RESOLUCIÓN NÚM. IN-CGR-RES-2025-0002

QUE ESTABLECE EL COMITÉ DE CIBERSEGUIRIDAD DE LA INFORMACIÓN EN LA CONTRALORÍA GENERAL DE LA REPÚBLICA

CONSIDERANDO PRIMERO: que la Constitución de la República Dominicana, en su artículo 247, establece que: "La Contraloría General de la República es el órgano del Poder Ejecutivo rector del control interno, ejerce la fiscalización interna y la evaluación del debido recaudo, manejo, uso e inversión de los recursos públicos y autoriza las órdenes de pago, previa comprobación del cumplimiento de los trámites legales y administrativos, de las instituciones bajo su ámbito, de conformidad con la ley";

CONSIDERANDO SEGUNDO: que la Contraloría General de la República tiene potestad reglamentaria, conforme al artículo 18, numeral 17 de la Ley núm. 10-07, el cual establece que es competencia del Contralor General de la República "dictar, en el marco de la presente ley y su reglamento de aplicación, el reglamento interno de la institución y las demás normas técnicas y administrativas que considere necesarias para el desarrollo de las atribuciones y funciones de la Contraloría General de la República";

VISTA: la Constitución de la República Dominicana de fecha 27 de octubre de dos mil veinticuatro (2024).

VISTA: la Ley núm. 200-04 General de Libre Acceso a la Información Pública, de fecha 28 de julio de dos mil cuatro (2004).

VISTA: la Ley núm. 10-07, que el Sistema Nacional de Control Interno y la Contraloría General de la República, de fecha 4 de enero de dos mil siete (2007).

VISTA: la Ley núm. 41-08 de Función Pública y crea la Secretaría de Administración Pública (Ministerio de Administración Pública).

VISTA: la Ley núm. 1-12, sobre la Estrategia Nacional de Desarrollo de la República Dominicana hasta el 2030, de fecha 25 de enero de dos mil doce (2012).

VISTA: la Ley núm. 247-12 Orgánica de la Administración Pública. G .0. núm.10691, de fecha 14 de agosto de 2012.

VISTA: la Ley núm. 107-13 sobre los Derechos de las personas en sus relaciones de la Administración Pública y de Procedimiento Administrativo.

En virtud de las atribuciones que le confiere a la Contraloría General de la República y la Ley núm. 10-07 que instituye el Sistema Nacional de Control Interno (Sinaci), se emite la siguiente:

RESOLUCIÓN

CAPÍTULO I
DEL OBJETO, ALCANCE, REPRESENTANTES Y RESPONSABILIDADES DEL COMITÉ DE CIBERSEGURIDAD

Artículo 1.- Objetivo del Comité de Ciberseguridad. El Comité de Ciberseguridad de la **CONTRALORÍA GENERAL DE LA REPÚBLICA DOMINICANA** tiene como objetivo principal coordinar, supervisar y gestionar la implementación de estrategias de seguridad cibernética, así como la respuesta a incidentes de seguridad que puedan afectar la integridad, confidencialidad y disponibilidad de los activos de información de la institución.

Artículo 2.- Alcance del Comité de Ciberseguridad. El Comité de Ciberseguridad de la **CONTRALORÍA GENERAL DE LA REPÚBLICA DOMINICANA** abarca la planificación, implementación y supervisión de todas las políticas y procedimientos de seguridad de la información, asegurando el cumplimiento con las normativas NORTIC A7 e ISO 27001. Su alcance incluye la gestión integral de incidentes, desde la prevención hasta la respuesta, así como la evaluación continua de riesgos y la aplicación de controles para proteger los activos tecnológicos de la institución. Además, el comité es responsable de fomentar una cultura de ciberseguridad mediante programas de capacitación, realizar auditorías periódicas, mantener una comunicación constante con la alta dirección para informar sobre el estado de la ciberseguridad y coordinar estrategias de mejora continua.

Artículo 3.- Crear el Comité de Ciberseguridad de la **CONTRALORÍA GENERAL DE LA REPÚBLICA DOMINICANA**, cuya misión será coordinar y supervisar todas las actividades de ciberseguridad para proteger los activos de información y asegurar la integridad de la infraestructura digital de la institución.

Artículo 4.- El Comité de Ciberseguridad estará conformado por representantes de las siguientes áreas:

- Contralor General de la República Dominicana.
- Director(a) de Tecnología de la Información (TI).
- Director(a) Planificación y Desarrollo.
- Director(a) Dirección de Recursos Humanos.
- Director(a) Dirección Administrativa y Financiera.
- Director(a) Dirección Jurídica.
- Director(a) Escuela Nacional del Control Interno.
- Encargado(a) de la División de Seguridad y Monitoreo.
- Encargado(a) de la División de Operaciones TI.
- Encargado(a) División de Desarrollo e Implementación de Sistema.
- Encargado(a) División de Administración Servicios TI.

Artículo 5.- Las responsabilidades del Comité de Ciberseguridad incluyen:

- Desarrollar y actualizar los planes de ciberseguridad para la **CONTRALORÍA GENERAL DE LA REPÚBLICA DOMINICANA**, asegurando el cumplimiento de la Norma NORTIC A7.
- Identificar y evaluar riesgos potenciales que puedan comprometer la ciberseguridad de la **CONTRALORÍA GENERAL DE LA REPÚBLICA DOMINICANA**, implementando medidas de mitigación.
- Realizar simulacros, ejercicios y capacitaciones que proporcionen respuestas ante incidentes de seguridad cibernética para validar la efectividad de los planes de contingencia.
- Asegurar el cumplimiento de las políticas de ciberseguridad en la institución, y documentar todas las actividades realizadas para evaluar el cumplimiento de las normativas.

Artículo 6.- El Comité de Ciberseguridad se reunirá trimestralmente y de manera extraordinaria en caso de incidentes críticos que pongan en riesgo la seguridad de los activos de información de la **CONTRALORÍA GENERAL DE LA REPÚBLICA DOMINICANA**.

Artículo 7.- La presidencia del Comité recaerá sobre el contralor general de la República Dominicana, quien liderará las reuniones, aprobará las medidas de ciberseguridad y coordinará la implementación de estas en toda la **CONTRALORÍA GENERAL DE LA REPÚBLICA DOMINICANA**.

Artículo 8.- Las decisiones se tomarán por consenso; en caso de no lograr consenso, se decidirá por mayoría simple. Por consiguiente, si se produjera un empate en la votación, se aplicará el voto de calidad del Presidente, es decir, que ese voto valdrá por dos (2).

Artículo 9.- Los miembros del Comité de Ciberseguridad deberán:

- Participar activamente en las reuniones y en la implementación de decisiones de ciberseguridad.
- Contribuir a la evaluación de riesgos y gestionar la mitigación de vulnerabilidades.
- Informar oportunamente de cualquier incidente de seguridad que comprometa los activos de información de la **CONTRALORÍA GENERAL DE LA REPÚBLICA DOMINICANA**.

Artículo 10.- Responsabilidades y Funciones en el Comité de Ciberseguridad

1.1 Presidente

a) Dirigir las reuniones del comité, estableciendo la agenda estratégica y asegurando la alineación de las actividades con los objetivos de seguridad de la **CONTRALORÍA GENERAL DE LA REPÚBLICA DOMINICANA**.
b) Evaluar y aprobar políticas, procedimientos, planes de acción o medidas de seguridad, asegurando el cumplimiento de los estándares de seguridad en la **CONTRALORÍA GENERAL DE LA REPÚBLICA DOMINICANA**.
c) Actuar como el principal portavoz del comité, frente a las decisiones y recomendaciones clave del comité.
d) Garantizar que el comité mantenga el cumplimiento con todas las normativas internas y externas de ciberseguridad, incluyendo la actualización de políticas, conforme a los cambios regulatorios.
e) Revisar periódicamente el desempeño del comité y de sus miembros, promoviendo la mejora continua en la gestión de la seguridad de la información.

f) Promover la importancia de la ciberseguridad en la organización, apoyando iniciativas de capacitación y concientización para todos los empleados.
g) Supervisar la respuesta a incidentes de alta criticidad.
h) Convocar reuniones de emergencia con el comité de ser necesario.

1.2 Secretario(a)

a) Preparar la agenda, coordinar las convocatorias y registrar las minutas de todas las reuniones del comité.
b) Facilitar la comunicación entre los miembros del comité y otros departamentos, asegurando el flujo eficiente de información relacionada con temas de ciberseguridad.
c) Mantener un archivo organizado de actas, informes y otros documentos relacionados con las actividades del comité, garantizando la confidencialidad y accesibilidad de la información.
d) Gestionar los recursos necesarios para la realización de las actividades del comité, como equipo de presentación, acceso a información y espacio físico para reuniones.
e) Asistir en la redacción de informes periódicos y comunicados internos sobre las actividades y decisiones del comité.
f) Asegurar que las reuniones se realicen conforme al calendario establecido y coordinar ajustes según las necesidades del comité.

1.3 Miembros

a) Participar activamente en todas las reuniones y discusiones del comité.
b) Aportar conocimientos específicos de su área para la toma de decisiones informadas sobre ciberseguridad.
c) Colaborar en la implementación de políticas, procedimientos y controles de seguridad.
d) Revisar planes, estrategias y políticas de seguridad propuestos.
e) Identificar y reportar riesgos y vulnerabilidades relacionados con la seguridad de la información según objetividad técnica.
f) Apoyar en la creación y revisión de informes de auditoría, evaluaciones de riesgos y análisis de incidentes.
g) Fomentar la cultura de seguridad de la información en la institución, promoviendo las mejores prácticas.
h) Involucrarse en las comprobaciones periódicas y auditorías de seguridad para garantizar la efectividad de los controles implementados y sugerir mejoras.
i) Asegurar que las políticas de seguridad de la información se implementen y respeten adecuadamente.
j) Fomentar una cultura de seguridad de la información, asegurando que todos los departamentos estén conscientes y comprometidos con la protección de los activos de información.
k) Participar en la elaboración y actualización de planes de respuesta a incidentes, colaborando en la contención y mitigación de riesgos.
l) Mantenerse informado sobre las últimas amenazas y tendencias en ciberseguridad para asesorar en la adopción de medidas preventivas efectivas.
m) Colaborar en la creación y verificación de informes de seguridad, evaluaciones de riesgos y resultados de auditorías.
n) Involucrarse en auditorías y comprobaciones de seguridad periódicas para asegurar que los controles sean efectivos y estén alineados con las mejores prácticas.

CAPÍTULO II
DISPOSICIONES GENERALES

Artículo 11.- Será responsabilidad del Comité de Ciberseguridad de la **CONTRALORÍA GENERAL DE LA REPÚBLICA DOMINICANA** dar seguimiento a la implementación y cumplimiento de los siguientes mecanismos de control:

1. **Autenticación multifactor:** exigir a todos los usuarios de la Contraloría General de la República la autenticación a través de múltiples factores para acceder a los sistemas de información.

2. **Gestionar los privilegios:** procurar el cumplimiento del sistema de gestión de privilegios que limite el acceso a los recursos de la red y los sistemas de información a los usuarios estrictamente necesarios.

3. **Auditoría de accesos:** solicitar auditoría periódica de todos los accesos a los sistemas de información en operación en la Contraloría General de la República, a fin de identificar actividades sospechosas.

4. **Cifrado:** deberán, en los casos necesarios, implementar el cifrado de datos en reposo y en tránsito para proteger la información confidencial.
5. **Respaldos regulares:** mantener y realizar copias de seguridad periódica de los datos y almacenarlas en un lugar seguro fuera de la institución.

6. **Análisis de riesgos:** realizar análisis de riesgos periódicos para identificar las amenazas y vulnerabilidades a las que está expuesta la organización.

7. **Gestión de parches:** mantener actualizados todos los sistemas operativos, aplicaciones y software con los parches de seguridad más recientes.

8. **Escaneo de vulnerabilidades:** realizar escaneos de vulnerabilidades de forma regular para identificar y corregir las debilidades en los sistemas de información.

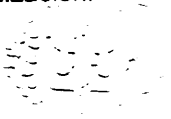
9. **Capacitación:** implementar un programa de capacitación en seguridad de la información para todos los empleados.

10. **Simulacros:** realizar simulacros de ataques cibernéticos para evaluar la preparación de la organización y mejorar los procedimientos de respuesta a incidentes.

11. **Plan de Recuperación ante Desastres:** desarrollar un plan de recuperación ante desastres que detalle los procedimientos a seguir en caso de un incidente de seguridad que afecte la disponibilidad de los sistemas de información.

Otros Controles

12. **Gestión de dispositivos móviles:** establecer políticas y controles para la gestión de dispositivos móviles que accedan a los sistemas de información de la organización.



13. **Seguridad en la nube:** si se utilizan servicios en la nube, implementar controles de seguridad adecuados para proteger los datos almacenados en la nube.

Artículo 12.- El Comité de Ciberseguridad deberá asegurar que los controles implementados en la Contraloría General de la República cumplan con los requisitos establecidos en el Decreto 685-22 y regulaciones aplicables, además de realizar evaluaciones periódicas de los controles de seguridad para garantizar su eficacia y colaborar con el Centro Nacional de Ciberseguridad (CNCS), a fin de obtener asesoramiento y apoyo en materia de ciberseguridad.

CAPÍTULO III
DISPOSICIONES FINALES

Primera: la presente resolución se implementa a partir de la fecha de su emisión, en cumplimiento de la Norma NORTIC A7, Ley núm. 10-07, Ley núm. 41-08, ISO 27001:2022 y otras normativas relacionadas, con el tema de la ciberseguridad.

Segundo: se instruye a todas las áreas estructurales de la **CONTRALORÍA GENERAL DE LA REPÚBLICA DOMINICANA** a colaborar con el Comité de Ciberseguridad para proteger los activos de información de la institución.

Tercero: el **contralor general de la República Dominicana** podrá realizar ajustes a esta resolución, en función de las necesidades emergentes que afecten la ciberseguridad institucional.

DADA en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, Capital de la República Dominicana, a los dos días (2) del mes de enero del año dos mil veinticinco (2025), año 180 de la Independencia y 161 de la Restauración.

Félix Antonio Santana García
Contralor General de la República Dominicana

CONTRALORÍA GENERAL DE LA REPÚBLICA
DESPACHO DEL CONTRALOR
SANTO DOMINGO, R.D.

FASG
jc