U. A. E. CONTADURÍA GENERAL DE LA NACIÓN

RESOLUCIÓN No. 383

(15 de noviembre de 2023)

Por la cual se designa al Oficial de Seguridad y Privacidad de la Información en la Contaduría General de la Nación y se asignan sus funciones.

EL CONTADOR GENERAL DE LA NACIÓN

En uso de sus atribuciones constitucionales y legales, en especial las que le Confiaren el literal g) del artículo 3 de la Ley 298 de 1996 y los numerales 8 y 17 del artículo 4o del Decreto No. 1693 de 2023, y

CONSIDERANDO:

Que el Decreto 1008 del 14 de junio de 2018, el cual establece los lineamientos generales de la Política de Gobierno Digital y subroga el Capítulo 1 del Título 9 la Parte 2 del Libro 2 del Decreto 1078 de 2015, Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, el cual determina que la seguridad de la información busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, elemento fundamental que permite el desarrollo del gobierno digital y privacidad de los datos

Que el artículo 2.2.17.5.6 del Decreto 620 del 2 de mayo de 2020, establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales, seguridad de la información y seguridad digital, determinando que los actores que realicen el tratamiento de la información, deberán contar con una estrategia de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio, en la que se lleve a cabo periódicamente una evaluación del riesgo de seguridad digital que incluya una identificación de las mejoras a implementar en el Sistema de Administración del Riesgo Operativo.

Que, para cumplir este propósito se debe contar con un fundamento normativo, políticas de ejecución, procedimientos, recursos técnicos, recursos administrativos y humanos necesarios para gestionar efectivamente el riesgo. En ese sentido, las entidades deben adoptar los lineamientos para la gestión de la seguridad de la información y seguridad digital que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

Que el CONPES 3995 de 2020, Política Nacional de Confianza y Seguridad Digital, fija como objetivo el de establecer medidas para desarrollar la confianza digital a través de la mejora en la seguridad digital de manera que, Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como, la adopción de modelos con énfasis en nuevas tecnologías.

Que el Decreto 338 del 8 de marzo de 2022, por el cual se adiciona el Título 21

a la Parte 2 del Libro 2 del Decreto 1078 de 2015 Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el modelo y las instancias de gestión de riesgos y atención de incidentes y se dictan otras disposiciones.

Que, con fundamento en lo anterior, se hace necesario disponer de un marco para la gobernanza de la seguridad digital en la Contaduría General de la Nación, así como implementar y aplicar Modelos de Gestión de Riesgos de Seguridad y un Modelo Institucional de Atención de Incidentes.

Que, en el Manual de Gobierno Digital, expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones, se establecen las pautas que deben aplicar las entidades públicas para la implementación de la Política de Gobierno Digital, entre ellas, la aplicación del Modelo de Seguridad y Privacidad de la Información (MSPI), cuyos lineamientos e indicadores permiten establecer el nivel de madurez en materia de seguridad digital para las entidades públicas.

Que el mencionado Manual se encuentra alineado con las buenas prácticas en seguridad (Norma ISC/IEC 27001:2013), con la Ley 1581 de 2012 que trata de la Protección de Datos Personales y con la Ley 1712 de 2014 (Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional).

Que la implementación del Modelo de Seguridad y Privacidad de la Información-MSPI- en la Contaduría General de la Nación está determinada por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la entidad, todo con el objetivo de, preservar la confidencialidad, integridad, disponibilidad de los activos de la información, garantizando la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo.

Que mediante la adopción del Modelo de Seguridad y Privacidad por parte de las entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información cumpliendo con la aplicación del concepto de Seguridad Digital.

Que para el cumplimiento del Modelo de Seguridad y Privacidad de la Información se debe establecer las funciones y responsabilidades del líder de la planeación, implementación y verificación a cargo del Oficial de Seguridad y Privacidad de la Información.

Que, en mérito de lo expuesto.

RESUELVE:

ARTÍCULO 1. Objeto. Establecer la forma de designación y las funciones del Oficial de Seguridad y Privacidad de la información en la Contaduría General de la Nación.

ARTÍCULO 2. Definiciones. Para efectos de la presente Resolución se tendrán en cuenta las siguientes definiciones:

Activo: En el contexto de Seguridad y Privacidad de la información son recursos tales como: hardware, software, de procesamiento, almacenamiento y comunicaciones, bases de datos (datos personales u otra información), información física y digital, procedimientos y recursos humanos asociados al manejo de los datos y la información misional, operativa y administrativa que utiliza la entidad para el desarrollo de sus actividades.

Activos de Información: Todo activo que recibe, produce, utiliza, transforma

o entrega la entidad y le representa valor.

Ambiente de Desarrollo: Conjunto de elementos de hardware y software como compiladores, editores, instaladores de lenguajes de programación, donde residen todos los recursos informáticos necesarios para efectuar tareas relacionadas con la generación o modificación de aplicaciones.

Ambiente de Producción: Conjunto de elementos de hardware y software que soportan los sistemas de información utilizados por los funcionarios para la ejecución de las operaciones de la entidad. En este ambiente deben residir aplicaciones en producción, bibliotecas o directorios que contengan archivos de datos, bases de datos, programas ejecutables o compilados.

Ambiente de Pruebas: Conjunto de elementos de hardware y software que soportan los sistemas de información utilizados para verificar la funcionalidad de los desarrollos de software y aplicativos y realizar los ajustes necesarios antes de ser puestos el funcionamiento en el ambiente de producción de la entidad.

Amenaza: Causa potencial de un incidente no deseado, el cuál puede afectar la confidencialidad, integridad y disponibilidad de un activo de información.

AIN: Análisis de Impacto al Negocio.

Confidencialidad: Propiedad que determina que la información solo esté disponible y sea revelada a individuos, entidades o procesos autorizados

Control: Medida que previene la materialización del riesgo.

Datos Abiertos: En los términos de la Ley 1712 de 2014, son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Disponibilidad: Es la propiedad de la información que permite que ésta sea accesible y utilizada cuando se requiera.

Incidente de Seguridad de la Información: Ocurrencia de un acto intencional o no intencional que tiene una alta probabilidad de afectar la información de la entidad, que a causa de este acto se vea afectada la operación y por lo tanto amenaza la seguridad de la información.

Integridad. Propiedad de salvaguardar la exactitud y estado completo de los activos de información. Condición que garantiza que la información consignada en un mensaje de datos ha permanecido completa e inalterada, salvo la adición autorizada de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación.

MSPI: Modelo de Seguridad y Privacidad de la Información

PHVA: Planear-Hacer-Verificar-Actuar. Enfoque de gestión simple e interactivo para probar cambios en procesos o soluciones a problemas, e impulsar su optimización continua a través del tiempo.

Riesgo de Seguridad y Privacidad de la Información: Posibilidad de ocurrencia de eventos asociados a los dominios del modelo de Seguridad y Privacidad de la Información bajo los estándares de la Norma ISO 27001 correspondientes a seguridad física, talento humano, contratación, seguridad en operaciones, gestión documental, datos personales, entre otros, que afecten la seguridad digital, la gestión documental y la protección de datos

Vulnerabilidad: Representa la vulnerabilidad de un activo que puede ser lesionado o explotado por una o más amenazas y afectar su confidencialidad, integridad y disponibilidad.

ARTÍCULO 3. Designación y Responsabilidad del Oficial de Seguridad y Privacidad de la Información. El Oficial de Seguridad y Privacidad de la Información será el Secretario General o quien haga sus veces

El Oficial de Seguridad y Privacidad de la Información será el responsable de liderar todo el ciclo de PHVA del MSPI, no obstante, para la correcta ejecución de sus funciones o decisiones se requiere del GIT de Apoyo Informático.

ARTÍCULO 4. Funciones del Oficial de Seguridad y Privacidad de la Información. Son funciones del Oficial de Seguridad y Privacidad de la Información de la Contaduría General de la Nación las siguientes:

1. Liderar el cumplimiento al ciclo PHVA del MSPI.

2. Definir y elaborar documentos que sean de su competencia para la operación del MSPI, actualizar y definir políticas. normas, procedimientos y estándares. manuales, metodologías del MSPI que sea de su competencia, así como apoyar otros procesos que requieran brindar lineamientos relacionados con seguridad de la información.

3. Realizar, proponer y exponer riesgos cibernéticos en materia de seguridad y privacidad de la información de acuerdo con los proyectos y/o procesos de la entidad.

4. Brindar acompañamiento a los procesos de la entidad en la identificación, clasificación de activos de información y tratamiento de riesgos de seguridad digital, que puedan comprometer las operaciones de la Contaduría General de la Nación y pueda amenazar la seguridad de la información de acuerdo con lo definido en la Política de Administración de Riesgos de la entidad.

5. Definir e implementar actividades de divulgación, campañas o capacitaciones de socialización sobre seguridad y privacidad de la información para servidores públicos, contratistas y partes interesadas que consulten o reciban servicios de la Contaduría General de la Nación.

6. Apoyar, proponer y hacer seguimiento a los procesos en los planes de mejoramiento pera dar cumplimiento a las recomendaciones en materia de seguridad y privacidad de la información.

7. Definir, implementar y aplicar el procedimiento de Gestión de Incidentes de Seguridad y Privacidad de la información en la entidad, con el fin de detectar, contener, reportar, evaluar, responder, tratar e identificar las lecciones aprendidas de incidentes de seguridad y privacidad de la información.

8. Hacer seguimiento y proponer los controles necesarios a los procesos en

la implementación de las Políticas de Seguridad y Privacidad de la Información en la Contaduría General de la Nación.

9. Adelantar acciones de articulación con la Coordinación del GIT de Apoyo Informático de la entidad sobre seguridad de la información y seguridad digital, para que pueda hacer seguimiento y tomar las decisiones adecuadas en esta materia.

10. Efectuar acompañamiento y dar recomendaciones a la alta dirección, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades de los líderes de los procesos en seguridad y privacidad de a información.

11. Realizar el análisis de riesgos a las aplicaciones y sistemas de información de uso de la Contaduría General de la Nación

12. Asesorar en la aplicación de la metodología para el mantenimiento de los planes de contingencia y continuidad de las funciones misionales de la Entidad.

13. Evaluar, seleccionar e implantar herramientas que faciliten la labor de seguridad y privacidad de la información.

14. Impartir lineamientos y hacer seguimiento para controlar el acceso a los sistemas de información y la modificación de privilegios.

15. Promover la formación, educación y el entrenamiento en seguridad y privacidad de la información.

16. Recibir capacitación en el tema de seguridad y privacidad de la información; mantenerse actualizado en nuevas amenazas y vulnerabilidades existentes con el fin de socializar y divulgar al interior de la entidad; adoptar mejores prácticas de seguridad de la información en la plataforma tecnológica y sistemas de información. Adicionalmente, poder replicar a todas las partes interesadas de la Contaduría General de la Nación los nuevos conocimientos aprendidos en el uso y apropiación de seguridad de la información.

17. Realizar estudios de penetración y pruebas de vulnerabilidades en todos los ambientes (Desarrollo, Pruebas, Producción y Contingencia) a los servidores, equipos de comunicación, seguridad y sistemas de información, resultado de los procesos de Gestión de Sistemas de Información y Gestión de Configuración y Activos de los Servicios de TI. De igual forma, recomendar controles o planes de tratamiento para la mitigación de las vulnerabilidades.

18. Informar al Comité Institucional de Gestión de Desempeño de la entidad cuando se presenten violaciones a los controles de seguridad de bases de datos que contengan datos personales y existan riesgos en la administración de la información de los titulares, para evaluar la pertinencia de informar a la Superintendencia de Industria y Comercio.

19. Coordinar y apoyar las auditorías internas y externas al sistema de gestión de seguridad de la información enmarcadas en las responsabilidades de la segunda línea de defensa de acuerdo con el Modelo Estándar de Control Interno, sin que en ningún caso pueda auditar su propio proceso.

20. Realizar seguimiento a la implementación de las recomendaciones en materia de seguridad de la información que hayan resultado de cada

auditoria.

21. Realizar el monitoreo del cumplimiento de las políticas y procedimientos que se establezcan en materia de seguridad de la información, sin perjuicio de aquellas tareas que realizan las autoridades de control.

22. Estar al tanto de las nuevas modalidades de ciberataques que pudieran llegar a afectar a la entidad en materia de seguridad y privacidad de la información, de acuerdo con su evaluación de riesgo y atendiendo criterios de razonabilidad.

23. Evaluar las medidas de seguridad, privacidad y circulación restringida en la transferencia de información a otras entidades para garantizar la autenticidad, integridad, disponibilidad, confidencialidad, el acceso y circulación restringida de la información, de conformidad con lo estipulado en el habilitador transversal de seguridad de la información de la Política de Gobierno Digital.

24. Reportar a la Oficina de Control Disciplinario Interno las presuntas violaciones de los servidores públicos al cumplimiento de las políticas del manual de seguridad y privacidad de la información, que generaron un incidente que afectó la integridad, la disponibilidad o confidencialidad de la información de la Entidad, para su respectiva investigación y acciones a las que haya lugar.

25. Aplicar las demás consideraciones que a juicio de la nación y la entidad contribuyan a elevar sus estándares de seguridad y privacidad de la información.

ARTÍCULO 5. Informe de avances con respecto de la Gestión del Oficial de Seguridad y Privacidad de la Información. El Oficial de Seguridad y Privacidad de la Información de la Contaduría General de la Nación, realizará informes con respecto al avance de su gestión semestralmente en el marco del Comité Institucional de Gestión y Desempeño.

ARTÍCULO 6. Enlaces de Activos de Información de la Contaduría General de la Nación: Conformado por servidores públicos de las diferentes dependencias, quienes son designados por los líderes de cada área. En este equipo se debe garantizar la representación de la totalidad de las dependencias de la Contaduría General de la Nación.

ARTÍCULO 7. Responsabilidades de los Enlaces de Activos de Información de la Contaduría General de la Nación: Los Enlaces tendrán la responsabilidad de:

1. Transferir al interior de sus áreas el conocimiento adquirido en materia de Seguridad y Privacidad de la Información, promoviendo la cultura de seguridad y privacidad de la información.

2. Realizar actividades de divulgación, socialización, comunicación de los temas relacionados son Seguridad y Privacidad de la Información.

3. Cumplir a cabalidad las políticas que imparta la Entidad a través del Manual de Políticas de Seguridad y Privacidad de la Información y demás documentos del Sistema Integrado de Gestión asociados a este.

4. Acompañar al Oficial de Seguridad y Privacidad de la Información en la identificación y etiquetado de los activos de información.

5. Acompañar al Oficial de Seguridad y Privacidad de la Información en la identificación de los riesgos, acciones de mejora y actividades para los controles a implementar.

6. Apoyar las auditorias en materia de Seguridad y Privacidad de la Información en caso de que le sean asignadas, sin que en ningún caso puedan auditar sus propios procesos

7 Participar activamente en las capacitaciones, sensibilizaciones que sobre Seguridad y Privacidad de la Información imparta la entidad.

8 Apoyar la implementación de los lineamientos impartidos por el Oficial de Seguridad y Privacidad de la Información en las respectivas dependencias de la entidad.

ARTÍCULO 8. Reuniones de los Enlaces de Activos de Información de la Contaduría General de la Nación. Los Enlaces se reunirán a solicitud del Oficial de Seguridad y Privacidad de la Información, tres (3) veces al año en reuniones ordinarias y extraordinariamente cuando las circunstancias lo ameriten.

ARTÍCULO 9. Vigencia. La presente Resolución rige a partir de la fecha de su publicación en el diario Oficial.

PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C., a los quince (15) días del mes de noviembre de 2023.

MAURICIO GÓMEZ VILLEGAS
Contador General de la Nación

Proyectó: César Augusto Rincón Vicentes, Asesor 1020-13
Revisó: Jamir Mosquera Rubio, Coordinador GIT Informática
Edgar Arturo Diaz Vipesco, Coordinador GIT de Jurídica
Freddy Castaño Pineda, Secretario General