CONTADURÍA GENERAL DE LA NACIÓN
Cuentas Claras, Estado Transparente

DECLARACIÓN DE APLICABILIDAD (SOA) ISO/IEC 27001:2022

JUNIO DE 2025

VERSIÓN	SECCIÓN	TIPO	FECHA (DD/MM/ AAAA)	AUTOR	OBSERVACIONES
1.0	Todas	Creación	9/6/2025	GIT de Apoyo Informático	Creación de un documento estructurado de la Declaración de aplicabilidad revisado y aprobado por el Equipo Operativo para el apoyo del Oficial de Seguridad y Privacidad de la Información el 09/06/2025

CONTENIDO

1. OBJETIVO

Este documento identifica los controles seleccionados para tratar los riesgos de seguridad de la información, conforme al Anexo A de la norma ISO/IEC 27001:2022, justificando su inclusión, exclusión o no aplicabilidad.

2. ALCANCE

Este documento aplica al sistema de gestión de seguridad de la información – SGSI implementado en la Contaduría General de la Nación, cubriendo los procesos de Normalización, Centralización, Consolidación y TICs en la Calle 26 # 69 - 76, Edificio Elemento Torre 1 (Aire) Piso 15

Descripción del alcance:
El Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) certifica que el SGSI ha sido auditado y aprobado con respecto a los requisitos especificados en la Norma ISO/IEC 27001 mediante el certificado CO-SI-CER660642 otorgado el 2019-01-11, y es aplicable al siguiente alcance: "Determinación de las políticas, principios y normas de contabilidad para el sector público colombiano. Unificación, centralización y consolidación de la información contable y elaboración del balance general Consolidado de la nación".

3. GOBIERNO

Para el gobierno de esta política, se designa la responsabilidad de Oficial de Seguridad y Privacidad de la Información en el Secretario General y se crea el equipo operativo de apoyo para el Oficial de Seguridad y Privacidad de la Información que tendrá la función primordial de contribuir a la gestión segura de los activos de información utilizados en la operación de los procesos de la CGN, reduciendo los riesgos asociados a la seguridad de la información y seguridad digital.

4. COMUNICACIÓN

La divulgación de la política será desarrollada a través de los diferentes procesos de la entidad y sus Grupos Internos de Trabajo (GIT) que conforman la estructura organizacional, con el apoyo fundamental de GIT Logístico de Capacitación y Prensa.

5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

La CGN, como órgano rector de la contabilidad pública en Colombia, con autoridad doctrinaria en la materia, que normaliza, centraliza y consolida la

contabilidad del sector público, para elaborar el Balance General de la Nación y de la Hacienda Pública, reconoce la información como un activo fundamental que debe ser protegido frente a amenazas internas o externas que puedan comprometer la confidencialidad, integridad y disponibilidad de esta.

Por lo anterior, la CGN establece estrategias y controles lógicos, físicos y digitales en el marco de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma ISO/IEC 27001, para asegurar la infraestructura crítica que soporta los procesos misionales, garantizando la disposición de recursos requeridos y adoptando un enfoque basado en la gestión de riesgos de seguridad de la información, la gestión de incidentes de seguridad de la información y la mejora continua del SGSI.

En cumplimiento de lo manifestado, la CGN se compromete a garantizar, verificar y cumplir todos los requisitos legales, reglamentarios, regulatorios, contractuales y de gestión documental, orientados a la mejora continua, la eficacia del SGSI, y al cumplimiento de los objetivos de seguridad de la información establecidos por la Alta Dirección.

6. CONTROLES SELECCIONADOS

La Declaración de Aplicabilidad detalla:

- Controles aplicables del Anexo A.
- Descripción de los controles
- Aplicable o no el control
- Justificación de inclusión o exclusión.
- Estado de implementación de cada control.

A continuación, se incluye la tabla con todos los controles seleccionados:

DECLARACION DE APLICABILIDAD ISO 27001:2022	
ENTIDAD EVALUADA	Contaduría General de la Nación
FECHA DE EVALUACIÓN	9/6/2025
CONTACTO	Ing. Anuar Edilson Vargas Calderon - Coordinador GIT de Apoyo Informático
ELABORADO POR	Ing Diana Murillo / Ing Raul Garay / Ing Martha Zomosa G.

	Código	Control	Descripción	Aplicable	Justificación
No	**A.5**	**Controles organizativos**			

1	A.5.1	Políticas para la seguridad de la información	Control La política de seguridad de la información y las políticas específicas asociadas deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal pertinente y partes interesadas pertinentes, y revisadas a intervalos planificados y cuando ocurran cambios significativos en la organización	Si	Se adopta este control para garantizar la idoneidad, adecuación y eficacia continuas en la alta dirección y el apoyo a la seguridad de la información de acuerdo con los requisitos de la entidad, legales, estatutarios, regulatorios y contractuales.
2	A.5.2	Funciones de seguridad de la información y Responsabilidades	Control Los roles y responsabilidades de seguridad de la información se deben definir y asignar de acuerdo con las necesidades de la organización	Si	Se adopta este control para definir y asignar las funciones y responsabilidades en Seguridad de la Información y que sea de conocimiento del personal de la Contaduría General de la Nación.
3	A.5.3	Separación de funciones	Control Los deberes y áreas de responsabilidad en conflicto deberían segregarse	Si	Se adopta este control para garantizar y prevenir errores, fraudes, evasión de los controles de seguridad de la información o mal uso de los activos al distribuir responsabilidades.
4	A.5.4	Responsabilidades de gestión	Control La Alta Dirección debe exigir a todo el personal la aplicación de la seguridad de la Información de acuerdo con la política de seguridad de la Información establecida, las políticas y los procedimientos específicos de la organización en los aspectos correspondientes.	Si	Se adopta este control para asegurar que la alta dirección cumpla con sus responsabilidades, tomen decisiones informadas, impulsen el cumplimiento de objetivos estratégicos y promuevan la mejora continua del Sistema de Gestión de Seguridad de la Información - SGSI
5	A.5.5	Contacto con las autoridades	Control La organización debe establecer y mantener contacto con las autoridades pertinentes.	Si	Se adopta este control para garantizar un intercambio adecuado de información sobre seguridad de la información entre la CGN y las autoridades legales, reguladoras y de entes de control pertinentes.
6	A.5.6	Contacto con grupos de interés especial	Control La organización debe establecer y mantener contacto con grupos de interés especial u otros foros y asociaciones profesionales especializados en Seguridad	Si	Se adopta este control para garantizar un intercambio apropiado de información en relación con la seguridad de la información, así como contar con información oportuna y actualizada acerca de nuevas tecnologías, amenazas, vulnerabilidades y sus soluciones relacionadas.

7	A.5.7	Inteligencia de amenazas	Control La información relativa a las amenazas a la seguridad de la información se debe recopilar y analizar para producir inteligencia de las amenazas.	Si	Se adopta este control para fortalecer la seguridad de la información de la CGN, identificar amenazas cibernéticas antes de que causen daño, mejorar la toma de decisiones, reducir riesgos y costos, cumplir con regulaciones, adaptarse a un entorno en constante evolución.
8	A.5.8	Seguridad de la información en la gestión de proyectos	Control La seguridad de la información se debe integrar en la gestión de proyectos	Si	Se adopta este control para asegurar que los riesgos de seguridad de la información se identifican y se abordan como parte de los proyectos de las áreas de la CGN.
9	A.5.9	Inventario de información y otros activos asociados	Control Se debe elaborar y mantener un inventario de la información y otros activos asociados, incluidos los propietarios	Si	Se adopta este control para identificar la información y demás activos relacionados con la CGN con el propósito de salvaguardar su seguridad de la información, asignando de manera apropiada la responsabilidad y propiedad correspondientes.
10	A.5.10	Uso aceptable de la información y otros activos asociados	Control Se deben identificar, documentar y implementar normas para el uso aceptable y procedimientos para el tratamiento de la información y otros activos asociados.	Si	Se adopta este control para proteger la información, prevenir riesgos, cumplir con regulaciones, mitigar amenazas cibernéticas, mejorar la eficiencia operativa, promover la conciencia de seguridad de la información en la CGN.
11	A.5.11	Devolución de activos	Control El personal y otras partes interesadas, según corresponda, deben devolver todos los activos de la organización en su posesión al cambiar o terminar su empleo, contrato o acuerdo	Si	Se adopta este control para resguardar los activos de la CGN en el contexto de procesos de cambio o finalización de empleo o contrato.
12	A.5.12	Clasificación de la información	Control La información se debe clasificar de acuerdo con las necesidades de seguridad de la información de la organización sobre la base de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas	Si	Se adopta este control para proteger la información, cumplir con regulaciones, controlar el acceso, preservar la confidencialidad y la privacidad, gestionar el ciclo de vida de la información.
13	A.5.13	Etiquetado de la información	Control Se debe elaborar y implementar un conjunto adecuado de procedimientos para el etiquetado de la información de conformidad con el sistema de clasificación de la	Si	Se adopta este control para facilitar la comunicación de la clasificación de la información y apoyar la automatización del procesamiento y gestión de la información.

			información adoptado por la organización.		
14	A.5.14	Transferencia de información	Control Las reglas, procedimientos o acuerdos de transferencia de información deben estar vigentes para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.	Si	Se adopta este control para mantener la seguridad de la información, cumplir con regulaciones de privacidad y garantizar la confidencialidad de los datos transferida entre la CGN y las partes interesadas externas.
15	A.5.15	Control de acceso	Control Las normas para controlar el acceso físico y lógico a la información y otros activos asociados se deben establecer e implementar sobre la base de los requisitos de seguridad empresarial y de la información	Si	Se adopta este control para asegurar el acceso autorizado y prevenir el acceso no autorizado a la información y otros activos asociados.
16	A.5.16	Gestión de identidades	Control Se debe gestionar el ciclo de vida completo de las identidades.	Si	Se adopta este control para permitir la identificación única de personas y sistemas que acceden a la información y otros activos asociados a la CGN, gestionar contraseñas y el ciclo de vida del usuario.
17	A.5.17	Información de autenticación	Control La asignación y gestión de la información de autenticación se debe controlar mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.	Si	Se adopta este control para controlar la asignación de contraseñas a través de un proceso de gestión formal y evitar fallas en los procesos de autenticación
18	A.5.18	Derechos de acceso	Control Los derechos de acceso a la información y otros activos asociados se deben aprovisionar, revisar, modificar y eliminar de acuerdo con la política y reglas específicas de la organización para el control de acceso.	Si	Se adopta este control para asegurar que los accesos a la información y otros activos asociados se autoricen, retiren o cambien de acuerdo a los requisitos de la CGN.
19	A.5.19	Seguridad de la información en las relaciones con los proveedores	Control Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.	Si	Se adopta este control para preservar un nivel preestablecido de seguridad de la información en las interacciones con los proveedores, identificando los riesgos de seguridad de la información asociados con los bienes y/o servicios de los proveedores.

20	A.5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores	Control Los requisitos pertinentes de seguridad de la información se deben establecer y acordar con cada proveedor en función del tipo de relación con el proveedor	Si	Se adopta este control para mantener un nivel acordado entre la CGN y los proveedores respecto a las obligaciones de ambas partes para cumplir con los requisitos pertinentes de seguridad de la información.
21	A.5.21	Gestión de la seguridad de la información en la cadena de suministro de las tecnologías de la información y comunicación (TIC)	Control Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados a la cadena de suministro de productos y servicios de TIC.	Si	Se adopta este control para asegurar que los requisitos sobre seguridad de información con relación a las tecnologías de información y comunicaciones se implementen en los acuerdos con los proveedores y la CGN y solicitar que su cadena de suministro de tecnología de información los cumpla.
22	A.5.22	Monitoreo, revisión y gestión del cambio en servicios de proveedores	Control La organización debe monitorear, revisar, evaluar y gestionar regularmente el cambio en las prácticas de seguridad de la información de los proveedores y la prestación de servicios.	Si	Se adopta este control para asegurar el cumplimiento de los términos y condiciones de seguridad de la información y prestación de servicios en línea con los acuerdos del proveedor, controlando en la CGN el impacto ante cambios en los servicios de proveedores o terceros.
23	A.5.23	Seguridad de la información para el uso de servicios en la nube	Control Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se deben establecer, de acuerdo con los requisitos de seguridad de la información de la organización	Si	Se adopta este control para proteger los datos en entornos de nube, gestionar riesgos, cumplir con regulaciones, controlar el acceso y la autenticación, mantener la seguridad de la infraestructura, monitorear amenazas, respaldar y recuperar la seguridad de la información para el uso de servicios en la nube.
24	A.5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	Control La organización debe planificar y preparar la gestión de incidentes de seguridad de la información mediante la definición, el establecimiento y la comunicación de procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información	Si	Se adopta este control para garantizar una respuesta rápida, eficaz, coherente y ordenada a los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad, cumplir con regulaciones, minimizar el impacto, proteger la información de la CGN.
25	A.5.25	Evaluación y decisión sobre eventos de seguridad de la información	Control La organización debe evaluar los eventos de seguridad de la información y debe decidir si clasificarse como incidentes de seguridad de la información	Si	Se adopta este control para ayudar a identificar el impacto, el alcance y asegurar una categorización y priorización efectiva de los eventos de seguridad de la información en la CGN.

26	A.5.26	Respuesta a incidentes de seguridad de la información	Control Los incidentes de seguridad de la información se deben responder de conformidad con los procedimientos documentados.	Si	Se adopta este control para establecer procedimientos de respuesta a los incidentes de seguridad de información en la CGN, que aseguren una respuesta eficiente y eficaz a los incidentes.
27	A.5.27	Aprender de los incidentes de seguridad de la información	Control Los conocimientos adquiridos a partir de incidentes de seguridad de la información se deben utilizar para reforzar y mejorar los controles de seguridad de la información.	Si	Se adopta este control para reducir la probabilidad o el impacto de futuros incidentes y mejorar los controles de seguridad de la CGN.
28	A.5.28	Obtención de pruebas	Control La organización debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.	Si	Se adopta este control para evitar que las evidencias necesarias sean destruidas intencional o accidentalmente antes de determinar la gravedad del incidente de seguridad de la información en la CGN , a fin de tomar acciones disciplinarias y legales.
29	A.5.29	Seguridad de la información durante la interrupción	Control La organización debe planificar cómo mantener la seguridad de la información en un nivel apropiado durante la interrupción.	Si	Se adopta este control para garantizar la continuidad del negocio, la recuperación efectiva ante desastres, la protección contra pérdida de la información, para mantener la disponibilidad durante una interrupción de los servicios.
30	A.5.30	Preparación de las TIC para la continuidad de las actividades	Control La preparación para las TIC se debe planificar, implementar, mantener y probar basado en los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC	Si	Se adopta este control para proteger la seguridad de la información asegurando la disponibilidad de la información de la CGN y otros activos asociados durante la ruptura.
31	A.5.31	Requisitos legales, estatutarios, reglamentarios y contractuales	Control Los requisitos legales, reglamentarios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos se deben identificar, documentar y mantener actualizados.	Si	Se adopta este control para asegurar el cumplimiento normativo, prevenir sanciones legales, proteger datos personales y propiedad intelectual.
32	A.5.32	Derechos de la propiedad intelectual	Control La organización debe implementar procedimientos apropiados para proteger derechos de propiedad intelectual.	Si	Se adopta este control para asegurar el cumplimiento de los requisitos legislativos, reglamentarios y contractuales respecto a los derechos de propiedad intelectual y el uso de los productos de software patentados en la CGN.

33	A.5.33	Protección de registros	Control Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso y liberación no autorizados	Si	Se adopta este control para proteger contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada de los registros de la CGN de acuerdo con los requisitos legislativos, reglamentarios, contractuales y regulatorios.
34	A.5.34	Privacidad y protección de la información de identificación personal (PII)	Control La organización debe identificar y cumplir con los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales	Si	Se adopta este control para garantizar el cumplimiento legal, estatutario, reglamentario, regulatorio y contractual relacionado con la seguridad de la información en la Protección de Datos Personales.
35	A.5.35	Examen independiente de la seguridad de la información	Control El enfoque de la organización para administrar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se debe revisar de forma independiente a intervalos planificados o cuando ocurran cambios significativos	Si	Se adopta este control para garantizar la idoneidad adecuación y eficacia en las revisiones periódicas independientes de la seguridad de información realizadas en la CGN.
36	A.5.36	Cumplimiento de políticas, reglas y estándares para la seguridad de la información	Control El cumplimiento de la política de seguridad de la información, el tema, las políticas específicas, las reglas y los estándares de la organización se debe revisar periódicamente.	Si	Se adopta este control para garantizar la implementación y operación de las políticas, reglas y estándares de seguridad de información aplicables en la CGN.
37	A.5.37	Procedimientos operativos documentados	Control Los procedimientos operativos de las instalaciones de procesamiento de la información se debe documentar y poner a disposición del personal que los necesite	Si	Se adopta este control para garantizar la operación segura y eficiente de las instalaciones de procesamiento de información, la consistencia operativa, cumplir con regulaciones, mejorar la eficiencia, facilitar la capacitación y formación, reducir la dependencia del personal clave e impulsar la mejora continua en la CGN.
	A.6	**Controles de personas**			

38	A.6.1	Chequeo	Control Las verificaciones de antecedentes de todos los candidatos para convertirse en personal se deben llevar a cabo antes de unirse a la organización y de forma continúa teniendo en cuenta las leyes, regulaciones y ética aplicables y deben ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos	Si	Se adopta este control para asegurar que se realicen las verificaciones pertinentes en los procesos de selección del personal de planta y contratistas, proveedores y terceros, y que sean idóneos para los roles en los cuales son considerados y reducir el riesgo de robo, fraude y/o mal uso de los activos de información de la CGN.
39	A.6.2	Términos y condiciones del empleo	Control Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización para la seguridad de la información	Si	Se adopta este control para asegurar que el personal de la CGN tenga conocimiento de sus obligaciones y restricciones respecto a la seguridad de la información.
40	A.6.3	Concienciación, educación y capacitación sobre la seguridad de la información	Control El personal de la organización y las partes interesadas pertinentes deben recibir información, educación y capacitación adecuadas sobre seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos del tema, según sea pertinente para su función laboral	Si	Se adopta este control para aumentar la conciencia y conocimiento sobre la seguridad de la información, con la finalidad de generar una cultura de seguridad en la CGN
41	A.6.4	Proceso disciplinario	Control Se debe formalizar y comunicar un proceso disciplinario para tomar medidas contra el personal y otras partes interesadas pertinentes que hayan cometido una violación de la política de seguridad de la información	Si	Se adopta este control para establecer un proceso disciplinario y manejar las fallas en la seguridad de la información asegurando en la CGN el tratamiento correcto y justo para el personal de planta, contratistas y/o terceros sospechosos de cometer incumplimientos de seguridad de la información.
42	A.6.5	Responsabilidades después de la terminación o cambio de empleo	Control Las responsabilidades y deberes de seguridad de la información que sigan siendo válidos después de la terminación o el cambio de empleo se debe definir, hacer cumplir y comunicar al personal pertinente y a otras partes interesadas	Si	Se adopta este control para asegurar que el personal de planta, contratistas o terceros, que se retiren o cambien de empleo de manera segura, devuelvan todos los activos de la CGN y se deshabiliten los derechos de acceso.

43	A.6.6	Acuerdos de confidencialidad o no divulgación	Control Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados y firmados periódicamente por el personal y otras partes interesadas pertinentes.	Si	Se adopta este control para proteger la información exigiendo el cumplimiento de políticas, lineamientos y/o controles en seguridad de la información.
44	A.6.7	Trabajo remoto	Control Las medidas de seguridad se deben implementar cuando el personal trabaje de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización	Si	Se adopta este control para implementar medidas de seguridad cuando el personal de planta y contratistas trabaja de forma remota para proteger la información accedida, procesada o almacenada fuera de las instalaciones de la CGN.
45	A.6.8	Informes de eventos de seguridad de la información	Control La organización debe proporcionar un mecanismo para que el personal informe oportunamente sobre los eventos de seguridad de la información observados o sospechosos a través de los canales apropiados	Si	Se adopta este control para proporcionar un mecanismo para que el personal informe los eventos de seguridad de la información observados o bajo sospecha a través de los canales apropiados de manera oportuna, contribuyendo también a minimizar los posibles riesgos de seguridad de la información y contribuyan con el mantenimiento y mejora continua de la seguridad de la información de la CGN.
	A.7	**Controles físicos**			
46	A.7.1	Perímetros de seguridad física	Control Los perímetros de seguridad se deben definir y utilizar para proteger las zonas que contengan información y otros activos asociados.	Si	Se adopta este control para prevenir el acceso físico no autorizado, así como cualquier daño o interferencia a la información de la CGN y otros activos asociados donde se procesa información.
47	A.7.2	Entrada física	Control Las zonas seguras deben estar protegidas por controles de entrada y puntos de acceso adecuados	Si	Se adopta este control para asegurar que únicamente se permita el acceso físico autorizado a la información de la CGN y demás activos vinculados.
48	A.7.3	Asegurar oficinas, habitaciones e instalaciones	Control Se debe diseñar e implementar la seguridad física de las oficinas, salas e instalaciones.	Si	Se adopta este control para prevenir el acceso físico no autorizado, así como el daño y la interferencia a la información de la CGN y otros activos asociados en oficinas, salas e instalaciones.

49	A.7.4	Monitoreo de seguridad física	Control Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados	Si	Se adopta este control para identificar y disuadir accesos no autorizados, supervisar a los visitantes y fortalecer la seguridad física integral de la CGN.
50	A.7.5	Protección contra amenazas físicas y ambientales	Control Se debe diseñar e implementar la protección contra las amenazas físicas y medioambientales, como las catástrofes naturales y otras amenazas físicas intencionadas o no intencionadas a las infraestructuras.	Si	Se adopta este control para prevenir o mitigar las consecuencias derivadas de eventos provocados por amenazas físicas y ambientales, proteger la infraestructura crítica y garantizar la disponibilidad de los servicios esenciales.
51	A.7.6	Trabajar en zonas seguras	Control Se deben diseñar e implementar medidas de seguridad para trabajar en zonas seguras	Si	Se adopta este control para definir los lineamientos para trabajar en áreas seguras y evitar accidentes y/o pérdidas de activos de información cuando se trabaja en las áreas restringidas (seguras) en la CGN.
52	A.7.7	Escritorio limpio y pantalla limpia	Control Se deben definir e implementar adecuadamente normas claras para los papeles y los soportes de almacenamiento extraíbles y normas claras sobre pantallas claras para las instalaciones de tratamiento de la información.	Si	Se adopta este control para disminuir los riesgos asociados con el acceso no autorizado, así como la posible pérdida y daño de la información almacenada en escritorios, pantallas y otros lugares accesibles, tanto durante el horario laboral como fuera de este.
53	A.7.8	Emplazamiento y protección de los equipos	Control El equipo debe estar situado de forma segura y protegida	Si	Se adopta este control para reducir las amenazas físicas y ambientales al proteger los activos usados en el procesamiento de información en la CGN.
54	A.7.9	Seguridad de los activos fuera de las instalaciones	Control Los activos externos deben estar protegidos.	Si	Se adopta este control para prevenir pérdidas, daños, robos, así como para evitar interrupciones en las operaciones asociados a los activos que se encuentran fuera de las instalaciones de la CGN.
55	A.7.10	Medios de almacenamiento	Control Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y disposición de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización	Si	Se adopta este control para asegurar exclusivamente la divulgación, modificación, eliminación o destrucción autorizada de la información almacenada en los medios de almacenamiento.

56	A.7.11	Utilidades de apoyo	Control Las instalaciones de procesamiento de la información deben estar protegidas contra los cortes de energía y otras interrupciones causadas por fallos en los servicios públicos de apoyo.	Si	Se adopta este control para proteger los activos usados en el procesamiento de información, frente a fallas de alimentación eléctrica o en las instalaciones de la CGN.
57	A.7.12	Seguridad del cableado	Control Los cables que transporten energía, datos o servicios de información de apoyo deben estar protegidos contra la interceptación, las interferencias o los daños.	Si	Se adopta este control para prevenir la pérdida, daño o compromiso de la información y otros activos relacionados, así como la interrupción de las operaciones de la CGN causada por fallos o interrupciones en los servicios públicos de apoyo, con el fin de salvaguardar la integridad de la información y garantizar la continuidad de las operaciones.
58	A.7.13	Mantenimiento de equipos	Control El equipo se debe mantener correctamente para asegurar la disponibilidad, integridad y confidencialidad de la información.	Si	Se adopta este control para asegurar que se realice el mantenimiento preventivo a los equipos con la finalidad de detectar posibles fallas que afecten su operatividad en la CGN.
59	A.7.14	Eliminación segura o reutilización de equipos	Control Los elementos de los equipos que contengan medios de almacenamiento se deben verificar para asegurarse de que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su disposición o reutilización.	Si	Se adopta este control para asegurar que los equipos no cuenten con información al momento de ser eliminados o reutilizados en la CGN.
	A.8	**Controles tecnológicos**			
60	A.8.1	Dispositivos de punto final de usuario	Control Se debe proteger la información almacenada, procesada o accesible a través de los dispositivos de punto final del usuario	Si	Se adopta este control para resguardar la información ante los riesgos derivados del uso de dispositivos terminales de usuario.
61	A.8.2	Derechos de acceso privilegiados	Control La asignación y el uso de los derechos de acceso privilegiado deben estar restringidos y gestionados.	Si	Se adopta este control para restringir y controlar la utilización y asignación de privilegios de acceso, de acuerdo al nivel que le corresponde dentro de la CGN.
62	A.8.3	Restricción de acceso a la información	Control El acceso a la información y a otros activos asociados se debe restringir de acuerdo con la política específica establecida sobre el control de acceso.	Si	Se adopta este control para garantizar solo el acceso autorizado y para evitar el acceso no autorizado a la información y otros activos asociados.

63	A.8.4	Acceso al código fuente	Control El acceso para leer o escribir sobre un código fuente, las herramientas de desarrollo, y las librerías de software se deben gestionar apropiadamente	Si	Se adopta este control para el desarrollo de aplicaciones y sistemas de información.
64	A.8.5	Autenticación segura	Control Se deben implementar tecnologías y procedimientos de autenticación seguros basados en restricciones de acceso a la información y en la política específica del tema sobre control de acceso.	Si	Se adopta este control para asegurar una autenticación segura para usuarios o entidades al otorgar acceso a sistemas, aplicaciones y servicios con el fin de proteger la información, prevenir accesos no autorizados, respaldar la gestión de identidades.
65	A.8.6	Gestión de capacidad	Control El uso de los recursos se debe monitorear y ajustar en función de las necesidades de capacidad actuales y previstas.	Si	Se adopta este control para gestionar y asegurar el desempeño requerido de las instalaciones de procesamiento de información, recursos humanos, oficinas y otras instalaciones y proyecciones futuras para asegurar su disponibilidad en la CGN.
66	A.8.7	Protección contra malware	Control La protección contra el malware se debe implementar y respaldar mediante la conciencia adecuada del usuario.	Si	Se adopta este control para asegurar la protección de la información y otros activos vinculados contra el malware, así como la aplicación de políticas de seguridad que fomenten prácticas seguras entre los usuarios.
67	A.8.8	Gestión de vulnerabilidades técnicas	Control Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a dichas vulnerabilidades y se deben adoptar las medidas apropiadas.	Si	Se adopta este control para prevenir la explotación de vulnerabilidades técnicas y evaluar el nivel de exposición de la infraestructura tecnológica de la CGN.
68	A.8.9	Gestión de la configuración	Control Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes se deben establecer, documentar, implementar, monitorear y revisar.	Si	Se adopta este control para asegurar el correcto funcionamiento del hardware, software, servicios y redes con la configuración de seguridad prescrita, así como prevenir alteraciones causadas por cambios no autorizados o incorrectos, garantizando el control de cambios autorizados y la aplicación de políticas que eviten ajustes no autorizados.

69	A.8.10	Eliminación de información	Control La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento se debe eliminar cuando ya no sea necesario	Si	Se adopta este control para prevenir la exposición innecesaria de información sensible y cumplir con los requisitos legales, estatutarios, reglamentarios, regulatorios y contractuales para la eliminación de información, así como la aplicación de procedimientos seguros para la eliminación y destrucción de datos cuando sea necesario.
70	A.8.11	Enmascaramiento de datos	Control El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre control de acceso y otras políticas relacionadas con temas específicos, y los requisitos comerciales, teniendo en cuenta la legislación aplicable	Si	Se adopta este control con el fin de proteger la información de identificación personal según la ley 1581 de 2012 de Protección de datos personales
71	A.8.12	Prevención de fuga de datos	Control Las medidas de prevención de fugas de datos se deben implementar a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.	Si	Se adopta este control para identificar y prevenir la divulgación y extracción no autorizada de información por parte de individuos o sistemas implementados, medidas de monitoreo y control, contribuyendo a mitigar riesgos y proteger la integridad y confidencialidad de la información almacenada, aplicando así un entorno seguro y resiliente.
72	A.8.13	Copia de seguridad de la información	Control Las copias de seguridad de la información, el software y los sistemas se deben mantener y probar periódicamente de conformidad con la política específica sobre copias de seguridad sobre temas específicos	Si	Se adopta este control para garantizar las copias de respaldo y su recuperación de desastres, incluyendo las pruebas periódicas respectivas
73	A.8.14	Redundancia de las instalaciones de procesamiento de información	Control Las instalaciones de procesamiento de la información se deben implantar con redundancia suficiente para cumplir los requisitos de disponibilidad	Si	Se adopta este control para asegurar el funcionamiento de las instalaciones de procesamiento de información y las funciones críticas de la CGN.

74	A.8.15	Registro	Control Los registros que guarden actividades, excepciones, fallas y otros eventos pertinentes se deben producir, almacenar, proteger y analizar	Si	Se adopta este control para registrar eventos, generar evidencia, detectar y prevenir fraudes o accesos no autorizados, identificar eventos de seguridad de la información facilitar la resolución y la toma de decisiones, promover la transparencia y la responsabilidad, mejorar la eficiencia operativa y fortalecer la seguridad de la información en CGN.
75	A.8.16	Actividades de supervisión	Control Se debe monitorear el comportamiento anómalo de las redes, los sistemas y las aplicaciones y se deben adoptar las medidas adecuadas para evaluar posibles incidentes de seguridad de la información.	Si	Se adopta este control para monitorear y garantizar la ejecución continua de actividades en las instalaciones de procesamiento de información.
76	A.8.17	Sincronización del reloj	Control Los relojes de los sistemas de procesamiento de información utilizados por la organización se deben sincronizar con las fuentes de tiempo aprobadas.	Si	Se adopta este control para facilitar la correlación y análisis de eventos vinculados a la seguridad, así como otros datos registrados, y respaldar las investigaciones relacionadas con incidentes de seguridad de la información permitiendo una comprensión más profunda de los eventos de seguridad, y posibilitarán la identificación y respuesta efectiva a posibles amenazas
77	A.8.18	Uso de programas de utilidad privilegiados	Control El uso de programas de utilidad que puedan ser capaces de anular los controles del sistema y de la aplicación debe restringirse y controlarse estrictamente.	Si	Se adopta este control para asegurar que el uso de programas de utilidad no cause daño al sistema y que los controles de aplicaciones para la seguridad de la información sean efectivos.
78	A.8.19	Instalación de software en sistemas operativos	Control Se deben implementar procedimientos y medidas para gestionar de forma segura la instalación de programas informáticos en los sistemas operativos	Si	Se adopta este control para asegurar la integridad de los sistemas operativos y prevenir la explotación de vulnerabilidades técnicas, incluyendo la aplicación puntual de parches y actualizaciones de seguridad, así como la configuración adecuada de los sistemas para minimizar las superficies de ataque.

79	A.8.20	Seguridad de redes	Control Las redes y los dispositivos de red deben estar asegurados, gestionados y controlados para proteger la información de los sistemas y las aplicaciones.	Si	Se adopta este control para resguardar la información en las redes y sus instalaciones de procesamiento de información de apoyo contra posibles compromisos a través de la red, protegiendo la integridad y confidencialidad de la información y fortaleciendo la resiliencia de las infraestructuras de red frente a amenazas cibernéticas.
80	A.8.21	Seguridad de los servicios de red	Control Se deben identificar, implementar y monitorear los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.	Si	Se adopta este control para proteger y garantizar la seguridad en el uso de los servicios de red de la CGN.
81	A.8.22	Segregación de redes	Control Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en las redes de la organización.	Si	Se adopta este control para segmentar las redes y servicios de información en base a su valor y clasificación de información almacenada en CGN.
82	A.8.23	Filtrado web	Control El acceso a sitios web externos se debe gestionar para reducir la exposición a contenido malicioso.	Si	Se adopta este control para garantizar la seguridad de la red, proteger contra amenazas cibernéticas, controlar contenido en CGN y prevenir el acceso a recursos web no autorizados.
83	A.8.24	Uso de criptografía	Control Se debe definir e implementar normas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.	Si	Se adopta este control para garantizar la confidencialidad, integridad, autenticidad y seguridad de la información de acuerdo con los requisitos del negocio y de seguridad de la información, considerando los requisitos legales, estatutarios, reglamentarios y contractuales relacionados a criptografía.
84	A.8.25	Ciclo de vida de desarrollo seguro	Control Se deben establecer e implementar normas para el desarrollo seguro de software y sistemas	Si	Se adopta este control para desarrollos o servicios de sistemas de información, requiriendo al proveedor de desarrollo el manejo de las buenas prácticas en desarrollo seguro.
85	A.8.26	Requisitos de seguridad de las aplicaciones	Control Los requisitos de seguridad de la información se deben identificar, especificar y aprobar al desarrollar o adquirir aplicaciones	Si	Se adopta este control para garantizar que las aplicaciones sean seguras desde el momento en que se desarrollan o adquieren hasta su implementación y operación en CGN.

86	A.8.27	Arquitectura de sistemas seguros y principios de ingeniería	Control Los principios para la ingeniería de sistemas seguros se deben establecer, documentar, mantener y implementar a cualquier actividad de desarrollo de sistemas de información	Si	Se adopta este control para asegurar que los sistemas de información se diseñen, implementen y operen de manera segura dentro del ciclo de vida del desarrollo.
87	A.8.28	Codificación segura	Control Los principios de codificación segura se deben implementar al desarrollo de programas informáticos	Si	Se adopta este control para asegurar que los sistemas de información se implementen mediante el desarrollo del manejo de las buenas prácticas en codificación segura.
88	A.8.29	Pruebas de seguridad en desarrollo y aceptación	Control Los procesos de ensayo de seguridad se deben definir y implementar en el ciclo de vida del desarrollo	Si	Se adopta este control para asegurar que las pruebas de seguridad se definan e implementen en el ciclo de vida del desarrollo
89	A.8.30	Desarrollo externalizado	Control La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados	Si	Se adopta este control en los casos de sistemas subcontratados mediante la revisión de sus actividades relacionadas con el desarrollo
90	A.8.31	Separación de entornos de desarrollo, prueba y producción	Control Los entornos de desarrollo, ensayo y producción deben estar separados y protegidos	Si	Se adopta este control aplicando Los entornos de desarrollo, pruebas y producción de manera separada y protegida
91	A.8.32	Gestión del cambio	Control Los cambios en las instalaciones de procesamiento de la información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios	Si	Se adopta este control para todos los cambios (modificaciones, ingresos o retiros) requeridos en los servicios tecnológicos de la CGN Security.
92	A.8.33	Información de la prueba	Control La información de las pruebas se debe seleccionar, proteger y gestionar adecuadamente	Si	Se aplicará a los requerimientos o contratos solicitados por los clientes.
93	A.8.34	Protección de los sistemas de información durante las pruebas de auditoría	Control Las pruebas de auditoría y otras actividades de aseguramiento que impliquen la evaluación de los sistemas operativos se deben planificar y acordar conjuntamente entre el probador y la dirección adecuada	Si	Se adopta este control para garantizar la integridad, la disponibilidad y la confidencialidad de los sistemas y datos durante el proceso de auditoría, al mismo tiempo que se cumple con los requisitos normativos, se minimizan los riesgos y se mejora la eficiencia y la confianza en los resultados de la auditoría.

Fuente: Propia

7. APROBACIÓN

Este documento ha sido revisado y aprobado por los integrantes del Equipo Operativo de apoyo al oficial de seguridad de la información el día 9 de junio de 2025.

8. OBSERVACIONES ADICIONALES

- Este documento será revisado al menos una vez al año o cuando haya cambios significativos en el SGSI o en los riesgos.

- Forma parte integral de la documentación del SGSI y está disponible para auditorías internas y externas.