SENADO
REPÚBLICA DOMINICANA
Dirección Técnica de Revisión Legislativa

Santo Domingo de Guzmán, D.N
20 de Julio de 2021.

DETEREL 388 /2021.

A la : Comisión Permanente de Transporte y Telecomunicaciones.

Vía : Licda. Rosemary Cedeño Nieves
Coordinadora de Comisiones Permanentes.

CC : Lic. José Carrasco Estévez.
Secretaria General Legislativa Interina.

De : Welnel D. Féliz F.
Director Departamento Técnico de Revisión Legislativa

Asunto : Opinión sobre el proyecto de Ley sobre Gestión de la Ciberseguridad en la República Dominicana

Ref. : Oficio No. 000006962 de fecha, 29 de abril de 2021
Expediente 00636-2021-PLO-SE

En atención a su comunicación de referencia, en la que nos solicita realizar el correspondiente estudio y remitir la opinión sobre el proyecto de ley indicado en el asunto. Después de analizar dicho proyecto, tenemos a bien expresarle lo siguiente:

Contenido

El proyecto de ley busca regular la prevención, gestión y respuestas a las amenazas e incidentes de ciberseguridad y otros aspectos relativos a la seguridad cibernética de las infraestructuras críticas en República Dominicana

Este proyecto de ley fue presentado por la Señora Faride Virginia Raful Soriano, Senadora de la República por el Distrito Nacional en fecha, 27 de mayo de 2021.

Facultad Legislativa Congresual:

La facultad legislativa congresual para legislar sobre esta materia está fundamentada en el Art. 93, numeral uno, literal q de la Constitución de la República que, enuncia lo siguiente: *"Legislar acerca de toda materia que no sea de la competencia de otro Poder del Estado y que no sea contraria a la Constitución."*

Procedimiento de Aprobación:

Por su naturaleza, el presente proyecto de ley para los fines de su aprobación, se rige por lo establecido en el artículo 113 de la Constitución de la República, que establece: ***"Las Leyes ordinarias son aquellas que por su naturaleza requieren para su aprobación la mayoría absoluta de los votos de los presentes de cada cámara".***

Desmonte Legal

El proyecto de ley se fundamenta en las siguientes disposiciones legales:

VISTA: La Constitución de la República Dominicana del 13 junio de 2015;

VISTA: La Ley Núm. 107-13, del 6 de agosto del año 2013, de Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo;

VISTA: La Ley Núm. 247-12, del 9 de agosto del año 2012, Orgánica de Administración Pública;

VISTA: La Ley No. 1-12, del 25 de enero del año 2012, sobre la Estrategia Nacional de Desarrollo 2030.

VISTA: La Ley Núm. 41-08, del 16 de enero de 2008, de Función Pública;

VISTA: La Ley Núm. 53-07, del 23 de abril del año 2007, sobre Crímenes y Delitos de Alta Tecnología;

VISTA: La Ley Núm. 13-07, del 5 de febrero del año 2017, que crea el Tribunal Contencioso Tributario y Administrativo;

VISTA: La Ley Núm. 200-04, del 28 de julio de 2004, General de Libre Acceso a la Información Pública;

VISTO: El Decreto Núm. 230-18, del 19 de junio del año 2018, que establece la Estrategia Nacional de Ciberseguridad 2018-2021 y que crea el Centro Nacional de Ciberseguridad;

VISTO: El Decreto No.134-14, del 9 de abril del año 2014, que establece el Reglamento de la Estrategia Nacional de Desarrollo 2030;

VISTA: La Resolución de la Asamblea General de las Naciones Unidas A/68/98 del 24 de junio de 2013 sobre el Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional

VISTA: La Resolución de la Asamblea General de las Naciones Unidas A/70/174 del 22 de julio de 2015 sobre el Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional;

VISTO: El Llamado de París para la Confianza y la Seguridad en el Ciberespacio;

VISTO: El Reporte Final de la Comisión Global sobre la Estabilidad en el Ciberespacio (GCCS) de noviembre de 2019.

En cuanto a los antecedentes legales que sustentan esta iniciativa legislativa, hemos observado que no están ordenando según los criterios establecidos por las normas de técnica legislativa, los cuales sugieren que los indicados antecedentes sean agrupados por categorías, siguiendo un orden o ascendente, por fechas y un orden jerárquico respetando la supremacía de la Constitución, seguido de los instrumentos internacionales ratificados por el Estado dominicano y continuando con los decretos y disposiciones de menor rango, en ese sentido, proponemos adecuar el contenido de los vistos y colocarlos en el texto de la iniciativa en estudio, de la siguiente forma:

Vista: La Constitución de la República;

Vista: La Resolución de la Asamblea General de las Naciones Unidas A/68/98, del 24 de junio de 2013, Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional;

Vista: La Resolución de la Asamblea General de las Naciones Unidas A/70/174, del 22 de julio de 2015, 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal;

Visto: El Llamamiento de París, del 12 de noviembre de 2018, para la confianza y la seguridad en el ciberespacio;

Visto: El Reporte Final de noviembre de 2019, de la Comisión Global sobre la Estabilidad en el Ciberespacio (GCCS).

Vista: La Ley núm. 200-04, del 28 de julio de 2004, Ley General de Libre Acceso a la Información Pública;

Vista: La Ley núm. 53-07, del 10 de abril del año 2007, sobre Crímenes y Delitos de Alta Tecnología;

Vista: La Ley núm. 41-08, del 16 de enero de 2008, de Función Pública y crea la Secretaria de Estado de Administración Pública;

Vista: La Ley núm. 1-12, del 25 de enero del año 2012, sobre la Estrategia Nacional de Desarrollo 2030;

Vista: La Ley núm. 247-12, del 9 de agosto del año 2012, Orgánica de Administración Pública;

Vista: La Ley núm. 107-13, del 6 de agosto del año 2013, de Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo;

Vista: La Ley núm. 13-07, del 5 de febrero del año 2017, que crea el Tribunal Contencioso Tributario y Administrativo;

Visto: El Decreto núm. 230-18, del 19 de junio de 2018, que establece y regula la Estrategia Nacional de Ciberseguridad 2018-2021;

Vista: El Decreto núm. 134-14, del 9 de abril del año 2014, que dicta el Reglamento de Aplicación de la Ley Orgánica No. 1-12, que establece la Estrategia Nacional de Desarrollo de la República Dominicana 2030;

Análisis Constitucional, Legal y de la Técnica Legislativa

Después de analizar el proyecto de ley en los aspectos legal, constitucional y de la técnica legislativa, **ENTENDEMOS** oportuno hacer los siguientes señalamientos:

1.- El artículo 5 del proyecto de ley establece lo siguiente: **Artículo 5.- Creación del Centro Nacional de Ciberseguridad.** Se crea el Centro Nacional de Ciberseguridad, como continuación de la actual dependencia homónima del Ministerio de la Presidencia, pasando a ser un ente derecho público con personalidad jurídica propia, autonomía funcional, presupuestaria, administrativa, técnica y patrimonio propio, adscrito al Ministerio de la Presidencia.

1.1.- Este artículo busca crear el Centro Nacional de Ciberseguridad como órgano de naturaleza autónoma perteneciente al Ministerio de la presidencia. Al respecto, debemos señalar lo siguiente:

1.- El artículo 27 de la Ley núm. 247-12, del 9 de agosto de 2012, Ley Orgánica de Administración Pública que señala la organización interna de los ministerios en orden jerárquico, establece lo siguiente:

> Artículo 27.-Organización interna de los ministerios. La organización interna de los ministerios será establecida mediante reglamento de él o la Presidente de la República, a propuesta del Ministerio de Administración Púbica de conformidad con los principios rectores y reglas básicas de organización y funcionamiento de la Administración Publica establecidos en la presente Ley Orgánica. La elaboración de la propuesta de organización deberá ser realizada por el Ministerio de Administración Pública en coordinación con el ministerio correspondiente. Los órganos de los ministerios con competencia sustantiva se relacionarán jerárquicamente en una estructura descendente de acuerdo a los siguientes niveles: viceministerios, direcciones generales, direcciones, departamentos, divisiones y secciones.

1.2.- Como se observa, mediante la ley orgánica organizadora de la administración pública se estableció la nomenclatura y la ordenación jerárquica de los órganos centralizados. Sin embargo, dicha ley no dispuso ninguna identificación destinada a los organismos autónomos. No obstante, el Estado, en los casos de creación de los indicados organismos, ha procedido a utilizar la denominación de "instituto", "corporaciones" o simplemente crear direcciones con carácter autónomo.

1.3.- En la especie, la denominación de centro es poco no es utilizada en el Estado y la última recayó en la creación del Centro de Importaciones e Inversiones, pero los demás órganos estatales de los últimos veinte años no han asumido tal denominación.

1.4.- Al respecto, esta dirección entiende que lo correcto es que se identifique como instituto, no como centro.

2.- El artículo 8 de este proyecto de ley establece: Artículo 8.- Carácter vinculante de las decisiones del Centro Nacional de Ciberseguridad (CNSC). Las decisiones que en materia de ciberseguridad sean tomadas por el Centro Nacional de Ciberseguridad, tendrán carácter obligatorio para todos los entes y órganos de la Administración Pública, así como las entidades privadas, especialmente aquellas infraestructuras críticas que proveen servicios esenciales.

2.1- Del contenido de este artículo inferimos que el Centro Nacional de Ciberseguridad trazará lineamientos en materia de ciberseguridad a todos los entes y órganos del Estado,

y por entes y órganos del Estado se refiera a ministerios, que son órganos de naturaleza constitucional y los denominados "órganos extrapoder" creados por la Constitución, revestidos de autonomía reforzada y con atribuciones especiales superiores a los demás órganos del gobierno central. En tal virtud, al indicar que las decisiones del Centro Nacional de Ciberseguridad tendrán carácter obligatorio, deja a los indicados ministerios y órganos extrapoder en una posición de subordinación y por ende jerárquicamente inferior al CNSC, generando una distorsión en las estructuras orgánicas de nuestro sistema Jurídico y en violación al principio de jerarquía establecido en la Constitución de la República y en la ley 247-12.

2.2.- En adición a lo indicado precedentemente, cabe precisar que la Administración se encuentra impedida de establecer decisiones que generen cumplimiento hacia los referidos entes y órganos constitucionales. A partir de la entrada en vigencia de la Constitución de 2010, el legislador delimitó la aplicabilidad de las disposiciones legales externas al régimen normativo propio de los órganos constitucionales, con la finalidad de preservar la autonomía que les ha conferido la Constitución, es preciso señalar que las decisiones de un órgano del Estado dominicano dependiente de un ministerio y de naturaleza jerárquicamente inferior a los órganos constitucionales, no pueden ser vinculantes y de carácter obligatorio para todos los entes y órganos de la administración pública, pues esto violentaría el criterio de separación de poderes y el sistema de frenos y contrapesos diseñados por la Carta Magna.

2.3- El criterio de separación de poderes se encuentra reforzado por nuestro Tribunal Constitucional en su sentencia núm. TC-01-15 que define y concreta lo que son los "Órganos Constitucionales Autónomos" u "Órganos Extrapoder", estableciendo lo siguiente: *(11.5..."Preciso es señalar que los órganos extrapoder son creados directamente por la Constitución para actualizar y perfeccionar el principio de la separación de los poderes, los cuales surgen de la necesidad de separar determinadas funciones públicas de los procesos normales de gobierno. En ese sentido: a. Constituyen órganos fundamentales del Estado, pues están situados en el vértice de la organización política, en posición de relativa paridad e independencia respecto de los poderes públicos tradicionales; b. escapan a toda línea jerárquica y a los controles de vigilancia y tutela jurídica de la autoridad rectora de la Administración Pública; c. reciben directamente de la Constitución el estatus y competencias esenciales que definen su posición institucional en la estructura del Estado...).;* Por lo antes explicado, consideramos que debe de adecuarse la redacción del artículo 8 con la finalidad de que se delimite a quienes compete la obligatoriedad de las decisiones en materias de ciberseguridad emanadas del CNSC, pudiendo indicar que tales decisiones serán vinculantes y de carácter obligatorio para entes y órganos que integran la Administración Pública centralizada, descentralizada funcional y territorialmente, organismos autónomos, empresas públicas y corporaciones de derecho público.

3.- El artículo 10 del proyecto indica: **Artículo 10.- De la estructura organizativa del Centro Nacional de Ciberseguridad.** El Centro Nacional de Ciberseguridad contará con las

siguientes dependencias básicas, las cuales estarán supervisadas por la Dirección Ejecutiva:

1. Una dirección denominada Equipo de Coordinación de Estrategias de Ciberseguridad, que tendrá por objeto la elaboración, desarrollo, actualización y evaluación de la Estrategia Nacional de Ciberseguridad, la formulación de políticas derivadas de dicha estrategia y la definición de las iniciativas, programas y proyectos que lleven a la realización exitosa de ésta;

2. Una dirección denominada Equipo Nacional de Respuestas a Incidentes Cibernéticos de la República Dominicana (CSIRT RD), que tiene a su cargo la prevención, detección y gestión de incidentes generados en los sistemas de información relevantes del Estado e infraestructuras críticas nacionales;

3. Una dirección administrativa y financiera; y,

4. Una dirección jurídica.

Párrafo.- El Centro Nacional de Ciberseguridad podrá crear otros equipos y dependencias según entienda necesario para el cumplimiento de esta ley.

3.1- El contenido del artículo anterior dispone la creación de un Equipo de Coordinación de Estrategias de Ciberseguridad y un Equipo Nacional de Respuestas a Incidentes Cibernéticos de la República Dominicana (CSIRT RD) como estructuras organizativas del Centro Nacional de Ciberseguridad, en tal sentido, debemos indicar que este tipo de estructuras internas no deben ser creadas por ley, la organización interna de estos órganos dependientes debe ser desarrollada vía reglamento, por lo que recomendamos referir su desarrollo al reglamento de la ley.

3.2.- Asimismo, las denominaciones internas a que se contrae el órgano no es cónsono con las estructuras. En efecto, si bien la Ley 247-12 no dispone expresamente la organización interna de los órganos extrapoder, hay que observar un mínimo de coherencia en el sistema jurídico, en el sentido de que debe mantener criterios propios de la ley, como lo son direcciones, departamentos, divisiones. Por tanto, la creación de "equipos" como órganos constituye una nomenclatura confusa, que no encuentra sustento en el sistema jurídico.

3.3.- La administración pública, aun con sus características, debe procurar la armonización de sus instituciones, empleando las nomenclaturas que le son propias y así poseer órganos estructuralmente homogéneos que eviten confusiones. Esta dirección entiende que estos denominados equipos deben ser considerados direcciones: "Dirección de coordinación de estrategia" y demás elementos.

4.- El artículo 11 establece: **Artículo 11.- Composición del Consejo Directivo del Centro Nacional de Ciberseguridad.** El Consejo Directivo estará compuesto por las siguientes entidades:

1) Ministerio de la Presidencia, el cual lo preside.
2) Dirección Ejecutiva, representada por su Director Ejecutivo, quien ostentará la calidad de secretario, máximo órgano administrativo y miembro de pleno derecho del Consejo, con voz, pero sin voto.
3) Ministerio de Defensa.
4) Ministerio de Interior y Policía.
5) Procuraduría General de la República.
6) Policía Nacional.
7) Departamento Nacional de Investigaciones.
8) Instituto Dominicano de las Telecomunicaciones.
9) Oficina Presidencial de Tecnologías de la Información y Comunicación.
10) El Ministerio de Relaciones Exteriores.
11) La Administración Monetaria y Financiera.

Párrafo I.- Los miembros del Consejo solo podrán hacerse representar en las reuniones por un funcionario de jerarquía inmediatamente inferior.

Párrafo II.- El Consejo Directivo tendrá la facultad, cuando el caso lo amerite, de solicitar la participación de otros representantes del Estado, tales como: el Poder Legislativo, el Poder Judicial, así como a representantes de la academia, operadores de infraestructuras críticas, del sector privado y la ciudadanía en general.

4.1- En cuanto a la integración del Consejo Directivo del Centro Nacional de Ciberseguridad, hemos observado que incluye a la Oficina Presidencial de Tecnología de la Información y Comunicación, por lo que cabe precisar, en primer lugar, que mediante Decreto núm. 54-21, del 2 de febrero de 2021, este organismo pasa a denominarse "Oficina Gubernamental de las Tecnologías de la Información y Comunicación (OGTIC)" como una dependencia del Ministerio de Administración Pública; en segundo lugar, consideramos que esta dependencia, como tal, no debe integrar el Consejo Directivo por tratarse de una estructura inferior frente a los demás miembros del Consejo, pues si bien es cierto que no existe impedimento legal que de forma expresa lo prohíba, no resulta recomendable que un órgano de características deliberativas para la toma de decisiones sobre una materia este integrado por organismos inferiores en comparación con los demás integrantes, por lo que sugerimos que sea el Ministerio de Administración Pública y no la OPTIC al que se señale como integrante del Consejo.

5.- El artículo 15 del proyecto expresa: **Artículo 15.- Impedimentos para la Dirección Ejecutiva.** No podrán ejercer la función de la Dirección Ejecutiva, las siguientes personas:

1. Los miembros del Congreso Nacional;
2. Los miembros activos del Poder Judicial;

3. Los que desempeñen cargos o empleos remunerados en cualesquiera de los organismos de Estado o de las municipalidades, ya sea por elección popular o mediante nombramiento, salvo los cargos de carácter docente;
4. Las personas que estuvieren *sub judice*, o cumpliendo condena o que hayan sido condenadas a penas aflictivas o infamantes;
5. Aquellas que por cualquier razón sean legalmente incapaces.

5.1- En cuanto al contenido del numeral 3, consideramos que no es necesario su desarrollo, pues lo establecido en este numeral está consagrado en el artículo 144 de la Constitución, el cual indica: ***Artículo 144.- Régimen de compensación.*** *Ningún funcionario o empleado del Estado puede desempeñar, de forma simultánea, más de un cargo remunerado, salvo la docencia. La ley establecerá las modalidades de compensación de las y los funcionarios y empleados del Estado, de acuerdo con los criterios de mérito y características de la prestación del servicio";* de igual forma, el artículo 151 de la Constitución establece la incompatibilidad laboral de los miembros del Poder Judicial al indicar: ***"Articulo 151.- Independencia del Poder Judicial…1)*** *La ley establecerá el régimen de responsabilidad y rendición de cuentas de jueces y funcionarios del Poder Judicial. El servicio en el Poder Judicial es incompatible con cualquier otra función pública o privada, excepto la docente. Sus integrantes no podrán optar por ningún cargo electivo público, ni participar en actividad político partidista*", contenido del numeral 2 del artículo 15 de esta propuesta.

6.- El artículo 16 de este proyecto de ley establece: **Artículo 16.- Designación.** La Dirección Ejecutiva será elegida por medio de un decreto del Poder Ejecutivo en base a una propuesta de tres candidatos presentada por los demás miembros del Consejo Directivo del Centro Nacional de Ciberseguridad.

Párrafo. - El mandato del Director Ejecutivo durará un período de cuatro años y no podrá ser elegido para nuevos períodos sucesivos.

6.1- En párrafo del artículo indica que el Director Ejecutivo del Consejo Directivo del Centro Nacional de Ciberseguridad durará un periodo de cuatro años, en ese sentido, consideramos que si lo que se quiere es que la gestión del Director Ejecutivo concluya con el periodo constitucional, debemos recordar que se trata de un funcionario de libre remoción y nombramiento, lo que quiere decir que así como el presidente tiene la facultad de nombrarlo también tiene la facultad de desvincularlo del cargo, por lo que entendemos que no se le debe imponer, mediante ley, el periodo de 4 años al Presidente de la República en caso de que este entienda que debe desvincular al funcionario público de su cargo antes de que concluya el indicado periodo.. Ahora bien, en caso de que el legislador decida dejar el periodo de gestión del Director Ejecutivo, lo que debiera indicar la ley es que el mandato del Director Ejecutivo durará un periodo de cuatro años contados a partir del inicio del periodo constitucional.

7.- Los artículos 19 y 20 del proyecto de ley que indican: **Articulo 19**.- **Atribuciones del**

Equipo de Coordinación de Estrategias de Ciberseguridad (ECEC). El Equipo de Coordinación de Estrategias de Ciberseguridad (ECEC) tendrá las siguientes atribuciones:

1. Definir políticas, establecer directrices y elaborar propuestas de estrategias y planes de acción para el desarrollo de la Estrategia Nacional de Ciberseguridad, a fin de que las entidades a las que correspondan su ejecución puedan gestionar los proyectos conforme a tales directrices;
2. Elaborar y mantener un catálogo de las actividades que sobre ciberseguridad desarrollen las instituciones involucradas;
3. Coordinar con los entes y órganos del Estado, en los ámbitos de sus respectivas competencias, la implementación y el cumplimiento de los objetivos y prioridades establecidos en la Estrategia Nacional de Ciberseguridad;
4. Sensibilizar a los distintos segmentos de la sociedad sobre la importancia de la ciberseguridad como la herramienta fundamental para asegurar los servicios que ofrecen a través de sus sistemas de información;
5. Evaluar las ejecutorias en el marco de la Estrategia Nacional de Ciberseguridad y reportar anualmente al Director Ejecutivo;
6. Apoyar, propiciar y liderar la creación de redes de cooperación entre los instituciones públicas, organizaciones académicas y entidades privadas para el impulso de la Estrategia Nacional de Ciberseguridad;
7. Contribuir a la difusión y promoción para la creación de una cultura nacional de ciberseguridad;
8. Contribuir a la adopción de una posición país unificada a través de la coordinación e integración de las iniciativas de los diferentes sectores de la sociedad vinculadas con la ciberseguridad;
9. Cualquier otra atribución que le sea encomendada por la Dirección Ejecutiva.

Articulo 20.- Atribuciones del Equipo de Respuestas a Incidentes Cibernéticos (CSIRT-RD). El Equipo de Respuestas a Incidentes Cibernéticos (CSIRT-RD) tendrá los siguientes cometidos:

1. Asistir en la respuesta a incidentes de ciberseguridad de los operadores de infraestructuras críticas
2. Coordinar con los responsables de la seguridad de la información de los operadores de infraestructuras críticas para la prevención, detección, manejo y recopilación de información sobre incidentes de ciberseguridad;
3. Asesorar y difundir información para incrementar los niveles de ciberseguridad,
4. Desarrollar herramientas, técnicas de protección y defensa de los operadores de infraestructuras críticas;
5. Alertar ante amenazas y vulnerabilidades de ciberseguridad en las infraestructuras críticas; críticas;
6. Realizar las tareas preventivas que correspondan, para garantizar la ciberseguridad de las infraestructuras críticas;
7. Realizar análisis forenses de los incidentes de ciberseguridad reportados que no constituyan un crimen o delito;
8. Centralizar los reportes y llevar un registro de toda la información sobre incidentes de ciberseguridad ocurridos en las infraestructuras críticas;

9. Fomentar el desarrollo de capacidades y buenas prácticas, así como la creación de Equipos Sectoriales de Respuestas a Incidentes;
10. Coordinar y asesorar los Equipos Sectoriales de Respuestas a Incidentes y entidades, tanto del nivel público como privado, y de la sociedad civil para responder ante incidentes de ciberseguridad;
11. Establecer y mantener un vínculo fluido y una relación colaborativa con otros organismos nacionales e internacionales de similar naturaleza;
12. Fomentar y coordinar la creación de laboratorios orientados a la investigación en temas de ciberseguridad; y
13. Cualquier otra función que le sea encomendada por la Dirección Ejecutiva.

Párrafo.-El personal del Equipo Nacional de Respuestas a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD) está autorizado para recibir y acceder a toda la información y los documentos necesarios para realizar sus funciones.

7.1.- Tal como explicamos precedentemente en el punto 3 de este informe, tanto el **Equipo de Coordinación de Estrategias de Ciberseguridad (ECEC)** como el **Equipo de Respuestas a Incidentes Cibernéticos (CSIRT-RD)** son estructuras organizativas de carácter interno cuyo desarrollo compete al reglamento de aplicación de la ley y no a la ley misma, por tanto, sugerimos remitir al reglamento el desarrollo de las atribuciones contenidas en los artículos 19 y 20.

8.- Los artículos 54 y 57 de la iniciativa de ley establecen: **Artículo 54.- Facultad sancionadora.** El Centro Nacional de Ciberseguridad, como órgano encargado de velar por el cumplimiento de la presente ley es el responsable por ejercer el régimen sancionador conforme se describe en el presente capítulo.

Artículo 57.- De las sanciones. A quienes incurran en las faltas administrativas en esta ley, el Centro Nacional de Ciberseguridad, sin perjuicio de las sanciones civiles y penales, serán sancionadas con una multa equivalente a un monto entre los veinte (20) y doscientos (200) salarios mínimos del sector público, observando el principio de proporcionalidad de las sanciones.

8.1.- El contenido de ambos artículos indican que el Centro Nacional de Ciberseguridad será el órgano responsable de ejercer el régimen sancionador y, por tanto, encargado de imponer las sanciones a la violación de las infracciones administrativas establecidas en la norma, ahora bien, a partir de la potestad sancionadora que el legislador pretende atribuir al CNSC debemos establecer algunas consideraciones.

8.2- La potestad sancionadora de los órganos administrativos y su capacidad exclusiva está definida en las leyes. En efecto, la ley 107-13 en su artículo 35 indica claramente que "**Su ejercicio corresponde exclusivamente a los órganos administrativos que la tengan legalmente atribuida"**, de allí que la atribución concedida previamente a un órgano del Estado limita el accionar de otro órgano estatal sobre tales atribuciones.

8.3- Siguiendo el criterio exclusivo sancionador, el legislador se ha cuidado de otorgar atribuciones administrativas exclusivas en su potestad sancionadora. Por ejemplo, A partir de lo establecido en la ley 41-08 de Función Pública, las sanciones administrativas por incumplimientos de sus funciones institucionales son impuestas por el mismo órgano en el cual el empleado infractor ejerce su función, bajo infracciones y sanciones previamente identificadas en la ley, debidamente proporcionales y correlativas, las cuales son identificadas por el órgano competente para su imposición.

8.4- Las atribuciones sancionadoras administrativas atribuidas al Centro Nacional de Ciberseguridad adquieren mayor dimensión cuando se trata de poderes del Estado o en órganos constitucionales extrapoder. En efecto, si el Centro Nacional de Ciberseguridad, en razón de su intervención poseyera la potestad sancionadora sobre empleados de estos poderes y órganos constitucionales, se violentaría claramente la separación de poderes del Estado, el cual abordamos y explicamos en el punto 2 de este informe.

8.5- En tal virtud, dada la exclusividad en la imposición de las sanciones administrativas, recomendamos que la labor del CNSC se limite a identificar violaciones e inobservancias legislativas, comunicando al órgano el resultado de la investigación, sin que imponga sanciones, sino que es cada órgano de la administración pública competente quien debe actuar para imponer la sanción debida por la violación a la ley.

9.- El artículo 55 del proyecto indica qué se considera faltas administrativas y establece:

Artículo 55.- Faltas administrativas. Se considerarán faltas administrativas las siguientes:

1. No cumplir con una comunicación de entrega de información requerida por el Centro Nacional de Ciberseguridad;
2. No cumplir con una notificación de cambios sustanciales en una infraestructura crítica;
3. No cumplir con designar un Punto de Contacto Único para una infraestructura crítica;
4. No cumplir con notificar un cambio de operador de una infraestructura crítica;
5. No cumplir con notificar los incidentes de ciberseguridad al Centro Nacional de Ciberseguridad;
6. No cumplir con notificar los incidentes de ciberseguridad a las personas posiblemente afectadas;
7. No cumplir con establecer mecanismos técnicos y procedimentales con el fin de detectar amenazas e incidentes de ciberseguridad;
8. No cumplir con enviar al Centro Nacional de Ciberseguridad un informe que incluya información sobre las causas de un incidente de ciberseguridad, el tiempo dedicado a su resolución, las medidas aplicadas y el impacto del mismo;
9. No cumplir con llevar a cabo auditorías o la evaluación de riesgo sobre su cumplimiento con esta ley;
10. No remitir la auditoría o la evaluación del riesgo de ciberseguridad al Centro Nacional de Ciberseguridad en los plazos establecidos;
11. No llevar a cabo las auditorías o la evaluación de riesgo de manera satisfactoria;

12. Realizar un cambio sustancial a una infraestructura crítica y no llevar a cabo la auditoría o evaluación de riesgo;
13. Obstruir o impedir que se lleve a cabo una auditoría o evaluación de riesgo;
14. No participar en un ejercicio de ciberseguridad requerido por el Centro Nacional de Ciberseguridad;
15. No proporcionar información, registros o documentos requeridos por el Centro Nacional de Ciberseguridad para responder a un incidente de ciberseguridad;
16. No cumplir con una orden emitida por el Centro Nacional de Ciberseguridad con la finalidad de prevenir, detectar o contrarrestar cualquier amenaza o incidente de ciberseguridad;
17. Obstruir al Centro Nacional de Ciberseguridad o a quien este designe para hacer cumplir cualquier medida emitida a fin de identificar, detectar o contrarrestar cualquier amenaza de ciberseguridad;
18. No cumplir con una orden de prohibición de utilizar un sistema de información o cualquiera de sus partes en caso de que el Centro Nacional de Ciberseguridad los haya notificado;
19. No cumplir con las disposiciones de los reglamentos dictados por el Centro Nacional de Ciberseguridad.

9.1- En efecto, el artículo anterior lista una serie de infracciones administrativas, a la vez que el articulo 57 del proyecto establece una única sanción de veinte (20) a doscientos (200) salarios mínimos del sector público para las indicadas faltas administrativas, por lo que podemos considerar todas las faltas de igual gravedad.

9.2.- Al respecto, es necesario señalar que en el contenido de esta norma no existen criterios objetivos que permitan afirmar que a un delito determinado le corresponde, como sanción proporcionada, determinada clase y cantidad de pena, en ese mismo orden, debemos señalar que en las construcciones de tipo penal o administrativo, las infracciones deben clasificarse por orden ascendente, desde leves hasta graves o muy graves. Esta afirmación, la fundamentamos en lo establecido por el Tribunal constitucional en su sentencia TC/0365/17, del 11 de julio de 2017, donde estableció que el legislador debe fijar "… una escala de penas que ordena los castigos en función de su gravedad, escala que a su vez servirá de elemento de comparación para analizar la proporcionalidad de una sanción o pena en particular".

9.3- Es así que, observar la coherencia punitiva permite un ordenamiento jurídico lógico y adecuado, sin sanciones cuantitativas desproporcionadas que induzcan a la desigualdad en la persecución del delito o la falta, es por eso que, para evitar ambigüedades en la consignación de las penalidades se debe tratar de establecer las sanciones lo más proporcional posible a la infracción estipulada, estableciendo un régimen sancionatorio con niveles de gravedad para las faltas y su debida sanción de manera proporcional, por lo que sugerimos calificar cada falta dentro de su gravedad y sancionarlas de manera congruente.

10.- El artículo 59 expresa: **Articulo 59.- Recurso de reconsideración.** Quienes sean sancionados por la comisión de las faltas administrativas contenidas en esta ley podrán ejercer un recurso de reconsideración con las formalidades y plazos establecidos en la Ley Núm. 107-13, sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo, por ante el mismo órgano que dictó la decisión. El recurso de reconsideración será ante el Consejo Directivo del Centro Nacional de Ciberseguridad.

10.1 – Este artículo manda a que el recurso administrativo en reconsideración sea llevado a cabo por ante el Consejo Directivo del Centro Nacional de Ciberseguridad, en ese sentido, tal como expusimos en el punto 8 de este informe, el ejercicio de la potestad sancionadora corresponde exclusivamente a los órganos administrativos que la tengan legalmente atribuida, por tanto, el recurso en reconsideración deberá ser por ante el órgano administrativo correspondiente que impuso la sanción.

11.- En cuanto al artículo 61 el mismo establece lo siguiente: **Artículo 61.- Sanciones al desacato durante un estado de alarma cibernética.** Toda persona que violente o vulnere las directrices o instrucciones emanadas por el Centro Nacional de Ciberseguridad (CNCS) durante un estado de alarma cibernética, atentando así contra los intereses fundamentales y seguridad de la nación, será sancionada de la siguiente forma:

1. El desacato de una persona debido a su negligencia que no haya tenido como consecuencia perjuicios, con multa equivalente entre cien (50) a quinientos (500) y/o prisión de entre tres (3) meses y un (1) año, considerando las razones de negligencia o imprudencia que determinaron la inobservancia.

2. El desacato de una persona en que se verifique la materialización de algún perjuicio será castigado con las penas que van desde las destinadas al acceso ilicitico a aquellas reservadas para los crímenes y delitos contra la nación cometidos mediante un sistema informático, electrónico, telemático o de telecomunicaciones contemplados en la legislación penal especializada en materia ciberdelincuencia, considerando la intención y la gravedad del perjuicio causado.

11.1.- En relación a las faltas establecidas en los numerales 1 y 2 del artículo anterior, las cuales citamos a continuación: "…el desacato de una persona debido a su negligencia que no haya tenido como consecuencia perjuicios" y "…el desacato de una persona en que se verifique la materialización de algún perjuicio", consideramos que no están planteadas de manera clara, ya que su redacción pudiera prestarse a múltiples interpretaciones pues se utilizan términos ambiguos e imprecisos, convirtiendo los mandatos en disposiciones que prohíjan la inseguridad jurídica y la violación de derechos humanos, en la medida en que los órganos administrativos y de justicia suelen recurrir a la analogía para aplicarlas, de allí que las personas pueden ser sujetos de acusaciones o procedimientos sobre la base de

infracciones o sanciones que correspondan a otro tipo de delitos o acusaciones, violando, además de los derechos fundamentales de las personas, el principio de legalidad. En ese orden la Corte Constitucional de Colombia en Sentencia T-391/07, del 22 de mayo de 2007, indico:

> *"…el nivel de precisión con el cual se han de formular las leyes correspondientes debe ser lo suficientemente específico y claro como para permitir que los individuos regulen su conducta de conformidad con ellas…".*

11.2. Por tanto, recomendamos establecer de manera directa y concreta las faltas a que refieren los contenidos antes indicados.

12.- El artículo 62 de esta iniciativa legislativa indica: **Articulo 62.- Disposición derogatoria.** Se derogan por sustitución los artículos 11 al 24 del Decreto Núm. 230-18 que establece la Estrategia Nacional de Ciberseguridad 2018-2021 y que crea el Centro Nacional de Ciberseguridad. La parte restante del Decreto estará vigente hasta que el Poder Ejecutivo establezca mediante decreto el reglamento de aplicación de la presente ley.

12.1 El contenido de este artículo busca derogar varios artículos del Decreto Núm. 230-18, a la vez que establece la vigencia de los artículos restantes del Decreto. En ese sentido, es importante recordar que la pieza legislativa en estudio es de rango superior al decreto, por lo que siendo ambos instrumentos legales de naturaleza distinta y jerarquía distintos, no es posible que uno modifique al otro, pues las modificaciones deben producirse mediante instrumentos de igual naturaleza. Las leyes deben ser modificadas por leyes y los decretos por decretos, garantizando así el principio del paralelismo de las formas, el cual establece que una norma jurídica tiene que ser dictada por un órgano siguiendo un determinado procedimiento y únicamente puede ser modificada o derogada por ese mismo órgano y con el mismo procedimiento.

Finalmente, después de lo analizado y señalado, **SOMOS DE OPINION**, que la comisión encargada del conocimiento del proyecto de ley se avoque a su estudio, observando su pertinencia y tomando en cuenta las observaciones antes señaladas.

Atentamente,

Welnel D. Feliz.
Director.