

Resumen

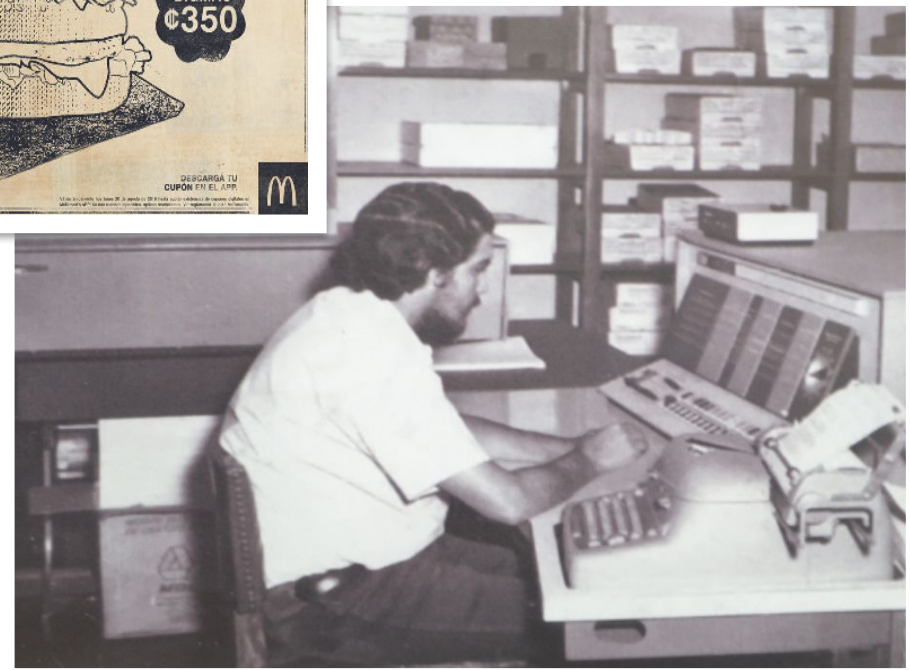
Estrategia Nacional de Ciberseguridad

2022-2027





La gerente general de la Junta de Protección Social (JPS) de Costa Rica, General del IICA, Manuel Otero, con la réplica del billete conmemorativo





Principios Rectores

Se rige al igual que la Política Nacional de Sociedad y Economía Basada en Conocimiento (PNESBC) en los siguientes principios rectores:



Respeto a la dignidad humana: debe responder a las necesidades e intereses de la población en condiciones de equidad, transparencia, participación e inclusión, superando los paradigmas de la discriminación en cualquier extensión.

Universalidad: debe generar las condiciones necesarias para que los avances en la producción del conocimiento basado en la ciencia y la tecnología estén al alcance de todas las personas.

Desarrollo humano: creación de las capacidades humanas por y para las personas, a través de la participación en los procesos que determinan sus vidas, y mediante la mejora de su calidad de vida.

Creación colaborativa: promueve la creación colaborativa en todas sus etapas, desde su formulación y hasta la evaluación de sus resultados, mediante la participación de la mayor cantidad de actores trabajando de manera conjunta con miras a un objetivo común.

Ética: garantiza que sus acciones estén dirigidas a socializar el conocimiento científico generado por la investigación y la innovación, desarrollando acciones éticas que sigan los códigos de conducta, promoviendo la creatividad y la productividad.

Política pública basada en datos. La utilización de datos en la formulación de políticas públicas asegura que las iniciativas estratégicas sean de beneficio para la mayor cantidad de personas, pero por sobre todo que sean adecuadas a sus necesidades a partir de la transformación de las condiciones actuales a mejores condiciones futuras

4 PRINCIPIOS ADICIONALES



1. Las personas son la prioridad

Las personas son el eje central en la estrategia.

- El uso de las TIC en los diferentes ámbitos de la vida cotidiana nos obliga a hacer partícipes de esta estrategia a todos los habitantes del país, por lo que la corresponsabilidad en el uso individual de dispositivos y redes será fundamental.
- Por lo anterior, se promoverá el uso de las TIC como un instrumento para el mejoramiento de la calidad de vida de manera segura, procurando generar conciencia por medio de la educación desde edades tempranas sobre los efectos del uso responsable.
- Se procurará que cualquier acción tenga como prioridad considerar la atención y mitigación de los riesgos que impacten prioritariamente a las poblaciones vulnerables como la niñez, la adolescencia, los adultos mayores, la población indígena y las personas con algún tipo de discapacidad.



2. Respeto a los Derechos Humanos y la Privacidad

- Garantizar el respeto a los derechos humanos, especialmente los relacionados con el acceso a las TIC, el acceso a la información y el respeto a la privacidad es fundamental.
- Las medidas y acciones que resulten de esta estrategia deberán en todo momento salvaguardar los derechos humanos y la privacidad de la información de los habitantes del país. Por lo tanto, esta estrategia se ha desarrollado teniendo en cuenta la necesidad de equilibrar la protección de todos los habitantes y el respeto de los derechos humanos básicos y fundamentales, con la necesidad de implementar medidas para mantenerlos seguros en línea.
- Esto incluye el respeto a la libertad de expresión, la libertad de palabra, el derecho a la privacidad, la libertad de opinión y la libertad de asociación. Del mismo modo, la presente estrategia emplea un enfoque de género para asegurar la igualdad de las personas en el ciberespacio



3. Coordinación y corresponsabilidad de múltiples partes interesadas.

La ciberseguridad es una responsabilidad compartida de todos los actores que participan en el ecosistema digital, lo cual incluye a los usuarios. Es imperativo que todas las acciones que se deriven de esta estrategia consideren, siempre que sea pertinente, la participación y aporte de todas las partes interesadas, la corresponsabilidad de estos y la necesidad de coordinación entre los distintos actores. Para el proceso de implementación, el apoyo de todos los sectores es fundamental, por esto, se deben considerar y promover los modelos público-público, público-privado y público-sociedad civil; según la idoneidad, requerimientos y alcances de los objetivos a implementar



4. Cooperación Internacional

La naturaleza transfronteriza de las tecnologías digitales hace que la temática de la ciberseguridad deba ser atendida desde una perspectiva global. Las amenazas cibernéticas no tienen fronteras, por ello la cooperación internacional se convierte en un eslabón primordial tanto para la atención de las amenazas como para la transferencia de conocimiento y el desarrollo de acciones locales y globales que ayuden a incrementar la confianza y la seguridad global. Por tanto, la construcción de alianzas, acuerdos y estrechamiento de lazos con otras entidades públicas y privadas que atienden las temáticas relacionadas a la ciberseguridad tanto a nivel regional e internacional deben ser elementos clave dentro de esta estrategia.



Ejes Transversales



Ejes transversales

- Coordinación Nacional
- Fortalecimiento del Ecosistema de Ciberseguridad
- Concientización y cultura
- Fortalecimiento de la cooperación cibernética internacional
- Gestión del riesgo
- Protección de Servicios Esenciales
- Fortalecimiento del marco legal en Ciberseguridad y TIC
- Gestión de la comunicación en crisis de ciberseguridad



Plan de acción

- 51 acciones puntuales
- Abierto de forma constante





Otras actividades

- Publicación del Código Nacional de Tecnologías Digitales
- Seminario con KISA el 23 de noviembre
- Invitación a Conferencia de Hacking y Ciberseguridad de Costa Rica: PWNED CR



PwnedCR 0x5





Agradecimiento

- OEA David Moreno y Orlando Garces por su liderazgo y guía experta
- ISACA: Vicepresidente técnica, Silvia y a los expertos Luis Gorgona y Raúl Rivera miembros de ISACA y a la official de Ciberseguridad de la UCR la Ing. Ana Cecilia Vargas y al apoyo Henry Lizano Director del Centro de Informática, por su trabajo en las Normas Técnicas para la Gestion y Control de las TICs
- CyberSec por el apoyo en la actualización del Código Nacional de Tecnologías Digitales
- TEC: Andrea Cavero directora del Departamento de Administración de Tecnologías de Información y Comunicaciones (DATIC) del TEC quién facilitó que un equipo de trabajo liderado por el profesor Melvin González Quesada generara las Políticas para Gestionar la Seguridad de la Información y Ciberseguridad como parte de la Estrategia Nacional de Ciberseguridad.
- CAMTIC en su capítulo de ciberseguridad, liderado por Diego González, en la actualización del proceso de Gestión de Respuesta a Incidentes Cibernéticos
- AWS: Marianella Sánchez, por el trabajo conjunto de AWS-OEA en la entrega de la Guía Estratégica para mejorar la postura de ciberseguridad de Costa Rica
- Mastercard: Marcelo, Raúl, Ronald, Andrés por el apoyo en la gestión de acciones propias de la ENC
- A todas las personas que han participado en los talleres y aportes para este paquete integrado de políticas

2022-2026



COSTA RICA

TRABAJANDO, DECIDIENDO, MEJORANDO