Enlace a Legislación Relacionada

**DE APROBACIÓN DE LA "ESTRATEGIA NACIONAL DE CIBERSEGURIDAD 2020-2025"**

**DECRETO PRESIDENCIAL N°. 24-2020,** aprobado el 24 de septiembre de 2020

Publicado en La Gaceta, Diario Oficial N°. 178 del 29 de septiembre de 2020

**Gobierno de Reconciliación y Unidad Nacional**
**Unida Nicaragua Triunfa**

**DECRETO PRESIDENCIAL N°. 24-2020**

El Presidente de la República de Nicaragua
Comandante Daniel Ortega Saavedra

**CONSIDERANDO**

**I**

Que el uso del ciberespacio representa un desafío global, por sus potenciales y diversas afectaciones económicas y sociales, demanda desarrollar una cultura de seguridad cibernética.

**II**

Que el Modelo Cristiano, Socialista y Solidario, garantiza la articulación, complementariedad y unidad del Gobierno y el pueblo organizado, para promover la restitución de derechos, la equidad y los Derechos Humanos de los y las nicaragüenses.

**III**

Que los ciudadanos, el Estado y la sociedad requieren contar con un Ciberespacio confiable y seguro que fortalezcan los actuales niveles de seguridad soberana en función del desarrollo sostenible del país.

En uso de las facultades que le confiere la Constitución Política

**HA DICTADO**

El siguiente:

**DECRETO**

**DE APROBACIÓN DE LA "ESTRATEGIA NACIONAL DE CIBERSEGURIDAD 2020 - 2025".**

**Artículo 1.** Apruébese la **"ESTRATEGIA NACIONAL DE CIBERSEGURIDAD 2020-2025",** la cual se anexa al presente Decreto Presidencial.

**Artículo 2.** Instruir al Ministerio de Relaciones Exteriores para que en conjunto con el Instituto Nicaragüense de Telecomunicaciones y Correos (TELCOR) y las instituciones que tengan competencia en el tema de ciberseguridad, elaboren el Plan de Acción correspondiente.

**Artículo 3.** El presente Decreto entrará en vigencia a partir de su publicación. Publíquese en La Gaceta, Diario Oficial.

Dado en la Ciudad de Managua, Casa de Gobierno, República de Nicaragua, el día veinticuatro de septiembre del año dos mil veinte. **Daniel Ortega Saavedra,** Presidente de la República de Nicaragua. **Paul Oquist Kelley,** Secretario Privado para Políticas Nacionales.

**Estrategia Nacional de Ciberseguridad**
**2020 – 2025**

## I. INTRODUCCIÓN

La adopción de las Tecnologías de Información y la Comunicación TIC, unido a la conectividad mediante el uso del Internet y la banda ancha, a nivel global, ha sido un promotor del desarrollo socioeconómico de los países. Su uso ha impactado en la competitividad a nivel mundial de manera positiva al mejorar la eficiencia y productividad.

Sin embargo, existen riesgos y amenazas cibernéticas asociadas al uso de las TIC's (Tecnologías de la información y comunicación), que requiere de los países, desarrollar estructuras organizacionales, estrategias, marcos jurídicos y capacidades de defensa avanzadas para enfrentarlas.

Lo antes mencionado, hace imprescindible contar con una Estrategia Nacional de Ciberseguridad para la gestión y minimización de riesgos ante este nuevo tipo de amenazas, así como las reglas para adquirir y operar tecnología, tomando en cuenta el contexto nacional e internacional en materia de ciberseguridad.

La Estrategia Nacional de Ciberseguridad (ENC) establece la posición de Nicaragua ante una nueva concepción de la ciberseguridad, en avance a sus esfuerzos por contribuir a la promoción del ciberespacio seguro y confiable dentro del territorio nicaragüense, en el marco de la Política de Seguridad Nacional.

## II. CONTEXTO (ANTECEDENTES)

En el contexto internacional, ante la vulnerabilidad que identifica la comunidad internacional en el uso del ciberespacio, la Organización de la Naciones Unidas y la Organización de los Estados Americanos han adoptado resoluciones dirigidas a la creación de una "Cultura Mundial de Seguridad Cibernética y la Protección de las Infraestructuras de Información Esenciales" y la adopción de una "Estrategia Interamericana Integral de Seguridad Cibernética: Un Enfoque Multidimensional y Multidisciplinario para la Creación de una Cultura de Seguridad Cibernética", respectivamente.

En la región latinoamericana los países, entre ellos Nicaragua, han iniciado la elaboración de estrategias de ciberseguridad para garantizar la protección de los derechos de los ciudadanos, del Estado y la sociedad en general en el uso de las TICs, adoptando y teniendo como referencias las resoluciones de las organizaciones antes mencionadas.

Por otra parte, la aplicación de políticas públicas, y las condiciones de estabilidad económica en Nicaragua, han permitido un incremento de la inversión y en particular, el desarrollo del sector de las telecomunicaciones, presentando logros importantes en cuanto al acceso y uso de las Tecnologías de la Información y Comunicación; así mismo, la ampliación de la infraestructura tecnológica de banda ancha, incidiendo de forma importante en el desarrollo económico y social del país.

En el marco de las políticas públicas de Nicaragua, en el PROGRAMA NACIONAL DE DESARROLLO HUMANO 2018-2021 contiene ejes de seguridad soberana y desarrollo de las telecomunicaciones, sobre los cuales se fundamenta la creación de la Estrategia Nacional de Ciberseguridad, que permite continuar implementando los planes y programas que garanticen que Nicaragua siga siendo el país más seguro de la región centroamericana.

En este sentido, aunque se cuenta con avances en materia de ciberseguridad, los ámbitos que requieren continuar fortaleciéndose por medio de la creación de una Estrategia Nacional de Ciberseguridad son: La estructura organizacional, el marco regulatorio; la infraestructura tecnológica; el talento humano del personal técnico; y primordialmente las capacidades de los ciudadanos en el uso seguro y responsable de las TIC's.

## III. PRINCIPIOS RECTORES

La Estrategia Nacional de Ciberseguridad de la República de Nicaragua está establecida sobre cuatro principios fundamentales:

### a. Garantía de la Soberanía y Protección de los Derechos de los ciudadanos en el Ciberespacio.

El Estado de Nicaragua, promueve, protege y salvaguarda su soberanía y los derechos de los ciudadanos, creando las condiciones para el uso soberano, seguro, responsable, libre y confiable del ciberespacio en el territorio nacional.

### b. Gestión de Riesgos y Capacidad de Resiliencia.

La Estrategia Nacional de Ciberseguridad considera la realización de acciones para contar con una infraestructura TIC, robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, aplicando las mejores prácticas internacionales en la gestión de riesgos.

### c. Protección y Defensa del Ciberespacio.

La ENC establece potenciar las capacidades técnicas, orientadas a la protección del Ciberespacio nicaragüense, infraestructura crítica, información y los servicios a la población, derivadas de ésta, cuya interrupción afectaría negativamente a los diferentes sectores económicos del país.

### d. Desarrollo de Alianzas y colaboraciones Nacionales e Internacionales.

Este principio promueve la articulación y cooperac1on entre las instituciones públicas y privadas, nacionales e internacionales para la implementación, desarrollo y consolidación de la Estrategia Nacional de Ciberseguridad.

## IV. ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

### a. Estructura y Alcances de la Estrategia.

La Estrategia Nacional de Ciberseguridad fija las directrices y líneas generales de acciones para hacer frente al desafío que representa para el país la vulnerabilidad del ciberespacio.

Esta Estrategia establece un modelo de gobernanza para la ciberseguridad nacional con un conjunto de herramientas,

políticas, conceptos de seguridad, directrices, métodos de gestión de riesgos, formación de talento humano especializado, prácticas idóneas y tecnologías que pueden utilizarse para proteger la información y los activos del territorio nicaragüense y a los usuarios en el ciberespacio nacional.

Así mismo, se basa en un esquema que contiene un objetivo general y dos objetivos específicos transversales a todos los ámbitos; ejes estratégicos dirigidos al fortalecimiento institucional; al fortalecimiento del marco administrativo y jurídico, a la educación, formación y capacitación; al fortalecimiento tecnológico; a la seguridad y resiliencia de los servicios e infraestructuras críticas a nivel nacional, todo ello, conforman una matriz estratégica para promover la ciberseguridad hacia un modelo presente y futuro.

La presente estrategia es de naturaleza dinámica, responde a un plazo de implementación de cinco años, la cual será actualizada de acuerdo a las necesidades del país; así como del resultado de las evaluaciones de amenazas a la ciberseguridad.

**b. Objetivo General**

Garantizar el uso soberano, seguro y confiable del ciberespacio, que permita el aprovechamiento de las TIC's como herramienta que contribuya a la paz, la estabilidad, la seguridad y el desarrollo sostenible del país.

**c. Objetivos Específicos**

1. Establecer las condiciones administrativas y jurídicas en materia de ciberseguridad.

2. Establecer las condiciones técnicas de seguridad y resiliencia de las TIC' s en infraestructuras críticas, del sector público y demás sectores económicos del país.

**d. Ejes Estratégicos**

| | |
|---|---|
| **EJE ESTRATÉGICO 1** | **FORTALACIMIENTO INSTITUCIONAL** |

**Líneas de Acción**

*a) Establecer un órgano de naturaleza consultiva en materia de Ciberseguridad integrado por instituciones públicas y privadas para la elaboración de propuestas de políticas, programas y Proyectos.*

*b) Establecer un órgano administrativo y técnico con el fin de implementar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.*

*c) Establecer un Equipo de Respuesta ante Emergencias Informáticas, para prevenir, mitigar y responder a los incidentes de ciberseguridad.*

*d) Desarrollar cooperación, intercambio, notificación y alertas entre las instituciones de gobierno e instituciones internacionales homólogas en materia de ciberseguridad.*

*e) Fortalecer y potenciar la participación de Nicaragua en eventos y foros internacionales en materia de ciberseguridad.*

*f) Fortalecer la colaboración entre los organismos competentes y relacionados a la administración de justicia.*

*g) Formular e implementar un sistema de indicadores que permita medir la eficacia y eficiencia de la Estrategia Nacional de Ciberseguridad.*

| | |
|---|---|
| **EJE ESTRATEGICO 2** | **FORTALECIMIENTO DEL MARCO JURÍDICO** |

**Líneas de Acción**

*a) Revisar y actualizar el marco jurídico y administrativo en materia de ciberseguridad y TJC's.*

*b) Fortalecer la cooperación internacional en materia de ciberseguridad.*

*c) Crear mecanismos ágiles y seguros para la denuncia ciudadana sobre hechos de cibercrimen.*

*d) Adoptar normas y prácticas internacionales relacionadas a la gestión de riesgos basadas en los estándares de la industria en materia de Ciberseguridad.*

| | |
|---|---|
| **EJE ESTRATÉGICO 3** | **EDUCACIÓN, FORMACIÓN Y CAPACITACIÓN** |

**Líneas de Acción**

*a) Promover e impulsar la formación en ciberseguridad en todas las instituciones del Estado, y profesionales del Derecho para el uso responsable y seguro de las TICs.*

*b) Procurar a los operadores jurídicos el acceso a información y recursos materiales que aseguren una mejor aplicación del marco jurídico y técnico, relacionado con la ciberdelincuencia.*

c) Incorporar en el sistema educativo nacional el conocimiento en ciberseguridad.

d) Impulsar una cultura de ciberseguridad en el territorio nacional con la articulación de actores relevantes, para la realización de foros y campañas de sensibilización.

e) Fortalecer alianzas entre el Estado, instituciones académicas y empresas privadas, para la formación de talento humano.

f) Promover el aprovechamiento de programas de capacitación y asistencia técnica internacional en materia de ciberseguridad.

g) Fomentar la cooperación, el intercambio de información, experiencia y conocimientos entre los órganos responsables de la investigación y los organismos judiciales nacionales e internacionales competentes en persecución de la ciberdelincuencia.

h) Promover la colaboración e investigación entre centros de capacitación y aprendizaje en materia de ciberseguridad.

| | |
|---|---|
| **EJE ESTRATÉGICO 4** | **FORTALECIMIENTO TECNOLOGICO** |

**Líneas de Acción**

*a) Impulsar y potenciar programas de apoyo especializados en investigación, desarrollo e innovación (I+D+i), en ciberseguridad dirigidos a universidades, empresas, pymes, etc. así mismo fortalecer el talento humano.*

*b) Impulsar políticas de uso, protección y aprovechamiento de Propiedad Intelectual derivadas de la investigación.*

*c) Implementar plataformas y tecnologías para la prevención, detección y respuesta a ciber incidentes.*

| | |
|---|---|
| **EJE ESTRATÉGICO 5** | **SEGURIRDAD Y RESILIENCIA DE LOS SERVICIOS E INFRAESTRUCTURAS CRITICAS A NIVEL NACIONAL** |

**Líneas de Acción**

a) Implementar planes de coordinación e intercambio de información entre los sectores públicos y privados para la gestión del riesgo.

b) Identificar los servicios e infraestructuras críticas a nivel nacional.

c) Formular políticas de seguridad e implementar protocolos de prevención, detección y respuesta ante ataques a los servicios, sistemas de información e infraestructuras críticas.

d) Establecer mecanismos para la prevención, detección, mitigación y restauración de los servicios e infraestructuras críticas.

**IV. GLOSARIO DE TERMINOS**

**Amenaza:** Signo o indicio que anuncia un peligro. Acción o evento susceptible de producirse, transformarse en agresión contra un entorno o unos recursos y actuar en detrimento de su seguridad Fuente: Guía de Ciberseguridad para los países en desarrollo. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU2007-PDF-S.pdf

**Ciberamenazas:** El potencial de un intento malicioso de dañar o interrumpir una red informática o sistema con acceso no autorizado a un dispositivo del sistema de control que utiliza una vía de comunicación de datos. Las amenazas para controlar los sistemas pueden provenir de numerosas fuentes, incluidos gobiernos hostiles, grupos terroristas, empleados descontentos e intrusos maliciosos.

Fuente: https://www.itu.int/dms pub/itu-d/opb/str/D-STRGCI.01-2018-PDF-E.pdf

**Cibercriminalidad o Cibercrimen:** Capacidad de acceder sin previo consentimiento a información y datos que son propiedad de gobiernos, personas o empresas.

Fuente: http://www.iri.edu.ar/wp-content/uploads/2016/11/syd 15 Entrevista_corbino_cibercrimen.pdf.

**Ciberespacio:** Ámbito virtual creado por medios informáticos.

Fuente: https://dle.rae.es/ciberespacio?m=form

**Ciberseguridad:** El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.

Fuente: UIT-T Rec. X.1205 (04/2008) Aspectos generales de la ciberseguridad https://www.itu.int/rec/T-REC-X. 1205-200804-I/es

**Economía Digital:** La economía digital se constituye como un ecosistema, en el que convergen la infraestructura de las redes de comunicación, los servicios de procesamiento y las tecnologías web, y las/os usuarias/os finales (individuos, empresas, gobierno), y será el grado de desarrollo y complementación de estos componentes lo que define el nivel de avance de cada país.

Fuente: https://es.wikipedia.org/wiki/Econom%C3 %A Da_digital#Definici %C3%B3 n

**ENC:** Estrategia Nacional de Ciberseguridad

**I+D+i:** Investigación, desarrollo e innovación.

**Infraestructura crítica:** El elemento, sistema o parte de este, situado en el país que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente al país.

Fuente: Definición adaptada de https://eur-lex.europa.eu/legal content/ES/TXT/?uri=CELEX:32008L0114

**ISP:** Proveedor de servicios de internet.

**Resiliencia:** Capacidad de la organización para manejar las diversas amenazas que enfrentan, mejorando su postura para mitigar o reducir los impactos asociados. Fuente: Instituto de Gestión de Continuidad de Negocios - Instituto BCM

**TIC's:** Tecnologías de la Información y la Comunicación Conjunto de tecnologías que permiten el tratamiento, la comunicación de los datos, el registro, presentación, creación, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica, eléctrica o electromagnética, entre otros.