UNIDAD ADMINISTRATIVA ESPECIAL
CONTADURIA GENERAL DE LA NACIÓN

GRUPO INTERNO DE TRABAJO DE PLANEACIÓN

ESTRATEGIA DE SEGURIDAD DIGITAL

BOGOTA, DICIEMBRE DE 2021

Dirección: Calle 26 # 69 -76 | Edificio Elemento
Torre 1 (Aire) - Pisos 3 y 15
Código Postal: 111071, Bogotá, Colombia
www.contaduria.gov.co | contactenos@contaduria.gov.co
PBX: +57 (601) 492 64 00

TABLA DE CONTENIDO

Dirección: Calle 26 # 69 -76 | Edificio Elemento
Torre 1 (Aire) - Pisos 3 y 15
Código Postal: 111071, Bogotá, Colombia
www.contaduria.gov.co | contactenos@contaduria.gov.co
PBX: +57 (601) 492 64 00

ESTRATEGIA DE SEGURIDAD DIGITAL

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 la Comunicaciones y que pretende *"Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital*"; para lo cual, la entidad ha adelantado acciones orientadas a fortalecer los habilitadores transversales "Seguridad de la información", "Arquitectura" y "Servicios ciudadanos digitales" que facilitan la implementación de TICs para el estado y TICs para la sociedad.

Específicamente en el habilitador transversal "Seguridad de la información" este componente se desarrolla, a través de lineamientos en materia de seguridad y privacidad de la información, así como de gestión de riesgos de seguridad digital, lo 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.

Dirección: Calle 26 # 69 -76 | Edificio Elemento
Torre 1 (Aire) - Pisos 3 y 15
Código Postal: 111071, Bogotá, Colombia
www.contaduria.gov.co | contactenos@contaduria.gov.co
PBX: +57 (601) 492 64 00

1. ALCANCE

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.

2. OBJETIVO

Definir estrategias para la seguridad digital en la CGN respondiendo a la necesidad de preservar la confidencialidad, integridad y disponibilidad de los activos de información. Y, además disminuyendo el nivel de riesgos asociado a los activos de información.

3. GLOSARIO

- **Activo de Información:** se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas...) que tenga valor para la organización.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
- **Controles:** Medida que permite reducir o mitigar un riesgo.
- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- **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
- **Integridad:** Propiedad de la información que busca preservar su exactitud y completitud.

- **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
- **Seguridad de la información**: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
- **Seguridad digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales**.**
- **Sistema de Gestión de Seguridad de la Información -SGSI:** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.

4. ROLES Y RESPONSABILIDADES

- Todo aquel que tenga acceso a la información de la CGN, es responsable de velar por la seguridad de la información a la que tiene acceso y de cumplir las políticas descritas en la Entidad.
- En el manual de seguridad de la información GTI-MAN01 y en la documentación (políticas, procedimientos, guías e instructivos) del SGSI se encuentran definidas las responsabilidades de seguridad de la información y seguridad digital para todos y cada uno de los funcionarios, contratistas y aquellos con acceso a información de la Entidad.

5. ANALISIS Y TRATAMIENTO DE RIESGOS

La gestión para los riesgos asociados a la seguridad digital de la Contaduría General de la Nación se realiza de acuerdo con la "Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital" - Versión 4 del Departamento Administrativo de la Función Pública (DAFP), y la "Guía de Gestión de Riesgos" del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

La CGN establece un plan de gestión de riesgos de seguridad digital en el cual se identifican las amenazas, las vulnerabilidades, el impacto y el nivel de riesgo asociados a los activos de información sin importar el nivel de criticidad que tienen para la entidad.

Los lideres de proceso con el acompañamiento del Oficial de Seguridad de la Información y/o quien haga sus veces, son los encargados de gestionar los riesgos de seguridad de la información-seguridad digital dentro de su área de responsabilidad.

La Gestión de riesgos de seguridad de la información-seguridad digital es aplicada sobre los procesos descritos dentro del alcance del Sistema de Gestión de Seguridad de la Información - SGSI.

La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información-seguridad digital que son pertinentes para las cuatro fases del proceso del Modelo de Seguridad y privacidad de la información-MSPI.

ETAPAS DEL MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDADDE LA INFORMACION
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

Etapas de la Gestión del Riesgo a lo Largo del MSPI-Fuente Guía de gestión de riesgos MINTIC

5.1 ETAPA PLANEAR

5.1.1 Contexto interno y externo

La Entidad ha realizado el análisis DOFA para establecer los factores internos y externos del contexto estratégico y ha determinado las necesidades y expectativas de sus partes interesadas para dar cumplimiento a las normas de calidad y a los riesgos de seguridad digital.

5.1.2 Valoración de los riesgos

Para la valoración de los riesgos se tienen en cuenta los siguientes aspectos:

Dirección: Calle 26 # 69 -76 | Edificio Elemento
Torre 1 (Aire) - Pisos 3 y 15
Código Postal: 111071, Bogotá, Colombia
www.contaduria.gov.co | contactenos@contaduria.gov.co
PBX: +57 (601) 492 64 00

- Una vez identificados los activos de información, se procede a la identificación de los riesgos en cada uno de los procesos dentro del alcance del SGSI.
- Se enumera el riesgo, para dar un orden consecutivo de los riesgos de seguridad de la información-seguridad digital.
- Se identifica el riesgo: con el fin de determinar que podría suceder que cause una pérdida potencial, de la confidencialidad, integridad y disponibilidad de la información. Se realiza una descripción clara de los riesgos de seguridad de la información-seguridad digital.
- Se determinan los criterios de impacto que son las consecuencias que puede ocasionar a la entidad la materialización del riesgo.
- Se determinan los criterios de probabilidad de ocurrencia de cada uno de los riesgos, probabilidad de la posibilidad de ocurrencia del riesgo y su calificación.
- Se valora el riesgo inherente, el riesgo al cual se está expuesto sin ningún tipo de control sobre el activo.
- Se realiza la evaluación de los controles establecidos para mitigar los riesgos: La evaluación de los controles se realiza cuando se ha establecido el riesgo inherente en cada uno de los procesos. Es importante anotar que la CGN cuenta con una declaración de aplicabilidad en la cual se contemplan los controles correspondientes al Anexo A de la norma NTC: ISO/IEC 27001.
- Una vez evaluados los controles se determina el riesgo residual sobre el cual se realizará el plan de tratamiento.

5.1.3 Planificación del tratamiento y aceptación del riesgo:

Una vez se obtienen los resultados del análisis de los riesgos de seguridad de la información-seguridad digital, se gestionan los riesgos residuales, se proponen acciones de mejora a través de planes de acción o de tratamiento, con la finalidad que la información siempre conserve las características de confidencialidad, integridad y disponibilidad de esta.

Los criterios definidos por la Contaduría General de la Nación para el tratamiento de los riesgos son:

Evitar el riesgo: tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.

Dirección: Calle 26 # 69 -76 | Edificio Elemento
Torre 1 (Aire) - Pisos 3 y 15
Código Postal: 111071, Bogotá, Colombia
www.contaduria.gov.co | contactenos@contaduria.gov.co
PBX: +57 (601) 492 64 00

Reducir el riesgo: El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad.

Aceptar el riesgo: Si el nivel de riesgo cumple con los criterios de aceptación de riesgo, no es necesario poner controles y el riesgo puede ser aceptado. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo. No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.

Compartir el riesgo: implementar mecanismos para transferir los riesgos con terceros, esto normalmente equivale a la suscripción de pólizas de seguro, acuerdos con proveedores y/o fabricantes, acuerdos con empresas del mismo sector para hacer uso de centros de instalaciones en caso de emergencias.

5.2 ETAPA IMPLEMENTAR

5.2.1 Implementación del plan de tratamiento del riesgo:

La Contaduría General de la Nación establece su plan de tratamiento de riesgos para los riesgos en nivel alto y extremo. Dicho plan requiere una definición clara de las actividades a desarrollar y en cada una debe contar con el registro de ítems definidos en el Mapa y Plan de Tratamiento de Riesgos de Seguridad de la Información-Seguridad Digital.

5.3 ETAPA GESTIONAR Y MEJORA CONTINUA

5.3.1 Seguimiento y monitoreo:

La Contaduría General de la Nación realiza el seguimiento y monitoreo a las medidas y/o controles planteados y evalúa la eficiencia en su implementación. Para esto, es necesario analizar el riesgo residual por probabilidad y por impacto.

Este monitoreo y seguimiento se realiza teniendo en cuenta los siguientes aspectos:

- Identificación de nuevos activos de información, incluidos en el alcance del SGSI.
- Modificaciones a los valores de los activos de información.
- Nuevas causantes de riesgos (amenazas y vulnerabilidades).
- Incidentes de seguridad digital.

El monitoreo y seguimiento debe estar a cargo de los responsables de los procesos y el responsable del Sistema de Gestión de Seguridad de la Información-SGSI.

Las actividades definidas para la realización del monitoreo y seguimiento son:

Dirección: Calle 26 # 69 -76 | Edificio Elemento
Torre 1 (Aire) - Pisos 3 y 15
Código Postal: 111071, Bogotá, Colombia
www.contaduria.gov.co | contactenos@contaduria.gov.co
PBX: +57 (601) 492 64 00

- Auditorías internas y externas al SGSI.
- Mesas de riesgos realizadas como mínimo 2 veces al año.
- Anualmente en reunión del informe de revisión por la Dirección.

6. ESTRATEGIAS SEGURIDAD DIGITAL VIGENCIA 2022

Actividad	Descripción	Entregable	Responsable
Actualización del panorama de riesgos de seguridad digital	Acompañar los procesos misionales en la identificación, valoración, evaluación y formulación de planes de tratamiento de riesgos de seguridad digital mínimo 2 veces en el año **Nota**: Es importante mencionar que la matriz de riesgos de seguridad es tecnológica, por tal razón los planes de tratamiento o acciones para mitigar la materialización de los riesgos dependen de las actividades que se realizan en los procesos del alcance del SGSI y estos son los responsables de las acciones y controles que deben implementar.	Plan de tratamiento de riesgos de seguridad Digital	Gestión TICS Planeación Integral Procesos Misionales
Seguimiento a la implementación de planes de tratamiento de riesgos	Realizar el seguimiento a la implementación de los planes de tratamiento de riesgos de seguridad digital que adopten los	Informe de seguimiento a la implementación de planes de tratamiento de riesgos	Planeación Integral

Dirección: Calle 26 # 69 -76 | Edificio Elemento
Torre 1 (Aire) - Pisos 3 y 15
Código Postal: 111071, Bogotá, Colombia
www.contaduria.gov.co | contactenos@contaduria.gov.co
PBX: +57 (601) 492 64 00

	procesos misionales y Gestión TICS		
Sensibilización y divulgación	Elaborar contenidos de sensibilización y divulgación de los componentes del sistema de gestión de seguridad de la información y apoyar su publicación en la intranet Institucional	Evidencias de sensibilizaciones realizadas.	Planeación Integral

Proyectó:(Llady Lorena Alvarez Cortés)
Revisó: (Henry Ramírez Montes)

Dirección: Calle 26 # 69 -76 | Edificio Elemento
Torre 1 (Aire) - Pisos 3 y 15
Código Postal: 111071, Bogotá, Colombia
www.contaduria.gov.co | contactenos@contaduria.gov.co
PBX: +57 (601) 492 64 00

Dirección: Calle 26 # 69 -76 | Edificio Elemento
Torre 1 (Aire) - Pisos 3 y 15
Código Postal: 111071, Bogotá, Colombia
www.contaduria.gov.co | contactenos@contaduria.gov.co
PBX: +57 (601) 492 64 00