# ANTEPROYECTO DE LEY CONSTITUCIONAL DEL CIBERESPACIO DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA

## Capítulo I

## Disposiciones Generales

### Objeto de la ley

**Artículo 1** La presente Ley tiene por objeto desarrollar los derechos constitucionales, principios orientadores, procesos , bases y lineamientos del ciberespacio de la República Bolivariana de Venezuela, con el objeto de contribuir a generar las condiciones que garanticen la seguridad de la Nación, el acceso seguro mediante la óptima operatividad de las Infraestructuras de Tecnologías de Información que lo constituyen, la protección de datos e Información, la seguridad y calidad del contenido que se encuentren en el mismo .

### Ámbito de aplicación

**Artículo 2** Las disposiciones de la presente Ley, se aplicarán a todo dato e información de personas naturales o jurídicas, en cuanto le resulte aplicable, de conformidad con el ordenamiento jurídico vigente en la República Bolivariana de Venezuela, independientemente de la naturaleza en la que se presente la información, la tecnología empleada, la ubicación o la categorización; de igual forma a los servicios, redes de comunicaciones, infraestructuras tecnológicas, usuarios, hardware, software, dispositivos tecnológicos, actividades y demás elementos que interactúen con el Ciberespacio de la República Bolivariana de Venezuela.

### Principios Generales que rigen el Ciberespacio de la República Bolivariana de Venezuela

**Artículo 3** El acceso al Ciberespacio de la República Bolivariana de Venezuela comprende el ejercicio de derechos consagrados en la Constitución de la República Bolivariana de Venezuela y leyes nacionales que deben regir para garantizar el libre acceso, uso seguro y responsable del mismo, de acuerdo al ordenamiento jurídico vigente en aras de contribuir a la consolidación de la seguridad y defensa nacional. En consecuencia se aplicará el desarrollo de los siguientes principios:

- Accesibilidad.
- Colaboración.
- Confidencialidad.
- Disponibilidad.
- Igualdad.
- Integridad.
- Interés Público.
- Interoperabilidad.
- Legalidad.
- No Repudio.
- Proporcionalidad.
- Protección de Datos.
- Protección y Defensa.
- Responsabilidad.
- Seguridad.
- Soberanía Ciberespacio.

**Definiciones**

**Artículo 4** A efectos de la presente ley, se entenderá por:

**Activos de Tecnologías de la Información:** Cualquier dato, información, elemento de una infraestructura tecnológica, tangible, intangible, que tenga valor para un individuo, organización o gobierno.

**Amenaza**: Es una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema o a los activos de la seguridad del Ciberespacio venezolano.

**Ciberespacio de la República Bolivariana de Venezuela:** Es el entorno de interacción digital conformado por elementos tangibles e intangibles, que se generan durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipos y personal relacionados con los sistemas informáticos cualesquiera sean estos y las telecomunicaciones que los vinculan, el cual permite el acceso, producción, transmisión y almacenaje de datos e información, e interacción **a través de una red de comunicaciones** por cualquier medio electrónico; así como también cualquier forma de ***actividad*** que se realice o tenga efectos o repercusiones para la República Bolivariana de Venezuela.

**Ciberdefensa:** Es el conjunto de acciones estratégicas, técnicas y legales, y/u operaciones activas o

pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informáticos y teleinformáticas de la defensa a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos tendentes a minimizar o neutralizar toda acción que genere o produzca riesgos, amenazas y agresiones al Ciberespacio venezolano.

**Ciberseguridad:** Es el conjunto de herramientas, políticas, prácticas idóneas, tendentes a proteger los dispositivos tecnológicos, usuarios, servicios/aplicaciones, sistemas de comunicaciones, comunicaciones, y la totalidad de la información transmitida y/o almacenada que constituyen el ciberespacio.

**Ciberterrorismo**: Ataques cometidos a través o contra cualquier componente del ciberespacio, c infraestructuras tecnológicas, con la finalidad de producir terror en la sociedad o desestabilización económica, política y social que afecten la paz interna, la independencia, defensa, seguridad y soberanía.

**Ciberterrorista**: Sujeto activo o persona que ejecuta acciones terroristas mediante uso de tecnologías de información y comunicación.

**CiberGuerra:** Utilización de las tecnologías de información y comunicación a través de las redes de comunicaciones para declarar y ejecutar acciones masivas en el ciberespacio contra Infraestructuras Críticas.

**Cibercrimen:** Actividad o acción criminal donde los servicios, software en el ciberespacio son usadas como medio o como fin para la comisión de un hecho punible .

**Cibercultura:** Conjunto de actividades que educan y sensibilizan a los usuarios en el buen uso del ciberespacio.

**Ciberespionaje:** Recolección y divulgación no autorizada de información privada o confidencial, en o desde el Ciberespacio .

**Dato**: Es la unidad mínima que compone una información, la cual representa un atributo a través de una representación simbólica para que sean comunicados, transmitidos o procesados .

**Datos sensibles** A los fines de la presente ley son aquellos datos referidos a la intimidad de una persona que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliaciòn sindical e información referente a la salud o a la vida sexual.

**Dispositivo tecnológico**: Cualquier elemento electrónico, óptico, magnético o de otra índole, bien

sea físico, lógico o su combinación, utilizado directa o indirectamente por uno o más usuarios para ejecutar al menos una de las siguientes acciones: entrada, procesamiento, salida, difusión de datos o información e interacción por cualquier medio.

**Hardware**: Equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que conforman un computador o sus componentes periféricos, conexiones, componentes y partes.

**Incidente de Seguridad:** Es todo aquel evento de Seguridad de Información, inesperados o no solicitados, que comprometen la operación de la gestión y amenazan la Seguridad de Información, que atente contra la seguridad, confidencialidad y normal operación o que constituya una amenaza para quebrantar los mecanismos de seguridad.

**Infraestructura crítica:** Es aquella Infraestructura Tecnológica cuyo funcionamiento es indispensable y no permite soluciones alternativas, están conformadas por las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales de la Nación, empleada en el desarrollo de sectores protegidos en virtud de su repercusión en los ámbitos de Seguridad y Defensa, Salud, Banca, Finanzas, Energía, Petróleo, Comunicaciones, Telefonía y cualquier otra infraestructura tecnológica que cumpla funciones de interés, cuya afectación pueda perjudicar gravemente el orden interno, económico, desarrollo estratégico, soberanía y seguridad, independientemente de la naturaleza pública o privada del órgano responsable de su gestión.

**Infraestructura tecnológica**: Conjunto de medios tecnológicos y sistemas en los cuales se soportan las bases para brindar servicios.

**Información**: Conjunto de datos agrupados que representa algo significativo para el usuario.

**Informática Forense:** Es una rama auxiliar de la ciencias forenses la cual mediante la aplicación de técnicas científicas y analíticas especializadas a infraestructuras tecnológicas que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

**Internet**: Sistema global de redes interconectadas en el dominio público.

**Medios Tecnológicos:** Cualquier componentes de software, hardware, instalaciones, dispositivos tecnológicos, redes de comunicaciones y demás elementos de las TIC .

**Proveedores de Servicios de Difusión de Mensajes** Propietarios o responsables de tecnologías de información y comunicación para la difusión de mensajes en medios electrónicos de acceso público.

**Proveedores de Servicios de Internet:** Entidad pública o privada que utilizan diversas tecnologías para brindar un servicio de conexión de Internet a sus usuarios.

**Proveedores de Servicios de TIC**: Entidad pública o privada que ofrezca a los usuarios un servicio de TIC.

**Redes de comunicaciones**: Constituye un medio para la conexión entre dos o más dispositivos tecnológicos para intercambio de datos e información.

**Servicios:** Serie de funcionalidades ofrecidas por un proveedor para satisfacer las necesidades de los usuarios en el ámbito de las TIC, como servicios de telefonía móvil, fija, Internet, radio, televisión, correo electrónico, entre otros.

**Software**: Información organizada en forma de programas de computación, procedimientos y documentación asociados, concebidos para realizar la operación de un sistema, de manera que pueda proveer de instrucciones a los computadores así como de data expresada en cualquier forma, con el objeto de que éstos realicen funciones específicas.

**Software Malicioso (Malware)**: Software diseñado con intenciones maliciosas que tiene características o capacidades para amenazar o causar daño directa o indirectamente a usuarios, infraestructura tecnológica y demás elementos del Ciberespacio venezolano.

**Tratamiento de datos**: Operaciones sistemáticas, efectuadas mediante procedimientos manuales o automatizados aplicados a los datos, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, posesión, acceso, manejo y en general el procesamiento de datos , así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

**Tecnología de Información y Comunicación (TIC)**: Tecnologías destinadas a la aplicación, análisis, estudio y procesamiento en forma automática de *datos* e información.

**Titulares de Datos** Cualquier propietario de datos personales o sensibles.

**Usuario**: Persona que se conecta directa o indirectamente a una red de comunicaciones utilizando uno o más dispositivos tecnológicos para hacer una determinada operación o acción.

### Interés y Orden Público

**Artículo 5** El Ciberespacio de la República Bolivariana de Venezuela es de interés público y estratégico para la Defensa Integral de la Nación, las disposiciones de la presente ley son de orden público, por lo que el Estado desarrollará políticas de seguridad, reglamentos, administración y control en su **acceso y uso**, para asegurar el bien común, la soberanía y la institucionalidad en beneficio de la Nación.

### Innovación y Aplicación de las Tecnologías de Información

**Artículo 6**

El Estado a través de la autoridad competente, fomentará el desarrollo y aplicación de tecnologías innovadoras relacionadas con el Ciberespacio de la República Bolivariana de Venezuela, dando prioridad a la independencia tecnológica del país. La implementación de tecnologías de información en el Ciberespacio venezolano se realizará de acuerdo a las leyes especiales vigentes que aplicables .

## Capítulo II

### Del Ciberespacio de la República Bolivariana de Venezuela

**Definición**

**Artículo 7** Es el entorno de interacción digital conformado por elementos tangibles e intangibles, que se generan durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipos y personal relacionados con los sistemas informáticos cualesquiera sean estos y las telecomunicaciones que los vinculan, el cual permite el acceso, producción, transmisión y almacenaje de datos e información, e interacción a través de una red de comunicaciones por cualquier medio; así como también cualquier forma de actividad que se realice o tenga efectos o repercusiones para la República Bolivariana de Venezuela.

**Componentes**

**Artículo 8** El Ciberespacio de la República Bolivariana de Venezuela**,** comprende la infraestructura tecnológica, servicios, usuarios, datos, información, actividades y demás elementos de tecnologías

de información y comunicación, que se encuentren o tengan efectos o repercusiones para la República Bolivariana de Venezuela. La seguridad en el Ciberespacio venezolano, para efectos de esta ley comprende: **Seguridad de Tecnologías de Información** y **Seguridad de Contenido**.

### Seguridad de Tecnologías de Información

**Artículo 9** La Seguridad de Tecnologías de Información, es el conjunto de Herramientas, Políticas, Normas o Procedimientos, implementadas para proteger los activos de información a objeto de preservar su confidencialidad, integridad, disponibilidad, autenticidad, no repudio y responsabilidad de la información.

### Seguridad de Contenido

**Artículo 10**

La Seguridad de Contenido, comprende el conjunto de Herramientas, Políticas, Normas o Procedimientos, acciones técnicas y jurídicas especializadas que deberá el órgano competente en materia de Ciberespacio de la República Bolivariana de Venezuela establecer mediante reglamento para garantizar el respeto, la paz, tolerancia y convivencia pacífica del país .

### Estado como garante de la Ciberseguridad.

**Artículo 11** El Estado a través de los órganos del Poder Público, las personas naturales y jurídicas y usuarios debe ejecutar las acciones de carácter preventivo que tengan por objeto asegurar el uso de las redes preservar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio, para garantizar el acceso y uso seguro del Ciberespacio, de acuerdo con el objeto de esta Ley.

La presente ley creará el órgano con competencia en materia del Ciberespacio de la República Bolivariana de Venezuela, el cual proporcionará apoyo técnico coordinado con el ente competente en formulación y ejecución de la políticas públicas destinada a contrarrestar el odio, fortalecer la convivencia pacífica y tolerancia en el país y salvaguardar la seguridad de la Nación.

### Seguridad en el Ciberespacio de la República Bolivariana de Venezuela

**Artículo 12** El órgano competente en materia del Ciberespacio de la República Bolivariana de Venezuela deberá establecer mediante reglamento las directrices para que sean elaboradas e

implementadas las políticas, acciones, para la protección del ciberespacio, así como la evaluación de riesgos que éste realice sobre los elementos que lo conforman.

### Corresponsabilidad en la seguridad del Ciberespacio de la República Bolivariana de Venezuela

**Artículo 13** Todos los órganos del Poder Público, personas jurídicas públicas o privadas y ciudadanos y ciudadanas, son corresponsables en la seguridad del ciberespacio de la República Bolivariana de Venezuela y deben colaborar con su protección y defensa, mediante su participación, accesos, apoyo y disposición activa en la ejecución de políticas, procedimientos y demás acciones de ciberseguridad que dicte el órgano competente en la materia y afines, de conformidad con la ley, reglamentos y resoluciones; para garantizar la protección del ciberespacio nacional, su confidencialidad, disponibilidad e integridad de los datos, el no repudio y la responsabilidad en su acceso y uso.

## Capitulo III

## Infraestructuras Críticas

### Definicion

**Artículo 14** Es aquella Infraestructura Tecnológica cuyo funcionamiento es indispensable y no permite soluciones alternativas, están conformadas por las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales de la Nación, empleada en el desarrollo de sectores protegidos en virtud de su repercusión en los ámbitos de Seguridad y Defensa, Salud, Banca, Finanzas, Energía, Petróleo, Comunicaciones, Telefonía y cualquier otra infraestructura tecnológica que cumpla funciones de interés, cuya afectación pueda perjudicar gravemente el orden interno, económico, desarrollo estratégico, soberanía y seguridad, independientemente de la naturaleza pública o privada del órgano responsable de su gestión.

### Seguridad de Información de Infraestructuras Críticas

**Artículo 15** La seguridad de Información de Infraestructuras Críticas comprenden el conjunto de medidas preventivas y reactivas a seguir por las organizaciones, para el resguardo y protección de los componentes del ciberespacio de las Infraestructuras Críticas del Estado venezolano.

El órgano competente para garantizar la seguridad en el Ciberespacio venezolano deberá dictar las políticas, lineamientos, normativa, reglamentación e instrucciones destinadas a proteger y resguardar las Infraestructuras Críticas.

**Acciones para la protección y seguridad de Infraestructuras Críticas**

**Artículo 16** El órgano u autoridad garante de la protección y seguridad del Ciberespacio, los operadores y los responsables de Infraestructuras Críticas, deberán adoptar las siguientes acciones para su protección y seguridad:

1. **Por parte del órgano o autoridad en materia de Ciberespacio:**

**a.** Definir la política general del operador para garantizar la seguridad de información integral del conjunto de instalaciones o sistemas de su propiedad o gestión.

b. Establecer las políticas referentes a la metodología de análisis de riesgos que garantice la continuidad de los servicios de información proporcionados por el operador de Infraestructuras Críticas y en la que se recojan los criterios de aplicación de las diferentes medidas de seguridad que se implementen para hacer frente a las amenazas, tanto físicas como lógicas que puedan existir, así como la realización de auditorías para verificar el cumplimiento de la misma.

c. Disponer y capacitar conjuntamente con los propietarios y operadores de Infraestructuras Críticas, el recurso humano que se dispondrá a pagarlas, en caso de incidentes de seguridad de información.
.

2. **Por parte de operadores o responsables de Infraestructuras Críticas:**

**a.** Elaborar Planes de Protección con medidas concretas y particulares a desarrollar para garantizar la seguridad integral de sus Infraestructuras Críticas, con miras a salvaguardar datos, información y servicios de vital importancia para el país, garantizando el correcto funcionamiento de los sistemas críticos de la Nación.

b. Incluir en los Planes de Protección Específicos todas aquellas medidas que los respectivos operadores consideren necesarias en función de los análisis de riesgos realizados respecto de las amenazas, en particular, las de origen terrorista sobre los sistemas de información

c. Establecer medidas de seguridad, basadas en los resultados del análisis de riesgos con criterios de proporcionalidad frente a las amenazas, considerando la seguridad y la eficacia

d. Ejecutar los planes de Protección de Infraestructuras Críticas, que incluyan las políticas, procesos, reglamentos, etc dictados por el órgano o autoridad garante de la protección del Ciberespacio y las medidas concretas para hacer frente a las amenazas que se ciernen sobre los sectores críticos.

e. Ejecutar la política de análisis de riesgo y prestar apoyo al ente competente en seguridad del Ciberespacio, para las auditorías respectivas.

f. Ejecutar el Plan de Apoyo Operativo según políticas dictadas por el ente competente en la protección del Ciberespacio, el cual contempla las medidas de vigilancia, protección o reacción ante contingencias. Este plan podrá ejecutarse por los funcionarios adscritos al órgano o autoridad garante de la protección del Ciberespacio de forma conjunta con los operadores o responsable de la Infraestructura Crítica, en caso de grave afectación, riesgos o amenazas de daños mayores.

g. Garantizar, en coordinación con el órgano o autoridad garante de la protección del Ciberespacio, la existencia y disponibilidad de recurso humano especializado capaz de ejecutar tareas y funciones en caso de indisponibilidad del personal habitual.

h. Garantizar al personal especializado adscrito a la autoridad competente en seguridad del Ciberespacio, la disponibilidad y acceso a espacios, equipos, datos e información *de* Infraestructuras Críticas.

## Inventario de Infraestructuras Críticas de la Nación

**Artículo 17** El Estado, a través del ente competente, será responsable de mantener actualizado un inventario detallado de las Infraestructuras Críticas existentes en la República Bolivariana de Venezuela, incluyendo su descripción, los medios de contacto con las mismas, el tipo de instalación, datos geográficos y de localización, información de seguridad, riesgos evaluados entre otros aspectos relevantes y será clasificado como secreto, por la alta sensibilidad para la seguridad nacional de la información contenida en dicho inventario.

## Responsabilidades de Propietarios y operadores de Infraestructura Crítica

**Articulo 18**

Cualquier entidad privada o pública, propietario, concesionario, intermediario, responsable u otro, de Infraestructura Crítica, deberá:

- Capacitar periódicamente y permitir acceso y uso al personal, designado por el ente competente en materia de Ciberespacio, para hacer frente a contingencias relacionadas con infraestructura crítica bajo su responsabilidad, cuando se emita el nivel de emergencia requerido. Los niveles de emergencias cuya gravedad amerite la intervención de la autoridad competente serán desarrollados en el Reglamento de la presente ley.

• Permitir el acompañamiento del ente en materia de Ciberespacio junto a otros entes relacionados, en la realización de auditorías periódicas destinadas a mitigar las acciones que pongan en riesgos la confiabilidad, integridad y disponibilidad de los datos e informaciones que administre la Infraestructura crítica correspondiente

• Suministrar información actualizada sobre contactos técnicos de la infraestructura crítica que administran, al ente competente, para el inventario respectivo.

• Acordar con la autoridad competente en materia de Ciberespacio, cláusulas de acceso a sus infraestructuras y suministro obligatorio de información por razones de razones de defensa y seguridad de la Nación, el orden interno y protección de los derechos e intereses ciudadanos

### Coordinación y suministro de datos e información para Objetivos de Seguridad

**Artículo 19** Los entes públicos y privados, garantizarán de manera oportuna el suministro de datos que administren, cuando el órgano o autoridad garante de la protección del Ciberespacio así lo requiera, a los fines de prevenir amenazas y contrarrestar daños que atenten contra la seguridad en el ciberespacio.

## Capítulo IV De la Protección de Datos e Información en el Ciberespacio de la República Bolivariana de Venezuela

### Protección de Datos Personales

**Artículo 20** Los usuarios del ciberespacio venezolano, según la presente ley, deberán respetar la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean éstos públicos o privados, respetando el derecho al honor y a la intimidad de las personas, así como también el acceso legal y seguro a la información que sobre las mismas se registre de conformidad a lo establecido en la normativa vigente.

### Medidas de Seguridad en la Protección de Datos

**Artículo 21** Las instituciones del Estado y demás personas naturales y jurídicas que administren datos personales o sensibles, deben adoptar medidas de seguridad de carácter técnico y organizativo necesarias para garantizar su protección, confidencialidad, integridad y disponibilidad, evitando su desaparición, alteración, pérdida, divulgación, consulta o tratamiento ilegal o no autorizado. Dichos órganos deberán implementar medidas de seguridad sobre datos capaces de detectar desviaciones y pérdida de información o de minimizar riesgos provenientes de la acción humana o tecnológica.

### Tratamiento de Datos Sensibles en el Ciberespacio de la República Bolivariana de Venezuela

**Artículo 22** La autoridad competente en el Ciberespacio Venezolano, podrá realizar cualquier operación o conjunto de operaciones mediante procedimientos manuales o automatizados aplicados a los datos sensibles o personales, tales como, la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos sin consentimiento de los afectados o interesados, sólo cuando sea necesario para el cumplimiento de las funciones de defensa nacional en materia de Seguridad de Tecnología de Información y Seguridad de Contenido, o para ejercer funciones de apoyo a la investigación penal.

### Del Acceso a Datos en órganos y entes prestadores de servicio

**Artículo 23** La autoridad competente en el Ciberespacio Venezolano, podrá requerir a los organismos públicos y privados prestadores de servicios a la colectividad archivos, registros, bases o bancos de datos personales o sensibles, a los fines de su resguardo y protección por razones de defensa y seguridad, el orden interno y protección de los derechos e intereses ciudadanos.

Los datos e informaciones y procesos de tratamiento deben ser suministrados de tal manera que puedan ser legibles y entendibles por la media de la población, bajo condiciones tecnológicas para que sean usados por el ente competente en materia de protección y seguridad del Ciberespacio de la República Bolivariana de Venezuela. El responsable o usuario debe proporcionar la información solicitada dentro de los días requeridos por dicho ente.

### Responsabilidades de los titulares de datos, proveedores de servicios y usuarios

**Artículo 24** Los titulares de datos, proveedores de servicios y usuarios a los fines de acceso y uso del Ciberespacio venezolano, deberán:

***1.*** Cumplir con los estándares y buenas prácticas de seguridad requeridos por el órgano

competente para el acceso y uso del Ciberespacio de la República Bolivariana de Venezuela.

***2.*** Reportar o denunciar a las autoridades competentes las situaciones irregulares o que puedan poner en riesgo o afectar el uso y acceso legal del Ciberespacio nacional; así como mensajes, información o contenidos que perjudique el honor la reputación, la privacidad de las personas y en especial, de niños, niñas y adolescentes; o bien que afecten la paz interna, orden político, económico, social y el bien común en general.

***3.*** Suministrar, cuando le sea solicitada por la autoridad competente, los datos, información, procesos y acceso a cualquier recurso tecnológico del que dispongan, en tiempo oportuno y dentro de los lapsos establecidos.

***4.*** Cooperar e intercambiar con los órganos del Poder Público información, datos y servicios a los fines de optimizar el acceso y uso seguro del Ciberespacio nacional.

***5.*** Contribuir con la difusión de la conciencia, protección y realización de los derechos y deberes de los usuarios del Ciberespacio venezolano.

***6.*** Defender y respetar la privacidad de información.

***7.*** Cumplir con las mejores prácticas y normas de seguridad en las Tecnologías de Información así como la realización de auditorías a los sistemas, que se encuentran en el Ciberespacio de la República Bolivariana de Venezuela.

***8.*** Participar en la promoción de una cibercultura.

***9.*** Cumplir con los deberes atribuidos mediante normas, leyes, reglamentos instrucciones, manuales, solicitudes, planes de acción y requerimientos en general, realizados por la autoridad competente para garantizar la Seguridad de Tecnologías de Información y Seguridad de Contenido del Ciberespacio venezolano.

**Responsabilidades de Proveedores de Servicios de Internet, operadores y afines**

**Artículo 25** Los Proveedores de Servicios de Internet, operadores y afines, que tengan operaciones en el territorio nacional, con el debido respeto a la normativa nacional vigente y en consecuencia deberán:

1. Permitir al ente competente en el Ciberespacio de la República Bolivariana de Venezuela, la supervisión, seguimiento y registro de datos e informaciones transmitidas a través de sus servicios, a los fines de protección y mantenimiento de la Seguridad en el Ciberespacio

venezolano.

2. Suministrar información solicitada por el ente competente, que permita esclarecer averiguaciones en el ámbito de la seguridad de información.

3. Cualquier otra obligación establecida en las leyes y demás normativa vigente en la materia.

**Responsabilidades de Proveedores de Servicios de Difusión de Mensajes**

**Artículo 26** Los Proveedores de Servicios de Difusión de Mensajes y afines, que tengan operaciones o difusión dentro del territorio nacional y del Ciberespacio Venezolano,deben actuar de conformidad con las disposiciones legales que rigen la materia .En consecuencia deben:

1. Evitar y neutralizar la difusión de información clasificada como confidencial por empresas públicas o privadas, datos personales y datos de carácter personal no autorizados.

2. Proveer al ente competente en Ciberespacio de la República Bolivariana de Venezuela, de los registros, resultas de monitoreo, acceso y control de usuarios infractores de las leyes vigentes.

3. Prevenir, denunciar, neutralizar o eliminar la difusión de datos e información que atenten contra el honor, vida privada, intimidad, propia imagen, reputación de las personas, publicidad engañosa e ilícitos, promoción del odio, intolerancia, discriminación, acoso, explotación sexual, pornografía infantil, desestabilización económica, política, social de la Nación.

4. Acatar la normativa vigente para uso del Ciberespacio venezolano y coordinar de forma expedita las acciones de seguridad de información de la plataforma que administran, con el ente competente en la materia.

5. Cualquier otra obligación establecida en las leyes y demás normativa vigente en la materia.

6. Cualquier otra obligación establecida en las leyes y demás normativa vigente en la materia.

**Capítulo V Sistema Nacional del Ciberespacio de la República Bolivariana de**

## Venezuela

**Artículo 27** El desarrollo, ejercicio y seguimiento de funciones y deberes sobre seguridad, infraestructura y resguardo de datos previstas en los Capítulos precedentes, serán ejercidos a través de los sistemas y subsistemas para el Ciberespacio a cargo de la autoridad competente que será creada en la presente Ley, y de acuerdo a las demás leyes vigentes que rigen la materia.

### Creación del Sistema Nacional del Ciberespacio de la República Bolivariana de Venezuela

**Artículo 28** Se crea el Sistema Nacional del Ciberespacio de la República Bolivariana de Venezuela a fin de resguardar la Confiabilidad, Integridad, Disponibilidad, y responsabilidad en el uso de los elementos del Ciberespacio, que se encuentren en órganos del Poder Público o que detenten prestadores privados de servicios, empresas privadas, personas naturales y jurídicas en general, así como la generación de contenidos en la red; que por su importancia, criticidad de funciones, tareas estratégicas e incidencia en la estabilidad económica, política, social, paz interna, independencia, defensa, seguridad y soberanía de la Nación, son de permanente, necesaria y especial resguardo.

**Funciones del Sistema Nacional del Ciberespacio de la República Bolivariana de Venezuela y subsistemas**

**Artículo 29** El Sistema Nacional del Ciberespacio de la República Bolivariana de Venezuela tiene por objeto, mitigar y mejorar la capacidad de respuesta del Estado frente a riesgos y amenazas derivados del desarrollo y dinámica del Ciberespacio venezolano. El Sistema Nacional del Ciberespacio está integrado por:

**Subsistema de Apoyo a la Criptografía Nacional**: Su objetivo es coordinar y apoyar junto al ente competente en la materia aspectos relacionados con garantizar la integridad, calidad e independencia tecnológica con medios y procesos dirigidos a homologar, aprobar, y registrar equipos y aplicaciones con soporte criptográfico que utiliza el Poder Público.

**Subsistema Nacional de Gestión de Incidentes Telemáticos. Sistema Nacional de Gestión de Incidentes Telemáticos (Vencert):** Su objetivo es garantizar los mecanismos destinados a prevenir, detectar y gestionar los incidentes de Seguridad de la Información, Seguridad Informática y Ciberseguridad, así como mitigar los riesgos y/o amenazas del ciberespacio que atentan contra los activos de información, servicios, infraestructuras de tecnologías de información e Infraestructuras Críticas que lo soportan, y que están en los órganos del Poder Público.

**Subsistema Nacional de Informática Forense**: Prestará servicios de peritaje, experticias, análisis y asesoría en informática forense sobre evidencias digitales.

**Subsistema Nacional de resguardo de Datos:** Regula y garantiza el resguardo, privacidad, integridad y confidencialidad de los datos, de los sujetos del Poder Público. A través de este subsistema se ejecutarán las funciones y tareas en materia de Resguardo de Datos desarrolladas en la presente ley.

El Reglamento respectivo establecerá los términos y condiciones de implementación del Sistema Nacional de Seguridad del Ciberespacio de la República Bolivariana de Venezuela.

### Órgano responsable

**Artículo 30** El desarrollo y funcionamiento efectivo del Sistema Nacional del Ciberespacio de la República Bolivariana de Venezuela será responsabilidad del órgano que creará la presente ley con competencia en ciberespacio, el cual desempeñará funciones de autoridad central en las áreas que constituyen el sistema, sin menoscabo de las funciones que la ley especial en materia de mensajes de datos y firmas electrónicas le atribuye a la Superintendencia de Certificaciones Electrónicas.

## Capítulo VI

## Del Centro Nacional del Ciberespacio de la República Bolivariana de Venezuela

### Creación del Centro Nacional del Ciberespacio de la República Bolivariana de Venezuela

**Artículo 31** Se crea el Centro Nacional del Ciberespacio de la República Bolivariana de Venezuela, como un instituto autónomo de derecho público, descentralizado funcionalmente, con personalidad jurídica y patrimonio propio, distinto e independiente de la República.

El Centro Nacional del Ciberespacio de la República Bolivariana de Venezuela tendrá autonomía presupuestaria, administrativa, financiera, técnica, normativa y de autogestión de los recursos, en las materias de su competencia, la cual se ejercerá de acuerdo con los lineamientos y políticas establecidos por el órgano de adscripción y con los privilegios y prerrogativas de la República.

**Patrimonio del Centro Nacional del Ciberespacio de la República Bolivariana de Venezuela**

**Artículo 32** El patrimonio del Centro Nacional del Ciberespacio de la República Bolivariana de Venezuela estará integrado por los recursos asignados en la Ley de Presupuesto para el ejercicio fiscal correspondiente, por ingresos y bienes asignados o transferidos por órganos y entes del Poder Público, bienes provenientes de donaciones, así como por los ingresos propios derivados de sus actividades y servicios prestados, por las multas e infracciones generadas en esta ley y demás ingresos, legados y aportes de origen lícito.

**Objeto del Centro Nacional del Ciberespacio de la República Bolivariana de Venezuela**

**Artículo 33** El Centro Nacional del Ciberespacio de la República Bolivariana de Venezuela como un Instituto Autónomo será el encargado de la Seguridad de las Tecnologías de Información y Contenido en el Ciberespacio venezolano.

El Centro Nacional del Ciberespacio de la República Bolivariana de Venezuela dictará medidas, reglamentos, normas y procedimientos a ser seguidos por propietarios de activos en el Ciberespacio venezolano, con la finalidad de proteger los activos de la organización y salvaguardar el ciberespacio Venezolano, con respecto a los siguientes Objetivos de Control de Seguridad de TI: Políticas de Seguridad de Información, Organización de la Seguridad de Información, Seguridad de los Recursos Humanos, Gestión de Activos de la Organización, Control de Acceso, Políticas Criptográficas, Seguridad física y del entorno, Seguridad Operacional, Seguridad de Comunicaciones, Adquisición, desarrollo y mantenimientos de sistemas, Relaciones con los proveedores, Incidentes de Seguridad de la Información, Seguridad de Información en la Continuidad de la Gestión, Cumplimiento de leyes y reglamentos y otros objetivos de control que puedan surgir en el ámbito de la Seguridad de Información para Tecnologías de Información.

**Autoridad Garante de la Seguridad de Contenido en el Ciberespacio de la República Bolivariana de Venezuela**

**Artículo 34**

El Centro Nacional del Ciberespacio de la República Bolivariana de Venezuela será la autoridad en materia de la Seguridad de Tecnologías de Información y Seguridad de Contenido, siendo sus políticas, directrices, acciones, métodos, instrucciones, manuales, recomendaciones y sanciones de obligatorio cumplimiento para preservar el Ciberespacio venezolano, de factores que puedan afectar la Disponibilidad, Confidencialidad, Integridad de los datos o informaciones, o atentar contra la convivencia pacífica y seguridad moral de la Nación, a través de texto, imagen, audio, video o

cualquier otro formato por medios electrónicos.

## Competencias del Centro Nacional del Ciberespacio de la República Bolivariana de Venezuela

**Artículo 35**

El Centro Nacional del Ciberespacio de la República Bolivariana de Venezuela tendrá las siguientes competencias:

**1.** Dictar y ejecutar las políticas en materia del Ciberespacio venezolano, de la Seguridad de las Tecnologías de Información y de la Seguridad de Contenido, garantizando el resguardo, confidencialidad, disponibilidad e integridad de los datos, atendiendo a los estándares internacionales y buenas prácticas al respecto, así como a los principios de legalidad e interoperabilidad entre instituciones del Poder Público, prestadores de servicios privados y demás personas naturales y jurídicas en general.

**2.** Planificar, dirigir, ejecutar y supervisar acciones relacionadas con el Ciberespacio venezolano, evitando su uso indebido, previniendo y neutralizando los factores internos o externos que puedan poner en riesgo la seguridad de su infraestructura tecnológica, redes de comunicaciones, servicios, información, usuarios y demás elementos que lo constituyen; así como los contenidos que atenten contra el honor, vida privada, intimidad, propia imagen, reputación de las personas, publicidad engañosa, promoción del odio, intolerancia, discriminación, acoso, explotación sexual, pornografía infantil, desestabilización económica, política y social de la Nación.

**3.** Ejercer las funciones del Sistema Nacional de Seguridad del Ciberespacio y ajustar su estructura organizativa a tales fines.

**4.** Proteger los derechos de los ciudadanos, proporcionando un Ciberespacio nacional seguro, mediante el establecimiento, implementación y seguimiento de medidas preventivas dirigidas a contrarrestar los efectos de actividades asociadas al cibercrimen, ciberataques, ciberterrorismo, ciberguerra y de mensajes con contenido perjudiciales para los ciudadanos individualmente considerados y para la colectividad.

**5.** Elaborar políticas, programas, normas y procedimientos destinados a garantizar la seguridad y resguardo en el Ciberespacio venezolano.

**6.** Dictar medidas cautelares de resguardo ante acciones que atenten contra la seguridad del Ciberespacio venezolano o vulneren la estabilidad económica, política, social, paz interna,

independencia, defensa, seguridad y soberanía de la Nación a través del ataque a sus componentes. En tales casos el Centro deberá monitorear y seguir la ejecución y cumplimiento de la medida preventiva dictada, hasta la sanción definitiva por el ente competente según la ley respectiva.

**7.**Reportar ante los órganos competentes la posible comisión de hechos que afecten al Ciberespacio venezolano y que puedan configurar delitos de acuerdo a los términos de esta ley, a los fines de que se determine la responsabilidad penal a que haya lugar.

**8**. Fomentar el desarrollo y aplicación de tecnologías innovadoras que den prioridad a la independencia tecnológica y que permitan contribuir con la seguridad del Ciberespacio venezolano.

**9**. Salvaguardar y aumentar la seguridad de la información en el Ciberespacio, mediante el avance en la construcción, establecimiento y mantenimiento de la infraestructura tecnológica.

**10**.Impulsar una cultura para potenciar las capacidades de prevención de los ciudadanos ante los posibles riesgos en el Ciberespacio venezolano, utilizando espacios de difusión y discusión e intercambio de ideas e información, herramientas tecnológicas o cualquier medio o recurso físico, digital o afín que abarque todos los sectores de interés para el desarrollo del país.

**11**. Potenciar con los organismos del Estado, las capacidades de investigación, desarrollo, prevención, detección, respuesta y coordinación en materia de seguridad y defensa para el resguardo del Ciberespacio venezolano.

**12**. Coordinar y dirigir con los órganos responsables de la seguridad de la Nación, las respuestas efectivas ante las emergencias generadas por amenazas, irrupciones, ataques y daños actuales y potenciales que atenten contra la seguridad del Ciberespacio venezolano.

**13**. Establecer mecanismos de intercambio de información, con otros entes competentes en materia de seguridad, con el propósito de hacer investigaciones sobre amenazas y hechos, que atenten contra la seguridad de todos los elementos que componen el Ciberespacio venezolano.

**14**. Establecer mecanismos de cooperación internacional mutua a través de convenios, acuerdos o tratados con otros países y promover la participación en la comunidad internacional en áreas de investigación, intercambio de experiencias internacionales, desarrollo y deliberaciones en materia de ciberseguridad, y demás actividades que prevengan y contrarresten acciones originadas del cibercrimen, ciberataques, ciberterrorismo, ciberguerra y afines.

**15**. Desarrollar estándares de seguridad de obligatorio cumplimiento para el correcto acceso y uso del Ciberespacio venezolano.

16.Establecer mecanismos de coordinación e intercambio con el Poder Público, así como instituciones privadas, nacionales e internacionales, especializadas en seguridad de la información y materias afines, con la finalidad de unificar criterios y mejorar prácticas para mitigar riesgos y amenazas en el ciberespacio.

17.Impulsar la seguridad de la información en el Ciberespacio, mediante el avance en la construcción, establecimiento y mantenimiento de infraestructura tecnológica y sistemas para salvaguardar y aumentar la seguridad de redes.

18.Dictar las políticas de seguridad de las Infraestructuras Críticas de la Nación y recomendaciones para las demás en materia de seguridad de redes, mediante reglamentos que se actualizarán según sea necesario.

19.Coordinar como autoridad central y responsable del Sistema Nacional de Protección de Seguridad Informática, con la Superintendencia de Servicio de Certificaciones Electrónicas las funciones relacionadas con la criptografía nacional vinculada a la materia de Certificaciones Electrónicas, sin menoscabo de las atribuciones conferidas por la ley especial sobre mensajes de datos y firmas electrónicas.

20.Elaborar y desarrollar políticas especiales de seguridad, reglamentación, administración y control de gestión de Infraestructuras Críticas, así como la aprobación de planes de Resguardo de Infraestructuras Críticas.

21. Desarrollar, actualizar, mantener y asegurar la base de datos sobre las Infraestructuras Críticas de la Nación.

22.Monitorear, hacer seguimiento, alertar, bloquear, sustanciar expedientes, en apoyo a los entes competentes, sobre contenidos en el Ciberespacio que atenten contra el honor, vida privada, intimidad, propia imagen, reputación de las personas, o publicidad engañosa e ilícito, promoción del odio, intolerancia, discriminación, acoso, explotación sexual, pornografía infantil, desestabilización económica, política, social de la Nación.

23.Iniciar de oficio o a instancia de parte, sustanciar y decidir los procedimientos administrativos de responsabilidad social, relativos a presuntas infracciones o irregularidades que atentan contra la Seguridad de Tecnología de Información.

**24.**Cualquier otra atribución que le confiera las leyes y demás instrumentos normativos.

## Organización y Funcionamiento

**Artículo 36** La estructura organizativa del Centro Nacional del Ciberespacio de la República Bolivariana de Venezuela será determinada en su Reglamento Interno y demás normativa que se dicten para distribuir las competencias otorgadas, así como su organización y funcionamiento, en la cual se deberá fijar el número, organización, competencias y procesos a realizar por las dependencias administrativas que lo integrarán. El Reglamento Interno será dictado por el Consejo Directivo del Centro.

### Dirección del Centro Nacional del Ciberespacio de la República Bolivariana de Venezuela

**Artìculo 37** La dirección del Centro Nacional del Ciberespacio de la República Bolivariana de Venezuela estará a cargo de un Consejo Directivo integrado por un Director o Directora General quien lo presidirá, y cuatro directores o directoras de libre nombramiento y remoción del Presidente de la República Bolivariana de Venezuela, cada uno de los cuales tendrá un suplente que serán designado o designada de la misma forma, y quien llenará las faltas temporales de los directores. Las ausencias temporales del Director o Directora general serán suplidas por el Director o Directora Principal que éste o ésta designe.

El Consejo Directivo del Centro Nacional del Ciberespacio de la República Bolivariana de Venezuela sesionará válidamente con la presencia del Director o Directora General, o quien haga sus veces, y dos de sus miembros. Las decisiones se tomarán por mayoría absoluta de los miembros presentes.

Los miembros del Consejo Directivo estarán sujetos a la responsabilidad civil, penal, disciplinaria y administrativa por sus decisiones, de conformidad con la ley.

## Capítulo VII

### Régimen Sancionatorio

**Artículo 38 Los Propietarios y operadores de Infraestructura Crítica** que incumplan con las obligaciones previstas en el artículo 18 de la presente ley, o que realicen acciones prohibidas en el Ciberespacio venezolano o incurran en cualquiera de los supuestos generadores de responsabilidad, serán sancionados con multas desde cincuenta mil hasta doscientas mil Unidades Tributarias (50.000 hasta 200.000 U.T).

**Artículo 39 Los titulares de datos, proveedores de servicios y usuarios** que incumplan con las obligaciones previstas en el artículo 24 de la presente ley, o que realicen acciones prohibidas en el Ciberespacio venezolano o incurran en cualquiera de los supuestos generadores de responsabilidad, serán sancionados con multas desde cincuenta mil hasta doscientas mil Unidades Tributarias (50.000 hasta 200.000 U.T).

**Artículo 40 Los Proveedores de Servicios de Internet, operadores y afines** que incumplan con las obligaciones previstas en el artículo 25 de la presente ley, o que realicen acciones prohibidas en el Ciberespacio venezolano o incurran en cualquiera de los supuestos generadores de responsabilidad, serán sancionados con multas desde cien mil hasta cuatrocientas mil Unidades Tributarias (100.000 hasta 400.000 U.T).

**Artículo 41** Los responsables por realizar acciones prohibidas en el Ciberespacio venezolano o por incurrir en cualquiera de los supuestos generadores de responsabilidad, serán sancionados con multas desde cien mil hasta doscientas mil Unidades Tributarias (100.000 hasta 200.000 U.T).

**Artículo 42** Son circunstancias agravantes: la reincidencia , gravedad del daño causado, la resistencia o falta de colaboración del presunto infractor para esclarecer los hechos.

**Artículo 43** Son circunstancias atenuantes: No haber tenido la intención de causar daño, la mínima incidencia o daño del hecho y la disposición a cooperar con la investigación administrativa por parte del presunto infractor.

**Artículo 44** El incumplimiento o inobservancia de una medida cautelar dictada por el Centro Nacional de Protección al Ciberespacio conforme a esta ley, será sancionado con la multa de trescientos mil hasta quinientas mil Unidades Tributarias (300.000 hasta 500.000 U.T).

## Procedimiento

**Artículo 45** Las sanciones previstas en los artículos precedentes respecto a los supuestos generadores de responsabilidad en materia de Seguridad de Tecnologías de la Información y lo relacionado al apoyo técnico con respecto a la Seguridad de Contenido, serán impuesta por el Centro Nacional de Protección al Ciberespacio según sus competencias, aplicando el procedimiento administrativo ordinario previsto en la Ley Orgánica de Procedimientos Administrativos atendiendo a los principios de legalidad, imparcialidad y proporcionalidad.

## Medidas Cautelares

**Artículo 46** El Centro Nacional de Protección al Ciberespacio de la República Bolivariana de Venezuela de acuerdo a sus competencias podrá de oficio o a solicitud de parte, dictar medidas cautelares, urgentes, necesarias y proporcionales a la amenaza o daño causado al Ciberespacio venezolano por factores que atentan contra la **Seguridad de Tecnología de la Información y Seguridad de Contenido,** con el objeto de impedir la continuidad de dicha amenaza o daño.

Para dictar las medidas cautelares se deberá atender a la intencionalidad o no de la amenaza o daño y a la ponderación en la afectación que se le pueda causar al presunto infractor con la medida, así como al daño que se le pueda ocasionar al denunciante, usuario o a la colectividad en general. Dichas medidas serán de cumplimiento obligatorio para las personas naturales y jurídicas de carácter públicas o privadas.

Las medidas cautelares deben ser dictadas en acto motivado que será notificado al presunto infractor en el lapso de dos días hábiles, contados a partir del acto que la acordó. Una vez acordadas la medida cautelar, el presunto infractor directamente afectado con la misma podrá oponerse a ella de forma escrita, dentro de los cinco días hábiles siguientes a la fecha de su notificación. En caso de oposición, se abrirá un lapso de cinco días hábiles para alegar y promover todo lo que a su favor y defensa estime pertinente, así como un lapso de cinco días hábiles para evacuar las pruebas. Transcurrido dicho lapso el Centro Nacional de Protección al Ciberespacio decidirá lo conducente mediante acto motivado dentro de los ocho días hábiles siguientes prorrogables, por igual lapso.

Las medidas cautelares referidas, serán las siguientes:

.- Bloqueo, destrucción, desactivación de factores que atenten contra las tecnologías de información y que impliquen amenazas y ataques que puedan afectar o dañar la seguridad en el Ciberespacio venezolano y la estabilidad económica, política y social de la Nación.

.- Neutralizar, prevenir, responder y defender con los recursos tecnológicos necesarios, las amenazas que atenten contra el Ciberespacio venezolano y cualquiera de sus componentes.

El Centro Nacional de Protección al Ciberespacio de la República Bolivariana de Venezuela ejecutará con los recursos tecnológicos disponibles las medidas dictadas en el marco de la aplicación de la Ley Constitucional Contra el Odio, por la Convivencia Pacífica y la Tolerancia.

## Prescripción

**Artículo 47** Las acciones para imponer las sanciones previstas en la presente ley prescriben en un término de cinco (05) años contados a partir de la fecha de la ocurrencia del supuesto generador de responsabilidad que dio lugar a las sanciones. La obligación de pagar las multas prescribe a los cuatro años, contados a partir de su notificación. La prescripción se interrumpe por la acción del Centro Nacional de Protección del Ciberespacio dirigida a regularizar, investigar, verificar o comprobar el hecho sancionable o el cumplimiento de la sanción. También se interrumpe por la actuación del sancionado para reconocer el hecho, o por la comisión de nuevos hechos iguales o similares que sean sancionables conforme a la presente ley.

## Disposiciones Derogatorias

**Primera:** Se deroga parcialmente la Ley de Infogobierno, en sus artículos 54,55 y 57.

**Segunda:** Se deroga parcialmente la Resolución N° 063 del 10 de noviembre de 2008, dictada por el Ministerio del Poder Popular para las Telecomunicaciones y la Informática. Gaceta Oficial N° 39056 del 11 de noviembre 2006, en cuanto a la adscripción del Sistema Nacional de Gestión de Incidentes Telemáticos (VenCert ).

**Tercera:** Cualquier otra norma que colida con lo establecido en esta Ley Constitucional queda derogada.

## Disposiciones Finales

**Primera:** La presente Ley Constitucional entrará en vigencia a partir de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

**Segunda: El ejecutivo Nacional tendrá un plazo de un (01) año contado a partir de la** publicación de la presente ley en la Gaceta Oficial de la República Bolivariana de Venezuela, para dictar los reglamentos necesarios para su desarrollo.