Versión: <Nro. Versión> (Estado, Observación, Ejecutor y Fecha).

- TIC-CDS-GDPR-CHIP - SeguridadWeb entidades.xls: Formato titulado "GUIONES DE PRUEBA DE SEGURIDAD". La información registrada en el formato presenta los datos de: No., Descripción, Campo, Resultados esperados, Resultados reales, y Primera Iteración Versión: 24.11.0 (Estado, Observación, Ejecutor y Fecha).

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó el Procedimiento Adquisición, Desarrollo y Mantenimiento de Software, aprobado por la alta dirección y socializado al interior de la entidad.

RECOMENDACIÓN

Es pertinente implementar el Procedimiento de Adquisición, Desarrollo y Mantenimiento de Software que asegure que todas las actividades relacionadas con el software cumplan con estándares de calidad, seguridad y eficiencia, alineándose con los objetivos estratégicos de la entidad. Este procedimiento debe incluir la planificación, ejecución, administración y verificación de todas las fases del ciclo de vida del software. Asimismo, debe gestionar la seguridad de la información en sistemas desarrollados internamente o adquiridos, garantizando la confidencialidad, integridad y disponibilidad de la información, y aplicarse tanto a nuevos desarrollos como a sistemas existentes que se actualizan o modifican.

2.5.6 Implementación de la Política para análisis y especificaciones de requisitos de seguridad de la información

Implementar la Política para análisis y especificaciones de requisitos de seguridad de la información, la cual debe incluir los requisitos para los nuevos sistemas de información o para mejoras a los sistemas de información existentes:

- Establecer el nivel de confianza requerido con relación a la identificación declarada de los usuarios, para obtener los requisitos de autenticación de usuario.
- Definir los procesos de suministro de acceso y de autorización para usuarios del negocio, al igual que para usuarios privilegiados o técnicos.
- Informar a los usuarios y operadores sobre sus deberes y responsabilidades.
- Definir las necesidades de protección de activos involucrados, en particular acerca de disponibilidad, confidencialidad, integridad.
- Definir los requisitos obtenidos de los procesos del negocio, tales como los requisitos de ingreso y seguimiento, y de no repudio.
- Establecer los requisitos exigidos por otros controles de seguridad, (interfaces con el ingreso o seguimiento, o los sistemas de detección de fuga de datos).

RESULTADO

Documentos aportados:

- Acuerdo Confidencialidad_Oralia Franco.pdf: Formato MAN01-FOR31 ACUERDO DE CONFIDENCIALIDAD Y ACEPTACIÓN DE LAS POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN. El acuerdo fija los términos y condiciones bajo los cuales las partes mantendrán la confidencialidad de los datos e información intercambiados entre la U.A.E. CGN y el Contratista o proveedor. Este último se obliga a no revelar, divulgar, exhibir, mostrar, comunicar, utilizar y/o emplear la información con persona natural o jurídica, en su favor o en el de terceros, que reciban de la otra parte y en consecuencia a mantenerla de manera confidencial y privada y a proteger dicha información para evitar su divulgación no autorizada, ejerciendo sobre esta el mismo grado de diligencia que utiliza para proteger información confidencial de su propiedad.

- GTI02-POL01 - Política de Administración de Usuarios y_o Contraseñas (4).pdf:

Documento titulado "POLITICA DE ADMINISTRACION DE USUARIOS Y/O CONTRASEÑAS". El documento establece lineamientos para la gestión de usuarios, perfiles y contraseñas. La política describe que será aplicada al control de acceso lógico a los componentes tecnológicos de: Administración de Infraestructura (Servidores y Switches); Administración de Herramientas de Seguridad (Perimetral y Lógica); Plataformas de procesamiento (o sistemas operativos); Bases de datos; Sistemas de información; y Servicios de red y comunicaciones.

- GTI010-FOR03 - Creación de usuarios aplicativo CHIP CLAUDIA PATRICIA MORALES.pdf y GTI010-FOR03-CACHIP_HPACHECO.pdf: Formatos titulados "CREACIÓN DE USUARIOS APLICATIVO CHIP", los cuales se utilizan para crear un usuario (funcionario o contratista) en el aplicativo CHIP, además de solicitar autorización a los módulos de: Entidades, Ordenamiento territorial, Categorías, Formularios, Mensajes, Consolidación, Documentos y términos, Seguridad, Categorización, Sistema integrado de gestión y otros.

- GTI010-FOR09 SolicitudCuenstasDeUsuario_VPN.pdf: Formato titulado "SOLICITUD CREACIÓN DE CUENTAS DE USUARIO INSTITUCIONAL Y/O VPN", el cual presenta dos (2) tipos de solicitud: Tipo de Servicio y Solicitud VPN. El formato para la solicitud de Tipo de Servicio presenta registrado los servicios de: Cuenta de usuario, Buzón de correo, ORFEO, Aplicativo mesa de servicio, Impresora, IBMCOGNOS, Servidor de archivos y Otros.

HALLAZGO

Revisada y analizada la información proporcionada, se identificó que no existe la Política de seguridad de la información para nuevos sistemas de información o para mejoras a los sistemas de información existentes, debidamente aprobado por la alta dirección y socializado al interior de la entidad.

RECOMENDACIÓN

Es pertinente implementar la Política de Seguridad de la Información para nuevos sistemas o mejoras de la Contaduría General de la Nación (CGN) que establezca directrices para asegurar que el desarrollo, implementación y mejora de los sistemas cumplan con los estándares de seguridad requeridos. Esta política debe garantizar la protección de la integridad, confidencialidad y disponibilidad de los datos, integrando medidas de seguridad desde las etapas iniciales de diseño hasta el mantenimiento continuo. Además, debe promover el cumplimiento de normativas, asignar responsabilidades específicas, y establecer procedimientos para la evaluación continua y la gestión de riesgos asociados a los sistemas de información.

2.5.7 Implementación de la Política para seguridad de servicios de las aplicaciones en redes públicas

La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas, se debe proteger de actividades fraudulentas, disputas contractuales y

divulgación y modificación no autorizadas con las siguientes directrices para la seguridad de servicios de las aplicaciones en redes públicas:

- Definir el nivel de confianza que cada parte requiere con relación a la identidad declarada por la otra parte, (por medio de autenticación).
- Establecer los procesos de autorización asociados con quien puede aprobar el contenido o expedir o firmar documentos transaccionales clave.
- Asegurar que los socios de comunicación estén completamente informados de sus autorizaciones para suministro o uso del servicio.
- Determinar y cumplir los requisitos para confidencialidad, integridad, prueba de despacho y recibo de documentos clave y el no repudio de los contratos, (asociados con procesos de ofertas y contratos).
- Definir el nivel de confianza requerido en la integridad de los documentos clave.
- Establecer los requisitos de protección de cualquier información confidencial.
- Definir la confidencialidad e integridad de cualquier transacción de pedidos, información de pagos, detalles de la dirección de entrega y confirmación de recibos.
- Definir el grado de verificación apropiado de la información de pago suministrada por un cliente.
- Seleccionar la forma de arreglo de pago más apropiado para protegerse contra fraude.
- Definir el nivel de protección requerido para mantener la confidencialidad e integridad de la información del pedido;
- Evitar la pérdida o duplicación de información de la transacción.
- Definir la responsabilidad civil asociada con cualquier transacción fraudulenta.
- Establecer los requisitos de seguros.
- De acuerdo a NIST se deben usar mecanismos de chequeo de la integridad para verificar la integridad del software, firmware, e información.

RESULTADO

Documentos aportados:

- Carta de Aceptacion_MC-002-24_TOKENS DIGITALES-CERTIFICADOS SSL.pdf: Documento titulado “FORMATO DE COMUNICACIÓN Y ACEPTACIÓN DE LA OFERTA”, el cual describe que la oferta presentada por la Sociedad Gestión de Seguridad Electrónica S.A. (GSE) para el Proceso de Mínima Cuantía No. MC-002-2024 ha sido aceptada, conforme al literal C del artículo 94 de la Ley 1474 de 2011 y la normativa de contratación pública (Ley 80 de 1993, Ley 1150 de 2007, Ley 1474 de 2011, y el Decreto 1082 de 2015). La propuesta, radicada el 6 de junio de 2024 por Iván Felipe Dallos Rueda, cumple con las condiciones técnicas, experiencia y capacidad jurídica exigidas. El contrato celebrado tiene por objeto la adquisición de cincuenta certificados digitales criptográficos tipo Función Pública y certificados digitales (SSL) para los dominios y subdominios de la UAE Contaduría General de la Nación. La ejecución del contrato deberá seguir las condiciones del proceso de selección y los ofrecimientos formulados en la oferta económica, y se formalizará una Orden en el SECOP II detallando las condiciones de ejecución.

- GTI07-POL01- Política de Desarrollo y Mantenimiento de Software: Documento descrito

en el numeral 2.4.9.

HALLAZGO

Revisada y analizada la información proporcionada, se identificó que no existe un documento que detalle las especificaciones de los servicios de aplicaciones que pasan sobre redes públicas para proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas, con las siguientes directrices para la seguridad de servicios de las aplicaciones en redes públicas.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar la Política para seguridad de servicios de las aplicaciones en redes públicas para proteger la información transmitida a través de redes públicas en los servicios de aplicaciones con el fin de prevenir fraudes, disputas contractuales y accesos no autorizados. Para ello, se deben establecer niveles de confianza y autenticación, definir procesos de autorización, y garantizar la confidencialidad e integridad de los documentos clave. Asimismo, es importante asegurar la información relacionada con transacciones y protegerla contra la pérdida o duplicación. Además, se deben asignar responsabilidades en casos de fraude y cumplir con los requisitos de seguros, utilizando mecanismos de verificación de integridad conforme a las normas del NIST.

2.5.8 Supervisión y Seguimiento de Desarrollo de Sistemas Contratados Externamente

La entidad debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente mediante la implementación de las siguientes directrices:

- Definir los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente.
- Establecer los requisitos contractuales para prácticas seguras de diseño, codificación y pruebas.
- Definir el suministro del modelo de amenaza aprobado, al desarrollador externo.
- Realizar los ensayos de aceptación para determinar la calidad y exactitud de los entregables.
- Definir la evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.
- Definir la evidencia de que se han hecho pruebas suficientes para proteger contra contenido malicioso intencional y no intencional en el momento de la entrega.
- Definir la evidencia de que se han hecho pruebas suficientes para proteger contra la presencia de vulnerabilidades conocidas.
- Definir los certificados de depósito de títulos en garantía; (el código fuente ya no está disponible).
- Establecer el derecho contractual con relación a procesos y controles de desarrollo de auditorías.
- Documentar eficaz del ambiente de construcción usado para crear entregables.

- Establecer que la organización es responsable de la conformidad con las leyes aplicables y con la verificación de la eficiencia del control.

HALLAZGO

Se identificó que la entidad dispone de aplicaciones adquiridas externamente (Ejm. SOA), a los cuales el proceso TICs no les hace Supervisión y Seguimiento de Desarrollo de Sistemas.

RECOMEDACIÓN

Dado que la seguridad informática tiene como objetivo establecer políticas y procedimientos preventivos para evitar la materialización de riesgos digitales y, en caso de ocurrir, minimizar su impacto, la Contaduría General de la Nación (CGN) debe, de manera proactiva, definir e implementar políticas claras. Estas políticas deben establecer lineamientos específicos para el desarrollo de software contratado externamente, asegurando que los proveedores cumplan con los estándares de seguridad, calidad y cumplimiento normativo. La implementación de estas políticas no solo fortalecerá la postura de seguridad de la entidad, sino que también garantizará que cualquier desarrollo externo se alinee con los objetivos y requisitos de seguridad de la CGN, mitigando potenciales riesgos y asegurando la integridad y confidencialidad de los sistemas de información.

2.5.9 Gestión de la instalación y acreditación de sistemas de información

Verificar la correcta instalación y acreditación de sistemas, asegurando la integridad y disponibilidad de estos, así como el cumplimiento de estándares de seguridad informática y regulaciones vigentes.

2.5.9.1 Criterios de adopción y de compra de TI - LI.GO.07

La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir los criterios y metodologías que direccionen la toma de decisiones de inversión en Tecnologías de la Información (TI), buscando el beneficio económico y de servicio de la institución.

La metodología y criterios de evaluación de alternativas de solución e inversión en TI, debe estar documentada, ser conocida y accesible por el personal del área de TI. Las metodologías reconocidas en mercado pueden utilizarse en este proceso.

Resultados de los ejercicios de evaluación de alternativas de solución e inversión de TI donde se utilizaron los criterios y la metodología. Así mismo, en los estudios de mercado que se realizan para los procesos de contratación de servicios o bienes de TI, se debe verificar la existencia de criterios técnicos, funcionales y financieros que permitan la toma de decisiones de manera objetiva.

RESULTADO

Para este criterio el proceso no aporto evidencia documental. Es importante contextualizar que, en cumplimiento de las funciones asignadas al GIT de Apoyo Tecnológico, el grupo interno de trabajo realiza actividades que permiten establecer criterios técnicos para las compras de bienes o servicios de Tecnología. Estos criterios no se encuentran documentados bajo una metodología que direccione la toma de decisiones de inversión en Tecnologías de la Información (TI).

HALLAZGO

Producto del resultado de la prueba se identificó que no se ha desarrollado una metodología y criterios de evaluación de alternativas de solución e inversión en TI. La ausencia de una metodología documentada y formal para la adopción y compra de TI puede afectar la objetividad en la toma de decisiones, la transparencia del proceso de adquisición y comprometer la capacidad de la entidad para responder adecuadamente a sus necesidades tecnológicas.

RECOMENDACIÓN

Es pertinente desarrollar y documentar una metodología que guíe todas las decisiones de inversión en TI, cumpliendo con los lineamientos establecidos por MinTIC.

2.5.9.2 Análisis de riesgos – LI.ST.14

La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar el análisis y gestión de los riegos asociados a su infraestructura tecnológica haciendo énfasis en aquellos que puedan comprometer la seguridad de la información o que puedan afectar la prestación de un servicio de TI.

Se debe implementar:

- Plan de pruebas de seguridad de la información.
- Matriz de riesgos de seguridad de la información.
- Informes de análisis de vulnerabilidades realizados.

RESULTADO

Documentos aportados:

- 13.2_Plan de Tratamiento de Riesgos de Seguridad de la Informacion_2023.xls: Documento titulado “FORMATO DE DESCRIPCIÓN DEL RIESGO”. El documento se divide en dos secciones principales. La primera, “DESCRIPCIÓ RIESGO”, incluye detalles sobre los activos y los riesgos asociados, tales como descripción del riesgo, amenazas, tipo, causas, consecuencias, procesos aplicables, y evaluación del riesgo inicial. La segunda sección, “MAPA Y TRATAMIENTO”, aborda el tratamiento de los riesgos identificados, proporcionando información sobre el riesgo residual, opciones de tratamiento, acciones,

controles, soporte e indicadores. En la sección “DESCRIPCIÓ RIESGO”, se identificaron cuatro activos con un total de 24 riesgos distribuidos en Hardware, Software y Servicios (3 riesgos), Información (9 riesgos), Talento Humano (11 riesgos), y Oportunidades (1 riesgo). En “MAPA Y TRATAMIENTO”, todos los riesgos están clasificados bajo la categoría de "Seguridad de la Información".

- 13.2_PlanDeTratamientoDeRiesgosCGN.pdf: Documento titulado “PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN”, cuyo control de cambios muestra una versión inicial del 29 de diciembre de 2023, incluye secciones clave como Introducción, Objetivo, Alcance, Definiciones, Condiciones generales, Estrategias de cumplimiento, Roles y responsabilidades, Funciones, Desarrollo del Plan de Tratamiento de Riesgos (PTRSPI) y Anexos. El apartado "9. Desarrollo del Plan de Tratamiento de Riesgos" establece que el propósito del PTRSPI es definir las actividades para la identificación, evaluación, tratamiento y aceptación de los riesgos de seguridad y privacidad asociados a los activos críticos de información de la entidad.

- 13.3_CGN_FINAL_RETEST_nov_2023.xls: El documento está organizado en tres secciones: CGN, CGN (2022) y CGN (2023). Cada sección detalla información sobre vulnerabilidades, incluyendo nombre, severidad, activos afectados, impacto, descripción, recomendaciones, CVSS, plataforma, responsable, evidencia, justificación, fecha de respuesta y estado de resolución. La sección CGN (2023) también incluye datos adicionales como IP afectada, puertos, criticidad, y código de vulnerabilidad. En general, el documento ofrece un seguimiento detallado de vulnerabilidades y sus respectivas soluciones a lo largo de los años.

- 13.3_Informe Análisis vulnerabilidades CGN V2.pdf: Documento titulado “ANÁLISIS DE VULNERABILIDADES”. El documento, elaborado por KAVANTIC S.A.S en noviembre de 2023, incluye secciones como Introducción, Alcance, Objetivo, Metodología de clasificación, Informe ejecutivo, Informe técnico, vulnerabilidades identificadas y Definiciones.

  El proveedor KAVANTIC fue contratado para realizar re-test de vulnerabilidades a las IP (Protocolo de Internet) internas y externas de la entidad, con el fin de identificar y/o detectar problemas de seguridad, y los servicios asociados. Mediante pruebas identificaron las vulnerabilidades, su nivel de riesgo, y con base en esto, generaron recomendaciones las cuales la entidad debe realizar la remediación y/o corrección.

HALLAZGO

Revisada y analizada la información proporcionada, se evidenció que la entidad no tiene identificados riesgos para la infraestructura tecnológica, incluyendo ciberataques, intrusiones, fallas en aplicaciones, fallos eléctricos, vandalismo, sabotaje, problemas de hardware, interrupciones de servicio, mantenimiento inadecuado, sobrecarga del sistema, latencia, configuraciones incorrectas, fallos en servicios externos, y problemas con proveedores, entre otros. Además, no se detectaron riesgos asociados a componentes críticos como servidores físicos y virtuales, routers, switches, firewalls, VPN, servicios DNS

y DHCP, sistemas de almacenamiento, UPS, generadores, y sistemas de climatización. Es esencial incluir estos riesgos en el proceso de identificación y tratamiento para asegurar una gestión integral de la seguridad y operatividad de la infraestructura IT.

En concordancia con lo anterior, no se dispone de un plan de tratamiento de riesgos que aborde específicamente la gestión de los riesgos asociados a la infraestructura tecnológica de la entidad, con especial énfasis en aquellos que puedan comprometer la seguridad de la información o afectar la prestación de servicios de TI.

RECOMENDACIÓN

Es pertinente realizar un análisis y gestión de los riesgos asociados a la infraestructura tecnológica de la entidad. Este análisis debe enfocarse en aquellos riesgos que puedan comprometer la seguridad de la información o afectar la prestación de servicios de TI. Para ello, se deben implementar las siguientes acciones:

- Desarrollar un plan de pruebas de seguridad de la información para evaluar las vulnerabilidades y asegurar la protección adecuada de los sistemas.

- Establecer una matriz de riesgos de seguridad de la información que permita identificar, clasificar y priorizar los riesgos según su impacto y probabilidad.

- Generar informes detallados de análisis de vulnerabilidades realizados, para monitorear y abordar las debilidades detectadas en la infraestructura tecnológica.

2.5.9.3 Implementación de la Política de Seguridad para la Privacidad y Confidencialidad

Implementar la Política de Seguridad para la Privacidad y Confidencialidad, aprobada por la alta Dirección y socializada al interior de la entidad con la descripción del tratamiento y protección de datos personales que deben ser aplicados, conforme a lo establecido en la normatividad vigente. La política de privacidad debe contener como mínimo lo siguiente:

- Ámbito de aplicación
- Excepción al ámbito de aplicación de las políticas de tratamiento de datos personales
- Principios del tratamiento de datos personales: Legalidad, Finalidad, Libertad, Veracidad o calidad, Transparencia, Acceso y circulación restringida, Seguridad y Confidencialidad.
- Derechos de los titulares.
- Autorización del titular.
- Deberes de los responsables del Tratamiento.
- Controles criptográficos.

RESULTADO

Documentos aportados:

- Acta No. 11 CIGD - 13 de octubre de 2022.pdf: Documento descrito en el numeral 2.2.3.

- PI24-POL01: Política de Privacidad y Protección de Datos Personales.pdf. Documento donde se indica que la Política de Privacidad y Protección de Datos Personales de la U.A.E Contaduría General de la Nación se aplica a todas las bases de datos y archivos que contengan datos personales bajo su tratamiento, incluyendo aquellos obtenidos antes de la Ley 1581 de 2012. La política busca proteger los intereses y necesidades de los titulares de la información, cumpliendo con la normatividad vigente en materia de protección de datos y el principio de responsabilidad.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó la Política de Seguridad para la Privacidad y Confidencialidad, aprobada por la alta dirección y socializado al interior de la entidad.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar la Política de Seguridad para la Privacidad y Confidencialidad para proteger la integridad, disponibilidad y confidencialidad de la información sensible, incluidos datos personales. Esta política debe prevenir accesos no autorizados, divulgaciones inapropiadas, alteraciones y destrucción de información. Además, debe promover una cultura de seguridad, establecer procedimientos de protección, identificar y mitigar riesgos, y asegurar la formación continua del personal. También debe incluir planes de contingencia y recuperación para garantizar la continuidad operativa ante incidentes de seguridad.

2.5.9.4 Implementación del Procedimiento para la gestión de códigos fuente de los programas

Control de acceso a códigos fuente de programas o componentes tecnológicos mediante la implementación del procedimiento para la gestión de códigos fuente de los programas, que incluya:

- Definir en donde sea posible, las librerías de fuentes de programas no se deben mantener en los sistemas operativos.
- Gestionar los códigos fuente de los programas y las librerías de las fuentes de los programas se debería hacer de acuerdo con procedimientos establecidos.
- Establecer que el personal de soporte debe tener acceso restringido a las librerías de las fuentes de los programas.
- Definir que la actualización de las librerías de fuentes de programas y elementos asociados, y la entrega de fuentes de programas a los programadores sólo se deben hacer una vez que se haya recibido autorización apropiada.
- Establecer que los listados de programas se deben mantener en un entorno seguro.
- Conservar un registro de auditoría de todos los accesos a las librerías de fuentes de programas.

- Mantener y copiar las bibliotecas de fuentes de programas a través de procedimientos estrictos de control de cambios.

RESULTADO

Documento aportado:

ControlDeAccesoFuentes.pdf: Documento titulado "Control de acceso CGN", el cual describe que la CGN utiliza dos repositorios de código: uno basado en Apache Subversion con Tortoise, y otro basado en Git con Gitea. Git y Subversion son sistemas de control de versiones de código abierto, mientras que Gitea ofrece servicios adicionales como revisión de código y colaboración. Tortoise es un software para control de versiones basado en Subversion. Además, la CGN emplea un recurso compartido en la red interna para almacenamiento de ejecutables y versiones de despliegues, y un servidor Nexus para administrar el repositorio de librerías.

HALLAZGO

De acuerdo con las evidencias aportadas por el proceso, no se identificó el Procedimiento de Control de acceso a códigos fuente de programas o componentes tecnológicos, debidamente aprobado por la alta dirección y socializado al interior de la entidad.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar el Procedimiento de Control de Acceso a Códigos Fuente debe incluir la ubicación segura de las librerías de códigos fuente, una gestión conforme a procedimientos establecidos, acceso restringido para el personal de soporte, actualizaciones y entregas solo con autorización, almacenamiento seguro de listados de programas, un registro de auditoría de accesos, y un estricto control de cambios para las copias y mantenimiento de las librerías.

2.5.9.5 Implementación de Directrices para Establecer y Proteger Ambientes de Desarrollo Seguro

La entidad debe establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas mediante las siguientes directrices para ambiente de desarrollo seguro:

- Carácter sensible de los datos que el sistema va a procesar, almacenar y transmitir.
- Definir los requisitos externos e internos aplicables, (reglamentaciones o políticas).
- Definir los controles de seguridad ya implementados por la organización, que brindan soportar al desarrollo del sistema.
- Establecer la confiabilidad del personal que trabaja en el ambiente.
- Definir el grado de contratación externa asociado con el desarrollo del sistema.
- Definir la necesidad de separación entre diferentes ambientes de desarrollo.

- Definir el control de acceso al ambiente de desarrollo.
- Establecer el seguimiento de los cambios en el ambiente y en los códigos almacenados ahí.
- Definir las copias de respaldo se almacenan en lugares seguros fuera del sitio.
- Definir el control sobre el movimiento de datos desde y hacia el ambiente.

RESULTADO

Documentos aportados:

- Ambiente – RT.ppt: Documento descrito en el numeral 2.5.2.

- GTI03-POL01 - Política de copias de respaldo.pdf: El documento establece lineamientos para el desarrollo y mantenimiento de software en la CGN, desde la viabilidad funcional hasta la liberación en producción. Define roles y funciones para los involucrados y detalla el ciclo de desarrollo como iteraciones de estimación, planificación, desarrollo y presentación de versiones. Las solicitudes se gestionan mediante la Mesa de Servicio, siguiendo los lineamientos de seguridad de OWASP. Se planifica tiempo para soporte y mantenimiento, con seguimiento semanal, y se revaloran actividades urgentes no planificadas. El desarrollo externo debe cumplir con acuerdos y políticas de seguridad, aplicando controles rigurosos y manteniendo control de versiones.

- GTI010-FOR04 - Solicitud_VPN_Ingeniero Desarrollo.pdf: Documento descrito en el numeral 2.1.14.

- GTI-PRC07 Desarrollo de software.pdf: Documento descrito en el numeral 2.4.9.

- GTI-PRC10 Seguridad de la información.pdf: Documento descrito en el numeral 2.1.14.

- Inventario Servidores AIX.xls: Documento descrito en el numeral 2.5.2.

- Manual de Seguridad de la Información.pdf: Documento descrito en el numeral 2.1.19.

HALLAZGO

Revisada y analizada la información proporcionada, se identificó que no se dispone de las políticas, procedimientos, y metodologías para proteger los ambientes de desarrollo durante las tareas de desarrollo e integración de sistemas de información a lo largo de todo el ciclo de vida de los sistemas. Esta carencia impide establecer un marco integral que garantice la seguridad y la integridad en todas las fases, desde la concepción y planificación inicial hasta el diseño, desarrollo, pruebas, integración, despliegue y mantenimiento continuo de los sistemas.

RECOMENDACIÓN

Desarrollar e implementar políticas, procedimientos y metodologías específicas para proteger los ambientes de desarrollo en todas las fases del ciclo de vida de los sistemas

de información. Este marco debe incluir directrices claras para la seguridad y la integridad, desde la concepción y planificación inicial hasta el despliegue y mantenimiento continuo. Asimismo, se debe establecer un proceso de revisión y actualización periódica de estas políticas para asegurar su alineación con las mejores prácticas de la industria y las normativas vigentes. Además, es importante proporcionar capacitación adecuada al personal involucrado para garantizar la correcta aplicación de estas medidas.

2.5.9.6 Pruebas de Seguridad y Detección de Incidentes en el Desarrollo de Software

Durante el desarrollo de software o de sistemas de información se debe llevar a cabo pruebas de funcionalidad de la seguridad que permitan identificar que para pasar a producción los desarrollos se realizan pruebas de seguridad y que los procesos de detección de incidentes son probados periódicamente.

RESULTADO

Documento aportado:

GTI07-FOR03 Documento Guiones de prueba de seguridad.xls: Documento descrito en el numeral 2.4.9.

HALLAZGO

De acuerdo con las evidencias aportadas por el proceso, se identificó que no se dispone de documentación y evidencias que permitan identificar que para pasar a producción los desarrollos se realizan pruebas de seguridad y que además los procesos de detección de incidentes son probados periódicamente.

RECOMENDACIÓN

Es pertinente implementar un procedimiento que garantice la realización de pruebas de seguridad antes de cualquier desarrollo de software o sistema de información sea puesto en producción. Este procedimiento debe incluir la validación de los desarrollos para que cumplan con los estándares de seguridad establecidos, así como la implementación de pruebas periódicas de los procesos de detección de incidentes. Además, se debe llevar un registro detallado de estas pruebas y sus resultados para asegurar la trazabilidad y la mejora continua en la gestión de la seguridad de la información.

2.5.9.7 Programas de Pruebas y Criterios de Aceptación para Nuevos Sistemas y Actualizaciones

Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de pruebas que incluyan criterios y especificaciones para la aceptación final. Estos planes deben garantizar que todas las funcionalidades, tanto nuevas como modificadas, sean evaluadas a través de pruebas de aceptación antes de su implementación en producción. Además, los criterios de aceptación deben ser

documentados y alineados con los objetivos de seguridad, funcionalidad, rendimiento y usabilidad de los sistemas de información, permitiendo una revisión detallada y asegurando que el sistema cumpla con los requisitos y expectativas definidos.

RESULTADO

Documentos aportados:

- GTI06-FOR02 ActaReciboSatisfaccionOC0009.pdf: Documento titulado "ACTA DE RECIBO A SATISFACCIÓN" asociado al procedimiento de certificación de software. El formato es utilizado para dar por aprobado y aceptado un requerimiento de desarrollo e implementación de software por parte de los usuarios (funcionales).

- GTI06-FOR03 ActaEntregaVersión24.11.0.pdf: Documento titulado "ACTA DE ENTREGA SISTEMA CHIP PRODUCCION" correspondiente a un formato asociado al procedimiento de certificación de software, utilizado para certificar y aprobar la realización de pruebas por parte de los usuarios (funcionales) de requerimientos de desarrollo de software.

HALLAZGO

Revisada y analizada la información proporcionada, se identificó la falta de planes de pruebas para revisar las pruebas de aceptación de sistemas de información. Este faltante se presenta tanto para los sistemas de información nuevos como para las actualizaciones y nuevas versiones. Adicionalmente, no se encontraron programas de prueba para aceptación ni criterios de aceptación relacionados.

Es fundamental entender que un programa de pruebas para aceptación es un plan detallado que define las actividades y procedimientos necesarios para evaluar y verificar que un sistema de información, una actualización o una nueva versión cumpla con los requisitos especificados y esté listo para su uso operativo. Estos programas aseguran la calidad, funcionalidad, seguridad y conformidad del sistema antes de su implementación.

RECOMENDACIÓN

Es pertinente desarrollar, implementar y mantener programas de pruebas de aceptación y criterios de aceptación definidos y documentados para todos los sistemas de información nuevos, actualizaciones y nuevas versiones, asegurando así su adecuado control y evaluación antes de su despliegue en producción.

2.5.9.8 Implementación de la Política para protección de datos de prueba

Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente de acuerdo con la Política para protección de datos de prueba con las siguientes directrices:

- Establecer los procedimientos de control de acceso, que se aplican a los sistemas de aplicación operacionales, se debe aplicar también a los sistemas de aplicación de pruebas.

- Tener una autorización separada cada vez que se copia información operacional a un ambiente de pruebas.
- Definir que la información operacional se debe borrar del ambiente de pruebas inmediatamente después de finalizar las pruebas.
- Establecer que el copiado y uso de la información operacional se debe logged para suministrar un rastro de auditoría.

RESULTADO

Documentos aportados:

- TIC-CDS-CHIP-V24110-GDPR-0009-GitCHIP_Captura_razon_reenvios.xls: Formato titulado "DOCUMENTOS GUIONES DE PRUEBA". La información registrada en el formato presenta los datos de: No. Evento, Descripción del Evento, Resultado Esperado, Medio de Verificación, Primera Iteración Versión: <24.11.0> (Estado, Observación, Ejecutor y Fecha), y Segunda Iteración Versión: <Nro. Versión> (Estado, Observación, Ejecutor y Fecha).

- UpdateEnvironmentQA.txt: Documento en el cual se registró un script para actualizar el ambiente de pruebas del sistema CHIP después de las restauraciones.

HALLAZGO

Revisada y analizada la información proporcionada, se identificó la falta de la Política para protección de datos de prueba.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar la Política protección de datos de prueba para establecer las directrices y procedimientos que garanticen la seguridad y confidencialidad de los datos utilizados en los ambientes de prueba. Esta política busca proteger la integridad y privacidad de la información sensible y/o personal; extraída de ambientes de producción durante el desarrollo, pruebas y validación de sistemas de información. Además, de mitigar los riesgos asociados con la exposición o alteración no autorizada de los datos, asegurando que todos los datos de prueba sean tratados de acuerdo con los estándares de seguridad de la información y las normativas legales vigentes.

2.5.10 Gestión de Cambios en la Implementación de los sistemas de información

Evaluar la gestión de cambios en los sistemas y procesos tecnológicos, incluyendo la planificación, autorización, implementación y seguimiento de cambios para minimizar riesgos y mantener la estabilidad del entorno tecnológico.

2.5.10.1 Implementación del Procedimiento de Gestión de Cambios

Implementación del Procedimiento de Gestión de Cambios, documentado, socializado y aprobado con las especificaciones de cómo la entidad realiza el control de cambios en la organización, los procesos de negocio y **los sistemas de información** de manera segura. Se deben especificar aspectos como identificación y registro de cambios significativos, planificación y pruebas previas de los cambios a realizar, valoración de impactos, tiempos de no disponibilidad del servicio, comunicación a las áreas pertinentes, procedimientos de rollback (reversa) entre otros.

RESULTADO

Documento aportado:

GTI-PRC10 Seguridad de la Información: Documento descrito en el numeral 2.1.14.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó el Procedimiento de Gestión de Cambios de los sistemas de información, aprobado por la alta dirección y socializado al interior de la entidad.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar el Procedimiento de Gestión de Cambios de los sistemas de información para establecer las actividades que permitan asegurar todas las modificaciones en la infraestructura tecnológica, sistemas de información, servicios de gestión de información y procesos de la entidad, de tal forma que se realicen de manera controlada y coordinada. Este procedimiento tiene como fin minimizar los riesgos asociados con los cambios, garantizar la continuidad del negocio y asegurar que los cambios se implementen de forma eficaz y eficiente. Además, busca asegurar que los cambios sean evaluados, aprobados y documentados adecuadamente, contribuyendo a la estabilidad, seguridad y confiabilidad de los sistemas y servicios tecnológicos de la entidad.

2.5.10.2 Implementación del Procedimiento de Control Software

Implementación del Procedimiento de Control Software, debidamente documentado, socializado y aprobado con las especificaciones de cómo la entidad realiza el control de software, es decir, como limita el uso o instalación de software no autorizado dentro de la entidad, quienes están autorizados para realizar la instalación de software, como se realizaría la gestión de las solicitudes de instalación de software para los usuarios, cómo se realiza el inventario de software dentro de la entidad entre otros aspectos.

RESULTADO

Documento aportado:

Manual de Seguridad de la Información.pdf: Documento descrito en el numeral 2.1.19.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó un Procedimiento de Control Software, aprobado por la alta dirección y socializado al interior de la entidad.

El procedimiento debe incluir actividades de cómo la entidad realiza el control de software, es decir, como limita el uso o instalación de software no autorizado dentro de la entidad, quienes están autorizados para realizar la instalación de software, como se realizaría la gestión de las solicitudes de instalación de software para los usuarios, cómo se realiza el inventario de software dentro de la entidad entre otros aspectos.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar el Procedimiento de Control Software para establecer las actividades que aseguren la gestión adecuada y segura del software utilizado en la entidad. Este procedimiento tiene como propósito garantizar la legalidad, integridad y disponibilidad del software, así como prevenir y mitigar riesgos asociados con el uso no autorizado o indebido de aplicaciones. Además, busca optimizar el uso de los recursos tecnológicos, asegurar el cumplimiento de licencias y acuerdos contractuales, y mantener un entorno operativo seguro y eficiente para apoyar las funciones y objetivos estratégicos de la entidad.

2.5.10.3 Revisión Técnica y Validación de Aplicaciones tras Cambios en la Plataforma Operativa

Revisión técnica de las aplicaciones o sistemas de información después de realizar cambios en la plataforma de operación, mediante la atención de las directrices de:

- Revisar los procedimientos de integridad y control de aplicaciones para asegurar que no estén comprometidos debido a los cambios en las plataformas de operaciones.
- Asegurar que la notificación de los cambios en la plataforma operativa se hace a tiempo para permitir las pruebas y revisiones apropiadas antes de la implementación.
- Asegurar que se hacen cambios apropiados en los planes de continuidad del negocio.

RESULTADO

Documentos aportados:

- GTI02-FOR04 Administración de cambios a TI_CA_CHIP_Julio04_Vr24.13.0.pdf, GTI02-FOR04 Administracion de cambios a TI_RT_BDMEV24.11.0Mayo10_2024.pdf, y GTI02-FOR04 Administración de cambios a TI_RT_CHIPDiciembre27Vr24.11.0.pdf: Tipo de documento descrito en el numeral 2.5.2.3.

- GTI07-POL01- Política de Desarrollo y Mantenimiento de Software.pdf: Documento

descrito en el numeral 2.4.9.

- Plan De Contingencia Tecnologica 2020.pdf: Documento titulado "PLAN DE CONTINGENCIA TECNOLÓGICA". El documento en su control de cambios indica que la versión inicial es del 13 de diciembre del 2012, fecha de aprobación el 12 de noviembre del 2020.

  El documento presenta contenidos que abarcan principalmente los siguientes apartados: Introducción, Glosario, Generalidades, Política de contingencia de los servicios tecnológicos de la CGN, Objetivos, Alcance, Roles y Responsabilidades, Estrategia, Escenarios, Plan de acción, Infraestructura de TI, Acuerdos de niveles de servicio de tecnología, Identificación de riesgos, Interrupciones y nivel de afectación a servicios de TI, Logística de contingencia, Pruebas y actualización, bibliografía, y anexos.

HALLAZGO

Revisada y analizada la información proporcionada, se identificó que no existe documentación que especifique lineamientos para la revisión técnica de las aplicaciones después de cambios en la plataforma de operación.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar una Política de revisión técnica de las aplicaciones después de cambios en la plataforma de operación para establecer las directrices que permitan asegurar todas las aplicaciones en su funcionamiento y mantengan su integridad y seguridad tras cualquier modificación en la infraestructura operativa. Esto incluye la identificación y resolución de posibles problemas técnicos, garantizando así la continuidad y fiabilidad de los servicios y la protección de los datos manejados por las aplicaciones.

2.5.10.4 Implementación de la Política de seguridad para los cambios de paquetes de software

Restricciones en los cambios a los paquetes de software mediante la implementación de la Política de seguridad para los cambios de paquetes de software con las siguientes directrices de restricciones en los cambios a los paquetes de software:

- Definir el riesgo de que los procesos de integridad y los controles incluidos se vean comprometidos.
- Obtener el consentimiento del vendedor.
- Obtener del vendedor los cambios requeridos, a medida que se actualiza el programa estándar.
- Evaluar el impacto, si la organización llega a ser responsable del mantenimiento futuro del software como resultado de los cambios.
- Definir la compatibilidad con otro software en uso.

RESULTADO

Documentos aportados:

- GTI02-FOR04 - Administración de cambios de TI HELENA.pdf: Documento titulado "ADMINISTRACIÓN DE CAMBIOS A TI" asociados al procedimiento de administración de la plataforma tecnológica, utilizado para solicitar cambios en la plataforma tecnológica de la CGN.

- GTI07-POL01- Política de Desarrollo y Mantenimiento de Software.pdf: Documento descrito en el numeral 2.4.9.

- Mantenimiento 05-08-2023 - Misional_Firmware.pdf: Documento que corresponde al Informe de Actividades sobre el mantenimiento preventivo contratado bajo la Licitación Pública No. 01 de 2022, presentado por Professional Services SAS (PSS).

  El informe comprende las actividades realizadas por el contratista durante el mantenimiento preventivo llevado a cabo el día 5 de agosto de 2023, en el marco del contrato Licitación Pública No. 01 de 2022. Las actividades correspondieron a: Actualización del firmware en la máquina Power 10, Actualización del firmware de la HMC V10 y Mantenimiento preventivo de la maquina Power 10.

- Matriz Riesgos Seguridad de la Información.xls: El documento registra dos secciones: "FORMATO DE DESCRIPCIÓN DEL RIESGO" y "MAPA Y PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN - SEGURIDAD DIGITAL", cada una con 23 registros que analizan riesgos asociados a hardware, software, servicios, información y talento humano. Estas secciones detallan activos, amenazas, causas, vulnerabilidades, consecuencias, evaluaciones de riesgo inicial y residual, opciones de tratamiento y acciones de control implementadas.

HALLAZGO

Revisada y analizada la información proporcionada, se identificó que no existe la Política de seguridad para los cambios de paquetes de software.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar la Política de Restricciones en los cambios a los paquetes de software para establecer las directrices que garanticen la estabilidad, integridad y seguridad de los sistemas de información al controlar y limitar las modificaciones a los paquetes de software. Esto se logra mediante la implementación de lineamientos y procedimientos formales que aseguran que cualquier cambio sea autorizado, evaluado y aprobado, evitando alteraciones no autorizadas que puedan comprometer la operación y funcionalidad de los sistemas.

2.6 ACUERDOS DE NIVEL DE SERVICIOS INTERNOS Y EXTERNOS

Revisar la administración de servicios con terceros, asegurando la efectividad de los Acuerdos de Nivel de Servicio (ANS), la supervisión de la calidad del servicio y la gestión de incidentes y problemas.

2.6.1 Integración de los Acuerdos de Nivel de Servicio (ANS) en Planes de Continuidad y Recuperación

Evaluar de manera integral que las políticas y estándares establecidos para la gestión, seguimiento y cumplimiento de los Acuerdos de Nivel de Servicio (ANS) estén adecuadamente integrados en el Plan de Continuidad del Negocio (BCP) y en el Plan de Recuperación ante Desastres (DRP). Esta integración debe asegurar que los ANS no solo cumplan con los requisitos operativos y de servicio en circunstancias normales, sino que también sean efectivamente mantenidos y aplicados durante situaciones de emergencia o interrupciones significativas. Adicionalmente, es fundamental que se realicen pruebas periódicas y revisiones de estos planes para confirmar su efectividad en la continuidad del servicio y la recuperación rápida y segura de las operaciones críticas.

RESULTADO

Documento aportado:

TIC-SEG-PCO_PlanDeContingenciaTecnologica2022: Documento titulado "PLAN DE CONTINGENCIA TECNOLÓGICA", el cual establece un marco de referencia para la recuperación de componentes tecnológicos, facilitando a los administradores de TI de la CGN la ejecución ordenada y eficiente de actividades de atención de incidentes. Establecer una estructura organizada que incluya personal, actividades, tiempos y recursos para optimizar la gestión de incidentes desde la detección hasta la solución. Involucrar a los administradores en todas las etapas del proceso para detectar vulnerabilidades, minimizar tiempos de respuesta y garantizar un monitoreo efectivo de la solución.

El documento en el apartado "12. ACUERDOS DE NIVELES DE SERVICIO DE TECNOLOGÍA", indica que el GIT de Apoyo Informático ha establecido los Acuerdos de Niveles de Servicio (ANS), para la prestación de los servicios definidos de acuerdo con el nivel de complejidad y afectación que cause sobre la infraestructura tecnológica, incluyendo los tiempos de recuperación que deben ser tenidos en cuenta en caso de contingencia.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificaron políticas y estándares establecidos para la gestión, seguimiento y cumplimiento de los Acuerdos de Nivel de Servicio (ANS) y que estén integrados en el Plan de Continuidad del Negocio.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar políticas y estándares establecidos para la gestión, seguimiento y cumplimiento de los Acuerdos de Nivel de Servicio (ANS). Estas políticas y estándares deben ser integradas al Plan de Continuidad del Negocio (BCP) para asegurar que los ANS se mantengan efectivos tanto en condiciones normales como durante emergencias o interrupciones. Además, es importante promover la apropiación de estas políticas entre el personal relevante, asegurando que todos los involucrados comprendan y cumplan con los requisitos establecidos. La integración debe incluir la documentación de procedimientos, la capacitación continua y la realización de pruebas periódicas para garantizar la eficacia y adaptabilidad de los ANS en el contexto del BCP.

2.6.2 Implementación de la Política de TI para la Gestión y Cumplimiento de los Acuerdos de Nivel de Servicio (ANS)

La entidad debe contar con una política de TI actualizada, formalmente aprobada y adecuadamente comunicada, alineada con la estrategia organizacional. Esta política debe integrar los lineamientos operativos y de seguridad informática aplicables a los Acuerdos de Nivel de Servicio (ANS). Su propósito es asegurar un seguimiento riguroso, el cumplimiento efectivo y la gestión continua de los ANS, garantizando que todas las áreas involucradas comprendan sus responsabilidades y actúen conforme a los estándares establecidos. Además, la política debe ser revisada periódicamente para adaptarse a cambios en la estrategia de la entidad, las mejores prácticas de la industria y las nuevas amenazas o vulnerabilidades en el entorno de TI.

RESULTADO

Documento aportado:

ManualSeguridadInformaciónDigitalV7.0.pdf: Documento descrito en el numeral 2.2.2.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificaron las especificaciones de la política de Tecnologías de la Información (TI) para integrar de manera explícita los lineamientos operativos y de seguridad informática aplicables a los Acuerdos de Nivel de Servicio (ANS).

RECOMENDACIÓN

Es pertinente que se desarrolle y actualice la política de Tecnologías de la Información (TI) para que integre de manera explícita los lineamientos operativos y de seguridad informática aplicables a los Acuerdos de Nivel de Servicio (ANS). Esta política debe ser formalmente aprobada y comunicada a todas las áreas relevantes, garantizando que se establezcan las responsabilidades, requisitos de cumplimiento, y mecanismos de seguimiento para asegurar la eficacia en la gestión de los ANS. Además, se recomienda

revisar periódicamente esta política para asegurar que continúe alineada con la estrategia organizacional, las mejores prácticas del sector y las nuevas necesidades de seguridad.

2.6.3 Capacidades de TI y Proyecciones para el Cumplimiento de los Acuerdos de Nivel de Servicio (ANS)

Definir las capacidades de TI necesarias para garantizar la prestación eficiente y continua de los servicios, junto con las proyecciones de capacidad requeridas para asegurar su operación futura. Este proceso debe incluir la atención y gestión de los lineamientos operativos y de seguridad informática aplicables a los Acuerdos de Nivel de Servicio (ANS). Es fundamental evaluar la capacidad tecnológica actual en relación con los ANS y las necesidades estratégicas de la entidad. Adicionalmente, se deben generar informes y resultados de las mediciones de capacidades existentes para asegurar el cumplimiento de los ANS, así como monitorear de manera continua el rendimiento de los servicios de TI y la gestión del talento humano involucrado en la ejecución de estos acuerdos.

RESULTADO

Documentos aportados:

MediciónCapacidad-032024.xls: Documento descrito en el numeral 2.4.1.

PlanCapacidadServiciosTI-V1-Nov2023.doc: Documento descrito en el numeral 2.4.1.

HALLAZGO

Revisada y analizada la información proporcionada, se identificó la ausencia de un plan integral que defina las capacidades de TI necesarias para la prestación efectiva de los servicios de TI y el cumplimiento de los Acuerdos de Nivel de Servicio (ANS). Este plan debería incluir proyecciones detalladas de las capacidades futuras requeridas, alineadas con la estrategia de TI establecida por la entidad. Además, se observó que no se han considerado las capacidades tecnológicas necesarias para asegurar el cumplimiento continuo de los ANS en un contexto de crecimiento y evolución de la entidad.

RECOMENDACIÓN

Es pertinente desarrollar un plan integral de capacidades de TI que esté alineado con su estrategia de TI y que contemple tanto las necesidades actuales como las futuras. Este plan debe incluir una evaluación de las capacidades tecnológicas necesarias para la prestación efectiva de los servicios de TI, garantizando el cumplimiento de los Acuerdos de Nivel de Servicio (ANS). Asimismo, es fundamental que el plan incorpore proyecciones detalladas que anticipen el crecimiento y evolución de la entidad, asegurando así que las capacidades de TI se ajusten a las demandas futuras y que se mantenga la continuidad operativa y el cumplimiento de los ANS en todo momento. Además, se recomienda establecer mecanismos de monitoreo y revisión periódicos para ajustar el plan según los cambios en las necesidades tecnológicas y en el entorno operativo de la entidad.

2.6.4 Seguimiento al cumplimiento de los Acuerdos de Nivel de Servicio (ANS)

Se deben mantener y documentar el seguimiento al cumplimiento de los Acuerdos de Nivel de Servicio (ANS) establecidos con las diferentes dependencias o instituciones. Estos ANS deben contemplar, de manera detallada, las características de oportunidad, disponibilidad y seguridad que los componentes de información requieren. Además, se debe asegurar la revisión periódica de estos acuerdos, evaluando su efectividad y realizando ajustes necesarios para garantizar que se mantengan alineados con los objetivos estratégicos de la organización y las normativas vigentes.

RESULTADO

Documento aportado:

ANS Medellín 2019.pdf: Documento titulado "Acuerdo de Niveles de Servicio Convenio entre CGN y Medellín, ANEXO 1" para establecer acuerdos de Niveles de Servicios – ANS bajo el convenio de cooperación entre Contaduría General de la Nación y el municipio de Medellín.

El documento en su contenido indica que establece los términos y condiciones a partir de los cuales la Contaduría General de la Nación proporcionará al municipio de Medellín el servicio de acceso al sistema CHIP; en particular al módulo de consolidación contable, así como los mecanismos de comunicación para la atención de incidentes y solicitudes. De igual manera, se destacan las condiciones esperadas en el servicio de centro de datos ofrecidos por el municipio de Medellín.

HALLAZGO

Revisada y analizada la información proporcionada, se identificó la ausencia de evidencias documentales del seguimiento al cumplimiento de los Acuerdos de Nivel de Servicio (ANS) establecidos con las dependencias o entidades externas, los cuales contemplan las características de oportunidad, disponibilidad y seguridad que requieran los componentes de información.

RECOMENDACIÓN

Es pertinente establecer y realizar el seguimiento a los Acuerdos de Nivel de Servicio (ANS) para garantizar el cumplimiento de los estándares acordados en cuanto a calidad, oportunidad, disponibilidad y seguridad de la información. Esto es esencial para mantener la integridad, confidencialidad y accesibilidad de los datos, asegurar la continuidad operativa, y cumplir con normativas vigentes. Además, el seguimiento debe identificar riesgos, promover mejoras en los ANS, y asegurar un intercambio de información confiable y seguro con entidades externas, fortaleciendo la confianza y alineación con los objetivos estratégicos de la entidad.

2.7 ADQUISICIÓN Y MANTENIMIENTO DE LOS SERVICIOS TECNOLÓGICOS (INFRAESTRUCTURA TECNOLÓGICA)

Analizar el desempeño, capacidad y disponibilidad de la infraestructura tecnológica, sistemas de información y servicios de gestión de información, identificando posibles cuellos de botella, puntos de fallo y oportunidades de mejora en la capacidad y rendimiento de estos.

2.7.1 Optimización de las compras de TI - LI.GO.06

La entidad debe realizar las compras de bienes o servicios de Tecnología a través de Acuerdos Marco de Precios (AMP) existentes, en caso de que apliquen, y dar prioridad a adquisiciones en modalidad de servicio o por demanda. Debe, además, propender por minimizar la compra de bienes de hardware.

RESULTADO

Los auditados aportaron evidencia documental de órdenes de compra que permiten establecer que la entidad realiza las compras de bienes o servicios de Tecnología a través de Acuerdos Marco de Precios (AMP) existentes.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó un documento maestro o procedimiento que establezca las características y condiciones para realizar las compras de bienes o servicios de Tecnología a través de AMP, de acuerdo a lo establecido en el lineamiento LI.GO.06 - Optimización de las compras de TI de MinTIC, que establece los lineamientos de los AMP para las adquisiciones de tecnología.

RECOMENDACIÓN

Es pertinente desarrollar y formalizar un documento maestro o procedimiento que detalle las características y condiciones para la adquisición de bienes o servicios de tecnología a través de Acuerdos Marco de Precios (AMP), en concordancia con el lineamiento LI.GO.06 de MinTIC sobre la optimización de compras de TI. Este documento o procedimiento debe establecer los criterios de selección, los procesos de evaluación, y los controles necesarios para asegurar que las adquisiciones se realicen de manera eficiente, transparente y conforme a las políticas nacionales, garantizando que se cumplan los objetivos estratégicos y operativos de la entidad en materia de tecnología.

2.7.2 Retorno de la inversión de TI - LI.GO.08.

La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe establecer la relación costo-beneficio y justificar la inversión de los proyectos de TI mediante casos de negocio e indicadores financieros, mediante la metodología y criterios de evaluación de alternativas de solución e inversión en TI, la cual debe estar documentada, ser conocida y accesible por el personal del área de TI.

Los criterios de evaluación deben estar identificados y como mínimo deben existir criterios de tipo técnico, funcional y financiero. La entidad debe cuantificar el valor público y el retorno de la inversión resultado de la implementación de los proyectos de TI.

Se debe verificar y comprobar que en los ejercicios de evaluación de alternativas de solución e inversión de TI se utilizaron los criterios y la metodología. Así mismo, en los estudios de mercado que se realizan para los procesos de contratación de servicios o bienes de TI, se debe verificar la existencia de criterios técnicos, funcionales y financieros que permitan la toma de decisiones de manera objetiva.

RESULTADO

Los auditados aportaron una variedad de documentos relacionados con la adquisición de un servidor para la infraestructura misional de la Contaduría General de la Nación. Entre estos documentos se incluyen fichas técnicas, pliego de condiciones de la licitación pública NRO. 01 del 2023, estudios previos de la licitación pública, un estudio del sector para la adquisición de equipos de computación en arquitectura Power de IBM, y el Resumen de Evaluación del Proceso SASI-004 de 2023.

En estos documentos se evidenció el uso de criterios técnicos, funcionales y financieros para los procesos licitatorios y de contratación, así como en los estudios de mercado realizados para la adquisición de servicios o bienes de Tecnologías de la Información (TI), cumpliendo con las directrices establecidas por Colombia Compra Eficiente para la contratación y compras estatales.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó un documento que establezca la relación costo-beneficio y justifique las inversiones en proyectos de TI. No se encontró evidencia de una metodología ni de criterios de evaluación que utilicen casos de negocio e indicadores financieros para respaldar las decisiones de inversión y evaluar alternativas de solución en TI. Esta carencia impide una justificación adecuada de las inversiones y compromete la capacidad para evaluar el valor y el impacto de los proyectos de TI en función de su costo y beneficio.

RECOMENDACIÓN

De acuerdo con el lineamiento LI.GO.08 - Retorno de la inversión de TI de MinTIC, es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar una metodología estructurada para la evaluación de inversiones en proyectos de TI. Esta metodología debe incluir criterios técnicos, funcionales y financieros que permitan establecer claramente la relación costo-beneficio y justificar las inversiones mediante casos de negocio e indicadores financieros. Además, debe ser conocida y accesible para el personal del Grupo de Integración Tecnológica (GIT) de Apoyo Tecnológico. La evaluación debe permitir cuantificar el valor público y el retorno de la inversión,

asegurando que los proyectos aporten el valor esperado y estén alineados con los objetivos estratégicos de la entidad.

2.7.3 Revisión de Evidencias Documentales para la Trazabilidad y Auditoría de Componentes de Información

Evidencias documentales del seguimiento y gestión de los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los componentes de información, según los lineamientos de trazabilidad y auditoría definidos para los componentes de información.

RESULTADO

Evidencias Auditoría sobre BD de CHIP Producción.pdf: El documento registra evidencias sobre el programa fn_audited de la base de datos (BD) del sistema CHIP del ambiente de Producción, con la cual se muestra la activación del "trace" o logs de auditoria de la base de datos de las tablas de roles, Security_option, Users, entidad, Security_object_type, Security_action.

En el documento se indica que se tienen creados triggers sobre las tablas auditadas, las cuales activan funciones que registran la auditoría sobre las tablas. Los registros de auditoría se almacenan en la tabla Audit_logs los cuales tienen los siguientes datos: Nombre de la tabla, Fecha de registro, Columna afectada, tipo de operación realizada (update, insert y delete), Usuario que realizó la operación, Aplicación desde la que se realizó la operación, Servidor o pc desde donde viene la conexión donde se hizo la operación, Valor anterior, y Nuevo valor.

HALLAZGO

Revisada y analizada la información proporcionada, se identificó la ausencia de evidencias documentales del seguimiento y gestión de los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de todos los sistemas de información de la CGN, según los lineamientos de trazabilidad y auditoría definidos para los componentes de los sistemas de información.

RECOMENDACIÓN

Es pertinente implementar un sistema de seguimiento y gestión integral para asegurar la trazabilidad y auditoría de todas las acciones relacionadas con la creación, actualización, modificación o borrado de datos en los sistemas de información de la Contaduría General de la Nación (CGN). Este sistema debe garantizar que todas las actividades sean completamente transparentes y verificables, y que cumplan con los lineamientos establecidos para proteger la integridad y seguridad de la información.

Es importante que todas las acciones realizadas sean registradas de manera clara y accesible, permitiendo identificar quién realizó cada acción y cuándo. Además, debe verificarse que estas actividades cumplan con las regulaciones y políticas internas,

evitando comprometer la integridad de los datos y proporcionando controles efectivos para prevenir y detectar modificaciones no autorizadas. El sistema debe facilitar auditorías internas y externas, identificar posibles brechas o irregularidades, y promover una cultura de responsabilidad al asegurar que las acciones sean atribuibles a personas o grupos específicos.

De otra parte, debe actuar como un mecanismo disuasorio contra el fraude y el uso indebido de los sistemas, permitiendo la mejora continua de los procesos y controles de seguridad. Finalmente, el sistema debe ofrecer información confiable que apoye la toma de decisiones informadas, creando un entorno de control robusto en el que todas las acciones estén documentadas y auditadas, garantizando así la integridad, seguridad y transparencia en la gestión de la información crítica.

2.8 PLANES DE CONTINUIDAD DEL NEGOCIO

Se evaluó la implementación de planes de continuidad del negocio (COB), incluyendo la identificación de riesgos, la elaboración de planes de contingencia y la realización de pruebas periódicas para asegurar la capacidad de recuperación frente a eventos adversos.

2.8.1 Revisión de la Planificación de Continuidad de Negocio y Recuperación de Desastres

- Revisar si la Entidad cuenta con un BCP (Bussines Continuity Plan) o DRP (Disaster Recovery Plan).

- Determinar si aplica para procesos críticos solamente o se han incluido otros procesos o por lo menos se ha reconocido la necesidad de ampliarlo a otros procesos.

- Evaluar si se ha incluido en estos planes y procedimientos los requisitos de seguridad de la información.

- Cumplimiento de la norma NTC ISO 22301 (referenciada por MinTIC) y el FURAG y la norma NTC ISO 27001.

Tener en cuenta que, en ausencia de una planificación formal de continuidad de negocio y recuperación de desastres, la dirección de seguridad de la información debería suponer que los requisitos de seguridad de la información siguen siendo los mismos en situaciones adversas, en comparación con las condiciones operacionales normales. Como alternativa, una organización puede llevar a cabo un análisis de impacto en el negocio (BIA por sus siglas en ingles) de los aspectos de seguridad de la información, para determinar los requisitos de seguridad de la información aplicables a situaciones adversas.

RESULTADO

Documentos aportados:

PlanContinuidadNegocio-2023.pdf: Documento descrito en el numeral 2.1.18.

TIC-SEG-PCO_PlanDeContingenciaTecnologica2022.pdf: Documento descrito en el numeral 2.6.1.

HALLAZGOS

1. El Plan de continuidad de negocio incumple los criterios establecidos en la "Guía para la preparación de las TIC para la continuidad del negocio del MinTIC" y la NTC ISO 22301, toda vez que:

- En el apartado "7.1.1 Análisis del Impacto del Negocio (BIA)" las descripciones no corresponden a las características de la entidad; toda vez que, el texto fue tomado literal de los conceptos establecidos por MinTIC en la Guía para la preparación de las TIC para la continuidad del negocio.

- No se identificó un informe específico del Análisis de Impacto del Negocio (BIA) que detalle las funciones y procesos críticos del negocio. Este informe es esencial y debe contener información básica sobre los recursos necesarios y los tiempos de recuperación para que la entidad pueda restablecer sus servicios y asegurar la continuidad del negocio.

- Es crucial que el documento generado en este análisis cumpla con los requisitos expuestos en las normas ISO/IEC 27001 y ISO/IEC 22301, proporcionando un marco detallado y preciso para la gestión de la continuidad del negocio. La ausencia de un informe detallado de BIA puede poner en riesgo la capacidad de la entidad para responder eficazmente a interrupciones y mantener la operatividad de sus servicios críticos.

- En el ítem "Estructura organizacional", se observó una tabla en donde se relacionaron los nombres del personal que en su momento estaba asociado a los principales cargos del organigrama de la entidad en lugar de roles, lo anterior también se observó en el ítem "Inventario de aplicativos informáticos del alcance del PCN" y en el aparte "7.2.1 Conformación de equipos", entre otros. Lo anterior, crea la posibilidad de desatención de una actividad o ejecución de un control al momento de cambiar el servidor público o colaborador de rol, dinámica propia de la institución al tener una planta globalizada.

- En el apartado "7.2.1.5 Plan de Pruebas" se establece que "El plan requiere ser probado periódicamente al menos una vez al año (…)". Sin embargo, al revisar las evidencias entregadas por los auditados, no se identificaron documentos que acrediten la realización de pruebas del Plan de Continuidad del Negocio (COB), por parte de la entidad. La ausencia de estas pruebas no solo impide la validación del plan, sino que también pone en riesgo la capacidad de la entidad para manejar interrupciones de manera adecuada. Además, la falta de evidencia puede resultar en incumplimientos normativos y afectar la confianza en la gestión de continuidad del negocio.

- En el aparte "7.3 GESTION" se observó que solo se trató el evento de fenómenos naturales sin considerar el espectro de eventos a los que está expuesta un organización,

entre otros: fallos en los sistemas de información, pérdida de datos críticos, interrupciones en el servicio de internet o telecomunicaciones, ataques cibernéticos y violaciones de seguridad (hackeo, malware, ransomware), amenazas físicas como vandalismo, robos o sabotajes, actos de terrorismo, enfermedades pandémicas que afecten a un gran número de empleados, pérdida repentina de personal clave, fallos en la infraestructura de servicios públicos (agua y electricidad), fallos en sistemas de transporte que impidan el acceso a las instalaciones, cambios en la legislación que afecten la operativa de la entidad, litigios importantes que puedan tener un impacto financiero o de reputación, cambios políticos que afecten el entorno regulatorio o económico, mal funcionamiento o fallos en equipos de producción, fallos operativos debido a errores del personal de la entidad los empleados e implementación incorrecta de procedimientos o configuraciones técnicas, entre otros.

- El documento titulado "PLAN DE CONTINUIDAD DE NEGOCIO DE TI", contiene datos que indican que se encuentra en un estado de borrador. Ejemplos de esto incluyen referencias como "Aprobación comité CIGD (xx/12/2023)" y "VERSIÓN X". Además, no se identificó evidencia de que el documento haya sido aprobado y socializado.

RECOMENDACIÓN

Realizar la actualización del Plan de Continuidad del Negocio (COB), teniendo en cuenta:

- Registro de las responsabilidades y funciones en términos de roles en lugar de nombres propios. Esto asegura la vigencia, actualización, y efectividad del plan, contribuyendo a la resiliencia organizacional y a la continuidad de las operaciones críticas de la entidad.

- Establecer pruebas documentadas del COB para asegurar su efectividad y capacidad de respuesta ante situaciones de interrupciones.

- Desarrollar de manera transversal el Plan de Continuidad del Negocio (COB), considerando la participación de todos los estamentos, líderes de procesos y dueños de los activos de información. Una vez definido, el plan debe ser aprobado por la alta gerencia e implementado en su totalidad.

2. El Plan de Continuidad de Tecnologías de la Información (o Plan de Continuidad de Tecnología) incumple los criterios establecidos en la "Guía para la preparación de las TIC para la continuidad del negocio del MinTIC" y la NTC ISO 22301, toda vez que:

- El desarrollo del Plan de Contingencia Tecnológica fue elaborado y llevado a cabo exclusivamente por el GIT de Apoyo Informático. Este proceso se realizó sin la participación transversal de la alta y media gerencia, líderes de procesos, dueños de los activos de información y otras partes interesadas relevantes.

- En el apartado "12. ACUERDOS DE NIVELES DE SERVICIO DE TECNOLOGÍA", la tabla listada carece de descripciones detalladas y específicas sobre varios conceptos cruciales, tales como: objetivos, términos técnicos y operativos, descripción detallada de los servicios, cobertura del servicio, indicadores de desempeño, tiempos específicos

para la atención y resolución de incidencias y solicitudes, responsabilidades del proveedor, responsabilidades del usuario, canales de comunicación, procedimientos de escalamiento, calendario para la revisión y actualización periódica del ANS, procedimientos para la incorporación de nuevos servicios o la modificación de los existentes, informes de desempeño, cláusulas de cumplimiento, penalidades, políticas de seguridad, y mecanismos de resolución.

Es fundamental destacar que la elaboración de un Plan de Contingencia Tecnológica debe involucrar a todas las partes interesadas relevantes dentro de la entidad. La participación activa de la alta y media gerencia, líderes de procesos y dueños de los activos de información es crucial para asegurar que el plan sea integral, efectivo y alineado con los objetivos y necesidades institucionales. Una participación transversal garantiza que se consideren todas las perspectivas y se cubran todos los aspectos críticos para la continuidad operativa de la entidad en caso de una contingencia tecnológica.

2.8.2 Implementación de la Política de Disponibilidad del Servicio de Información

Implementación de la Política de Disponibilidad del Servicio e Información, debidamente aprobado por la alta Dirección y socializada al interior de la entidad junto con las especificaciones del plan de continuidad del negocio con el fin de asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y procesos misionales de la entidad, ante el evento de un incidente de seguridad de la información. La política de disponibilidad debe incluir como mínimo los siguientes aspectos:

- Niveles de disponibilidad.
- Planes de recuperación.
- Acuerdos de Nivel de servicio.
- Segregación de ambientes.
- Gestión de Cambios.

RESULTADO

Documentos aportados:

- Acta No. 11 CIGD - 13 de octubre de 2022.pdf: Documento descrito en el numeral 2.2.3.

- Manual de Seguridad de la Información 2022.pdf: Documento descrito en el numeral 2.1.19.

- PlanContinuidadNegocio-2023.pdf: Documento descrito en el numeral 2.1.18.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó la Política de Disponibilidad del Servicio e Información, debidamente aprobado por la alta dirección y socializado al interior de la entidad.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar la Política de Disponibilidad del Servicio e Información para establecer directrices con el fin de asegurar los servicios críticos y la información de las operaciones institucionales y que estén siempre disponibles y accesibles según se requiera. Esta política debe garantizar la continuidad operativa frente a interrupciones o incidentes que puedan afectar la infraestructura tecnológica, los sistemas de información y los servicios de gestión de información. Además, debe promover la implementación de medidas preventivas y correctivas para minimizar el impacto de posibles interrupciones, asegurando que los usuarios internos y externos puedan acceder de manera oportuna y confiable a los recursos tecnológicos y la información necesaria para cumplir con sus funciones y responsabilidades.

2.8.3 Implementación del Procedimiento de Gestión de la Continuidad de Negocio

Implementación del Procedimiento de Gestión de la Continuidad de Negocio, debidamente documentado, socializado y aprobado con las especificaciones de cómo la entidad garantizará la continuidad para todos sus procesos (de ser posible o por lo menos los misionales), identificando los procesos críticos que tendrán mayor prioridad en las fases de recuperación ante algún desastre o incidente crítico.

El procedimiento debe indicar los pasos a seguir cuando existan estas situaciones adversas, quienes deberán actuar (incluyendo las terceras partes o proveedores), los tiempos a cumplir, los procesos alternos o que permitan continuar con el proceso de manera temporal.

RESULTADO

Documentos aportados:

- GTI-PRC10 Seguridad de la Información.pdf: Documento descrito en el numeral 2.1.14.

- Presentaciones CGN - PlanDeContinuidad_2022.ppt: Documento titulado “Revisión y Actualización del Plan de Continuidad del Negocio - CGN”, el cual tiene como objetivo socializar los temas relacionados con la Política Continuidad de Negocio respecto a responder, recuperar, reanudar y restaurar adecuadamente las operaciones de negocio ante la materialización de eventualidades tecnológicas, en escenarios de catástrofe que puedan comprometer la seguridad del personal, la continuidad de las operaciones o la prestación de los servicios críticos para las partes interesadas de la CGN.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó el Procedimiento de Gestión de la Continuidad de Negocio, debidamente aprobado por la alta dirección y socializado al interior de la entidad.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar el Procedimiento de Gestión de la Continuidad de Negocio para establecer las actividades que garantizan que la entidad esté preparada para responder eficazmente a eventos disruptivos, minimizando el impacto en las operaciones críticas. Este procedimiento debe asegurar la continuidad de los servicios esenciales y la rápida recuperación de las funciones clave, protegiendo los intereses de los interesados, la reputación de la entidad y el cumplimiento de sus obligaciones legales y regulatorias. Además, establece las actividades para la planificación, implementación, mantenimiento y mejora continua de estrategias y planes de continuidad del negocio, promoviendo una cultura organizacional resiliente y proactiva frente a posibles contingencias.

2.8.4 Realización Revisiones de Acciones y Planes de Mejora

Evidencias documentales que soportan la realización de la actividad de Revisiones de Acciones o Planes de Mejora (Respuesta a no conformidades).

RESULTADO

Documentos aportados:

- Plan de Mejoramiento_Icontec2022.xls y Planes de Mejoramiento_ICONTEC2023.xls: Documentos titulados "PLAN DE MEJORAMIENTO SIGI", relacionados con el procedimiento "No Conformidades, Acción Correctiva, Preventiva y Planes de Mejoramiento". Los documentos registran información con respecto a los procesos institucionales los hallazgos o situaciones identificadas. La información registrada presenta los datos de: #, proceso, fuente de evaluación, descripción del hallazgo o situación detectada, tipo de hallazgo u observación, tipo de acción, análisis causa, descripción acción a realizar, producto esperado, fecha iniciación de la acción, fecha finalización de la acción, responsable de la acción, seguimiento y estado.

- TIC-GES-AUD-2022-ICON-NoConformidadesISO27001-2022.doc y TIC-GES-PLM-2023-SAC_27001ContaduriaGeneraldelaNacion-Renovacion_2023.doc: Documentos titulados "ANEXO 1, CORRECCIONES, CAUSAS Y ACCIONES CORRECTIVAS, los cuales corresponden a formatos de solitud de atención a no conformidades de un informe de auditoría de sistemas de gestión del ICONTEC.

HALLAZGO

Revisada y analizada la información proporcionada, se identificó la ausencia de evidencias documentales que respalden las actividades de revisión de acciones o planes de mejora (respuesta a no conformidades) relacionadas con el Modelo de Seguridad y Privacidad de la Información (MSPI). La falta de estas evidencias documentales dificulta verificar que se estén tomando medidas correctivas adecuadas y oportunas para abordar las no conformidades identificadas, lo cual es esencial para mantener la integridad y efectividad del MSPI. Es importante establecer y mantener registros detallados de todas las acciones de mejora para asegurar un seguimiento riguroso y la implementación efectiva de las correcciones necesarias.

RECOMENDACIÓN

Es pertinente establecer y mantener un sistema para la documentación de todas las actividades relacionadas con la revisión de acciones y planes de mejora en respuesta a no conformidades dentro del Modelo de Seguridad y Privacidad de la Información (MSPI). Se recomienda implementar procedimientos formales para registrar y conservar todos los documentos relacionados con las acciones de mejora, incluyendo planes de acción, seguimientos, y revisiones. Estos registros deben ser accesibles para garantizar que se realice un seguimiento riguroso y se confirme la efectividad de las correcciones aplicadas, asegurando así la integridad del sistema y el cumplimiento de las normas establecidas.

2.9 SEGURIDAD INFORMÁTICA

Verificar las medidas de seguridad informática implementadas, incluyendo controles de acceso, monitoreo de actividad, gestión de vulnerabilidades, y respuesta ante incidentes, entre otros, para proteger la confidencialidad, integridad y disponibilidad de la información institucional.

2.9.1 Criterio: Seguridad informática – LI.ST.15

La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar controles de seguridad informática para gestionar los riesgos que atenten contra la disponibilidad, integridad y confidencialidad de la Información, mediante mecanismos de seguridad de la información que deben estar implementados en los servicios tecnológicos, sistemas de información y servicios de gestión de información, tales como:

Mecanismos Preventivos: Cualquier actividad o proceso que tenga la entidad definido y destinado a prevenir la ocurrencia de un ataque informático, por ejemplo, el monitoreo de la información y de los bienes, registro de las actividades que se realizan en la organización y control de todos los activos y de quienes acceden a ellos.

Mecanismos detectores: Todo aquello que este destinado a detectar lo que pueda ser una amenaza para los bienes, como por ejemplo las personas y equipos de monitoreo que pueden detectar cualquier intruso u anomalía en la entidad.

Mecanismos correctivos: Todo aquello que este destinado a la reparación de errores cometidos o daños causados una vez que se ha cometido un ataque.

RESULTADO

Documentos aportados:

- 1.Activos de información.xls: Documento descrito en el numeral 2.9.2.1.

- 1.Registro Detallado Activos TI.xls: El documento detalla quince secciones que registran una variedad de activos tecnológicos en la Contaduría General de la Nación (CGN). Estas secciones incluyen listados de switches, servidores, firewalls, aplicaciones, cintas de datos, computadoras y otros activos, así como detalles sobre licencias y repuestos. La revisión de estas secciones muestra una identificación y clasificación clara de los activos, con descripciones detalladas y categorización por tipo. Sin embargo, se observó una falta de información en aspectos clave de la caracterización de los activos conforme a las normas ISO 55000 e ISO IEC 27005, como propietario, custodio, configuración, versiones de software, valor financiero, medidas de seguridad implementadas, y otros detalles críticos para una gestión integral de los activos.

- 2.Matriz de Tratamiento de Riesgos de Seguridad de la Informacion_2023.xls: El documento está dividido en dos secciones principales. La primera, titulada "DESCRIPCIÓN RIESGO", proporciona un formato para registrar riesgos, incluyendo datos como número de activo, descripción del riesgo, amenaza, vulnerabilidad, y evaluación del riesgo inicial, con un total de 23 registros. La segunda sección, "MAPA Y TRATAMIENTO", detalla el plan de tratamiento para estos riesgos, incluyendo riesgos residuales, opciones de tratamiento, acciones, controles y indicadores, también con 23 registros. La revisión de estas secciones muestra un análisis de riesgos asociados a hardware, software, servicios, información y talento humano.

En la revisión del documento "1.Activos de Información", se constató la omisión de activos clave, como: Información Financiera y Contable, Información Legal y Regulatoria, Información de Gestión y Desempeño, Información de Gestión Contractual, Información de Planes Estratégicos y Operativos, Información de Gestión Documental, Información Confidencial de Funcionarios, Contratistas y Proveedores, Información de Sistemas de Gestión de Servicios de TI, Información de Configuraciones de Servidores y Dispositivos de Red, e Información de Configuración de Seguridad (firewalls, routers, switches).

Además, en las cuatro secciones del archivo mencionadas, se identificó la falta de documentación sobre la implementación de mecanismos de seguridad para proteger la información en los sistemas y servicios tecnológicos de la entidad. En particular, no se registraron mecanismos preventivos necesarios como el monitoreo de la información, el registro de actividades y el control de acceso a los activos.

En la revisión del archivo "2. Matriz de Tratamiento de Riesgos de Seguridad de la Información_2023", se observó que los controles registrados son reproducciones literales

de la norma ISO 27001, sin adaptación a los riesgos específicos, lo que limita la eficacia en la gestión de riesgos digitales.

HALLAZGO

Según las evidencias aportadas por los auditados, no se identificaron documentos que detallen los mecanismos de seguridad de la información de los servicios tecnológicos, sistemas de información y servicios de gestión de información de la entidad.

RECOMENDACIÓN

Para garantizar una protección integral y efectiva de los servicios tecnológicos, sistemas de información y servicios de gestión de información, es importante que la entidad implemente de manera robusta y coordinada los mecanismos de seguridad en tres áreas clave. En primer lugar, los mecanismos preventivos deben ser reforzados mediante la implementación de políticas y procedimientos claros que incluyan el monitoreo continuo de sistemas, el registro exhaustivo de actividades y un control riguroso sobre los activos y accesos. En segundo lugar, los mecanismos detectores deben ser establecidos para identificar y alertar sobre posibles amenazas o anomalías.

Lo anterior, implica la instalación de herramientas de detección de intrusiones y anomalías que proporcionen alertas tempranas y permitan una rápida respuesta ante posibles incidentes. Finalmente, los mecanismos correctivos deben incluir un plan detallado de respuesta a incidentes que contemple la identificación, contención y reparación de daños causados por ataques. La implementación de procedimientos de recuperación efectivos y la garantía de disponibilidad de copias de seguridad actualizadas son esenciales para minimizar el impacto de cualquier brecha de seguridad.

2.9.2 Formación y entrenamiento de usuarios

Revisar los programas de formación y entrenamiento de usuarios, asegurando que el personal esté adecuadamente capacitado para utilizar la infraestructura tecnológica, los sistemas de información y los servicios de gestión de información de manera segura y eficiente.

2.9.2.1 Implementación de la Política y Procedimiento de Capacitación y Sensibilización en Seguridad de La Información

Implementación de la Política y del Procedimiento de Capacitación y Sensibilización en Seguridad de la Información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad con las especificaciones en cuanto a la formación del personal en temas relacionados con la seguridad de la información, cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano. Esta política debe contener los siguientes parámetros.

El compromiso de la alta dirección en destinar los recursos suficientes para desarrollar los programas.

¿Quiénes deberán ser entrenados? ¿Quiénes deberán ser sensibilizados?
La obligación de los usuarios a asistir a los eventos o cursos de capacitación.
Revisión periódica de resultados de capacitaciones para mejoramiento de los procesos.
Definir los roles y responsabilidades de quienes diseñarán los programas, quienes los comunicarán.
Documentación sobre planes de estudio y desarrollo de los programas.
Compromisos y obligaciones por parte del personal capacitado.
Contener políticas adicionales relacionadas directamente con el debido comportamiento de los usuarios como: Política De Escritorio Limpio, Política De Uso Aceptable y Ética Empresarial.

RESULTADO

Documentos aportados:

- Acta No. 11 CIGD - 13 de octubre de 2022.pdf: Documento descrito en el numeral 2.2.3.

- Manual de Seguridad de la Información 2022: Documento descrito en el numeral 2.1.19.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó la Política y el Procedimiento de Capacitación y Sensibilización en Seguridad de la Información, debidamente aprobado por la alta dirección y socializado al interior de la entidad.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar la Política y el Procedimiento de Capacitación y Sensibilización en Seguridad de la Información para garantizar que todos los funcionarios, contratistas y terceros comprendan los riesgos de seguridad y estén capacitados para mitigarlos eficazmente. La política y el procedimiento deben fomentar una cultura de seguridad informática mediante la implementación de programas de formación periódicos que cubran aspectos técnicos y comportamientos seguros. Debe incluir el compromiso de la alta dirección, definir quién debe ser capacitado, establecer la obligatoriedad de la asistencia a capacitaciones, revisar periódicamente los resultados para mejorar los procesos, y detallar roles y responsabilidades en el diseño y comunicación de los programas. Además, debe documentar los planes de estudio, compromisos del personal y políticas relacionadas como la de Escritorio Limpio, Uso Aceptable y Ética Empresarial.

2.9.3 Gestión de Plan de Acción y Evidencias en el Monitoreo del Modelo MSPI

Plan de acción derivado del monitoreo y evaluación del análisis de resultados de la aplicación de indicadores de Uso y Apropiación definidos para el modelo MSPI.

Evidencia documental de la atención y gestión de las acciones del plan.

Las acciones derivadas deben contar con una asignación de fechas de cumplimiento y responsables.

Las evidencias deben corresponder con las actividades y acciones definidas en el plan de acción definido.

RESULTADO

Documento aportado:

CGN PLAN DE COMUNICACIONES 2024.pdf: Documento descrito en el numeral 2.9.3.

HALLAZGO

Revisada y analizada la información proporcionada, se identificó la ausencia de evidencias documentales que permitan constatar la atención y gestión del Plan de acción derivado del monitoreo y evaluación del análisis de resultados de la aplicación de indicadores de Uso y Apropiación definidos para el modelo MSPI.

RECOMENDACIÓN

Es pertinente que la atención y gestión del Plan de Acción derivado del monitoreo y evaluación de los indicadores de Uso y Apropiación del modelo de Madurez de Seguridad y Protección de la Información (MSPI) asegure un enfoque eficaz en la optimización continua de este modelo. Es crucial que los indicadores se utilicen para identificar áreas de mejora, permitiendo ajustes que fortalezcan la seguridad y protección de la información. Además, se debe garantizar que estos resultados se alineen con los objetivos estratégicos de la entidad, promoviendo una mayor apropiación del modelo MSPI por parte de los usuarios.

Lo anterior, incluye la implementación de un ciclo de monitoreo y ajuste continuo, la documentación detallada de los resultados y la colaboración efectiva entre todas las áreas involucradas. La gestión adecuada de este plan debe también reforzar la cultura organizacional en seguridad de la información, asegurando que el modelo MSPI no solo cumpla con las normativas aplicables, sino que también se ajuste a las necesidades de la entidad para maximizar su efectividad y apoyo a la estrategia general.

2.9.4 Seguridad en la administración de operaciones de tecnología

Analizar la administración de operaciones de tecnología, incluyendo la supervisión de procesos diarios, la gestión de incidentes y problemas, y la generación de informes de rendimiento y cumplimiento para la toma de decisiones informadas.

2.9.4.1 Disposición del inventario de activos de información

Disposición del inventario de activos de información, revisado y aprobado por la alta Dirección y revisar:

- Ultima vez que se actualizó
- Que señale bajo algún criterio la importancia del activo
- Que señale el propietario del activo
- Revisar quien(es) el(los) encargado(s) de actualizar y revisar el inventario de activos y cada cuanto se realiza esta revisión.

Se deben considerar como activos el personal, dispositivos, sistemas e instalaciones físicas que permiten a la entidad cumplir con su misión y objetivos, dada su importancia y riesgos estratégicos.

RESULTADO

Documentos aportados:

- 1.Activos de información.xls: El documento se compone de cuatro secciones que describen el inventario de activos de seguridad de la información en la Contaduría General de la Nación. La primera sección ofrece un índice para las demás secciones. La segunda sección detalla el inventario de activos de tipo información, con seis registros. La tercera sección abarca el inventario de hardware, software y servicios, con 248 registros. La cuarta sección incluye el inventario de activos relacionados con el talento humano, con 14 registros.

- PI28-FOR01 Formato activos de informacion-TICs.xls: Documento ubicado en el portal web institucional de la UEA Contaduría General de la Nación (CGN) bajo el enlace https://www.contaduria.gov.co/productos/-/document_library/SNUXvXyrbcKS/view_file/6175409, modificado el 19 de noviembre del 2024.

  El documento se compone de dos secciones dedicadas al inventario de activos de información. La primera sección, relacionada con el proceso de Gestión TICs, contiene 224 registros clasificados en hardware (72), software (143), información (6), y servicios (3). La segunda sección incluye 14 registros de activos de talento humano, clasificados en contratistas (11) y personal de planta (3). Ambas secciones comparten la misma versión y código de procedimiento, aprobados el 24 de octubre de 2019.

HALLAZGO

Revisada y analizada la información proporcionada, se identificó que esta solo hace referencia al proceso de "Gestión TICs", omitiendo otros procesos relevantes de la entidad. Entre estos procesos no documentados se encuentran los procesos de: Gestión Jurídica, Gestión de Recursos Financieros, Gestión Administrativa, Consolidación de la Información y Centralización de la Información, entre otros.

RECOMENDACIÓN

Es pertinente revisar, contextualizar, aprobar, implementar y apropiar el inventario de activos de información de la entidad, abarque todos los procesos críticos, más allá de la "Gestión TICs", incluyendo áreas como la Gestión Jurídica, recursos financieros y administrativos, para garantizar el cumplimiento normativo, la sostenibilidad financiera y la eficiencia operativa. Los activos de información deben alinearse con los objetivos de la Contaduría General de la Nación (CGN), no solo para cumplir con normativas, sino para integrar la seguridad de la información en las operaciones, proteger los activos, optimizar la asignación de recursos, y definir planes de contingencia y procedimientos de gestión de incidentes.

2.9.4.2 Gestión de Servicios Tecnológicos, Control de Activos y Matriz de Riesgos de Seguridad Informática

Inventario de servicios tecnológicos detallando los controles de seguridad informática asociados al acceso, trazabilidad, modificación o pérdida de información.

Matriz de riesgos que analice aspectos que atenten contra la disponibilidad, integridad y confidencialidad de la información y proponga los controles necesarios

Solicitar el procedimiento para asegurar la asignación oportuna de la propiedad de los activos. Tener en cuenta que la propiedad se debería asignar cuando los activos se crean o cuando son entregados a la Entidad.

De acuerdo a las mejores prácticas el propietario de los activos (individuo o entidad, que es responsable por el activo) tiene las siguientes responsabilidades:

- Asegurarse de que los activos están inventariados.
- Asegurarse de que los activos están clasificados y protegidos apropiadamente.
- Definir y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes, teniendo en cuenta las políticas de control de acceso aplicables.
- Asegurarse del manejo apropiado del activo cuando es eliminado o destruido.

RESULTADO

Documento aportado:

GTI-PRC11.pdf: Documento descrito en el numeral 2.1.21.

HALLAZGO

Revisada y analizada la información proporcionada, se identificó la ausencia de un procedimiento para asegurar la asignación oportuna de la propiedad de los activos. Además, no presentan las condiciones necesarias para guiar la implementación de dicho procedimiento, lo que puede generar ambigüedades en su ejecución. Asimismo, no se han definido las responsabilidades de los roles involucrados, lo cual es esencial para asignar,

entender y cumplir de manera efectiva las funciones de cada parte involucrada en la gestión de activos. La falta de este marco puede comprometer la adecuada protección, clasificación y manejo de los activos, afectando la seguridad y operatividad de la entidad.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar un procedimiento para asegurar la asignación de la propiedad de los activos dentro de la entidad. Este procedimiento debe incluir directrices sobre cómo se asigna la propiedad desde la creación o adquisición de los activos, y debe establecer las condiciones necesarias para guiar su implementación, evitando cualquier ambigüedad en su ejecución. Asimismo, es importante definir y documentar las responsabilidades específicas de todos los roles involucrados en la gestión de activos. Cada parte debe tener un entendimiento de sus funciones y obligaciones, lo que permitirá una protección, clasificación y manejo adecuado de los activos. Además, se recomienda realizar revisiones periódicas de este procedimiento y de las responsabilidades asignadas, para asegurar su efectividad y adaptación a posibles cambios en la organización.

2.9.4.3 Implementación de la Política de No Repudio

Documento con la Política de No Repudio, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad, con la referencia a la capacidad de no repudio con el fin de que los usuarios eviten haber realizado alguna acción. La política deberá incluir mínimo los siguientes aspectos:

- Trazabilidad.
- Retención.
- Auditoría.
- Intercambio electrónico de información.

RESULTADO

Documentos aportados:

- Acta No. 11 CIGD - 13 de octubre de 2022.pdf: Documento descrito en el numeral 2.2.3.

- Manual de Seguridad de la Información 2022: Documento descrito en el numeral 2.1.19.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó la Política de No Repudio, aprobada por la alta dirección y socializada al interior de la entidad.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar la Política de No Repudio, la cual debe establecer las directrices mediante las cuales se indica a los funcionarios, contratistas y proveedores involucrados en la realización de transacciones operativas o comunicaciones, para que no puedan negar su participación en estas, de tal manera que se garantice la autenticidad de las transacciones o comunicaciones realizadas, evitando manipulaciones que puedan poner en riesgo la transparencia y la confianza de las operaciones y comunicaciones institucionales. La política deberá incluir mínimo los siguientes aspectos: Trazabilidad, Retención, Auditoría, Intercambio electrónico de información, entre otros

2.9.4.4 Implementación de la Política de Registro y Auditoría

Documento con la Política de Registro y Auditoría, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad, con las especificaciones del mantenimiento de las evidencias de las actividades y acciones que afectan los activos de información. Esta política deberá contener:

- Responsabilidad.
- Almacenamiento de registros.
- Normatividad.
- Garantía cumplimiento.
- Periodicidad.

RESULTADO

Para este criterio, el proceso auditado no aportó evidencias documentales.

HALLAZGO

De acuerdo con las evidencias aportadas, se identificó la ausencia de la Política de Registro y Auditoría, debidamente aprobada por la alta dirección y socializada al interior de la entidad.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar la Política de Registro y Auditoría para establecer las directrices y procedimientos sistemáticos que permitan la creación, almacenamiento, protección, y análisis de registros y auditorías dentro de la entidad. Esta política busca asegurar la integridad, disponibilidad, y confidencialidad de los registros de actividades de usuario, eventos del sistema, y auditorías de seguridad. Además, pretende cumplir con requisitos regulatorios, normativos y de cumplimiento, proporcionando evidencia verificable de las acciones realizadas en los sistemas y datos críticos institucionales.

2.9.4.5 Implementación de la Política de Gestión de Incidentes de Seguridad de la Información

Documento con la Política de Gestión de Incidentes de Seguridad de la Información, debidamente aprobada por la alta Dirección y socializada al interior de la Entidad con las especificaciones de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información. Debe ir dirigida a todos los usuarios que tienen un acceso autorizado a cualquier sistema de información. La política debe contemplar para su elaboración los siguientes parámetros:

- Debe estar aprobada por la alta dirección, certificando así el compromiso con el proceso.
- Visión General.
- Definir responsables.
- Actividades.
- Documentación.
- Descripción del Equipo que manejará los Incidentes.
- Aspectos Legales.

RESULTADO

Documentos aportados:

- Acta No. 11 CIGD - 13 de octubre de 2022: Documento descrito en el numeral 2.2.3.

- Manual de Seguridad de la Información 2022: Documento descrito en el numeral 2.1.19.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó la Política de Gestión de Incidentes de Seguridad de la Información, debidamente aprobada por la alta dirección y socializada al interior de la entidad.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar la Política de Gestión de Incidentes de Seguridad de la Información para establecer las directrices que permitan implementar un marco estructurado y eficaz, con el fin detectar, responder, mitigar y gestionar los incidentes de seguridad de la información dentro de la Entidad. Esta política tiene como propósito principal reducir al mínimo el impacto de los incidentes de seguridad, proteger los activos de información crítica y mantener la continuidad del negocio. Además, busca definir roles y responsabilidades para los equipos de respuesta a incidentes, establecer procedimientos detallados para la notificación y manejo de incidentes, y promover la mejora continua mediante la revisión y la actualización periódica de los procesos de gestión de incidentes.

2.9.4.6 Implementación del Procedimiento de Ingreso y Desvinculación del Personal

Documento con el Procedimiento de Ingreso y Desvinculación del Personal, debidamente documentado, socializado y aprobado con las especificaciones de como la entidad gestiona de manera segura el ingreso y desvinculación, incluyendo temas como verificación de antecedentes, firma de acuerdos de confidencialidad, recepción de entregables requeridos para generar paz y salvos entre otras características.

Este procedimiento va de la mano con el área de gestión de recursos humanos o contratación puede generarse con su colaboración.

RESULTADO

Documentos aportados:

- GAD22-FOR03 Paz y salvo de desvinculación o terminación de contrato.pdf: Formato de Paz y Salvo por Desvinculación o Terminación de Contrato.

- GAD-PRC21 Retiro de privilegios a contratistas.pdf: Procedimiento titulado "RETIRO DE PRIVILEGIOS A CONTRATISTAS", el cual establece las actividades para conceder o retirar los permisos de cuentas de usuarios institucionales a los contratistas.

- GTH-PCR20 Desvinculación del personal de planta.pdf: Procedimiento titulado "DESVINCULACIÓN DEL PERSONAL DE PLANTA", el cual establece las actividades para formalizar el retiro o desvinculación de los servidores públicos de la CGN.

- GTH-PRC19 Selección y vinculación del personal de planta.pdf: Procedimiento titulado "SELECCIÓN Y VINCULACIÓN DE PERSONAL DE PLANTA", el cual establece las actividades para realizar la selección y vinculación de los Servidores Públicos de la CGN.

Revisada y analizada la información proporcionada, se identificó el Procedimiento de Ingreso y Desvinculación del Personal, debidamente aprobado por la alta dirección y socializado al interior de la entidad. Este procedimiento incluye elementos esenciales como Introducción, Objetivo, Objetivos específicos, Alcance, Condiciones de implementación, Roles y Responsabilidades, entre otros aspectos necesarios para su adecuada comprensión y aplicación.

2.9.4.7 Implementación del Procedimiento de Transferencia de Información

Documento con el Procedimiento de Transferencia de Información, debidamente documentado, socializado y aprobado con las especificaciones de **cómo la entidad realiza la transmisión o transferencia de la información de manera segura dentro de la entidad o con entidades externas, donde se apliquen métodos para proteger la información de interceptación, copiado, modificación y/o destrucción, junto con las especificaciones de los acuerdos de confidencialidad y no divulgación, que deben estar actualizados y revisados constantemente,**

donde se incluyan condiciones sobre la información que se va a proteger, la duración del acuerdo, responsabilidades, propietarios de la información, acciones en caso de incumplimiento, entre otros.

RESULTADO

Documentos aportados:

- Manual de Seguridad de la Información.pdf: El documento presenta contenidos que abarcan principalmente los siguientes apartados: Descripción, Referencia normativa, Definiciones, Cumplimiento y Principios, Propósito, Alcance, Generalidades, Política del SGSI - Sistema de Gestión de Seguridad de la Información de la CGN, Objetivos del Sistema de Gestión de Seguridad de la Información, Revisión de la política y el manual de seguridad de la información y digital, Roles y Responsabilidades, Separación de deberes, Contacto con Autoridades y Grupos de interés, Políticas de Seguridad de la Información y Digital, y Bibliografía.

- IPSEC GTI10-FOR08 Formato de Solicitud VPN.pdf: Formato para solicitar la instalación de VPN (Virtual Private Network) o red privada virtual. Este mecanismo de control permite establecer una conexión protegida al utilizar redes públicas. Las VPN cifran el tráfico en internet, lo que dificulta a terceros el seguimiento de las actividades en línea y el robo de datos.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó el Procedimiento de Transferencia de Información (“*cómo la entidad realiza la transmisión o transferencia de la información de manera segura dentro de la entidad o con entidades externas, donde se apliquen métodos para proteger la información de interceptación, copiado, modificación y/o destrucción, junto con las especificaciones de los acuerdos de confidencialidad y no divulgación, que deben estar actualizados y revisados constantemente, donde se incluyan condiciones sobre la información que se va a proteger, la duración del acuerdo, responsabilidades, propietarios de la información, acciones en caso de incumplimiento, entre otros***.”**), debidamente aprobado por la alta dirección y socializado al interior de la entidad.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar el Procedimiento de Transferencia de Información para establecer las actividades que permitan asegurar la transferencia de datos e información, tanto dentro como fuera de la entidad de manera segura, confiable y conforme a las políticas de seguridad de la información. Este procedimiento busca proteger la integridad, confidencialidad y disponibilidad de los datos durante su transmisión, minimizando riesgos asociados a pérdidas, accesos no autorizados y posibles compromisos de seguridad. Además, se pretende garantizar que todos los procesos de transferencia cumplan con las normativas

legales y regulaciones aplicables, asegurando la correcta gestión y protección de la información en tránsito.

El procedimiento incluye actividades de cómo la entidad realiza la transmisión o transferencia de la información de manera segura dentro de la entidad o con entidades externas, donde se apliquen métodos para proteger la información de interceptación, copiado, modificación y/o destrucción, junto con las especificaciones de los acuerdos de confidencialidad y no divulgación, que deben estar actualizados y revisados constantemente, donde se incluyan condiciones sobre la información que se va a proteger, la duración del acuerdo, responsabilidades, propietarios de la información, y acciones en caso de incumplimiento, entre otros.

2.9.4.8 Revisión y Validación del Inventario de Activos de Información

Actividades de Revisión del Inventario de Activos, consistente en la verificación que se lleva a cabo para determinar si un activo de información continua o no siendo parte del inventario, o si los valores de evaluación asignados en el inventario y clasificación de activos de Información deben ser modificados.

La documentación de la actividad de Revisión del Inventario de Activos, debe contener la información que hace referencia a aquellas razones por las cuales debió realizarse una revisión o validación, tales como:

- Actualizaciones al proceso al que pertenece el activo.
- Adición de actividades al proceso.
- Inclusión de nuevos registros de calidad, nuevos registros de referencia ó procesos y procedimientos.
- Inclusión de un nuevo activo.
- Desaparición de un área, proceso o cargo en la entidad que tenía asignado el rol de propietario o custodio (Cambios Organizacionales).
- Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados.
- Cambios físicos de la ubicación de activos de información.

RESULTADO

Documento aportado:

TIC-GES-SGC-PROC-GEA-RegistroDetalladoActivosTI (1).xls: El documento pertenece al proceso de Gestión TICs y al procedimiento de Administración de Activos de TIC, con fecha de aprobación del 11-09-2018, código GTI11-FOR01 y versión 1. El documento incluye varias secciones que detallan distintos activos de la entidad, como switches, servidores, firewalls, computadoras, laptops, software, impresoras y otros equipos. Sin embargo, algunas secciones carecen de títulos, lo que puede complicar su identificación y gestión. Los datos registrados abarcan información técnica y logística, incluyendo ubicación, especificaciones del equipo, proveedores y detalles de compra.

HALLAZGO

De acuerdo con la documentación aportada por el proceso, no se identificó evidencia documental que dé cuenta de la realización de la actividad de Revisión del Inventario de Activos, consistente en la verificación que se lleva a cabo para determinar si un activo de información continua o no siendo parte del inventario, o si los valores de evaluación asignados en el inventario y clasificación de activos de Información deben ser modificados.

RECOMENDACIÓN

Es pertinente realizar la actividad de Revisión del Inventario de Activos, que incluya de manera detallada las razones que motivaron dicha revisión o validación. Esta revisión debe considerar:

- Actualizaciones al proceso al que pertenece el activo.
- Incorporación de nuevas actividades al proceso.
- Inclusión de nuevos registros de calidad, registros de referencia, procesos o procedimientos.
- Adición de un nuevo activo al inventario.
- Cambios organizacionales, como la desaparición de un área, proceso o cargo en la entidad que tenía asignado el rol de propietario o custodio del activo.
- Migraciones o cambios en los sistemas de información donde se almacenan o reposan los activos previamente inventariados.
- Modificaciones físicas en la ubicación de los activos de información.

2.9.4.9 Programa para la gestión de documentos y expedientes digitales

Documento donde se especifiquen el Programa para la gestión de documentos y expedientes digitales con las especificaciones de los procesos para la planeación, producción, gestión y trámite, organización, transferencia, disposición, preservación y valoración de los documentos digitales de archivo.

Documento donde se especifique el cumplimiento de los elementos esenciales tales como: autenticidad, integridad, inalterabilidad, fiabilidad, disponibilidad y conservación, que garanticen que los documentos digitales mantienen su valor de evidencia a lo largo del ciclo de vida, incluyendo los expedientes mixtos (híbridos), digitales y electrónicos.

RESULTADO

Documentos aportados:

- POLÍTICA INSTITUCIONAL DE GESTIÓN DOCUMENTAL.pdf. Documento actualizado en noviembre de 2023 con la versión 2, el cual abarca aspectos de la gestión documental, incluyendo introducción, alcance, objetivos, marco conceptual y normativo, y políticas institucionales. Establece lineamientos para la creación, manejo, conservación y disposición final de documentos en diversos medios, con el objetivo de modernizar la gestión administrativa en la UAE Contaduría General de la Nación (CGN). Además,

menciona brevemente la gestión de documentos electrónicos y digitales, destacando la planificación e implementación del sistema de gestión documental electrónico, con énfasis en principios como interoperabilidad, seguridad y preservación a lo largo del ciclo de vida de los documentos.

- PROGRAMA DE GESTIÓN DOCUMENTAL PGD.pdf: El documento, versión 7.1 de noviembre de 2023, aborda la gestión documental en la Unidad Administrativa Especial (UAE) Contaduría General de la Nación (CGN). Incluye apartados como Introducción, Alcance, Objetivos, Lineamientos, Fases de Implementación, Subprogramas Específicos, Armonización con MECI, y Glosario.

  El documento detalla la implementación de instrumentos archivísticos para asegurar el cumplimiento de los lineamientos del Archivo General de la Nación (AGN), permitiendo la recuperación y disponibilidad de la documentación en diversos soportes.

  El Subprograma de Normalización de Formas y Formularios Electrónicos establece directrices para estandarizar documentos físicos y electrónicos, promoviendo políticas de cero papeles y facilitando la gestión documental.

  El Subprograma de Gestión de Documentos y Expedientes Electrónicos busca diseñar y supervisar estrategias para la administración de documentos electrónicos, asegurando su integridad y disponibilidad.

  Ambos subprogramas incluyen actividades detalladas para 2024-2027, enfocadas en diagnóstico, normalización, parametrización y gestión de documentos electrónicos y digitales.

- SISTEMA INTEGRADO DE CONSERVACIÓN – SIC.pdf: El documento, versión 2 de noviembre de 2023, establece los lineamientos para la conservación y preservación de documentos en la Unidad Administrativa Especial (UEA) Contaduría General de la Nación (CGN), el cual presenta los apartes de: Introducción, Alcance, Objetivos, Plan de conservación documental, Plan de preservación digital a largo plazo, y Glosario.

  El documento establece directrices claras para asegurar la integridad y accesibilidad de los documentos durante todo su ciclo de vida, sin importar el medio utilizado. Detalla un proceso organizado para la selección y gestión de recursos digitales importantes, incluyendo un cronograma que abarca actividades clave como inventario, clasificación y análisis de riesgos. En cuanto a las políticas de preservación digital, el documento aborda principios fundamentales, estrategias, roles, gestión de metadatos y protección legal. Además, proporciona una visión detallada de la infraestructura tecnológica necesaria, cubriendo aspectos de hardware, software, redes y políticas de seguridad y mantenimiento. Se subraya la importancia de realizar auditorías, revisiones de políticas y el uso de herramientas de monitoreo para garantizar la eficacia en la preservación digital. El documento también incluye actividades técnicas, económicas y estratégicas para asegurar la accesibilidad continua de la información, con un enfoque en avances tecnológicos, presupuestos y formación en preservación digital. En conjunto, ofrece una

estructura completa para la gestión documental, que incluye la evaluación continua y la adaptación a cambios tecnológicos y estratégicos.

Como resultado de la revisión documental y de la reunión virtual realizada con el equipo de Gestión Documental se evidenció que la entidad está llevando a cabo las acciones relacionadas con este criterio.

2.9.4.10 Implementación y ejecución de los indicadores de gestión de seguridad y privacidad de la información

Documento donde en su contenido se especifique como mínimo los siguientes indicadores de gestión de seguridad y privacidad de la información:

- Organización de seguridad de la información.
- Cubrimiento del MSPI en activos de información.
- Tratamientos de eventos relacionados en marco de seguridad y privacidad de la información.
- Plan de sensibilización.
- Cumplimiento de políticas de seguridad de la información en la entidad.
- Identificación de lineamientos de seguridad de la entidad.
- Verificación del control de acceso.
- Aseguramiento en la adquisición y mantenimiento de software.
- Implementación de los procesos de registro y auditoría.
- Políticas de privacidad y confidencialidad.
- Verificación de las políticas de integridad de la información.
- Políticas de disponibilidad del servicio y la información.
- Ataques informáticos a la entidad.
- Porcentaje de disponibilidad de los servicios de gobierno en línea que presta la entidad.
- Porcentaje de implementación de controles.

Cada control debe tener los parámetros de Identificador, Definición, Objetivo, Tipo de indicador, Descripción de variables, Formula, Fuente de información, Metas y Observaciones.

RESULTADO

Documento aportado:

TIC-GES-IND-2022-ConsolidadoIndicador2022.xls y TIC-GES-IND-2023-ConsolidadoIndicador2023.xls: El documento se divide en dos secciones principales:

Seguridad: Esta sección, titulada "Indicador Calidad SGSI: Pérdida de Disponibilidad, Integridad y Confidencialidad de la Información", presenta 15 registros que incluyen aspectos como la autorización y autenticación de usuarios, el uso de módems y VPNs, y la gestión del acceso remoto. Se utiliza una fórmula para calcular el porcentaje de cumplimiento de la Política de Seguridad Informática, evaluando los requisitos específicos como reportes de creación de usuario y registro detallado de TI.

Proceso Gestión TICs: Llamada "Fortalecimiento de la Plataforma Tecnológica para la Prestación de los Servicios de la CGN Nacional Indicadores del GIT Informática Año 2023", esta sección detalla ocho indicadores clave sobre la disponibilidad de internet, LAN, plataformas misionales y de gestión, soporte, y servicios informáticos contratados. También se describe el desempeño y las actividades asociadas a cada indicador, incluyendo la evaluación de fallas, mantenimientos, y la contratación de servicios. Además, el archivo incluye una sección llamada "Hoja de Vida Indicadores - Proyecto Inversión", que proporciona detalles sobre indicadores específicos relacionados con la disponibilidad y efectividad de la infraestructura tecnológica, el cumplimiento de metas de inversión, y la ejecución del plan estratégico de TI.

Revisado y analizado el contenido del documento, es posible deducir que los indicadores miden la disponibilidad de los servicios de infraestructura tecnológica, aplicativos o plataforma de gestión, servicios de soporte, y en general el cumplimiento y avance de actividades relacionadas con los proyectos de TI, Plan anual de AE, y Plan estratégico de TI, entre otros.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó la implementación de documentos donde en su contenido se especifique como mínimo los indicadores de gestión de seguridad y privacidad de la información indicados en el criterio, en donde cada control debe tener los parámetros de Identificador, Definición, Objetivo, Tipo de indicador, Descripción de variables, Formula, Fuente de información, Metas y Observaciones.

RECOMENDACIÓN

Para fortalecer la gestión de seguridad y privacidad de la información en la entidad, es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar los indicadores indicados en el criterio.

2.9.4.11 Implementación del Proceso para la gestión y la identificación de los usuarios.

Implementación del proceso para la gestión y la identificación de los usuarios, el cual debe incluir:

- Identificaciones únicas para los usuarios, que les permita estar vinculados a sus acciones y mantener la responsabilidad por ellas; el uso de identificaciones compartidas solo se debe permitir cuando sea necesario por razones operativas o del negocio, y se aprueban y documentan.
- Deshabilitar o retirar inmediatamente las identificaciones de los usuarios que han dejado la organización.
- Identificar y eliminar o deshabilitar periódicamente las identificaciones de usuario redundantes.
- Asegurar que las identificaciones de usuario redundantes no se asignen a otros

usuarios.

RESULTADO

Documentos aportados:

- GTI010-FOR02- Natali Rios.pdf: Documento descrito en el numeral 2.1.14.
- GTI010-FOR04 - Solicitud de cuentas de usuario institucional - VPN Juan Sebastian Olaya Perdomo-.pdf: Documento descrito en el numeral 2.1.14.
- GTI-PRC10 Seguridad de la Información.pdf: Documento descrito en el numeral 2.1.14.
- PazSalvo_AndresRodriguez-: Formato titulado "PAZ Y SALVO POR RETIRO DE LA ENTIDAD", mediante el cual se establece que una persona se encuentra a paz y salvo con la entidad al retirarse de esta. El formato presenta los conceptos de: Inventario elementos devolutivos, Tarjeta parqueadero, Entrega de documentos y devolución de préstamos documentales, Nómina y capacitación, Carné, Tarjeta de proximidad, Informe final de entrega del cargo/supervisión del contrato, Backup, Medio Magnético y ORFEO.

HALLAZGO

Bajo el entendido que un proceso de gestión es una serie de actividades, procedimientos y decisiones estructuradas y sistemáticas que una entidad lleva a cabo para planificar, ejecutar, supervisar y mejorar sus operaciones y objetivos; revisada y analizada la información proporcionada, no se identificó el proceso para la gestión y la identificación de los usuarios, el cual debe incluir lo establecido en el criterio.

RECOMENDACIÓN

Es pertinente desarrollar e implementar un proceso integral que cubra todas las fases de la gestión de usuarios dentro de la entidad. Este proceso debe incluir la identificación clara de roles y responsabilidades, la creación sistemática y validación de credenciales de acceso, y la implementación de mecanismos de autorización y revisión periódica. Además, se debe establecer un registro detallado y documentado de todas las actividades relacionadas con la gestión de usuarios, junto con procedimientos de monitoreo y auditoría para garantizar la integridad y adecuación de los accesos asignados. La incorporación de capacitación regular para el personal en relación con estos procedimientos es crucial para asegurar el cumplimiento de las políticas y la protección de la información.

2.9.4.12 Implementación del proceso para la gestión y administración de los derechos de acceso a la información.

Disponer de un proceso para la gestión y administración de los derechos de acceso a la información y a los activos asociados con instalaciones de procesamiento de información,

antes de que el empleo termine o cambie, dependiendo de la evaluación de factores de riesgo que incluya:

- Gestión y evaluación de la terminación o cambio del empleado, el usuario de la parte externa o la dirección, y la razón de la terminación.
- Revisión de las responsabilidades actuales del empleado, el usuario de la parte externa o cualquier otro usuario.
- Valor de los activos accesibles en la actualidad.

RESULTADO

Documento aportado:

GTI-PRC10 Seguridad de la Información.pdf: Documento descrito en el numeral 2.1.14.

El flujograma de acceso a sistemas de información y administración de usuarios y contraseñas del procedimiento es un componente del proceso de gestión y administración de los derechos de acceso a la información y a los activos asociados con las instalaciones de procesamiento de información. Sin embargo, es de entenderse que este flujograma, por sí solo, no constituye el proceso completo. El proceso de gestión y administración de derechos de acceso abarca una serie de actividades integrales, que incluyen la planificación, implementación, monitoreo y mejora continua de los controles de acceso. Estas actividades están destinadas a asegurar que los usuarios tengan acceso adecuado a la información necesaria para sus funciones, mientras se protege la confidencialidad, integridad y disponibilidad de los datos y sistemas de la entidad.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó un proceso para la gestión y administración de los derechos de acceso a la información y a los activos asociados con instalaciones de procesamiento de información, antes de que el empleo termine o cambie.

RECOMENDACIÓN

Es pertinente establecer e implementar un proceso formal y documentado para la gestión y administración de los derechos de acceso a la información y a los activos relacionados con las instalaciones de procesamiento de información. Este proceso debe activarse antes de la finalización del empleo o de cualquier cambio en la función de la labor, usuario externo o directivo, y debe basarse en una evaluación integral de los factores de riesgo.

El procedimiento debe incluir una revisión detallada de las responsabilidades actuales del usuario, así como del valor y la sensibilidad de los activos a los que tiene acceso. Además, es esencial coordinar la revocación o modificación de los derechos de acceso de manera oportuna, garantizando que ningún acceso no autorizado quede activo una vez que el empleo termine o las funciones cambien. Este proceso también debe incluir auditorías

periódicas para asegurar que los derechos de acceso estén actualizados y que se cumplan las políticas de seguridad de la información.

2.9.4.13 Implementación de la Política del Uso de programas utilitarios privilegiados

Disponer de la Política del Uso de programas utilitarios privilegiados para el uso de programas utilitarios con la capacidad de anular los controles de sistemas y de aplicaciones, que incluyan.

- Utilizar procedimientos de identificación, autenticación y autorización para los programas utilitarios.
- Separar los programas utilitarios del software de aplicaciones.
- Limitar el uso de programas utilitarios al número mínimo práctico de usuarios confiables y autorizados.
- Autorizar el uso adhoc de programas utilitarios.
- Limitar la disponibilidad de los programas utilitarios.
- Registrar el uso de los programas utilitarios.
- Definir y documentar los niveles de autorización para los programas utilitarios.
- Retirar o deshabilitar todos los programas utilitarios innecesarios.
- No poner a disposición los programas utilitarios a los usuarios que tengan acceso a aplicaciones en sistemas en donde se requiera la separación de deberes.

RESULTADO

Documento aportado:

Manual de Seguridad de la Información 2022.pdf: El documento aborda diversos aspectos clave relacionados con la gestión de la seguridad de la información en la Contaduría General de la Nación (CGN). Incluye apartados sobre la descripción, normativa, definiciones, roles y responsabilidades, políticas específicas como teletrabajo, acceso a recursos de información, uso de internet y control de virus, entre otros. Se destacan responsabilidades del personal de infraestructura en la seguridad de la información, lineamientos para teletrabajo, restricciones en la instalación de software y hardware, cumplimiento de derechos de autor, y medidas contra el uso no autorizado de herramientas que puedan comprometer la seguridad.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó la Política para el Uso de programas utilitarios privilegiados, debidamente aprobada por la alta dirección y socializado al interior de la entidad.

RECOMENDACIÓN

Es pertinente establecer una política para el uso de programas utilitarios privilegiados, con directrices que incluyan procedimientos de identificación, autenticación y

autorización; la separación de estos programas del software de aplicaciones; la limitación de su uso a un mínimo de usuarios confiables y autorizados; y la autorización del uso ad hoc. Además, se debe registrar su uso, definir niveles de autorización, deshabilitar programas innecesarios y evitar que estén disponibles para usuarios con acceso a aplicaciones en sistemas que requieran separación de deberes.

2.9.4.14 Implementación de la Política de seguridad a los activos que se encuentran fuera de las instalaciones de la entidad

De acuerdo con la NIST (National Institute of Standards and Technology) se deben catalogar los sistemas de información externos.

Documentación con las siguientes directrices para proteger los equipos fuera de las instalaciones:

- Establecer que los equipos y medios retirados de las instalaciones no se deben dejar sin vigilancia en lugares públicos.
- Seguir en todo momento las instrucciones del fabricante para proteger los equipos, (contra exposición a campos electromagnéticos fuertes).
- Controlar los lugares fuera de las instalaciones, tales como trabajo en la casa, teletrabajo y sitios temporales se deben determinar mediante una valoración de riesgos y se deben aplicar los controles adecuados según sean apropiados, (gabinetes de archivo con llave, política de escritorio limpio, controles de acceso para computadores y comunicación segura con la oficina).
- Establecer que cuando el equipo que se encuentra afuera de las instalaciones es transferido entre diferentes individuos y partes externas, llevar un registro que defina la cadena de custodia para el equipo, que incluya al menos los nombres y las organizaciones de los responsables del equipo.

RESULTADO

Documentos aportados:

- Manual de Seguridad de la Información 2022.pdf: El documento abarca varios apartados clave, incluyendo la política del Sistema de Gestión de Seguridad de la Información (SGSI) de la CGN y sus objetivos, además de roles y responsabilidades. Destaca la política para el uso de dispositivos móviles, que establece su uso exclusivo para actividades institucionales y requiere protección contra accesos no autorizados, pérdida o robo. También se detalla la política de teletrabajo y trabajo remoto, que sigue la Resolución 224 de 2022 y define medidas de seguridad como el uso de VPN y métodos de autenticación. Se prohíbe la instalación de software no autorizado y el uso de recursos para fines no institucionales.

- RESOLUCIÓN No. 163 DE 2022 Teletrabajo.pdf: Resolución mediante la cual se adopta la modalidad de Teletrabajo en la Unidad Administrativa Especial Contaduría General de la Nación-CGN. La Resolución describe las obligaciones tanto de los servidores públicos como de la CGN en el marco del teletrabajo, según lo establecido en la

Resolución. Los servidores públicos deben dedicar su jornada laboral a sus funciones, seguir normas de seguridad, mantener comunicación constante con sus superiores, y garantizar la seguridad en el uso de sistemas informáticos. Además, deben asistir a reuniones, cumplir con las normas de seguridad y salud, y participar en el sistema de gestión institucional (SIGI). La CGN, por su parte, debe definir procesos y herramientas para implementar el teletrabajo, coordinar con diferentes dependencias, asegurar la igualdad en el teletrabajo, y supervisar el cumplimiento de los lineamientos establecidos.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó la Política de seguridad a los activos que se encuentran fuera de las instalaciones de la entidad, teniendo en cuenta los diferentes riesgos de trabajar en dichas instalaciones, debidamente aprobada por la alta dirección y socializado al interior de la entidad.

RECOMENDACIÓN

Es pertinente desarrollar e implementar la política de seguridad para activos fuera de las instalaciones de la entidad, conforme a la normativa NIST, la cual establece una serie de directrices para proteger dichos activos ante los riesgos de trabajar fuera de las instalaciones. Estas directrices incluyen evitar dejar equipos sin vigilancia en lugares públicos, seguir las recomendaciones del fabricante para protegerlos, y controlar los entornos de trabajo externos a través de una evaluación de riesgos. Además, se enfatiza la importancia de la autenticación multifactor, el uso de contraseñas robustas, el cifrado de datos, y la restricción de acceso a personal autorizado. La política también aboga por la implementación de medidas físicas y tecnológicas, como mochilas seguras, software antivirus, VPNs, y soluciones de gestión de dispositivos móviles (MDM). Asimismo, se subraya la necesidad de realizar copias de seguridad regulares, mantener la capacitación continua en seguridad para el personal, y llevar a cabo auditorías periódicas para asegurar el cumplimiento de las políticas. Por último, se establece un plan de respuesta a incidentes, con procedimientos específicos para manejar situaciones de seguridad fuera de las instalaciones, y se insiste en la protección contra daños físicos y electromagnéticos.

2.9.5 Gestión de seguridad en el desarrollo y mantenimiento de sistemas de información

La gestión de seguridad en el desarrollo y mantenimiento de sistemas de información comprende la gestión de desarrollo y mantenimiento de software, la aplicación de prácticas de desarrollo o compra de aplicaciones, la revisión de código o versionamiento de componentes tecnológicos, la gestión de versiones de parcheo y la implementación de actualizaciones para mantener la integridad y seguridad de los sistemas de información.

2.9.5.1 Políticas y estándares para la gestión y gobernabilidad de TI – LI.ES.06

La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe identificar y definir las políticas y estándares que faciliten la gestión y la gobernabilidad

de TI, contemplando por lo menos los siguientes temas: seguridad, continuidad del negocio, gestión de información, adquisición tecnológica, desarrollo e implantación de sistemas de información, acceso a la tecnología y uso de las facilidades por parte de los usuarios. Así mismo, se debe contar con un proceso integrado entre las instituciones del sector que permita asegurar el cumplimiento y actualización de las políticas y estándares de TI.

RESULTADO

Documentos aportados:

- ManualSeguridadInformaciónDigitalV7.0.pdf: Documento descrito en el numeral 2.2.2.
- Manual de Seguridad de la Información y Digital.pdf: Documento descrito en el numeral 2.9.2.7.

HALLAZGO

Según las evidencias aportadas por el proceso, no se identificaron documentos para las políticas operativas y las políticas de seguridad informática, más allá de las descripciones incluidas en el Manual de Seguridad de la Información y Digital.

RECOMENDACIÓN

Acorde a lo establecido en el MSPI es importante que las políticas operativas y de seguridad informática se documenten de manera individual y detallada, asegurando que cada una contenga todos los componentes necesarios para su correcta implementación y cumplimiento. Esto no solo facilita la comprensión y aplicación de estas, sino que también garantiza que todos los aspectos críticos de la seguridad informática y operativa sean abordados y conforme a las mejores prácticas establecidas, de tal manera que, para cada una de ellas se desarrollen los conceptos de: Claridad y Especificidad, Focalización en Temas Específicos, Facilidad de Actualización, Responsabilidad y Cumplimiento, Facilidad de evaluación y el seguimiento del cumplimiento, Mitigación de Riesgos y Adaptabilidad a Cambios Normativos, entre otros, según lo establecido en la normatividad vigente.

2.9.5.2 Implementación del Procedimiento Retiro de Activos Informáticos

Implementación del Procedimiento Retiro de Activos, debidamente documentado, socializado y aprobado con las especificaciones de cómo los activos son retirados de la entidad con previa autorización, junto con el flujo de las solicitudes, autorizaciones y el control que tendrá el activo fuera de la entidad, así como también los controles de seguridad que deberá incluir el equipo cuando esté por fuera (controles criptográficos, cifrado de discos, etc.)

RESULTADO

Documento aportado:

GTI-PRC11 Gestión de activos de información.pdf: Documento descrito en el numeral 2.1.21.

HALLAZGO

Según las evidencias aportadas por el proceso, no se identificó el Procedimiento de Retiro de Activos Informáticos, debidamente aprobado por la alta dirección y socializado al interior de la entidad.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar el Procedimiento de Retiro de Activos Informáticos para asegurar que la desincorporación de los activos de la entidad se realice de manera controlada, segura y eficiente. Este procedimiento debe garantizar la identificación, documentación y eliminación adecuada de los activos informáticos, cumpliendo con todas las normativas y políticas internas aplicables. Además, debe proteger la información confidencial y mitigar los riesgos de pérdida, robo o uso indebido de los activos retirados, preservando así la integridad y seguridad de los recursos y datos institucionales.

El procedimiento debe detallar cómo los activos informáticos se retiran de la entidad con la debida autorización, estableciendo un flujo para las solicitudes y aprobaciones. También debe incluir controles rigurosos sobre el estado de los activos fuera de la entidad y las medidas de seguridad que deben aplicarse, tales como controles criptográficos y cifrados de discos.

2.9.5.3 Implementación del Procedimiento de Protección Contra Códigos Maliciosos

Implementación del Procedimiento de Protección Contra Códigos Maliciosos, debidamente documentado, socializado y aprobado por el comité que integre los sistemas de gestión institucional con las especificaciones de cómo la entidad realiza la protección contra códigos maliciosos teniendo en cuenta, que controles utiliza (hardware o software), como se instalan y se actualizan las plataformas de detección, definición de procedimientos o instructivos específicos sobre el modo de operación de la plataforma, reporte y recuperación de ataques contra software malicioso, implementación de procedimientos para recolectar información de manera regular como suscripción a listas de correo.

RESULTADO

Los auditados no aportaron evidencias documentales para este criterio con las directrices y medidas para prevenir, detectar, y mitigar el impacto de amenazas relacionadas con códigos maliciosos, como virus, malware, ransomware y otros tipos de software dañino.

HALLAZGO

Según las evidencias aportadas por el proceso, no se identificó el Procedimiento de Protección contra Códigos Maliciosos, debidamente aprobado por la alta dirección y socializado al interior de la entidad.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar el Procedimiento de Protección Contra Códigos Maliciosos con las actividades para mantener controles efectivos que permitan prevenir, detectar y mitigar el impacto de códigos maliciosos en los sistemas de información de la entidad. Este procedimiento debe asegurar la integridad, confidencialidad y disponibilidad de los datos y recursos tecnológicos, implementando medidas como la instalación y actualización de software antivirus, la configuración de filtros de seguridad, la educación y concienciación del personal, y la realización de auditorías y monitoreos constantes. De este modo, se busca minimizar los riesgos asociados a malware, virus y otras amenazas cibernéticas, garantizando un entorno seguro para las operaciones institucionales.

2.9.5.4 Caracterización de activos de información, que contengan datos personales

Caracterización de activos de información, que contengan datos personales para identificar, clasificar y documentar todos los activos de información que almacenan, procesan o transmiten datos personales. Este proceso tiene como finalidad asegurar que se implementen medidas de protección para salvaguardar la privacidad y seguridad de la información personal, en cumplimiento con las normativas y leyes de protección de datos aplicables. La caracterización permite evaluar el valor, la sensibilidad y el riesgo asociado con cada activo, facilitando la implementación de controles de seguridad específicos y la gestión efectiva de riesgos. Asimismo, ayuda a garantizar que los datos personales sean manejados de forma segura, minimizando el riesgo de acceso no autorizado, pérdida o exposición indebida, y contribuyendo a la protección de los derechos de los individuos.

RESULTADO

Documento aportado:

TIC-GES-SGC-PROC-GEA-RegistroDetalladoActivosTI (1).xls: Documento descrito en el numeral 2.9.2.8.

HALLAZGO

Según las evidencias aportadas por el proceso, no se identificó evidencia documental con la caracterización de activos de información que contengan datos personales.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar una caracterización de activos de información, que contengan datos personales para identificar, clasificar y documentar todos los activos de información que almacenan, procesan o transmiten datos personales.

2.9.5.5 Implementación de los Criterios de Impacto en la seguridad de la información

Implementación de los Criterios de Impacto en la seguridad de la información en donde se desarrollen los criterios de impacto del riesgo y especificarlos en términos del grado de daño o de los costos para la entidad, causados por un evento de seguridad de la información, considerando los siguientes aspectos:

- Nivel de clasificación de los activos de información de los procesos.
- Brechas en la seguridad de la información (ejemplo: perdidas de confidencialidad, integridad y disponibilidad de la información)
- Operaciones deterioradas
- Perdida del negocio y del valor financiero
- Alteración de planes y fechas limites
- Daños para la reputación
- Incumplimiento de los requisitos legales.

RESULTADO

Documento aportado:

Matriz Riesgos Seguridad de la Información.xls: Documento descrito en el numeral 2.1.6.

HALLAZGO

Según las evidencias aportadas por el proceso, no se identifico un documento con los criterios de impacto del riesgo y sus especificaciones en términos del grado de daño o de los costos para la entidad, causados por un evento de seguridad de la información.

RECOMENDACIÓN

Es pertinente implementar un enfoque detallado en la evaluación del impacto de los riesgos, considerando el grado de daño o costos potenciales para la entidad. Este enfoque debe incluir el desarrollo de criterios específicos que evalúen el impacto de los eventos de seguridad en diversos aspectos clave. Primero, es fundamental clasificar los activos de información de acuerdo con su importancia y sensibilidad, lo que permitirá una evaluación más precisa del impacto. Segundo, se deben identificar y analizar las brechas en la seguridad, tales como la pérdida de confidencialidad, integridad y disponibilidad de la información, y sus consecuencias asociadas. Además, es crucial evaluar cómo los incidentes pueden deteriorar las operaciones, afectar el valor financiero y los ingresos, alterar planes y fechas límites, y dañar la reputación de la entidad. Finalmente, es

necesario considerar el riesgo de incumplimiento de requisitos legales, que puede resultar en sanciones y repercusiones adicionales.

2.9.5.6 Implementación del Proceso de gestión de derechos de acceso privilegiado

Disponer de la asignación de derechos de acceso privilegiado a través de un proceso de autorización formal con los siguientes pasos:

- Identificar los derechos de acceso privilegiado asociados con cada sistema o proceso, (sistema operativo, sistema de gestión de bases de datos, y cada aplicación) y los usuarios a los que es necesario asignar.
- Definir o establecer los derechos de acceso privilegiado a usuarios con base en la necesidad de uso y caso por caso, alineada con la política de control de acceso.
- Mantener un proceso de autorización y un registro de todos los privilegios asignados. Sólo se debe suministrar derechos de acceso cuando el proceso de autorización esté completo.
- Definir los requisitos para la expiración de los derechos de acceso privilegiado.
- Establecer los derechos de acceso privilegiado a través de una identificación de usuario diferente de la usada para las actividades regulares del negocio. Las actividades regulares del negocio no se ejecutan desde una identificación privilegiada.
- Tener las competencias de los usuarios con derechos de acceso privilegiado y su revisión periódica para verificar si están en línea con sus deberes.
- Establecer y mantener procedimientos genéricos para evitar el uso no autorizado de identificaciones de usuario de administración genérica, de acuerdo con las capacidades de configuración del sistema.
- Establecer la confidencialidad de la información de autenticación secreta, para las identificaciones de usuario de administración genérica, cuando se comparta (cambiar las contraseñas con frecuencia, y cuando un usuario privilegiado ha dejado el trabajo o cambia de trabajo, comunicarlas entre los usuarios privilegiados con los mecanismos apropiados).

RESULTADO

Documento aportado:

GTI02-POL01-Política de Administración de Usuarios y o Contraseñas.pdf: Documento descrito en el numeral 2.5.6.

Es importante tener presente que la política GTI02-POL01 forma parte del proceso de gestión de usuarios y contraseñas; pero no es el Proceso de gestión de derechos de acceso privilegiado, bajo el entendido que un proceso de gestión es una serie de actividades, procedimientos y decisiones estructuradas y sistemáticas que una entidad lleva a cabo para planificar, ejecutar, supervisar y mejorar sus operaciones y objetivos.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó un Proceso de gestión de derechos de acceso privilegiado.

RECOMENDACIÓN

Es pertinente implementar un proceso para la asignación de derechos de acceso privilegiado, asegurando que estos sean gestionados de manera controlada y alineados con las políticas de seguridad de la entidad. Este proceso debe comenzar con la identificación de los derechos de acceso privilegiado necesarios para cada sistema o proceso y los usuarios correspondientes, garantizando que solo aquellos con una necesidad justificada reciban dichos privilegios. Es importante que al establecer un proceso de autorización se incluya un registro detallado de todos los privilegios asignados, y asegurar que los derechos de acceso solo se otorguen una vez que este proceso esté completamente validado. Además, se deben definir criterios para la expiración de estos derechos, asegurando que sean revisados y actualizados periódicamente.

Es recomendable que los usuarios con acceso privilegiado utilicen identificaciones específicas para estas tareas, separadas de aquellas usadas para las actividades regulares del negocio, para minimizar riesgos de seguridad. Adicionalmente, es necesario crear procedimientos que prevengan el uso no autorizado de identificaciones de administración genérica, y garantizar la confidencialidad de la información de autenticación, especialmente en casos de rotación de personal. Finalmente, es esencial que las competencias de los usuarios con acceso privilegiado sean revisadas regularmente para asegurar que se alineen con sus responsabilidades, y que se mantengan altos estándares de seguridad en la gestión de estas credenciales.

2.9.5.7 Implementación del Proceso para la gestión de información de autenticación secreta de usuarios

Disponer de un proceso para la gestión de información de autenticación secreta de usuarios, que incluya:

- Establecer la firma de una declaración para mantener confidencial la información de autenticación secreta personal, y mantener la información de autenticación secreta del grupo (cuando es compartida) únicamente dentro de los miembros del grupo; esta declaración firmada se puede incluir en los términos y condiciones del empleo para todos los que los usuarios.
- Estipular que todos los usuarios deben mantener su propia información de autenticación secreta, y se les suministra una autentificación secreta temporal segura, que se obligue a cambiar al usarla por primera vez.
- Establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle la nueva información de autenticación secreta de reemplazo o temporal.
- Definir que la información de autenticación secreta temporal se suministra a los usuarios de una manera segura; y se evitar utilizar partes externas o de mensajes de correo electrónico no protegidos (texto claro).

- Establecer que la información de autenticación secreta temporal es única para un individuo y no es fácil de adivinar.
- Definir que los usuarios deben acusar recibo de la información de autenticación secreta;
- Establecer que la información de autenticación secreta por defecto, del fabricante, se modifica después de la instalación de los sistemas o software.

RESULTADO

Documentos aportados:

- Acuerdo Confidencialidad_Oralia Franco.pdf: Documento descrito en el numeral 2.5.6.

- GTI010-FOR02- Natali Rios.pdf: Documento descrito en el numeral 2.1.14.

- GTI010-FOR04 - Solicitud de cuentas de usuario institucional - VPN Juan Sebastian Olaya Perdomo-.pdf: Documento descrito en el numeral 2.1.14.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó un Proceso para la gestión de información de autenticación secreta de usuarios.

RECOMENDACIÓN

Es pertinente implementar un proceso integral y seguro para la gestión de la información de autenticación secreta de usuarios, que garantice la confidencialidad y protección de las credenciales. Este proceso debe incluir la firma de una declaración por parte de los usuarios, comprometiéndose a mantener la confidencialidad de su información de autenticación secreta personal y, en caso de credenciales compartidas, a restringir su conocimiento únicamente a los miembros autorizados del grupo. Esta declaración puede integrarse en los términos y condiciones de empleo y contratación. Además, se debe estipular que cada usuario es responsable de su propia información de autenticación secreta, y que, al recibir una credencial temporal segura, está obligado a cambiarla al primer uso.

Es fundamental establecer procedimientos que verifiquen la identidad del usuario antes de proporcionarle nuevas credenciales temporales o de reemplazo, asegurando que este proceso se realice de manera segura y evitando el uso de canales inseguros como correos electrónicos no protegidos. También se debe asegurar que las credenciales temporales sean únicas para cada individuo y difíciles de adivinar. Asimismo, es necesario que los usuarios acusen recibo de la nueva información de autenticación secreta y que cualquier credencial predeterminada del fabricante sea modificada inmediatamente después de la instalación de sistemas o software, fortaleciendo así la seguridad de la entidad.

2.9.5.8 Implementación de la Política de protección de transacciones de los servicios de las aplicaciones

La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada mediante la implementación de la Política de protección de transacciones de los servicios de las aplicaciones, teniendo en cuenta:

- Definir el uso de firmas electrónicas por cada una de las partes involucradas en la transacción.
- Establecer todos los aspectos de la transacción, es decir, asegurar: definir la información de autenticación secreta de usuario, de todas las partes, se valide y verifique; definir a transacción permanezca confidencial y mantener la privacidad asociada con todas las partes involucradas.
- Definir la trayectoria de las comunicaciones entre todas las partes involucradas esté encriptada.
- Definir los protocolos usados para comunicarse entre todas las partes involucradas estén asegurados.
- Asegurar que el almacenamiento de los detalles de la transacción esté afuera de cualquier entorno accesible públicamente, (en una plataforma de almacenamiento existente en la intranet de la organización, y no retenido ni expuesto en un medio de almacenamiento accesible directamente desde Internet).
- Utilizar una autoridad confiable (para los propósitos de emitir y mantener firmas digitales o certificados digitales), la seguridad está integrada e incluida en todo el proceso de gestión de certificados/firmas de un extremo a otro.

RESULTADO

Documentos aportados:

- Carta de Aceptacion_MC-002-24_TOKENS DIGITALES-CERTIFICADOS SSL.pdf: Documento titulado "FORMATO DE COMUNICACIÓN Y ACEPTACIÓN DE LA OFERTA", el cual describe que la oferta presentada por la Sociedad Gestión de Seguridad Electrónica S.A. (GSE) para el Proceso de Mínima Cuantía No. MC-002-2024 ha sido aceptada, conforme al literal C del artículo 94 de la Ley 1474 de 2011 y la normativa de contratación pública (Ley 80 de 1993, Ley 1150 de 2007, Ley 1474 de 2011, y el Decreto 1082 de 2015). La propuesta, radicada el 6 de junio de 2024 por Iván Felipe Dallos Rueda, cumple con las condiciones técnicas, experiencia y capacidad jurídica exigidas. El contrato celebrado tiene por objeto la adquisición de cincuenta certificados digitales criptográficos tipo Función Pública y certificados digitales (SSL) para los dominios y subdominios de la UAE Contaduría General de la Nación. La ejecución del contrato deberá seguir las condiciones del proceso de selección y los ofrecimientos formulados en la oferta económica, y se formalizará una Orden en el SECOP II detallando las condiciones de ejecución.

- GTI07-POL01- Política de Desarrollo y Mantenimiento de Software.pdf: Documento

descrito en el numeral 2.4.9.

- GTI10-POL01 - Política de Acceso a la Red Privada Virtual de la CGN.pdf: Documento descrito en el numeral 2.1.14.

HALLAZGO

Revisada y analizada la información proporcionada, no se identificó la Política de protección de las transacciones de los servicios de las aplicaciones para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada, debidamente aprobado por la alta dirección y socializado al interior de la entidad.

RECOMENDACIÓN

Es pertinente desarrollar, revisar, contextualizar, aprobar, implementar y apropiar la Política de protección de las transacciones de los servicios de las aplicaciones para establecer las directrices que garanticen la seguridad y la integridad de las transacciones realizadas a través de las aplicaciones de la entidad. Esta política busca prevenir la transmisión incompleta, el enrutamiento incorrecto, la alteración no autorizada de mensajes, la divulgación no autorizada, así como la duplicación o reproducción no autorizada de mensajes. Para ello, se deben implementar medidas técnicas y procedimientos que aseguran que toda transacción sea transmitida y recibida de manera íntegra y segura, manteniendo la confidencialidad y autenticidad de la información y minimizando los riesgos de accesos indebidos o manipulaciones malintencionadas.