UNIDAD ADMINISTRATIVA ESPECIAL CONTADURIA GENERAL DE LA NACIÓN

GRUPO INTERNO DE TRABAJO DE PLANEACIÓN

ESTRATEGIA DE SEGURIDAD DIGITAL

BOGOTA, DICEMBRE 2022

Contenido

ESTRATEGIA DE SEGURIDAD DIGITAL

1. INTRODUCCIÓN

La U.A.E Contaduría General de la Nación, desarrolla una gestión segura y provee un ambiente adecuado para la óptima operación de los activos de información y la plataforma tecnológica que soporta los procesos misionales, asegurando la confidencialidad, disponibilidad, e integridad de la información.

La CGN se alinea a la política de gobierno digital que impulsa el gobierno nacional a través del Ministerio de las Tecnologías de la Información y las Comunicaciones la cual propende por la transformación digital pública y busca fortalecer la relación Ciudadano – Estado, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública"; para lo cual, la entidad ha adelantado acciones orientadas a fortalecer los habilitadores transversales "Seguridad y Privacidad de la Información", "Arquitectura", "Cultura y apropiación" y "Servicios ciudadanos digitales" que corresponden a las capacidades para desarrollar las líneas de acción y las capacidades para el uso y aprovechamiento de las TICS en cumplimiento del objetivo de la Política de Seguridad Digital.

Específicamente en el habilitador transversal "Seguridad y Privacidad de la información" este componente se desarrolla, a través de lineamientos en materia de seguridad y privacidad de la información, así como la gestión de riesgos de seguridad digital, los cuales soportan las acciones establecidas por la entidad para proteger los activos de información a través del "Modelo de Seguridad y Privacidad de la Información (MSPI)" para lo cual la CGN al encontrarse certificada bajo la norma ISO/IEC 27001, confirma el compromiso de las directivas de la entidad con los temas de seguridad de la información. Para lo anterior, la CGN ha implementado el modelo sugerido por MinTIC desarrollando los lineamientos de la norma internacional; y da mantenimiento al ciclo de operación del mismo, por lo tanto, el desarrollo de esta estrategia se alinea con el Plan de Seguridad y Privacidad de la Información. La Estrategia establece específicamente las acciones y las métricas que permitan alcanzar el nivel de madurez deseado para garantizar la confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

El desarrollo de la Estrategia de Seguridad Digital 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.

Inicia con la definición de la Estrategia, continua con la ejecución y finaliza con el seguimiento y medición de los logros alcanzados.

3. REFERENCIA NORMATIVA

Ley Estatutaria 1266 del 31 de diciembre de 2008: Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales.
Ley 1273 del 5 de enero de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
CONPES 3701 DE 2011: Lineamientos de Política para Ciberseguridad y Ciberdefensa.
Ley Estatutaria 1581 De 2012: Protección de Datos Personales, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional. **Decreto 1377 De 2013:** Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012. Añade dos nuevos capítulos al Código Penal Colombiano:
Capitulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos;
Capitulo Segundo: De los atentados informáticos y otras infracciones. Como se puede ver en el primer capítulo, esta Ley está muy ligada a la ISO27000, lo cual coloca al País a la vanguardia en legislación de seguridad de la información, abriendo así la posibilidad de nuevas entradas con este tema.
Decreto 1074 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro

Nacional de Bases de Datos. Artículos 25 y 26.

Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Decreto 1083 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

CONPES 3854 DE 2016: Política Nacional de Seguridad Digital.

Decreto 1008 de 2018: Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"

CONPES 3975 DE 2019: Política Nacional para la Transformación Digital e Inteligencia Artificial.

Resolución 193 de 19 de junio de 2019: por el cual se crea el Sistema de Gestión y Desempeño de la Unidad Administrativa Especial (UAE) Contaduría General de la Nación (CGN) y se dictan otras disposiciones.

CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital.

Resolución 500 de 2021: Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

Decreto 338 de 2022: "Por el cual se adiciona el Titulo 21 a la parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.

Resolución 746 de 2022: Por el cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen los lineamientos adicionales a los establecidos en la Resolución 500 de 2021.

Resolución 767 de 2022: Por el cual se fortalece el Modelo imparten lineamientos generales de la Política de Gobierno Digital y otras disposiciones y en particular lo referente a las como Habilitador transversal de la Seguridad y Privacidad de la Información.

4. DEFINICIONES

Activos de información: Los activos de información son datos o información propietaria en medios electrónicos, impreso o entre otros medios, considerados sensibles o críticos para el cumplimiento de los objetivos de la CGN.

Amenaza: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.

Análisis de Riesgo: Proceso que se realiza para identificar las causas, las posibles amenazas, las consecuencias y así determinar el nivel riesgos puedan afectar los activos de información.

Base de datos personales: Conjunto organizado de datos personales que sea objeto de tratamiento (Ley 1581 de 2012, art.3).

CIGD – Sigla Comité Institucional de Gestión y Desempeño.

Confidencialidad: Es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona.

Control: Medida que modifica y mitiga el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Disponibilidad: Acceso a la información cuando se requiere, teniendo en cuenta la privacidad.

Gestión de Riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

GIT: Sigla Grupo Interno de Trabajo.

Incidente de seguridad de la información: Un incidente de seguridad de la Información está indicado por un único evento o una serie de eventos de Seguridad de la Información indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de la entidad y de amenazar la seguridad de la información.

Integridad: Es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (impacto). (ISO/IEC 27000).

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Seguridad digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

Vulnerabilidad: Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

5. MARCO CONTEXTUAL Y METODOLOGÍA

De acuerdo con los lineamientos de la Guía *G.ES.05 Diseño e implementación de una estrategia de seguridad de la Información de MinTIC*, el presente documento se genera a partir de los pasos definidos en la metodología y para lo cual se identifican los siguientes aspectos:
Estado actual de seguridad de la información en la institución.
Activos de información clasificados con base en sensibilidad y criticidad.
Meta establecida de seguridad digital.

6. ESTADO ACTUAL

Teniendo en cuenta que la CGN se encuentra certificada en la Norma Técnica Colombiana ISO/IEC 27001, y que ha adoptado e implementado el Modelo de Seguridad y Privacidad de la información, e identificado a través de la herramienta de autodiagnóstico (Análisis GAP) dispuesta por MinTIC, el estado actual de la Entidad respecto a la Seguridad y privacidad de la Información, la cual se gestiona y monitorea a través del ciclo PHVA; Actualmente la entidad se encuentra en un nivel de madurez **Administrado**, esto de acuerdo con los criterios que tiene la herramienta. Este nivel de madurez se determina a través de la implementación de los controles, los cuales se monitorean, se miden y se toman acciones permanentemente en determinados procesos que no están funcionando eficientemente o necesitan seguimiento.

Figura No. 1 Evaluación Efectividad de los controles Brecha Anexo A ISO 27001:2013
Fuente: Herramienta de autodiagnóstico vigencia 2022

7. OBJETIVOS DE LA ESTRATEGIA DE SEGURIDAD DIGITAL

Los siguientes objetivos de la Estrategia de Seguridad Digital de la CGN se alinean con los objetivos estratégicos institucionales No. 12. "*Preservar la confidencialidad, integridad y disponibilidad de la información de la CGN (Objetivo SGSI)"* y No.14. "*Disponer de la infraestructura tecnológica que asegure la sostenibilidad de los sistemas de información de la CGN".*

La gestión de riesgos en la CGN se realiza conforme a lo establecido en la Política de Administración del Riesgo, adoptada en la Resolución 501 de 2018, así mismo, se tiene en cuenta los lineamientos establecidos por MINTIC en la materia – Modelo de Riesgos de Seguridad Digital - Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (DAFP).

Se tienen definidos en la declaración de aplicabilidad y en la matriz de riesgos, los controles para proteger los activos de información y la infraestructura crítica para garantizar la seguridad de la información de la Entidad.

El estado de implementación del SGSI con que cuenta la entidad garantiza la seguridad de la información a través del establecimiento de políticas, procedimientos y controles para la protección de la información institucional.

Se tienen implementado indicadores que permiten medir y monitorear la protección de la información en cuanto a pérdida de disponibilidad, confidencialidad e integridad.

El sistema de gestión de Seguridad de la Información está integrado con el Modelo de Seguridad y Privacidad de la información y se articula y complementa con los otros sistemas de gestión. Los objetivos definidos son:

7.1. Objetivo General

Definir y desarrollar las acciones para alcanzar un estado de madurez deseado en materia de seguridad digital, respondiendo a la necesidad de preservar la confidencialidad, integridad y disponibilidad de los activos e infraestructura crítica con que cuenta la entidad, disminuyendo el nivel de los riesgos de dicha infraestructura.

7.2 Objetivos específicos

Establecer acciones para el aseguramiento de la infraestructura critica de la entidad y optimizar los niveles de protección de la información de la CGN.

Actualizar el inventario de la infraestructura crítica y realizar una adecuada gestión de riesgos de seguridad digital.

Monitorear y fortalecer los controles definidos para disminuir el nivel de riesgo asociado a los activos de información e infraestructura crítica.
Adoptar estrategias para fortalecer las capacidades de los usuarios internos y partes interesadas en materia de ciberseguridad.
Realizar ejercicios de simulación de incidentes de seguridad digital al interior de la CGN para garantizar los recursos necesarios ante la materialización de una amenaza.

8. ROLES Y RESPONSABILIDADES

En el Plan de Seguridad y Privacidad de la Información se encuentran definidos los roles, las responsabilidades y las funciones de todos los funcionarios y colaboradores que tienen acceso a la información de la Entidad.

9. ESTADO DEL NIVEL DE MADUREZ DESEADO

De acuerdo a las actividades planteadas en el Plan de Seguridad y Privacidad de la Información para la vigencia 2023, la meta de implementación del Modelo de Seguridad y Privacidad de la Información es alcanzar un estado de madurez en el nivel Optimizado, lo cual permitiría desarrollar iniciativas, definir controles y mejores prácticas para el fortalecimiento de la administración de los activos de información e infraestructura crítica de la entidad, todo esto basado en los resultados de mejora continua en materia de seguridad digital.
En este sentido,
La CGN ha definido los roles y responsabilidades de seguridad de la información.
Tiene una Política de Seguridad y políticas específicas en el Manual de seguridad de la Información actualizada y divulgada a través del sitio web y aceptada por los servidores públicos, colaboradores y partes interesadas.
La CGN posee mecanismos para proteger la infraestructura tecnológica y

el centro de procesamiento de datos que asegura la operación de los procesos, recursos tecnológicos, la red de datos y la infraestructura crítica garantizando la seguridad de la información.
Monitorea permanentemente los controles definidos y toma acciones para mejorar su desempeño.

10. DETERMINAR EL NIVEL DE RIESGO

La CGN ha determinado el apetito del riesgo relacionado con los riesgos de seguridad de la información como *aceptables* aquellos ubicados en el nivel de riesgo bajo (política de administración del riesgo, numeral 13).
El mapa de riesgos de Seguridad de la información y Seguridad Digital está planteado conforme a lo indicado en el Anexo A de la Norma Técnica Colombiana ISO/IEC 27001:2013, estableciendo al interior de la Entidad: políticas, lineamientos, procedimientos, formatos y controles para su tratamiento.
La metodología utilizada para el manejo de los Riesgos de Seguridad Digital es la dispuesta por el Departamento Administrativo de la Función Pública (DAFP) y la cual está declarada por la Política de Administración de Riesgos de la CGN.
Adicional a ello, la CGN administra los riesgos de Seguridad Digital teniendo en cuenta el *Modelo Nacional de gestión de riesgo de seguridad digital - Guía de orientación para la gestión de riesgo de seguridad digital en el gobierno nacional, territoriales y sector público.*

11. PLAN DE ACCIÓN

Para mantener y fortalecer la estrategia de Seguridad Digital, se debe realizar la identificación de los activos de tecnologías de operación y tecnologías de la información que posee la CGN, lo que permitiría redefinir y actualizar el inventario de infraestructura critica, la cual se lidera y se consolida de manera articulada con el Ministerio de Hacienda.
Para lo cual se define la siguiente hoja de ruta para su adecuado desarrollo:

Acción Estratégica	Meta	Actividades	Fecha de Inicio	Fecha de Finalización	Indicador	Resultado
Fortalecer las capacidades Institucionales en temas de Defensa y Seguridad Digital mediante la participación en redes interinstitucionales.	Implementar actividades de cooperación para intercambiar recursos administrativos, técnicos, operativos, tecnológicos y humanos con el fin de prevenir incidentes de seguridad digital.	1. Mesas de trabajo	15/02/2023	29/12/2023	No. De reuniones realizadas	Actas de reuniones
Actualizar el inventario de infraestructura crítica de la CGN.	Actualizar el inventario de infraestructura crítica en todos los procesos de la CGN.	1. Actualizar la infraestructura crítica y los servicios esenciales 2. Realizar la clasificación de la infraestructura crítica y los servicios esenciales inventariados	15/02/2023	31/05/2023	No. De activos de infraestructura crítica actualizados	Matriz de infraestructura crítica actualizada y aprobada

Realizar la gestión de riesgo de la infraestructura crítica y servicios esenciales de la CGN	Realizar el proceso de Identificación, Análisis y Evaluación de Riesgos de todos los activos de infraestructura crítica de la CGN	1. Realizar la identificación del riesgo y analizar las amenazas, las vulnerabilidades de los activos e infraestructura crítica. 2. Realizar la evaluación del riesgo, teniendo en cuenta el impacto y la probabilidad de ocurrencia. 3. Identificar y definir los controles para el tratamiento de riesgo. 4. Definir el plan de tratamiento de riesgos y aceptación del mismo.	1/06/2023	15/11/2023	No. de activos e infraestructura crítica evaluada y valorada.	Evaluación y tratamiento de riesgo.

Implementar y ejecutar un plan de apropiación y toma de conciencia de la información y seguridad digital	Implementar el plan de capacitación, sensibilización y toma de conciencia sobre temas de ciberseguridad	1. Realizar plan de capacitación y sensibilización 2. Diseñar y ejecutar las estrategias de sensibilización y capacitación. 3. Capacitar a los usuarios internos y partes interesadas sobre los boletines de CSIRT. 4. Realizar encuestas de uso y apropiación del plan.	01/02/2023	29/12/2023	No. de capacitaciones ejecutadas No. de personas sensibilizadas en temas de ciberseguridad Encuestas realizadas en temas de ciberseguridad	Plan de Sensibilización y toma de conciencia en temas relacionados con seguridad de la Información y Seguridad Digital

Fortalecer los mecanismos para desarrollar las capacidades de resiliencia ante incidentes cibernéticos	Realizar un (1) ejercicio de simulación de incidente de seguridad y un (1) ejercicio de ingeniería social, para la prevención ante ataques cibernéticos	1. Realizar ejercicio de simulación de incidentes de seguridad digital al interior de la CGN 2. Realizar ejercicio simulado de ingeniería social al personal de la CGN. 3. Identificar y documentar las lecciones aprendidas sobre los ejercicios de simulación realizados.	1/05/2023	29/12/2023	Ejercicio de simulación de incidentes de seguridad realizado Ejercicio de simulación de ingeniería social realizado	Plan de simulación de incidente e ingeniería social. Lecciones aprendidas.
Revisión y Actualización de la Estrategia de Seguridad Digital	Realizar la revisión, ajustes y actualización de la Estrategia de Seguridad Digital con la finalidad de dar cumplimiento a la Normatividad vigente.	Revisión y ajuste del documento dado cumplimiento a los lineamientos y guías de MinTIC.	15/02/2023	29/09/2023	Estrategia actualizada	Estrategia de Seguridad Digital Actualizada y aprobada

12. BIBLIOGRAFÍA

MinTic (2019), Guía G.ES.05 Diseño e implementación de una estrategia de seguridad de la Información. Versión 1.2

MinTic (2022), Manual de Gobierno Digital.

Gobierno de Colombia - Modelo Nacional de gestión de riesgo de seguridad digital - Guía de orientación para la gestión de riesgo de seguridad digital en el gobierno nacional, territoriales y sector público.

MinTic (2018), Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD)- ANEXO 4 Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas.

U.A.E Contaduría General de la Nación (2022), Política de Administración del Riesgo.

U.A.E Contaduría General de la Nación (2018), Resolución 5001 de 2018 - Política de Administración del Riesgo.

U.A.E Contaduría General de la Nación - Plan de Continuidad Negocio - Anexos.

MinTic (2019), G14 - Plan de Capacitación, Sensibilización Y Comunicación De Seguridad De La Información. Versión 1.2

CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
12-2021	V1	Elaboración de la Estrategia
15-12-2022	V2	Actualización documento

Elaboró: Ing. Oralia Franco
Revisó: Ing. Martha Zornosa Guerra
Aprobó: Ing. Martha Zornosa Guerra