Bogotá D.C., 23 de octubre de 2023

Honorables Representantes

CIRO ANTONIO RODRIGUEZ PINZON
CRISTOBAL CAICEDO ANGULO
DANIEL CARVALHO MEJIA
DIEGO FERNANDO CAICEDO
LINA MARIA GARRIDO MARTIN
DOLCEY OSCAR TORRES ROMERO
HAIVER RINCON GUTIERREZ
PEDRO BARACUTAO GARCIA
JAIME RAUL SALAMANCA
YULIETH ANDREA SANCHEZ

Comisión Sexta
CONGRESO DE LA REPUBLICA
La Ciudad

Asunto: **Comentarios respecto a la Ponencia para Primer Debate del Proyecto de Ley 023 de 2023 Cámara "Por la cual se crea la Agencia Nacional de Seguridad Digital y Asuntos espaciales"**

Honorables Representantes,

Comienzo por extenderles nuestros más cordiales saludos de parte de la Cámara Colombiana de Informática y Telecomunicaciones – CCIT, organización gremial que agrupa a las más importantes empresas del sector de las Tecnologías de la Información y las Comunicaciones de Colombia. En ese sentido, hemos venido trabajando en el país por más de 30 años contribuyendo activamente desde el Sector TIC a la eliminación de barreras para la evolución tecnológica, promoviendo el cierre de la brecha digital, la democratización y la masificación de las TIC, así como el acceso de todos los ciudadanos a la sociedad y economía del conocimiento.

En esta ocasión nos dirigimos a Usted, con el fin de respetuosamente presentar nuestros al Ponencia para Primer Debate del Proyecto de Ley 023 de 2023 Cámara "*Por la cual se crea la Agencia Nacional de Seguridad Digital y Asuntos espaciales"*. En ese sentido, presentamos las siguientes observaciones.

1. Comentarios generales

1.1. Comentarios respecto al contexto y objeto de la Agencia

El objeto del Proyecto de Ley menciona que se establecerá una institucionalidad. Al respecto, llamamos la atención que como está formulado, el alcance del Proyecto de Ley no establece de manera general la institucionalidad para la seguridad digital, sino una nueva entidad que hará parte de la institucionalidad existente, y que liderará la política en esta materia. Al respecto, la institucionalidad y gobernanza de la seguridad digital han sido previamente definidos en el Decreto 338 de 2022.

De igual manera, es importante tener en cuenta que junto con anterior al CONPES 3995 de 2020, ya se han aprobado otros documentos CONPES sobre seguridad digital/ciberseguridad, o que

tratan temas relacionados, que son relevantes para entender la evolución de la política y de la normatividad en la materia: Documento CONPES 3701 de 2011, (Ciberseguridad y Ciberdefensa), Documento CONPES 3854 de 2016 (Seguridad Digital) y Documento CONPES 3975 de 2019 (Transformación Digital).

De otro lado, la única finalidad de la Agencia no debería ser sancionar a aquellas empresas que no presenten los reportes de información. Al contrario, consideramos que la aproximación para crear una agencia de ciberseguridad debería ser diferente, en un marco colaborativo entre en sector público y el privado, cuyo objetivo sea el fortalecimiento de herramientas de ciberseguridad enfocadas a la prevención, detección y respuesta a incidentes de ciberseguridad. En esa nota, consideramos que se debe promover la participación de las empresas en plataformas sectoriales para el intercambio y análisis de información, así como para la medida del riesgo sectorial y la propuesta de acciones que lo mitiguen.

Por lo tanto, es importante reconocer que la creación de una nueva entidad encargada de liderar la política en materia de seguridad digital es un paso significativo. Sin embargo, se debe garantizar una coordinación efectiva con la institucionalidad existente y los documentos CONPES previamente aprobados para evitar duplicaciones y asegurar una implementación eficiente de las políticas de seguridad digital.

1.2. Comentarios respecto a los reportes de información y la confidencialidad de la información compartida a la agencia

Sin embargo, el Proyecto de Ley se enfoca en crear unos reportes de información y un régimen sancionatorio, sin realizar un análisis sobre la finalidad de entrega de información sensible para las operaciones de las empresas desde el punto de vista de competencia, datos personales e información, sin especificar cual es el beneficio de entregar esta información o para que será utilizada la misma. Así las cosas, es de la mayor importancia que se garantice la adecuada protección y confidencialidad de la información recolectada por la Agencia.

En la memoria justificativa adjunta al Proyecto de Ley, se mencionan ciberataques tanto en entidades públicas como privadas, sin embargo, al adentrarse en la lectura del proyecto, el mismo se convierte en un listado de obligaciones para las empresas del sector TIC y una delegación de funciones en diferentes entidades, comités y ministerios, inclusive actividades de vigilancia y control, dejando de lado las obligaciones del sector público.

Así pues, es iimportante considerar el equilibrio entre la recolección de información sensible y la confidencialidad, integridad, y disponibilidad de dicha información. El Proyecto de Ley debe definir claramente los beneficios y propósitos de recopilar esta información y asegurar que se mantenga protegida de manera adecuada. La atención a la protección de datos personales y la competencia en el manejo de la información son aspectos críticos que deben ser abordados de manera cuidadosa para evitar posibles repercusiones negativas.

Carrera 11B # 99-25, oficina 11-113 - Bogotá, Colombia • PBX: +57 (1) 756 3456 • www.ccit.org.co

2. Comentarios particulares

2.1. Comentarios respecto al artículo 2 "Principios"

En cuanto al principio de enfoque basado en riesgos, consideramos pertinente a modificarlo a "Principio de enfoque de gestión efectiva de riesgos". Asimismo, el término comúnmente utilizado en políticas de seguridad digital es "gestión de riesgos". En ese sentido, también proponemos cambiar "enfoque basado en riesgos" por "enfoque basado en gestión efectiva de riesgos". Al respecto, por "efectiva" se entiende una gestión eficaz (que logre los objetivos) y eficiente (que se consigan las metas al menor costo posible, o utilizando la menor cantidad posible de recursos). En línea con el comentario anterior se sugiere modificar la redacción así: "de tal forma que la definición y aplicación de medidas de gestión de riesgos de seguridad digital considere los riesgos existentes, así como los costos y beneficios de dichas medidas".

> ***"ARTÍCULO 2**. Principios. En el desarrollo, interpretación y aplicación de la presente Ley, además de los principios constitucionales, se aplicarán los que a continuación se prevén. (…)*
>
> *Principio de **enfoque basado en gestión efectiva de riesgos**: La seguridad de la información y la ciberseguridad deberá estar basada en el **enfoque basado en gestión efectiva de riesgos de tal forma que la definición y aplicación de medidas de gestión de riesgos de seguridad digital considere los riesgos existentes, así como los costos y beneficios de dichas medidas.***
>
> *Principio de Integridad: El Estado desarrollará, a través de las entidades y organismos competentes las acciones necesarias para elevar la confiabilidad y la exactitud de los datos o información de forma que se evite su manipulación, su adulteración y cambios por personas, entidades o procesos no autorizados, **basándose en buenas prácticas y estándares internacionales"***

2.2. Comentarios respecto al artículo 3 "Definiciones"

Consideramos pertinente complementar la definición de Ciberataque, en el sentido de incluir la triada CIA (Confidencialidad, Integridad y Disponibilidad) de seguridad de la información dentro de la concepción de esta, así como la noción de que esta ocurre ante un acceso no autorizado o una afectación a alguna afectación causada por terceros no autorizados. Asimismo, es relevante incluir en la definición de Incidente de seguridad digital, que este también puede afectar los servicios prestados sobre sistemas de información. En ese sentido, proponemos la siguiente redacción:

> ***"ARTÍCULO 3.** Definiciones. Para los efectos de la presente Ley, se adoptan las siguientes definiciones: (…)*

Carrera 11B # 99-25, oficina 11-113 - Bogotá, Colombia • PBX: +57 (1) 756 3456 • www.ccit.org.co

b. Ciberataque: Acción realizada a través de medios o instrumentos digitales o tecnológicos con el objetivo de afectar servicios a la ciudadanía o Infraestructuras Críticas cibernéticas o servicios esenciales, así como la seguridad de las personas. ***Este tipo de acciones comprometen la disponibilidad, integridad y confidencialidad de la información, y que se realizan mediante el acceso no autorizado o afectación de los sistemas de información y de las infraestructuras que lo soportan.*** *(…)*

e. Incidente de seguridad digital: Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; ***o de los servicios ofrecidos a través de dichos sistemas;*** *o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable."*

2.3. Comentarios respecto al artículo 5 "Misión"

Respetuosamente sugerimos hacer referencia al Modelo de Seguridad y Privacidad de la Información, que se encuentra definido en la Resolución MinTIC 500 de 2021 y Resolución MinTIC 746 de 2022. Asimismo, la referencia al Modelo de Seguridad y Privacidad de la Información es importante para garantizar que la Agencia se adhiera a los estándares y prácticas establecidos. En ese sentido proponemos actualizar de redacción de la siguiente manera:

"ARTÍCULO 5. *Misión. La Agencia, es responsable* ***de liderar y fortalecer la gestión del Estado en materia de seguridad digital,*** *coadyuvar en mantener un modelo de Ciberseguridad y la gestión de seguridad de la Información en las entidades del estado y de las personas naturales y jurídicas de derecho privado. Adicionalmente apoyará, articulará la identificación y protección de las infraestructuras críticas del país* ***en materia de seguridad digital*** *con las autoridades y entidades competentes. Coordinar y cooperar con la identificación de amenazas, vulnerabilidades, con el propósito de asegurar las plataformas del estado a través de la confidencialidad, integridad y disponibilidad de la información o de los activos empleados para su transmisión, reproducción, procesamiento o almacenamiento, asociados a los sistemas de información de la Entidades o en el ciberespacio para uso de la ciudadanía y del estado colombiano. En asuntos espaciales, la agencia es la responsable de ejercer como autoridad espacial nacional estableciendo un marco de gobernanza e institucionalidad que dictamine una Política Espacial Colombiana. Adicionalmente trazará una visión de largo plazo del sector espacial del país articulando entes públicos y privados y de cooperación internacional a fin de dinamizar la industria espacial colombiana y a su vez generen productos y servicios que contribuyan al desarrollo socioeconómico del país."*

2.4. Comentarios respecto al artículo 7 "Objetivos"

Carrera 11B # 99-25, oficina 11-113 - Bogotá, Colombia • PBX: +57 (1) 756 3456 • www.ccit.org.co

Con el fin de complementar los objetivos de la Agencia, respetuosamente recomendamos modificar la redacción de la siguiente manera, incluyendo lo relativo a identificación de amenazas, de la siguiente manera:

> ***"ARTÍCULO 7**. Objetivos. La Agencia, será un organismo de carácter técnico especializado que tendrá como objeto la planificación, articulación y coordinación de las políticas de gestión de los riesgos de seguridad digital en el país, **identificación y** prevención de amenazas internas o externas contra el ecosistema digital del país, fortalecimiento de la confianza y seguridad de todas las partes interesadas en el ámbito digital, así como de las políticas de gobernanza, institucionalidad y programas y estrategias del sector espacial."*

2.5. Comentarios respecto al artículo 9 "Funciones de la Agencia"

La precisión en la redacción de las funciones, incluyendo la protección del ecosistema digital en materia de seguridad digital, es necesaria para definir claramente el alcance de sus responsabilidades. En cuanto al numeral 1, consideramos pertinente precisar que esta Agencia deberá trabajar en coordinación con las instancias de decisión del modelo de gobernanza de la seguridad digital del país, definidas en el Decreto 338 de 2022. Por lo que proponemos la siguiente redacción:

> *"1. Coordinar con los actores del ecosistema de seguridad digital, el entendimiento y fortalecimiento de la gestión de los riesgos e incidentes de seguridad digital, ciberseguridad y protección de datos de la información que soportan la operación del estado. **La Agencia deberá trabajar en coordinación con las instancias de decisión del modelo de gobernanza de la seguridad digital del país, definidas en el Decreto 338 de 2022.**"*

En cuanto al numeral 2, consideramos pertinente mencionar que se seguirán las mejores prácticas y estándares internacionales en ejercicio de esta función, de la siguiente manera:

> *"2. Liderar la implementación de políticas tendientes al fortalecimiento del nivel de madurez de seguridad digital en las entidades del estado y coadyuvar en la implementación de mejores prácticas de seguridad en los sectores económicos y en la ciudadanía, **siguiendo buenas prácticas y estándares internacionales**."*

En cuanto al numeral 4, sugerimos precisar esta función, en especial la palabra "asegurar" y su alcance general sobre el ecosistema digital y su gobernanza. Una redacción alternativa podría ser la siguiente:

> ***"4. Liderar la protección del ecosistema digital en materia de seguridad digital, así como la protección del modelo de gobernanza de la seguridad digital del país"***

Carrera 11B # 99-25, oficina 11-113 - Bogotá, Colombia • PBX: +57 (1) 756 3456 • www.ccit.org.co

En cuanto al numeral 5 y 6, consideramos que no es concreto ni específico el alcance de la palabra "contribuir" en esta función. Asimismo, es relevante mencionar la coordinación con las demás entidades del modelo de atención y gestión de incidentes. Por lo tanto, sugerimos la siguiente redacción:

> *"5.* ~~***Contribuir a***~~ ***Liderar y coordinar la respuesta oficial del Estado para*** *la protección y defensa del ciberespacio ante actos de penetración, infiltración, espionaje, sabotaje u otras actividades cuando atenten gravemente contra la administración pública y las infraestructuras críticas y proteger a las instituciones de nivel nacional y territorial de la influencia de organizaciones criminales.* ***Esta función de realizará en coordinación con los actores del modelo nacional de atención y gestión de incidentes (COLCERT, CSIRT Gobierno y CSIRT sectoriales), establecidos en el Decreto 338 de 2022****."*
>
> *"6.* ***Liderar y coordinar la respuesta oficial del Estado para*** ~~***Contribuir a***~~ *la protección de recursos tecnológicos y económicos de la Nación, cuando su amenaza comprometa el orden público."*

En cuanto al numeral 7, de nuevo es pertinente mencionar la implementación de normas y estándares internacionales que sean ampliamente reconocidos por la industria. De igual manera, esta función corresponde a una actividad continua, por lo que no resultaría conveniente definir un único plazo en el tiempo. Así las cosas, proponemos la siguiente redacción:

> ***"7. Implementar normas técnicas y estándares internacionales, así como*** *establecer protocolos, procesos y procedimientos,* ***basados en certificaciones y estándares internacionales reconocidos por la industria,*** *dirigidos a las entidades del estado y empresas privadas* ***conforme a las funciones establecidas en el presente artículo*** *que contribuyan a preservar la confidencialidad, integridad y disponibilidad de la información del país, para reducir los riesgos de seguridad digital de las entidades del estado, de los diferentes sectores económicos y de los ciudadanos, respetando la confidencialidad y protegiendo el buen nombre de los sujetos obligados.* ~~***Los cuales deberán ser expedidos dentro seis (6) meses siguientes a la expedición de la presente ley."***~~

En cuanto al numeral 8, recomendamos la siguiente redacción para enfatizar el rol de la Agencia como apoyo para las demás entidades del Estado en sus estrategias de seguridad digital. En ese sentido, proponemos la siguiente redacción.

> ***"8. Apoyar a las entidades del Estado en el fortalecimiento de las capacidades y competencias*** ~~***Fortalecer las capacidades y competencias***~~ ***en seguridad digital de los servidores públicos, trabajadores oficiales, contratistas, proveedores y demás grupos de interés que accedan a la información del estado colombiano."***

En cuanto al numeral 11, consideramos precisar de la siguiente manera la protección del ecosistema, especificando que es en materia de seguridad digital:

> ***"11.*** *Desarrollar actividades de protección del ecosistema digital* ***en materia de seguridad digital*** *en cooperación con los demás organismos nacionales e internacionales, así como con otras entidades del Estado y personas jurídicas de derecho privado que administren u operen infraestructuras críticas"*

Por último, en cuanto a los asuntos de seguridad digital, otras funciones adicionales que podrían ser relevantes son:

> *"- Apoyar a las entidades del estado en la evaluación de riesgos en materia de seguridad digital, así como en al análisis de amenazas cibernéticas.*
>
> *- Prestar asesoría técnica en materia de seguridad digital a las demás entidades del gobierno nacional, así como a las entidades del estado y empresas privadas que operen infraestructuras críticas.*

De otro lado en cuanto a los asuntos espaciales, consideramos pertinente agregar la siguiente función, con el fin de enfocar el rol de la Agencia en la promoción de servicios satelitales en el país:

> *"Adquirir, gestionar y proveer la capacidad satelital necesaria para el cumplimiento de las políticas de gobernanza, institucionalidad, programas y estrategias del sector espacial, con el propósito de promover la seguridad digital y la productividad de los diferentes sectores del país".*

2.6. Comentarios respecto al artículo 10 "Órganos de dirección y administración"

Respecto a la secretaría del Consejo que se plantea, respetuosamente sugerimos que se determine dentro del marco reglamentario de la Agencia, ya que dependerá de la dinámica administrativa de la misma.

2.7. Comentarios respecto al artículo 12 "Director general y sus funciones"

En cuanto al numeral 13 del artículo, consideramos pertinente aclarar el alcance de la contribución de valorización mencionada, en el marco de una Agencia Nacional de Seguridad Digital y Asuntos Espaciales, para que no quede sujeta a interpretaciones ambiguas y se entienda claramente su objetivo en el contexto de una Agencia Nacional de Seguridad Digital y Asuntos Espaciales.

2.8. Comentarios respecto al artículo 13 "Dirección de Seguridad Digital"

Carrera 11B # 99-25, oficina 11-113 - Bogotá, Colombia • PBX: +57 (1) 756 3456 • www.ccit.org.co

En cuanto al numeral 3 del artículo, consideramos pertinente tener en cuenta la experiencia del sector privado a la hora de establecer las políticas y acciones de la Agencia. Con eso en mente, proponemos la siguiente redacción:

> *"3. Aplicar las políticas, acciones y protocolos de seguridad digital a nivel nacional,* ***adoptando políticas, protocolos y/o directrices basadas en las normas del sector, así como en certificaciones reconocidas por la industria****."*

Asimismo, sugerimos, dentro de las funciones de la Dirección de Seguridad Digital incluir el establecimiento de políticas y lineamientos para garantizar la seguridad digital en el uso de redes y la prestación de servicios de telecomunicaciones basados en la prevención, mitigación y control del riesgo de conformidad con estándares internacionales de seguridad y convenios de ciberseguridad adoptados por Colombia. ~~En ese sentido proponemos la siguiente redacción:~~

2.9. Comentarios respecto al artículo 16

Consideramos que se debe propender por una autorregulación, que permita flexibilidad en las organizaciones para adaptar las mejores prácticas. En ese sentido, no es necesario esperar la legislación, cuando desde la industria se pueden adoptar buenas prácticas de manera anticipada y ser los primeros. Las empresas el sector privado son las más interesadas en aplicar los más altos estándares en materia de seguridad digital, y ya hacen lo propio.

2.10. Comentarios respecto al artículo 17

El artículo contiene conceptos indeterminados tales como riesgo, amenaza y evento que requieren una definición con un alcance claro y detallado, de forma tal que las entidades tanto públicas como privadas tengan certeza qué tipo de eventos se deben reportar y cuáles son los factores para la materialización de eventos. En igual sentido, no resulta procedente la imposición de sanciones por la ausencia de reporte de riesgos para personas jurídicas de derecho privado que administren u operen infraestructuras críticas, dado que, el riesgo en sí mismo, no debería ser penalizable.

En caso de existir penalización por ausencia de reporte, está debe restringirse a ausencia de reportes de eventos de materialización, previo a un procedimiento de reporte definido en los reglamentos. En igual sentido, las sanciones deberían estar estructuradas bajo esquemas de graduación de responsabilidad con base en la diligencia demostrada o la omisión de esta y en el impacto del evento. De esta forma, se garantizan esquemas de penalización garantistas. La estructura de sanciones debe estar definida en los reglamentos.

De otro lado, el deber de información de las entidades públicas y privadas debe restringirse únicamente a la información de eventos de materialización de amenazas, bajo los criterios de impacto definidos en los reglamentos expedidos. Asimismo, se sugiere eliminar el esquema de penalizaciones por ausencia de reporte de riesgos y restringir dicho esquema a la ausencia de reporte de eventos bajo definición de impacto, procesos y alcance. El esquema de penalización

por ausencia de reporte debe estar definido en reglamentos atendiendo a criterios de gradualidad por impacto y negligencia de la entidad privada o publicada obligada a reportar. Con esto en mente, respetuosamente proponemos la siguiente redacción:

> *"ARTÍCULO 17. Las entidades del Estado y las personas jurídicas de derecho privado deberán informar a la Agencia, los eventos de materialización de amenazas perpetradas contra sus infraestructuras, en los términos que defina la reglamentación que para el efecto expida la Agencia. En caso de que las personas jurídicas de derecho privado que administren u operen infraestructuras críticas, no informen de los riesgos o eventos en el tiempo establecido por la Agencia, se les podrá imponer las sanciones establecidas en los reglamentos emitidos por la Agencia a través del desarrollo del proceso sancionatorio."*

Asimismo, es crucial definir claramente los conceptos de riesgo, amenaza y evento en el contexto de la ley, para que las entidades comprendan qué tipos de eventos deben reportar y bajo qué criterios.

Además, identificamos las siguientes dificultades en el régimen sancionatorio propuesto por el Proyecto de Ley:

- Duplicidad de reportes de información. En cuanto a los reportes de información, es importante que el Proyecto de Ley contemple la coordinación entre entidades del sector como la CRC, el MINTIC y la SIC, con el fin de ser coherentes con las normas previamente expedidas con el fin de evitar la duplicidad de información entregada a estas entidades. Por ejemplo, la Circular No. 02 de 2015 de la SIC, establece que se deben reportar los incidentes de seguridad, relacionados con datos personales. Por su parte la Resolución CRC 5569 de 2018, en materia de gestión de seguridad en redes de telecomunicaciones, incluye dos reportes de información, i) a la CRC y ii) al ColCert.

La imposición de más obligaciones, para los operadores de telecomunicaciones, desconoce entre otros postulados jurídicos el de seguridad jurídica. En ese orden de ideas, se deben tener en cuenta las normas existentes sobre ciberseguridad que aplican a los mismos, con el fin de no imponer nuevas obligaciones regulatorias a los operadores.

En suma, es necesario evitar aumentar el número de reportes ya realizados por los PRSTM, los cuales representan una carga operativa importante para los mismos, máxime cuando el MINTIC manifestó en el Modelo Nacional de Gestión de Riesgos de Seguridad Digital, que los reportes para las entidades privadas son una invitación "como ejercicio colaborativo en el fortalecimiento de la seguridad digital del país".

- Confidencialidad de los reportes de información. Adicionalmente, echamos de menos en la exposición de motivos del Proyecto de Ley en comento, un análisis sobre la confidencialidad de la información, ya que el tema de los reportes de información que pretende implementar el proyecto debe ser abordado desde la óptica de la confidencialidad.

Carrera 11B # 99-25, oficina 11-113 - Bogotá, Colombia • PBX: +57 (1) 756 3456 • www.ccit.org.co

Este aspecto, es inherente a cualquier entrega de información por parte de los operadores de servicios de telecomunicaciones. Las entidades receptoras de cualquier tipo de información generada en este contexto de incidentes de seguridad deben contar con un sistema robusto que permita garantizar el envío seguro de la información y la conservación de esta. Así como la justificación legal para el uso de la información, aspectos que no se encuentran incluidos en el texto.

Es importante que exista una definición previa de los mecanismos electrónicos y digitales, que van a garantizar la confidencialidad de la información enviada por los obligados, su conservación y acceso no autorizados o malintencionados, así como el uso que se va a realizar de la misma, ya que se trata, de información con un componente reputacional muy importante para las compañías, que, por ende, debe protegerse al amparo de las normas que así lo establecen.

- Carga operativa. El Proyecto de Ley establece que se deben informar, en un plazo máximo de dos días, los ciberataques. Lo anterior, obliga a las empresas a establecer dos frentes de acción cuando se presente un incidente de seguridad que potencialmente cumpla los requerimientos para el reporte: i) un frente debería concentrarse en contener el incidente y recuperar las operaciones afectadas, ii) un segundo frente a preparar y enviar el reporte en caso de requerirse.

Para lograr atender los dos frentes descritos, dentro del tiempo máximo de dos días dado por el Proyecto de Ley, sin afectar las tareas de contención que serían las prioritarias y en las que la totalidad de los recursos se encontrarán concentrados, se desviaría el objetivo primordial para contener el impacto. Esto significa, que este requerimiento implicará sobrecarga operativa que puede representar un riesgo para la contención efectiva de los incidentes, de lo contrario las empresas se ubicarían en una posición de incumplimiento y posible investigación y sanción.

Adicionalmente, es necesario resaltar que, dados los recursos contemplados para la Agencia, solo necesitaría dicha información para fines analíticos y estadísticos posteriores, por lo que no se entiende que valor brinda que el reporte se entregue dentro de los dos días exigidos.

Esperando haber aportado de manera positiva con nuestros aportes, nos ponemos a sus órdenes en caso de tener alguna duda o inquietud sobre los mismos.

Agradeciendo la atención prestada, me suscribo de Ustedes con sentimientos de consideración y aprecio.

Cordialmente,

ALBERTO SAMUEL YOHAI
Presidente
Cámara Colombiana de Informática y Telecomunicaciones – CCIT