TECCOM 2025

AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES

GOBIERNO DE COSTA RICA

Protección de Datos Personales en proyectos de IA

Construcción desde los principios

EDUCACIÓN CONTINUA CPIC

CPIC COLEGIO DE PROFESIONALES EN INFORMÁTICA Y COMPUTACIÓN

Wendy Rivera Román
Directora Nacional

Ley No. 8968

- Aplicable a bases de datos automatizadas o manuales, en lo público o privado y aplica a todo el ciclo de los datos. No existe una "excepción para la IA" en la normativa de protección de datos.
- Define tratamiento como:

  > “cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros.”

- Inventario de tipo de datos acceso irrestricto, acceso restringido sensibles y comportamiento crediticio.
- Cumplimiento de obligaciones del responsable.
- **Desafíos IA con respecto a los datos personales** : sesgos algorítmicos, inferencias no deseadas, uso de grandes volúmenes de datos sensibles, opacidad de los modelos .

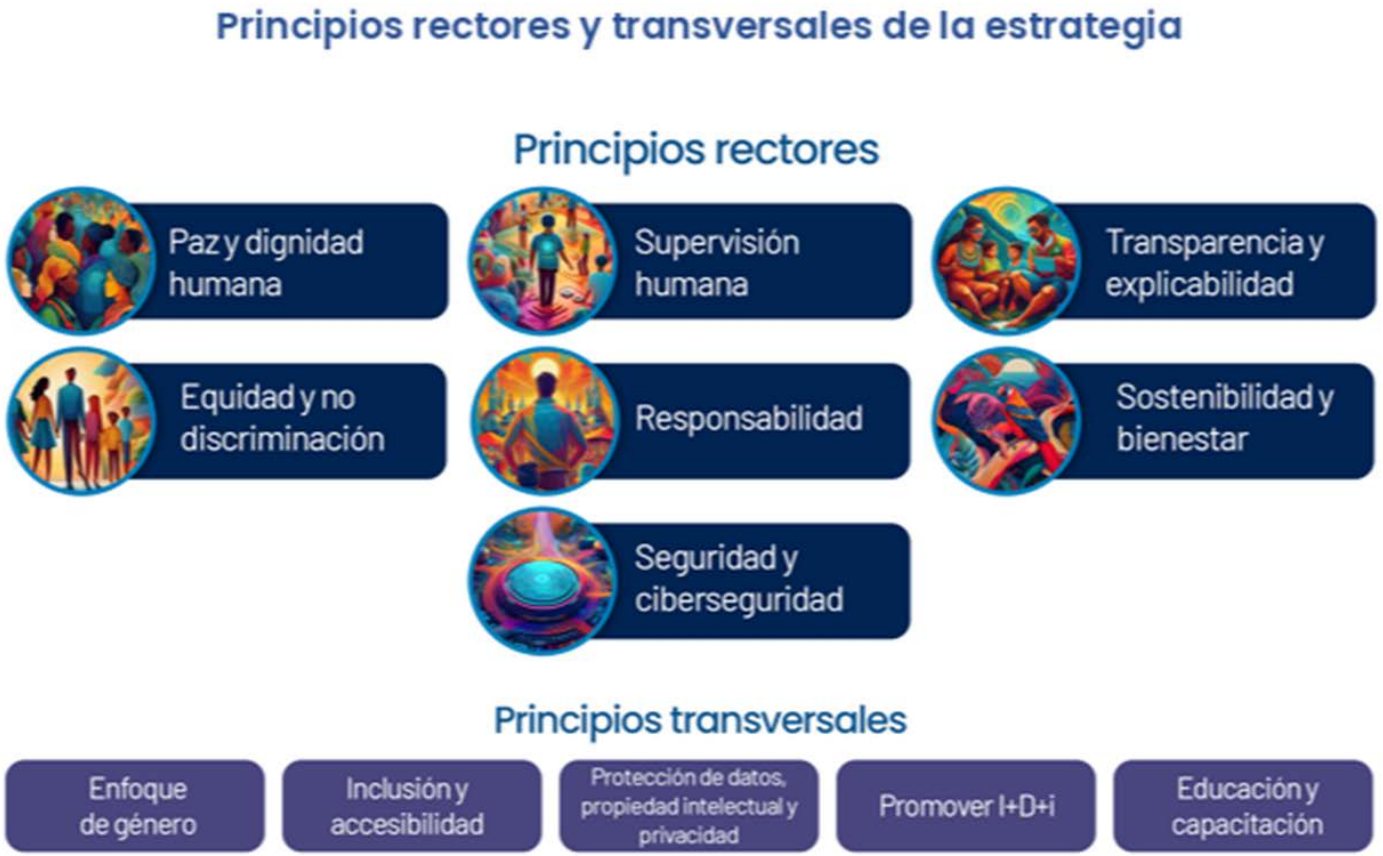
TECCOM 2025

AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES | GOBIERNO DE COSTA RICA

EDUCACIÓN CONTINUA CPIC

CPIC COLEGIO DE PROFESIONALES EN INFORMÁTICA Y COMPUTACIÓN

Estrategia Nacional de IA



Principios protección de datos

- ***Licitud***
  - Base legal
  - Disposiciones específicas del sector
  - Previsiones de contratos
  - Consentimiento informado
  - Deber de informar

- ***Finalidad****
  - Fines específicos, explícitos y legítimos
  - Indicación explícita de uso y finalidades de IA
  - No enfatizando datos sensibles
  - Prohibido cambiar la finalidad sin el consentimiento del titular.
  - Datos sin finalidad no deben existir
  - Reutilización: Anonimización, desvinculación, técnicas de privacidad diferencial o datos sintéticos

Principios protección de datos

- ***Transparencia-Explicabilidad****
  - Uso de datos
  - Usuarios comprendan cómo se usan sus datos y riesgos
  - Cómo funciona el algoritmo
  - Decisiones automatizadas.
  - Confiabilidad de las decisiones
  - Información completa, actualizada, oportuna, adecuada.

- . ***Calidad de la información***
  - Datos inexactos o incompletos pueden llevar a resultados discriminatorios o erróneos por parte de los algoritmos.
  - Revisión periódica de exactitud, veracidad y actualidad, generan predicciones acertadas o no.
  - Plazo de conservación
  - Ejercicio de derechos.

Principios protección de datos

- ***Principio de seguridad***
  - Adopción de medidas técnicas y organizativas adecuadas para proteger los datos personales contra el acceso no autorizado, la alteración, pérdida o destrucción.
  - Análisis de factores y acciones mínimas.
  - Interconexión de datos y efectos
  - Programa de capacitación y actualización

- ***Principio de Lealtad***
  - Prohibición de utilizar engaño, fraude para recolección
  - Intereses del titular y su bienestar
  - Titular debe poder revertir decisiones automatizadas y ejercicio de derechos

Principios protección de datos

- ***Principio de confidencialidad***
  - Mantener secreto de los datos a los que se tenga acceso y subsiste aunque se deje el cargo
  - Definición de roles y niveles de acceso
  - Definición de responsabilidades de intermediarios tecnológicos y de servicios y encargados
  - No es sinónimo de cumplimiento integral de la norma

- ***Minimización***
  - Recolectar lo necesario
  - Disminución de riesgos

*Responsabilidad proactiva**

- El responsable del tratamiento debe ser capaz de demostrar el cumplimiento de los principios y la normativa desde el diseño.
- Responsabilidad de decisiones
- Evaluación de impacto/ análisis de riesgos (sostenibilidad financiera)
- Registro de tratamiento, trazabilidad
- Mecanismos de auditoría de protección de datos.
- Generación de políticas exigibles, ejemplo de retención de modelos, datos de entrenamiento, borrado seguro, implementación de estándares, certificaciones y mecanismos de autorregulación, roles y responsabilidades, otros.
- Medidas técnicas y organizativas para proteger los datos. Ejemplo. Evaluar requerimiento de cifrado, control de acceso, auditorías de seguridad, ciberseguridad en el ciclo de vida de la IA

TECCOM 2025

AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES | GOBIERNO DE COSTA RICA

EDUCACIÓN CONTINUA CPIC

CPIC COLEGIO DE PROFESIONALES EN INFORMÁTICA Y COMPUTACIÓN

Principios protección de datos

- ***Principio de proporcionalidad***

  - Solo datos necesarios para finalidades formalizadas.
  - Uso de datos adecuados, pertinentes y relevantes a la finalidad
  - Análisis de mecanismos menos invasivos para lograr finalidades.
  - Evaluaciones de impacto previo pero también evaluaciones periódicas para analizar si continua siendo requeridos los datos
  - Busca proteger los derechos de los titulares, impactando de forma positiva y generando confianza.

Privacidad desde el Diseño y por Defecto

- Aplicable a todo el ciclo de vida del proyecto para garantizar la privacidad y seguridad.
  - **En Diseño:** Evaluación de impacto de privacidad para identificar riesgos antes de codificar. Sandbox
  - **Fase de Recolección de Datos:** determinación de métodos menos invasivos, Anonimización/seudonimización, aprendizaje federado, datos sintéticos.
  - **Fase de Entrenamiento:** Uso de técnicas de para proteger privacidad
  - **Fase de Despliegue:** Mecanismos de "explicabilidad" para entender decisiones algorítmicas, monitoreo continuo.
  - **Fase de actualización**: monitoreo constante para identificar sesgos

Observaciones finales

- La IA verdaderamente innovadora es aquella que respeta y protege a las personas y se convierte en un catalizador de la confianza al contar con salvaguardas sólidas y un uso ético de los datos.

- La PRODHAB tiene dentro de sus atribuciones el velar por el cumplimiento de la normativa y podemos ser un aliado para el desarrollo responsable de la IA, siempre que parta del marco de legalidad y de la privacidad desde el diseño

- La conformación de equipos interdisciplinarios es una estrategia crucial para disminuir los sesgos y fomentar una IA más ética, segura, justa, confiable, equitativa y beneficiosa para todos. Y debe procurar incluirse a todas las partes involucradas.

- Desarrollo de contratos o instrumentos jurídicos apropiados, que permitan supervisión de las partes intervinientes y la individualización de responsabilidades.

- Contar con un marco de gobernanza de los datos y códigos éticos.

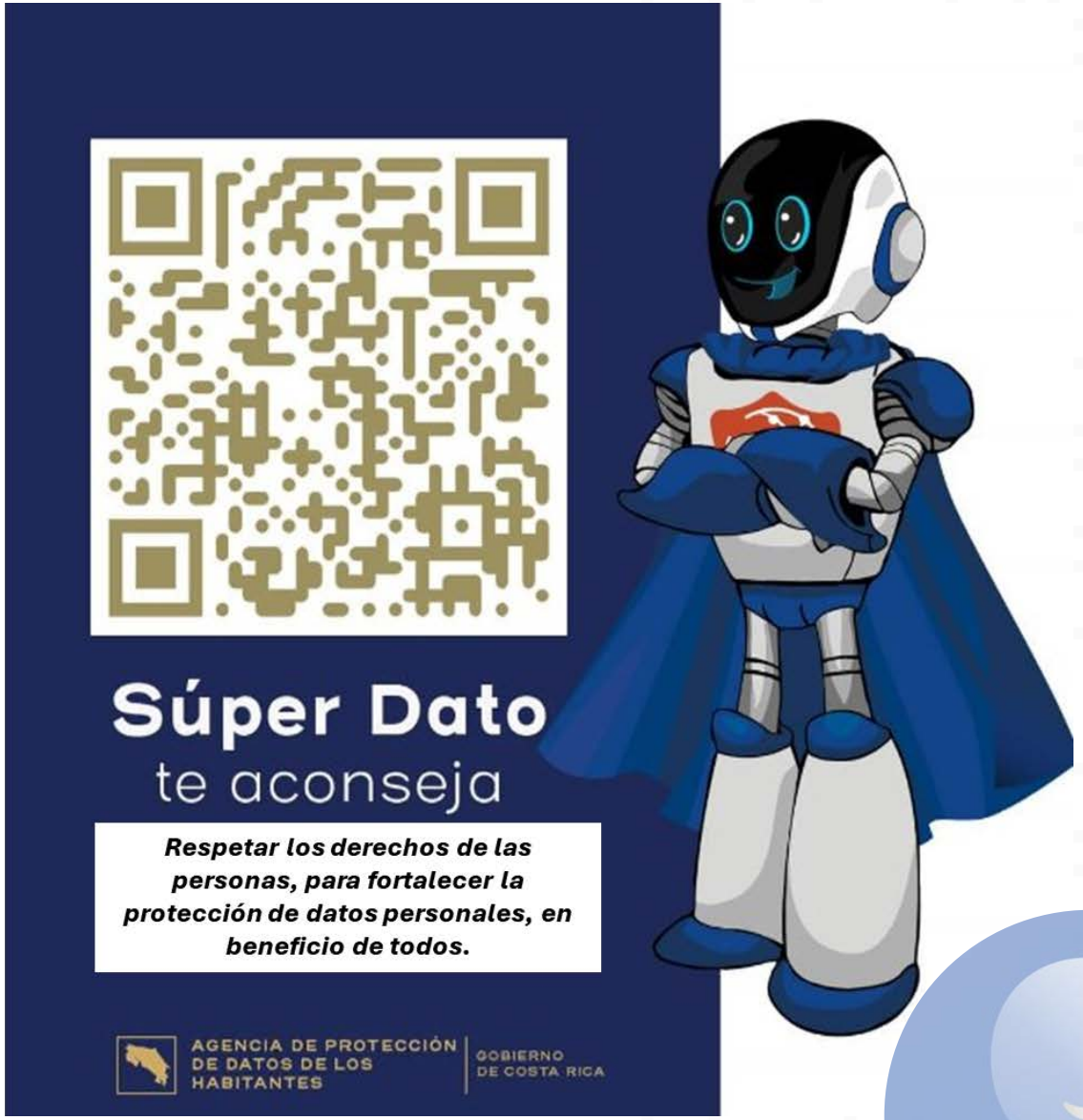
- Importancia de la formación continua .

- Consulta de guías
  - Recomendaciones Generales para el Tratamiento de Datos en Inteligencia Artificial- RIPD
  - Orientaciones Específicas para el Cumplimiento de los Principios y Derechos que Rigen la Protección de los Datos Personales en los Proyectos de Inteligencia-RIPD
  - Guía para entidades públicas y privadas en materia de Transparencia y Protección de Datos Personales para una Inteligencia Artificial responsable AAIP
  - Normas IA UE
  - Marco de gestión de riesgos de IA del NIS
  - OCDE, UNESCO, GPA

Fomentar la cultura de la protección de datos dentro del equipo.

TECCOM 2025

Muchas gracias!



EDUCACIÓN CONTINUA CPIC

CPIC
COLEGIO DE PROFESIONALES EN INFORMÁTICA Y COMPUTACIÓN