Cuaderno 1

Soberanía Digital en Uruguay

Apuntes para una agenda digital estratégica de desarrollo nacional

Pablo Salomón de León

Soberanía Digital en Uruguay:

Nuestro futuro tecnológico explicado en sencillo

Introducción

Vivimos tiempos en los que la claridad es un bien escaso. A veces parece que todo avanza tan rápido que apenas alcanzamos a comprender una tendencia y ya nos vemos arrastrados por ella. Y si alguna vez esta distancia fue peligrosa, es hoy, en plena revolución digital, cuando esa brecha puede definir la dignidad, la autonomía y hasta el destino de un país.

"Soberanía digital" es una expresión que, hace apenas una década, parecía reservada a foros internacionales, documentos técnicos y debates entre especialistas. Era un tema para gurúes, para funcionarios de organismos globales, para visionarios con tiempo para pensar el futuro. Hoy, sin embargo, recorre los medios, aparece en la sobremesa familiar, en la charla con los colegas, y –aunque sea de forma sutil– empieza a tocar el corazón de quienes deciden, enseñan, emprenden o, simplemente, buscan vivir sin depender del capricho de otros.

Déjeme, lector, que arranque desde lo cotidiano, como me gusta a mí, desde lo que cualquiera puede ver y sentir si se detiene un minuto en el día a día. Es lunes en Montevideo. El mate calienta la mano, la radio repite una noticia del exterior y, mientras la ciudad despabila, el celular

vibra con notificaciones: quizás mensajes de la familia, recordatorios de una agenda digital, un aviso de que una factura se puede pagar en línea, un resumen de noticias que alguien reenvió por WhatsApp. Un padre recibe el boletín digital del liceo de su hijo, una abuela revisa desde su tablet si el pago de su jubilación está disponible, y un joven repasa un tutorial de matemática antes de salir a trabajar. Si alguna vez pensó que todo esto "no tiene nada que ver conmigo", lo invito a reconsiderarlo.

Porque lo digital, aunque no lo veamos ni lo toquemos, es el nuevo suelo que pisamos. Sostiene la vida diaria con una discreción casi absoluta. No exagero: en menos de una generación, pasamos del sobre de papel a la firma electrónica, del almacén del barrio a la pasarela de pagos digital, de la libreta escolar al diploma en PDF. Hace no mucho, un trámite requería perder una tarde entre oficinas; hoy, el documento llega por correo electrónico o se descarga desde una web.

Ahora, haga el ejercicio de imaginar por un momento que ese entramado –ese tejido invisible que hoy damos por sentado– estuviera en manos de otros, sometido a reglas ajenas, o incluso amenazado por decisiones que se toman a miles de kilómetros, sin voz ni voto de nuestra parte. Imagine que, de la noche a la mañana, alguien apaga el interruptor y dejamos de poder acceder a la plataforma educativa, a la información de salud, a los registros civiles, o a la posibilidad de transferir nuestro propio dinero. No se trata de ciencia ficción ni de una visión catastrofista; es una posibilidad tan concreta que ya ha sido advertida por expertos una y otra vez, pero rara vez se traduce en términos comprensibles para la mayoría.

Eso es lo que me propongo en este cuaderno: no sembrar alarma, sino invitar a la reflexión y, sobre todo, a la acción informada. Lo digital no es un lujo ni una moda pasajera: es el campo de batalla donde hoy se juegan los derechos, las oportunidades, la equidad y, ni más ni

menos, la identidad nacional. Soberanía, en este contexto, no significa cerrarse al mundo ni temerle a lo nuevo, sino ser capaces de decidir sobre lo que nos pertenece, construir soluciones propias y defenderlas con cabeza fría y corazón dispuesto.

De la energía eléctrica al control digital

Recuerdo, años atrás, una conversación con un colega mientras el país avanzaba en migrar sistemas estatales a la nube y a servicios digitales globales. Él me preguntó si no era mejor mover todo "al exterior", porque sonaba más eficiente, moderno y, según muchos, inevitable. Le respondí entonces –y lo sigo diciendo hoy– con una comparación muy simple: *"Imaginá que todo el sistema eléctrico del país dependiera de una llave que no está en Uruguay. ¿Cuánto tiempo tardaríamos en preocuparnos por el control, la calidad y el acceso?"*

En aquel momento la comparación sonaba exagerada. Hoy, es tan obvia que asombra que siga siendo necesario explicarla. Si la infraestructura digital está fuera de nuestro alcance, también lo está nuestra capacidad de respuesta ante cualquier crisis. Y cuando dependemos de lo que decidan otros, perdemos algo más que comodidad: resignamos autonomía, libertad y hasta la dignidad de poder defender nuestros propios intereses.

La soberanía digital empieza en lo pequeño

No se trata solo de cables, centros de datos o servidores. La soberanía digital se construye, como todo lo que perdura, desde lo pequeño: elegir plataformas que prioricen la privacidad, participar en debates públicos sobre datos personales, enseñar a los más chicos a distinguir una noticia falsa de un comunicado oficial. Va mucho más allá del código fuente o de los cables submarinos: es cultura, es política, es educación y es ética.

Y, sobre todo, es una responsabilidad compartida. No escribo estas páginas para expertos ni para técnicos. Quiero que sean útiles para el docente que busca entender por qué vale la pena usar software libre en la escuela, para la madre que se preocupa por la privacidad de sus hijos en las redes sociales, para el emprendedor que quiere diversificar sus herramientas sin quedar atado a un solo proveedor, para el jubilado que –con esfuerzo– aprende a leer el diario digital y no quiere ser víctima de un fraude bancario. La soberanía digital atraviesa todas esas realidades, porque, en el fondo, es la suma de pequeñas decisiones cotidianas las que, al final del día, marcan la diferencia.

He visto muchas veces cómo se subestima el valor de lo local. En cada charla, taller o encuentro en barrios y escuelas, la pregunta se repite: "¿No es mejor usar lo que ya existe, lo que nos dan las grandes empresas?" Mi respuesta, siempre, es la misma: depende para qué, y cómo se use. No se trata de rechazar la innovación ni de ignorar los avances globales. Se trata de entender que cada país –y cada comunidad– tiene particularidades, modos de hablar, necesidades y problemas que solo pueden resolverse mirando hacia adentro, antes que hacia afuera.

Y lo cierto es que ejemplos sobran. El Plan Ceibal, la red de fibra óptica al hogar, las plataformas de trámites en línea, los centros de datos nacionales. Todos esos logros fueron posibles porque hubo decisión política, convicción colectiva y una apuesta –muchas veces contracorriente– por lo propio. ¿Se cometieron errores, hubo demoras y dificultades? Por supuesto. Pero los beneficios permanecen, y hoy permiten que Uruguay sea un referente en inclusión digital, con desafíos pendientes, sí, pero también con fortalezas que ningún país puede darse el lujo de subestimar.

Permítame, lector, compartirle tres ideas clave que orientan este cuaderno desde el principio.

Primera: la soberanía se construye en el día a día. No alcanza con leyes ni con centros de datos imponentes. Hace falta que cada persona –cada uruguayo y uruguaya– entienda, aunque sea en términos básicos, por qué importa saber dónde van sus datos, quién los procesa y qué se hace con ellos.

Segunda: el talento local es la mayor garantía de autonomía. He sido testigo –y parte– de proyectos que nacieron con recursos modestos, pero con voluntad y creatividad extraordinarias. Desde laboratorios escolares hasta pequeñas iniciativas barriales, la inteligencia artificial, la ciberseguridad y el software hecho en Uruguay ya existen y pueden escalar. No necesitamos esperar a que nos "salve" la próxima gran innovación extranjera: podemos construir desde acá, con lo que tenemos, y mejorar paso a paso.

Tercera: soberanía no es lo mismo que aislamiento. No se trata de levantar muros ni de mirar con desconfianza a todo lo que viene de afuera. Se trata, más bien, de establecer reglas propias, de colaborar desde una posición de fuerza y dignidad, y de ser capaces de elegir cuándo y cómo compartir nuestros recursos, nuestro conocimiento y nuestros datos. Soberano no es quien se encierra, sino quien decide con libertad y con información.

El papel de la ciudadanía y la cultura digital

Lo digital –como la energía eléctrica– es parte de nuestra vida diaria. Pero, a diferencia de la luz, cuya falta se nota de inmediato, los problemas de soberanía digital pueden pasar desapercibidos hasta que es tarde. Una plataforma que cambia sus reglas de un día para el otro; una aplicación que decide limitar el acceso desde Uruguay; una fuga de datos personales que termina explotada fuera de nuestro control. No son amenazas teóricas: son escenarios posibles que otros países ya han vivido.

Por eso, la soberanía digital es, antes que nada, una cultura. Es saber hacer preguntas, exigir transparencia, participar en la discusión pública. Es enseñar en familia y en la escuela por qué una contraseña robusta es importante; es elegir servicios nacionales cuando sea posible; es no resignar el control a cambio de una falsa comodidad.

Y es, también, aprender a ver el futuro. Me gusta pensar que la verdadera inteligencia no es saber muchas cosas, sino ver lo que viene, prepararse para los cambios y actuar a tiempo. Si usted logra, leyendo este cuaderno, adelantarse a los problemas y fortalecer su entorno –personal, familiar, profesional– el esfuerzo estará más que justificado.

Lo local, lo global y el desafío de la inteligencia artificial

Los avances de Uruguay no son menores. Ser parte del grupo Digital 9, haber llevado la fibra óptica a casi todo el país, haber creado una identidad digital robusta y tener una Estrategia Nacional de Inteligencia Artificial son hechos concretos. Pero –y aquí hago un quiebre– el desafío de la soberanía digital no termina en la infraestructura ni en las leyes: está en el control de los algoritmos, en la capacidad de auditar y decidir cómo usamos la inteligencia artificial.

Hoy el mundo enfrenta una nueva ola de dependencia: los modelos de inteligencia artificial que procesan información pública, educativa, sanitaria y financiera suelen ser entrenados en contextos, lenguas y valores ajenos. Uruguay tiene la oportunidad –y la obligación– de dar un paso más y comenzar a desarrollar modelos propios, alineados con sus intereses, su cultura y sus necesidades.

No se trata de rechazar la colaboración ni de aislarnos, sino de construir una base nacional que nos permita elegir, negociar y –cuando sea necesario– defendernos con dignidad y eficacia.

Llamado al lector

Quisiera, en este punto, hacerle una invitación: tome este cuaderno como una herramienta flexible, no como una sentencia cerrada. Está escrito para ser subrayado, comentado, adaptado y compartido. Cada capítulo terminará con propuestas prácticas, enlaces útiles y preguntas para debatir. Siéntase libre de discutir, criticar y mejorar lo que aquí se plantea. Así se construye la soberanía: en comunidad, con diálogo y con espíritu crítico.

Habrá quienes digan que es imposible competir con las grandes empresas tecnológicas, que nuestro aporte es marginal, o que la tendencia global es irreversible. Respeto esas posiciones. Pero, en lo personal, prefiero apostar por el esfuerzo propio, por la suma de pequeñas acciones que, juntas, pueden torcer el rumbo de los acontecimientos. Vale más un gramo de hacer que un kilo de decir. Lo repito a diario y aquí lo dejo escrito: en la soberanía digital, la acción concreta –por pequeña que sea– pesa más que el discurso vacío.

El camino no está libre de obstáculos. Hay barreras técnicas, legales, económicas y culturales. Construir centros de datos, formar técnicos, actualizar leyes y promover la participación ciudadana requiere recursos y tiempo. Pero los desafíos no deben servir de excusa para la inacción. Cada paso cuenta: desde elegir una contraseña robusta hasta exigir transparencia en el uso de datos públicos, desde enseñar a los más jóvenes a reconocer un intento de phishing hasta impulsar políticas que protejan el interés nacional.

A lo largo de este cuaderno, analizaremos lo que ya se hizo bien –y lo que falta por mejorar–, sin complacencia pero también sin caer en el pesimismo. Hablaremos de amenazas y riesgos, sí, pero sobre todo de oportunidades: cómo transformar la resiliencia en una fortaleza, cómo

usar la inteligencia artificial y el blockchain para el bien común, cómo construir una ciudadanía digital informada y protagonista.

Este es un llamado, no a la resignación, sino a la construcción colectiva de un futuro en el que Uruguay sea dueño de su destino digital.

La soberanía digital no es un plan lejano ni una consigna para especialistas. Es, desde ahora, una agenda de supervivencia y de dignidad. Cada página que sigue es una invitación a participar, a preguntarse y a actuar.

Le propongo, entonces, un pacto sencillo: imaginar un Uruguay donde el algoritmo no sea una amenaza lejana, sino un recurso al servicio de todos. Donde el conocimiento circule libremente, pero bajo reglas que el país mismo decide. Donde la nube no sea solo de otros, sino también nuestra, construida y protegida por y para los uruguayos.

Al final de este cuaderno, probablemente tendrá más preguntas que respuestas. Y está bien que así sea. Porque la soberanía digital es un proceso, no un punto de llegada. Un desafío que se renueva cada día, en cada acto y en cada decisión.

Lo invito a abrir la siguiente página y recorrer juntos este viaje. No hay fórmulas mágicas ni atajos, pero sí caminos posibles. El primer paso, siempre, es informarse y participar.

Bienvenido.
Empecemos juntos este recorrido.

— Pablo Salomón de León

Capítulo 1

Soberanía digital en Uruguay: del ejemplo regional al desafío de la inteligencia artificial nacional

Vivimos en un país que ha sabido desafiar la lógica de las periferias y la dependencia, aun siendo pequeño en territorio y población. Uruguay, desde hace más de una década, se convirtió en referencia regional y global en políticas digitales, inclusión tecnológica, infraestructura de conectividad y ciudadanía digital. Muchos países, incluso del primer mundo, han venido a mirar lo que aquí se logró, con recursos limitados pero con visión y perseverancia. Pero la historia de la soberanía digital uruguaya no termina en la conectividad: apenas está por empezar su capítulo más desafiante, el de la autonomía en inteligencia artificial.

1.1 ¿Qué significa "soberanía digital" y por qué importa hoy?

Cuando hablo de soberanía digital, no me refiero solo a tener fibra óptica, acceso a internet y trámites en línea. Soberanía es, ante todo, **la capacidad real de decidir, gestionar y proteger nuestros datos, nuestras infraestructuras críticas y, cada vez más, los algoritmos que dan forma a nuestra vida social, política y económica**. Significa tener poder de elección: que si mañana cambian las reglas de juego en el mundo, Uruguay no quede a merced de lo que decidan en un consejo directivo de una multinacional o en el despacho de un funcionario extranjero.

La soberanía digital, en este sentido, es tan importante como la seguridad energética, la gestión del agua o la defensa nacional. No se trata de autarquía, sino de **reducir riesgos, ganar margen de maniobra y poder responder ante crisis o amenazas externas sin quedar paralizados ni hipotecar el futuro**.

1.2 Uruguay: un modelo avanzado en América Latina

Basta mirar los datos: Uruguay es líder regional en gobierno digital, siendo parte del exclusivo grupo Digital 9 junto a potencias como Estonia, Israel y Reino Unido. Nuestra penetración de internet supera el 90%, la cobertura de banda ancha móvil es de las más altas del continente, y el Plan Ceibal sigue siendo motivo de orgullo y estudio en el mundo entero.

Esta base no es solo tecnológica: es también institucional. Hemos avanzado en legislación de datos personales, creación de agencias especializadas y promoción de la participación ciudadana. Uruguay aprobó su Estrategia Nacional de Inteligencia Artificial (2024–2030) y la Estrategia Nacional de Ciberseguridad, sentando bases firmes para el futuro.

Pero —y aquí está el punto de quiebre— la soberanía digital no es estática.
Lo que nos trajo hasta aquí no nos garantiza el control en la próxima ola tecnológica. La inteligencia artificial representa ese nuevo escalón: un cambio de paradigma que puede profundizar nuestra autonomía… o abrir nuevas dependencias.

1.3 De la infraestructura al algoritmo: un nuevo territorio para la soberanía

Durante mucho tiempo, la discusión fue "¿quién maneja los cables, los servidores, los centros de datos?". Hoy la pregunta es "¿quién decide cómo funcionan los algoritmos que gestionan información pública, educación, salud, seguridad, y hasta la interpretación de nuestras leyes?"

La infraestructura importa, pero el software —y en especial la inteligencia artificial— determina cada vez más qué podemos hacer, cómo lo hacemos, y bajo qué condiciones.

No es lo mismo que la base de datos de una escuela esté alojada en Montevideo que en un país extranjero; pero tampoco es lo mismo usar un sistema de recomendación educativo hecho para escuelas de Texas, que uno creado con la realidad uruguaya en mente.

Los algoritmos importan porque contienen una visión del mundo. Si esos algoritmos se entrenan solo con datos extranjeros, reflejarán prioridades, prejuicios y valores ajenos. Por eso, la soberanía digital en 2025 es también —y sobre todo— **soberanía algorítmica**.

1.4 Uruguay, ejemplo real: lo que se ha logrado

Mucho se ha escrito sobre los hitos de Uruguay en gobierno digital. Aquí algunos puntos a destacar:

- **Digital 9 (D9):** Uruguay es el único país latinoamericano en esta red, que reúne a los países con los gobiernos digitales más avanzados.
- **Plan Ceibal:** Educación digital inclusiva desde 2007. Todos los estudiantes de primaria y buena parte de secundaria cuentan con dispositivos y acceso.
- **Cobertura de internet:** 93% de la población conectada; 92,3% de cobertura móvil.
- **Marco normativo:** Ley de protección de datos personales, agencias de ciberseguridad, participación en estándares internacionales.
- **Estrategia de IA:** Aprobada en 2024, marca el rumbo para el desarrollo responsable, ético y propio de inteligencia artificial.

Este avance no es menor. Nos permitió transitar la pandemia con servicios digitales sólidos, bancarizar a la población, reducir la brecha educativa, y fomentar el desarrollo de startups tecnológicas.

Pero —y esto hay que decirlo con claridad—, lo más difícil está por venir.

1.5 La trampa de la dependencia: lecciones para el futuro

Uruguay se ha beneficiado de la apertura y la colaboración internacional. Pero eso tiene riesgos:

- **Dependencia de plataformas extranjeras:** Muchos servicios críticos funcionan en nubes o sistemas globales. Un cambio de política, una sanción o un conflicto internacional puede dejar fuera de servicio trámites, registros o servicios básicos.
- **Fuga de datos:** Cada vez que usamos plataformas no auditadas ni controladas localmente, nuestros datos pueden terminar siendo explotados comercial o políticamente.
- **Sesgos y agendas ajenas:** Si el software que usamos para la educación, la salud o la justicia está diseñado con valores, prioridades o normas externas, nuestros procesos y decisiones pueden ser influenciados, aún sin darnos cuenta.

Aquí la analogía con la energía eléctrica es directa: ningún país dejaría la gestión de su red energética en manos exclusivas de una multinacional extranjera, por eficiente que fuera. En lo digital, tampoco podemos resignar el control de los algoritmos que procesan información nacional sensible.

1.6 El salto a la inteligencia artificial nacional: ¿por qué y para qué?

El debate internacional ya no es "si" los países deben desarrollar inteligencia artificial propia, sino "cómo" y "cuándo" hacerlo. En mi experiencia —y aquí lo pongo en primera persona—, entrenar pequeños modelos, como "Celestito01" y "Celestito02", fue una

forma de demostrar que **sí se puede** empezar desde abajo, incluso en casa, con recursos limitados pero con mucha curiosidad y disciplina.

Celestito01 alcanzó unos 400 parámetros; Celestito02 escaló a más de 2.200 parámetros, con 70.000 filas de datos por 10 columnas. No es un prodigio técnico, ni aspira a serlo. Es un experimento que muestra el valor de la experiencia directa: **es posible entender, adaptar y crear modelos ajustados a nuestras propias necesidades**. La lección es clara: si podemos hacerlo en casa, el país puede —y debe— hacerlo en equipo, con visión y políticas de Estado.

¿Por qué apostar a la IA nacional?

- **Autonomía:** Decidir cómo funcionan los algoritmos que rigen servicios críticos, sin depender de empresas o gobiernos extranjeros.
- **Identidad y contexto:** Adaptar los sistemas a la realidad uruguaya, con datos propios, lenguaje propio y prioridades nacionales.
- **Seguridad:** Minimizar riesgos de filtraciones, usos indebidos o manipulación de datos sensibles.
- **Innovación y desarrollo:** Generar empleo, conocimiento y empresas tecnológicas propias que no solo consuman, sino que creen.

1.7 El desafío ético y social

La soberanía digital no es solo técnica. Implica debates sobre privacidad, derechos, valores sociales y ética. ¿Qué datos estamos dispuestos a compartir? ¿Cómo se protege a las minorías frente a algoritmos entrenados en contextos diferentes? ¿Quién supervisa y audita el funcionamiento de los sistemas?

La Estrategia Nacional de IA de Uruguay contempla estos desafíos. Promueve una IA ética, inclusiva y responsable. Pero queda mucho por hacer: capacitar a los funcionarios, educar a la población, fortalecer la auditoría y el control social.

1.8 El rol de la ciudadanía y del Estado

La soberanía digital no es un asunto solo de técnicos o de burócratas. Cada ciudadano puede —y debe— informarse, exigir transparencia y participar en las discusiones sobre tecnología.

El Estado, por su parte, tiene la obligación de invertir, regular, fomentar la investigación y proteger el interés nacional.

Algunas acciones concretas:

- **Favorecer software y servicios auditables y locales** en la educación, la salud y la gestión pública.
- **Promover alianzas público-privadas** que prioricen el desarrollo de talento nacional.
- **Apoyar proyectos de IA experimental** en universidades, empresas y sociedad civil.
- **Garantizar el acceso y la capacitación en competencias digitales** para todos los uruguayos.

1.9 El futuro es ahora

Uruguay está en un momento bisagra. Tenemos una base tecnológica e institucional sólida, pero el desafío ahora es no quedar rezagados en la carrera de la inteligencia artificial. Nuestra soberanía digital no será total mientras los modelos que determinan el acceso, la equidad y la seguridad dependan de algoritmos diseñados en el norte global.

Hoy podemos ser líderes no solo en conectividad, sino también en autonomía algorítmica. Podemos construir soluciones propias, auditar lo que usamos, y abrir caminos para que la IA sea una herramienta de desarrollo nacional, alineada con nuestros valores y necesidades. ***¡Vale más un gramo de hacer que un kilo de decir!***

Capítulo 2

De la posta a la fibra: hitos y lecciones del Uruguay tecnológico

---

2.1 Un país pequeño que piensa en grande

A lo largo del siglo XX, Uruguay forjó una identidad nacional sustentada en la educación pública, políticas sociales avanzadas y una vocación de anticiparse a su tiempo: fuimos pioneros en legislar las ocho horas laborales y en consolidar una enseñanza laica, gratuita y obligatoria. Esta pulsión modernizadora encontró su continuidad natural en la revolución digital. Este capítulo recorre los hitos que, desde los años noventa hasta hoy, posicionaron al país como referente regional en inclusión tecnológica, sin ocultar tropiezos ni desafíos pendientes. La intención es doble: mostrar por qué —y cómo— construimos ventajas que hoy alimentan la soberanía digital, y extraer lecciones para no confiarlo todo al piloto automático.

2.2 Primeras señales: Internet llega al Río de la Plata (1994-2000)

En 1994, ANTEL lanzó su primer servicio de acceso conmutado a Internet; el famoso módem de 14.400 bps se transformó en el símbolo de una puerta recién abierta. En 1997 nació Adinet, el primer

proveedor masivo, y poco después surgieron los primeros portales .uy.
Aquella etapa pionera, aunque limitada en ancho de banda, sembró dos elementos clave:

1. **Presencia temprana del Estado como garante:** la empresa pública asumió el rol de proveer conectividad básica con tarifas reguladas.
2. **Cultura de comunidad técnica:** universidades, clubes de ciencia y los primeros cibercafés establecieron redes de colaboración que serían vitales para proyectos futuros.

A comienzos de 2001, Uruguay superaba el medio millón de usuarios de Internet —más del 15% de la población, cifra notable para la región.

2.3 Plan Ceibal (2007): la apuesta educativa que reescribió la historia

Si hubiera que elegir un hito que sintetiza la visión social de la tecnología en Uruguay, ése sería el Plan Ceibal. Inspirado en la iniciativa "One Laptop per Child", se propuso algo que sonaba descabellado: entregar una computadora portátil a cada alumno y maestro de la escuela pública.

Las críticas iniciales abundaban: "¿No sería mejor invertir en más maestros?". Pero la ejecución demostró que una cosa no excluía la otra:

- **Cobertura universal:** en menos de cuatro años se distribuyeron más de 380.000 XO.
- **Red de conectividad escolar:** cada centro educativo recibió acceso a Internet; muchas zonas rurales se conectaron por primera vez gracias a enlaces satelitales.
- **Material local:** surgieron contenidos curriculares en castellano y, más tarde, en lengua de señas, guaraní y portuñol.

La lección mayor de Ceibal fue política: una decisión presidencial respaldada por consenso parlamentario y social puede mover montañas. Desde el punto de vista de soberanía, Ceibal demostró que el Estado no solo compra tecnología, sino que puede gestar un ecosistema completo —soporte, contenidos, evaluación— bajo control nacional.

2.4 Fibra óptica al hogar (2011-2018): el salto de infraestructura

Uruguay volvió a sorprender cuando ANTEL anunció el plan de sustituir progresivamente la vieja red de cobre por FTTH (Fiber to the Home). Hubo escépticos: "¿Para qué tanta velocidad si apenas usamos correo y redes sociales?"
La respuesta se vio en tres frentes:

1. **Velocidades simétricas:** permitieron que pequeñas empresas exportaran software desde apartamentos ubicado, por ejemplo, en el barrio Cordón.
2. **Videoconsulta médica y educación a distancia:** se volvieron viables mucho antes de la pandemia.
3. **Atracción de datacenters extranjeros:** compañías regionales eligieron Montevideo por la baja latencia y la estabilidad eléctrica.

Para 2020, más del 85% de los hogares contaban con fibra; hoy la cifra ronda el 92%, ubicando a Uruguay al nivel de Corea del Sur en penetración. Este despliegue no solo potenció la economía, sino que consolidó infraestructura crítica bajo titularidad estatal, factor decisivo en tiempos de guerras de cables submarinos y sanciones globales.

2.5 AGESIC de la identidad digital a la inteligencia artificial (2008-presente)

La Agencia de Gobierno Electrónico y Sociedad de la Información (AGESIC) nació con dos mandatos: simplificar trámites y garantizar la seguridad de la información pública. Su legado incluye:

La **Agencia de Gobierno Electrónico y Sociedad de la Información** nació con un doble mandato: simplificar trámites y proteger la información pública. En menos de dos décadas construyó los pilares de la república digital:

- **Portal gub.uy**: más de 2 500 trámites en línea.
- **Cédula de Identidad Electrónica**: cada uruguayo puede firmar documentos digitales con validez legal.
- **Marco normativo sólido**: Ley 18 331 de protección de datos (2008) y decretos de interoperabilidad, firma y seguridad.

Ese legado dotó al Estado de eficiencia y a la ciudadanía de comodidad, generando confianza en plataformas propias: desde exámenes médicos remotos hasta sesiones parlamentarias híbridas.

Con la infraestructura madura, AGESIC amplió su agenda. En 2024 presentó el primer **informe nacional sobre regulación de IA**, tras

consultas públicas y talleres con expertos. El documento sienta las bases de una **ley-marco de IA** que:

1. **Incorpora principios éticos** —transparencia, explicabilidad y rendición de cuentas— como obligación para todo sistema que maneje datos ciudadanos.
2. **Propone un Comité Nacional de IA** para auditar algoritmos críticos y actualizar la norma cada dos años.
3. **Garantiza la portabilidad y la privacidad**, alineando la innovación con los derechos fundamentales.
4. **Refuerza capacidades estatales**, con becas y posgrados para formar auditores y desarrolladores locales.

El borrador legal, en redacción interministerial a fines de 2025, consolida la idea de que **soberanía digital no es solo infraestructura: es también gobernar la inteligencia que corre sobre esa infraestructura**. Cuando la norma entre en vigor, Uruguay integrará, en un mismo cuerpo, identidad digital, protección de datos y gobernanza de IA, reforzando la confianza en su ecosistema tecnológico propio antes que en soluciones extranjeras.

2.6 El Data Center de Pando (2016): datos al amparo de leyes uruguayas

ANTEL inauguró en 2016 un complejo de 12.000 m² con certificación Tier III+. Su importancia excede lo técnico:

- **Aloja información crítica** de ministerios y empresas privadas que prefieren jurisdicción local.
- **Nodo de intercambio regional:** conecta rutas hacia Paraguay y sur de Brasil, reduciendo latencia.

- **Laboratorio de virtualización:** se prueban soluciones de IA ligadas a salud y agro.

Alojar datos dentro de fronteras significa que cualquier litigio se resuelve bajo la ley uruguaya y que los procedimientos de acceso quedan sujetos a nuestra constitución.

2.7 Red Ibirapitá (2015): inclusión senior y desafío cultural

Si Ceibal democratizó la infancia, Ibirapitá hizo lo propio con los adultos mayores: entrega de tablets, capacitación y soporte gratuitos. El programa demostró que la inclusión no termina a los 18 años: más de 250.000 jubilados aprendieron a realizar videollamadas con nietos, pagar facturas y leer prensa en línea.

Desde la perspectiva de la soberanía digital, esto significa ensanchar la base de usuarios críticos: un abuelo que distingue un correo oficial de un intento de fraude es la mejor defensa contra el cibercrimen.

2.8 La parada obligatoria: ¿qué falta por hacer?

Brecha rural persistente:
Aunque la fibra cubre la mayoría de las localidades, aún existen zonas de sierra o cuchilla donde la señal es satelital y costosa.

Ciberseguridad a medio camino:
El CERTuy atiende incidentes crecientes, pero requiere más presupuesto y especialización, especialmente en análisis forense y respuesta a ransomware.

Monopolio selectivo de plataformas:
El comercio electrónico pivota sobre pasarelas foráneas; la cultura

digital circula en redes globales cuyas políticas no consideran el contexto nacional.

Talento en fuga:
Ingenieros formados por Ceibal y universidades terminan contratados por multinacionales remotas. Uruguay debe retener capital humano con desafíos y salarios competitivos.

2.9 Cuatro lecciones estratégicas

1. **Voluntad política sostenida vence el escepticismo:**
   Ceibal y Fibra fueron posibles porque gobiernos de distinto signo mantuvieron el rumbo.
2. **Infraestructura + alfabetización = valor real:**
   No basta con cables; se precisan docentes y campañas que enseñen a usarlos.
3. **Modelo estatal-privado híbrido:**
   ANTEL lidera, pero abre sus redes a operadores; el Data Center aloja tanto a ministerios como a startups.
4. **Pequeños proyectos, gran demostración:**
   Un asistente local como CELESTITO prueba que Uruguay puede producir IA pertinente sin presupuestos de Big Tech.

2.10 Camino a 2040: de usuarios a productores

Para la próxima década, el reto no es solo mantener lo ganado, sino multiplicar la capacidad de producción tecnológica propia. ¿Cómo?

- **Clusters de IA y biotecnología** con incentivos para exportar servicios de alto valor agregado.

- **Licencias públicas y repositorios**: el software estatal liberado para que liceos y cooperativas lo adapten.
- **Compre público innovador:** cada licitación debería premiar soluciones que transfieran conocimiento al país.
- **Certificación de ciberseguridad nacional:** sello "Hecho en Uruguay, auditado en Uruguay".

2.11 Cierre: un pacto implícito en clave celeste

Cada hito repasa un hilo común: educación, Estado y ciudadanía empujan juntos. Ese pacto no está escrito; se revalida cada vez que un docente actualiza material en CREA, que un jubilado envía un mensaje por Ibirapitá, o que un técnico revisa la temperatura de los racks en Pando a las tres de la mañana.

Soberanía digital, en Uruguay, empezó siendo una idea generosa y hoy se traduce en prácticas diarias.

Pero ningún logro es irreversible. Así como un vendaval puede voltear un puente, un cambio geopolítico o un ciberataque masivo podría comprometer décadas de avance. Por eso este cuaderno insiste: **conocer la ruta recorrida es tan urgente como imaginar la próxima**.

En el capítulo siguiente, exploraremos los riesgos que acechan —desde el ransomware a la desinformación— y las estrategias para blindar el camino que hemos abierto.

Capítulo 3

La nueva frontera: amenazas y desafíos a la soberanía digital uruguaya

3.1 De los corsarios al ransomware: cómo cambió el mapa de riesgos

Si algo nos enseñó la historia nacional, es que la palabra "amenaza" siempre estuvo presente, aunque su rostro cambió con el tiempo. En tiempos de Artigas, las amenazas eran tangibles: un destacamento enemigo cruzando el río, una flotilla portuguesa bloqueando el puerto, el enemigo a la vista. Hoy, la soberanía enfrenta otro tipo de frontera: invisible, virtual, impredecible. Basta que un atacante pulse Enter desde cualquier huso horario para paralizar un ministerio, secuestrar la base de datos de un hospital o manipular la conversación pública en redes sociales.

La soberanía digital, ese "patio trasero" que se extiende más allá de los límites físicos, nos vuelve tan vulnerables como cualquier país con mayores recursos. Este capítulo no busca sembrar miedo, sino demostrar que cada riesgo es también un aviso y una tarea pendiente: cada punto débil marca dónde invertir, a quién capacitar, qué norma reformar o qué práctica revisar. Al final, propongo un kit de supervivencia nacional que combina tecnología, educación, ley y cooperación internacional.

3.2 Ataques directos a infraestructuras críticas

La informatización de los sistemas que garantizan luz, agua, transporte y salud nos dio eficiencia… y superficie de ataque. Los ejemplos internacionales abundan: en 2021, el oleoducto Colonial en EE.UU. fue detenido por ransomware; hospitales europeos sufrieron colapsos similares en años recientes. Uruguay, con una red eléctrica casi 100% digitalizada y un sistema único de historias clínicas electrónicas, no es demasiado pequeño como para pasar desapercibido; por el contrario, su alta conectividad lo convierte en un objetivo atractivo para grupos criminales que buscan grietas fáciles.

El vector típico suele ser un simple phishing: roba credenciales de un técnico y, desde ahí, se mueve lateralmente hasta los servidores OT (Operational Technology). El impacto potencial puede ir desde apagones en barrios enteros, incidentes en estaciones de bombeo de agua o fugas masivas de datos de pacientes. La lección es clara: la ciberseguridad OT debe tener el mismo presupuesto y atención que el mantenimiento mecánico tradicional. Sin ello, la turbina más robusta puede quedar inutilizada por un simple script.

3.3 Dependencia monopólica: el riesgo silencioso

Hay amenazas que no llegan con sirenas ni alarmas rojas, sino disfrazadas de comodidad. Uruguay, como la mayoría del mundo, confía su nube pública, mensajería, pasarelas de pagos y hasta la analítica escolar a cuatro o cinco conglomerados globales. Mientras todo funciona, reina la ilusión de estabilidad. Pero basta una disputa geopolítica, una sanción extraterritorial o un aumento unilateral de tarifas para darnos cuenta de que el interruptor no está en nuestras manos.

Las situaciones hipotéticas —pero perfectamente plausibles— ilustran el punto:

- Una reforma fiscal en la sede matriz de un proveedor SaaS dispara los costos del sistema hospitalario nacional.
- Un litigio de patentes fuerza la desactivación temporal de la función de firma digital que usan miles de ciudadanos.
- Un bloqueo comercial deja sin acceso a actualizaciones de la base de datos catastral, afectando a inmobiliarias y gobiernos locales.

El antídoto no es el aislamiento, sino la diversificación inteligente: copias en centros de datos nacionales, proveedores regionales y, sobre todo, estándares abiertos que permitan migrar con rapidez si el gigante mundial decide cambiar las reglas.

3.4 Desinformación y manipulación cognitiva

Si la electricidad es la savia del Estado digital, la información es la sangre que circula por la sociedad. Plataformas masivas y algoritmos opacos determinan qué ve cada uruguayo cuando desbloquea su teléfono. Aun sin mala fe, la priorización automática de contenidos puede crear burbujas de información que distorsionan la percepción pública. Si a esto sumamos campañas organizadas de trolls, bots y granjas de memes, se entra en el terreno de la guerra cognitiva: dividir comunidades, erosionar la confianza democrática y deslegitimar políticas de salud o ambiente.

Entre 2018 y 2024, el Laboratorio de Ciberseguridad de la Udelar identificó al menos 17 "operaciones de influencia" asociadas a actores extranjeros, con efectos que van desde rumores locales hasta hashtags nacionales manipulados. Soberanía digital, aquí, significa proteger el terreno mental: alfabetizar en verificación de fuentes, transparentar la

publicidad política y exigir rendición de cuentas sobre los algoritmos de recomendación. La defensa ante este tipo de amenaza es tanto técnica como cultural y educativa.

3.5 Brecha digital interna: la amenaza que divide por dentro

No todas las amenazas vienen de afuera. También existe el riesgo de construir dos Uruguayes: uno hiperconectado, bilingüe en Python y Swift, y otro que lucha por señal 3G y recicla contraseñas por miedo a olvidarlas. La brecha digital no es solo geográfica (campo/ciudad), sino también etaria, socioeconómica y de género. Mientras siga abierta, la pirámide será inestable: un ciberfraude masivo puede vaciar los ahorros de miles de adultos mayores, o un apagón digital educativo puede dejar a zonas rurales fuera de juego.

Plan Ceibal e Ibirapitá han funcionado como escudos, pero necesitan constante actualización: dispositivos con más memoria, talleres de ciberseguridad para jubilados, conectividad satelital asequible en zonas rurales. Una brecha ancha es una herida en la soberanía: la cadena es tan fuerte como su eslabón más débil.

3.6 Cadena de suministro de software y hardware

El caso SolarWinds en 2020 demostró que basta adulterar una simple librería de actualización para infectar miles de organismos. Uruguay importa la mayoría de sus routers, microcontroladores y bibliotecas de código: cada componente puede ser un caballo de Troya. Si no auditamos firmware ni exigimos la declaración de materiales de software (SBOM) en licitaciones, podemos introducir fallas sistémicas antes de que el servicio esté en funcionamiento.

La solución emergente pasa por protocolos de aprovisionamiento cero-confianza, exigir firmas digitales en cada actualización y formar equipos de análisis de firmware en la academia nacional. La cooperación regional —compartir reportes de vulnerabilidad con Chile, Argentina y Brasil— multiplica la capacidad de detección y respuesta.

3.7 Marco legal: la carrera contra el reloj

Las leyes suelen llegar tarde. La Ley 18.331 (protección de datos) fue pionera en 2008, pero la disrupción de la IA generativa y los deepfakes exige nuevos artículos sobre consentimiento, copyright y responsabilidad algorítmica. Sin actualización, los conflictos inéditos se resuelven con normas pensadas para otra era. La misma lentitud afecta la agilidad comercial: licitaciones tecnológicas que demoran 18 meses suelen quedar obsoletas antes de adjudicarse.

Un marco legal soberano debe ser principialista (centrado en valores) y no solo prescriptivo (centrado en marcas). Necesitamos regulación flexible, con sandbox regulatorios para innovar y salvaguardas firmes sobre privacidad y control democrático.

3.8 Caso de simulación: el día que la nube se apagó

Para ilustrar la confluencia de amenazas, imaginemos un ataque de ransomware que impacta simultáneamente a dos proveedores SaaS extranjeros que alojan módulos de facturación del sistema de salud y certificados de firma electrónica. Los hospitales no pueden emitir órdenes de compra, el BPS retrasa pagos, y los ciudadanos no logran validar trámites urgentes.

En el mejor de los casos, un plan de contingencia local levanta un cluster de respaldo en el Data Center de Pando (uno de los principales de la región) , se restauran backups diarios y se reactivan servicios en seis horas.

En el peor de los casos, los backups estaban en la misma nube comprometida; la restauración depende de negociar con criminales. El gobierno entra en modo crisis, la población pierde confianza y el daño económico y reputacional se multiplica. La moraleja es simple: lo que parece un gasto redundante (copias offline, clusters locales) es, en realidad, un seguro de soberanía.

3.9 Estrategias de resiliencia: del escritorio al Senado

La resiliencia digital no se improvisa: se planifica, se ejercita y se financia. Algunas estrategias concretas incluyen:

1. **Duplicidad geográfica:** dos data centers en regiones distintas y contratos con nubes públicas que acepten replicar en Uruguay.
2. **Formación de ciberdefensores:** programas como "Malla Oro" para jóvenes técnicos, con becas a cambio de años de servicio en CERTuy.
3. **Inteligencia colaborativa:** red regional de intercambio de telemetría (Argentina, Brasil, Chile, Uruguay), con alertas en tiempo real.
4. **Gobernanza algorítmica:** comité nacional de auditoría de IA que revise software estatal, exija explicación de sesgos y fije umbrales de riesgo.

5. **Derecho a la portabilidad:** ley que obligue a proveedores SaaS a entregar, sin costo, una copia completa y legible de las bases de datos al finalizar el contrato.

6. **Alfabetización continua:** clubes de ciberseguridad en secundaria y créditos universitarios por voluntariado de capacitación a adultos mayores.

3.10 Manos a la obra: acciones inmediatas en cada sector

La soberanía digital se fortalece cuando cada sector asume su parte.

- **Ciudadanía:** activar doble factor en correo y banca. Resultado: menos cuentas secuestradas, menos vectores de ataque.
- **PyME:** utilizar plataformas nacionales y alojar backups en data centers locales. Así, se apoya a proveedores uruguayos y se asegura la redundancia bajo leyes propias.
- **Docentes:** incluir módulos de verificación de fuentes y educación digital. Resultado: generaciones menos vulnerables a la desinformación.
- **Intendencias:** mapear activos críticos (semáforos, bombeo, cámaras) y actualizar software trimestralmente. Esto reduce vulnerabilidades y mejora la continuidad de servicios esenciales.
- **Legisladores:** impulsar reformas legales para tipificar delitos digitales emergentes, como el deepfake electoral. Blindaje legal para la democracia.

Cada una de estas acciones, aunque parezca menor, suma a la defensa colectiva y multiplica la capacidad de respuesta nacional.

3.11 Mirando de frente al riesgo sin caer en paranoia

Reconocer la vulnerabilidad no es declararse derrotado; es el primer acto de confianza de una república con ciudadanía informada. Uruguay ha sorteado tormentas mayores —crisis económica, pandemia, sequía histórica— gracias a la articulación público-privada y a la densidad de tejido social. Esa misma articulación debe extenderse al ámbito digital.

La buena noticia es que partimos con ventajas: infraestructura de fibra óptica, cultura cooperativa, tradición de software libre y un Estado ágil en su escala. La mala noticia es que los adversarios —ciberdelincuentes, monopolios, campañas de desinformación— evolucionan rápido. Dormirse en los laureles es retroceder.

Este capítulo mapeó el terreno minado. En el próximo daremos un giro propositivo: cómo transformar los riesgos en oportunidades, pasar de la defensa a la ofensiva creativa y usar la inteligencia artificial, el blockchain y las ciudades inteligentes como palancas de prosperidad nacional bajo control ciudadano. El desafío es grande; la recompensa mayor: un Uruguay que mire al 2040 con la serenidad de quien conoce y cuida su casa.

Capítulo 4

Tus datos, tu reflejo: privacidad y autodeterminación en la era de los gigantes algoritmos

4.1 Una huella que no se borra con la marea

Hace dos siglos, cuando una carreta cruzaba los balnearios del Este, sus ruedas dejaban surcos profundos en la arena. Bastaba el vaivén de la marea para borrar el rastro. Hoy, las huellas que producimos a diario —likes, búsquedas, selfies, geolocalizaciones, tickets electrónicos— no las borra ninguna ola: quedan replicadas en servidores dispersos por Montevideo, São Paulo, Virginia o Singapur.

Cada gesto digital, por inocente que parezca, compone un retrato probabilístico de quién sos, qué pensás, cuánto gastás, con quién te reunís y, con un poco de minería de datos, hasta qué harás mañana. La soberanía digital no se entiende sin soberanía de los datos personales, porque lo que se conoce o se induce sobre un individuo se puede proyectar a colectivos y, en última instancia, influir sobre la democracia misma.

4.2 De la libreta de almacén a la economía de los perfiles

En los años setenta, el almacenero barrial llevaba un cuaderno donde anotaba los fiados, conocía tus gustos, sabía cuánto demorabas en pagar. Esa relación se basaba en la proximidad y la confianza. En 2025, la "libreta" es un motor analítico que teje millones de transacciones para ajustar precios dinámicos, diseñar microcréditos o perfilar votantes. La escala cambió, el poder también.

- **Valor económico:** Los informes internacionales de big-data anticipan que el mercado global de datos personales superará los 400 mil millones de dólares en 2030.
- **Valor político:** Empresas de microsegmentación publicitaria colocan contenidos diferentes a cada usuario según su "perfil de susceptibilidad".
- **Valor social:** Algoritmos de puntuación crediticia, escolar o sanitaria, si son opacos, pueden perpetuar sesgos y discriminaciones invisibles.

Uruguay, con su alta conectividad (más del 92 % de hogares con fibra) y uso masivo de redes, es un productor neto de datos. La pregunta ya no es si generamos valor, sino quién lo captura y bajo qué reglas.

4.3 Marco normativo uruguayo: fortalezas y zonas grises

La Ley 18.331 (2008) fue pionera en Latinoamérica: creó la autoridad nacional de datos personales, exigió consentimiento informado y reconoció los derechos de acceso, rectificación y supresión. Sin embargo, el tsunami tecnológico posterior plantea desafíos que la norma —pensada para bases de datos tradicionales— no alcanza a cubrir del todo:

1. **Algoritmos que deciden:** La ley menciona "procesamiento automatizado", pero no exige explicabilidad ni auditoría de sesgos.
2. **Transferencias internacionales:** Pide "niveles adecuados de protección" en el país receptor, pero la nube híbrida y los contratos con subprocesadores diluyen la trazabilidad.

3. **Portabilidad estructurada:** El derecho a llevar tus datos a otro proveedor (como en el GDPR europeo) carece aún de protocolos técnicos obligatorios.

El Parlamento estudia una reforma que contemple IA, identidad descentralizada y sanciones proporcionadas. Mientras tanto, la brecha entre ley y práctica se cuela por resquicios, sobre todo en el sector privado.

4.4 Riesgos concretos si bajamos la guardia

No hace falta irse a escenarios de ciencia ficción para entender los peligros. Basta imaginar casos como:

- **Rastreo ubicuo:** Apps de delivery comparten geolocalización con brokers extranjeros. Impacto: exposición de movimientos de autoridades, patrones de consumo, rutinas de seguridad.
- **Perfilado político:** Empresas de publicidad importan datos de redes sociales para microdirigir mensajes electorales. Impacto: distorsión del debate democrático, ventaja competitiva para quien tiene más datos o más presupuesto.
- **Deepfakes verosímiles:** Videos falsos atribuyen declaraciones a líderes locales horas antes del cierre de campaña. Impacto: caos informativo, riesgo de violencia, decisiones de voto basadas en mentiras.

Estos ejemplos muestran que la privacidad personal es también un asunto de soberanía nacional.

4.5 Buenas prácticas (y por qué todavía fallan)

Sabemos qué hacer, pero transformar buenas prácticas en rutina requiere más incentivos y recursos. Algunas claves:

1. **Consentimiento informado:**
   Marcar "sí, acepto" en letra chica no es consentimiento real. Hay que reemplazar formularios extensos por paneles de control claros y sencillos.

2. **Minimización de datos:**
   Guardar solo lo necesario. Si la app de linterna pide acceso a tus contactos, sospechá. Las empresas deben anonimizar registros antiguos y rotarlos a backups offline.

3. **Cifrado end-to-end:**
   Es obligatorio en mensajería y recomendable en correos y nubes. Sin embargo, muchos servicios empresariales cifran solo en tránsito, no en reposo, para poder indexar datos.

4. **Auditorías externas:**
   Los sistemas críticos deberían certificarse cada año. El problema: falta masa crítica de auditores locales y recurrir a firmas internacionales encarece y demora los resultados.

5. **Educación ciudadana:**
   Campañas sobre contraseñas, doble factor y estafas. Sin embargo, los presupuestos compiten con otras prioridades y el mensaje técnico suele perderse.

En síntesis: la teoría está clara, pero necesitamos voluntad política, recursos y una cultura digital que haga de la privacidad un reflejo cotidiano.

4.6 El dilema de la economía de datos local

Uruguay quiere promover la analítica avanzada y las startups de IA. Para eso, necesita datos. El dilema: ¿cómo conciliar innovación con privacidad? Hay tres modelos posibles:

1. **Todo abierto salvo excepción:**
   Seudonimizar y publicar datasets públicos (tránsito, meteorología, resultados de exámenes) para uso libre.
   Riesgo: correlaciones externas pueden reidentificar personas.

2. **Aprobación caso por caso:**
   Comités de ética que evalúan cada proyecto. Ralentiza la investigación y puede derivar en discrecionalidad.

3. **Espacios de datos soberanos:**
   Infraestructura segura donde investigadores acceden a vistas agregadas sin llevarse los datos crudos. Requiere inversión, pero multiplica el valor y protege la fuente.

El Ministerio de Salud ensaya el tercer modelo con su Data Lake, logrando diagnósticos más rápidos sin exponer identidades. La soberanía reside en la arquitectura, no en un sí/no absoluto.

4.7 Caso nacional: del carné de vacunación físico al QR en blockchain

Durante la pandemia, Uruguay emitió certificados COVID con QR verificable. La autoridad de datos personales exigió que el código no almacenara datos sensibles, solo un identificador contrastable contra servidores locales. Más adelante, se evaluó guardar los hashes en una cadena de bloques ligera.

- **Ventaja:** Imposible falsificar certificados.
- **Desafío:** Decidir cuánto metadata incluir sin exponer datos personales, como fecha exacta de vacunación, lote o centro.

El piloto derivó en una guía de "diseño soberano" que hoy se aplica a otras credenciales digitales, como licencias de conducir o carnés de manipulador de alimentos.
Moraleja: la tecnología de moda no es solución si no se diseña la privacidad desde el inicio.

4.8 De usuario a custodio: qué podés hacer hoy mismo

El cambio real empieza en lo cotidiano. Algunas acciones simples que podés tomar:

1. Revisá los permisos de tus apps: cámara, micrófono, ubicación.
2. Usá contraseñas largas (frases de varias palabras) y activá el doble factor.
3. Usá pseudónimos en foros; no repitas tu número de cédula innecesariamente.
4. Solicitá tus datos a cualquier empresa local (tenés derecho) y revisá qué saben sobre vos.
5. Denunciá el spam político no solicitado; la autoridad nacional investiga y puede sancionar.

Ningún paso es heroico, pero juntos dibujan un cerco que disuade abusos y eleva el estándar de todos.

4.9 Hoja de ruta nacional: políticas para la década

El futuro de la privacidad uruguaya depende de la capacidad de actualizar normas y hábitos.

Las siguientes metas constituyen una propuesta estratégica, inspirada en debates nacionales e internacionales, pero aún no forman parte de la legislación vigente. Son recomendaciones de horizonte deseable para Uruguay:

- **2025-2027:**
  Reformar la Ley 18.331, incluir "explicabilidad algorítmica" y derecho de portabilidad. Que todos los organismos públicos publiquen sus políticas de IA.

- **2027-2030:**
  Crear un Centro Nacional de Anonimización para datasets públicos y privados. Al menos 50 proyectos de investigación y desarrollo usando datos seudonimizados locales.

- **2030-2032:**
  Ley de geolocalización laboral: las apps de delivery solo rastrean durante el horario de trabajo. Objetivo: cero sanciones internacionales por violaciones de privacidad.

- **2032-2035:**
  Red de datatrustes cooperativos: ciudadanos ceden datos a cambio de beneficios y voto en su uso. Que un millón de uruguayos participen en la gobernanza de sus propios datos.

4.10 Fronteras futuras: biometría, neurodatos y el cuerpo como contraseña

El reemplazo de contraseñas por huellas, rostros e incluso pulsos cerebrales avanza rápido. Pero un rostro filtrado puede convertirse en una "llave maestra" irrecuperable. Uruguay debería anticiparse:

- Prohibir la recolección masiva de biometría en espacios públicos, salvo orden judicial.
- Limitar y licenciar el uso de neurodatos (p.ej., para investigación médica), con plazos claros y consentimiento específico.
- Fomentar estándares de biometría local en dispositivo, evitando bases centralizadas.

La meta: no hipotecar rasgos inmutables a cambio de comodidad.

4.11 Cierre: privacidad, el cimiento de la soberanía

Las democracias sólidas se construyen sobre el respeto a la esfera individual. Cuando los datos se transforman en mercancía sin reglas, el ciudadano se vuelve objeto de experimentación, no sujeto de derechos. Uruguay, por su escala y cohesión social, tiene la oportunidad de ser laboratorio de buenas prácticas: datasets abiertos, sí, pero seguros; IA en salud, sí, pero auditada; comercio electrónico, sí, pero con pasarelas transparentes y respetuosas de la ubicación.

Si la soberanía digital es el barco, la privacidad es su casco: invisible para el ojo inexperto, pero decisiva para que la nave no haga agua. Los próximos capítulos mostrarán cómo esa nave puede, además de resistir tormentas, impulsar nuevos motores: inteligencia artificial nacional, blockchain público y ciudades que piensan con sus vecinos.

La travesía sigue. El timón, más que nunca, está en manos de todos.

Capítulo 5

Cables, antenas y bits de confianza: infraestructura y conectividad para una soberanía que se sostenga

5.1 Redes que vertebran la república digital

No hay soberanía sin territorio, y en el siglo XXI el territorio también se compone de tubos de fibra del grosor de un cabello, antenas que laten a gigahercios y centros de datos que funcionan como corazones tecnológicos, regulando su temperatura al milímetro. Decisiones que antes parecían abstractas —educación, salud, finanzas— terminan viajando por esa retícula invisible, tan real como el pavimento. Por eso, este capítulo se centra en la infraestructura física y lógica que hace posible la vida digital uruguaya: cómo estamos, qué nos falta y, sobre todo, cómo garantizar que siga siendo nuestra, aun cuando cambien los vientos comerciales o geopolíticos.

5.2 La fibra óptica: columna vertebral invisible

Uruguay apostó temprano por la fibra FTTH (Fiber to the Home) y hoy supera el 92% de los hogares conectados, un porcentaje que rivaliza con Corea del Sur o Noruega. Pero tener alta penetración no es lo mismo que tener resiliencia. Hay dos retos principales en el horizonte:

- **Redundancia interurbana:**
  Muchos tramos rurales dependen de una sola ruta. Un corte accidental deja aislados pueblos enteros. La propuesta es clara: trazar anillos secundarios usando los ductos existentes de UTE y la caminería nacional, con un cofinanciamiento entre intendencias y ANTEL.

- **Salud de la planta:**
  Un 18% de las ONT instaladas en 2015 se acerca al fin de su vida útil; fallos silenciosos degradan la velocidad y experiencia del usuario. Aquí urge un plan de renovación escalonada, priorizando zonas clave: teletrabajo, educación remota y áreas turísticas donde la economía depende de la conectividad.

La buena noticia es que el know-how está en casa: ANTEL y sus cooperativas subcontratistas ya cuentan con cuadrillas entrenadas. Lo que falta es presupuesto sostenido y coordinación fina con municipios para evitar obras repetidas o soluciones parche.

5.3 El horizonte 5G y el debate sobre espectro soberano

El 5G no es solo "más megas en el móvil"; habilita latencias de un dígito, lo que permite desde telecirugía hasta robótica agrícola y monitoreo urbano en tiempo real.

En 2023 ANTEL obtuvo las primeras bandas, pero las empresas privadas también reclaman su espacio para dinamizar la competencia. Desde la óptica de la soberanía, hay tres puntos innegociables:

- Apostar por una **arquitectura abierta (O-RAN)**, que evita el bloqueo de un único proveedor.
- Exigir que el "core" de la red, donde se enrutan llamadas de emergencia y datos críticos, permanezca en territorio nacional.
- Licitar el espectro bajo reglas claras: obligaciones de cobertura rural, cláusulas de ciberseguridad auditables por el CERTuy y la exigencia de compartir antenas en zonas de baja densidad, para no desperdiciar recursos.

La clave no está solo en la pluralidad de operadores, sino en que quien explote 5G acepte mantener las puertas traseras fuera y cumpla con los estándares de seguridad y acceso universal.

5.4 Cuando el cielo es la red: satélites y globos estratosféricos

Para los 180.000 uruguayos que viven en parajes lejanos, internet satelital o los radioenlaces de microonda son su único lazo digital. Hoy, la constelación geoestacionaria de ANTEL se complementa con servicios LEO privados, que ofrecen latencias de 40 milisegundos y se reciben con antenas de 50 cm.

Pero hay desafíos soberanos:

- La **jurisdicción foránea**: el tráfico suele pasar primero por EE.UU. o Europa, quedando los metadatos bajo otras leyes.
- Un **modelo de precios volátil**: lo que empieza barato por promoción puede duplicar costos a los pocos años.

La estrategia para Uruguay debe ser precisa: establecer acuerdos de tránsito IPv6 que permitan conectar los backhauls directamente a gateways en Pando, y asegurar la participación activa del Estado en consorcios regionales de SmallSats impulsados por la Agencia Latinoamericana y Caribeña del Espacio (ALCE). Además, se exploran globos solares sobre la Cuchilla Grande para dar cobertura 4G a zonas amplias con un costo mínimo.

5.5 Del centro al borde: data centers, nube híbrida y edge soberano

El Data Center de Pando, certificado Tier III+, es un hito nacional. Pero la tendencia global es descentralizar, distribuir la capacidad para bajar la latencia y resistir fallos.

- El **core** debe estar siempre en territorio nacional: Pando y un segundo sitio de respaldo, idealmente en el litoral, para diversificar riesgos eléctricos o sísmicos.
- A nivel **departamental**, mini-salas (mini-rooms) dentro de hospitales o campus universitarios, con racks blindados y UPS, pueden ejecutar IA local o cachear contenido educativo y sanitario.
- En el **borde ciudadano**, routers comunitarios con chips de inferencia aceleran aplicaciones críticas sin enviar todos los datos a la nube.

La ventaja es tangible: ni un ataque DDoS ni un corte de fibra deja incomunicada a la escuela rural, y la baja latencia se vuelve un argumento de peso para futuros convenios de telemedicina internacional.

5.6 KWh verdes: la energía como factor de autonomía

Nuestra matriz eléctrica es 98% renovable, pero no garantiza disponibilidad ininterrumpida para clusters de computación que consumen megavatios.

Algunas recomendaciones:

- **Contratos de reserva cruzada UTE–privados**: parques solares que puedan inyectar energía al grid cuando haya picos de demanda IA.
- **Micro-hidro en riego**: el sector agrointeligente puede generar excedentes útiles para nodos edge en silos y tambos robotizados.
- **Reciclaje nacional de baterías de litio-hierro**: aprovechar las baterías de ómnibus eléctricos para backups de data centers.

Así, la computación crítica no dependerá del diésel importado, y la huella de carbono sigue siendo un diferencial atractivo para captar servicios europeos sujetos a regulaciones verdes.

5.7 Brecha rural: soluciones de bolsillo y de comunidad

La conectividad no siempre requiere infraestructura cara; muchas veces un router Wi-Fi tribal hace la diferencia. Experiencias piloto lo demuestran:

- En **Lo Prado, Florida**, vecinos montaron una red mesh con firmware libre y comparten un enlace satelital.
- En **Chuy Frontera**, antenas comunitarias aprovechan el 4G de ambos países; la intendencia subsidia hardware y los vecinos comparten ancho de banda por domicilio.
- En escuelas rurales, el **Plan Ceibal** testeó que una XO puede funcionar como hotspot y compartir datos al caserío.

La lección: el Estado debe regular y acompañar, pero no necesariamente monopolizar. La flexibilidad en licencias de espectro y microfinanciamiento a cooperativas logra lo que la economía de escala no justifica.

5.8 Seguridad de la infraestructura: blindaje sin candados de oro

Tener cables y antenas es solo el principio; protegerlos es la siguiente etapa.
La seguridad se juega en varias capas:

- **Física:** el robo de fibra o el vandalismo de antenas requiere sensores IoT y colaboración entre operadoras para un seguro compartido.
- **Lógica:** los ataques de tipo BGP hijacking se previenen con protocolos RPKI y notificaciones rápidas al CERTuy.
- **Operacional:** nada de contraseñas por defecto en routers y auditoría semestral independiente para garantizar estándares.

Aquí no hay espacio para el lujo: la fortaleza está en la disciplina, no en el blindaje dorado.

5.9 Un plan país en cinco hitos (2025-2035)

La hoja de ruta para la década debe tener metas concretas, pero integradas al sentido común uruguayo:

- Para 2026, todos los hospitales conectados a edge local redundante, con latencia mínima.
- Para 2027, duplicar las rutas de fibra en zonas serranas y eliminar localidades desconectadas.

- Para 2029, asegurar un 5G universal con el core en territorio nacional y casi total cobertura poblacional.
- Para 2031, 50 MW de cómputo IA alimentado 100% con energía renovable y sin fósiles para data centers críticos.
- Para 2035, lograr cobertura mínima de 50 Mb/s simétricos en todo el país, cerrando la brecha urbano-rural a menos de 10 Mb/s.

5.10 "Manos a la obra": qué puede hacer cada uno

La soberanía digital se construye con acciones en todos los niveles:

- **Municipios:** mapear postes ociosos y ofrecerlos como punto de antena, a cambio de conexión gratuita para espacios públicos y culturales.
- **PyMEs:** contratar hosting en Pando o cooperativas nacionales; exigir cifrado y reclamar cláusulas de protección de datos.
- **Centros educativos:** instalar sensores y compartir datos climáticos, enseñar a los estudiantes a graficar y analizar información real.
- **Consumidores:** elegir proveedores que publiquen reportes de transparencia y premiar buenas prácticas con la billetera.
- **Ingenieros:** contribuir al firmware abierto de routers nacionales, auditar código y compartir mejoras con la comunidad.

Cada eslabón suma al tejido invisible de la República digital.

5.11 Conclusión: un esqueleto de vidrio que hay que ir templando

La infraestructura es como esos esqueletos de hierro y vidrio del Mercado del Puerto: parece rígida, pero necesita un mantenimiento constante.

Uruguay tiene un andamiaje envidiable: fibra extensa, energía renovable, identidad digital madura. La misión de la próxima década es templarlo: reforzar anillos, diversificar proveedores, almacenar copias en territorio nacional y, sobre todo, incluir a cada rincón del mapa.

Porque la soberanía digital no se declama: se cablea, se energiza, se audita y se comparte. Y cada metro de fibra, cada antena que conecta a una casa lejana, es —en definitiva— otro ladrillo en la muralla invisible que protege la república frente a la incertidumbre global.

Capítulo 6

Inteligencia artificial "hecha en casa": el experimento CELESTE y la ruta para que cualquier uruguayo entrene su propio modelo

6.1 La IA ya no vive solo en Silicon Valley

Durante años, la inteligencia artificial fue vista como un coto cerrado de grandes corporaciones y laboratorios extranjeros. Hoy, esa barrera se ha roto. No solo por la masificación de bibliotecas de código abierto y hardware asequible, sino porque el conocimiento ha dejado de ser un secreto. Ahora, en Uruguay, cualquier persona con una computadora y curiosidad puede entrenar su propio modelo de IA. ¿Suena ambicioso? Este capítulo lo demuestra paso a paso, sin adornos y con pruebas: así se entrenó el modelo CELESTITO02, íntegramente en casa, usando datos sintéticos.

6.2 La semilla: un problema cotidiano y una respuesta local

Todo comenzó con una pregunta muy simple: ¿cómo podemos automatizar, por ejemplo, la asignación de localidades y radios para trámites, sin depender de grandes plataformas externas ni exponer datos reales? La respuesta fue crear datos sintéticos: identidades ficticias pero estructuradas como las reales, con documento, nombre, dirección, localidad, código postal y teléfono. Así se garantizaría la privacidad y, al mismo tiempo, se demostraría la viabilidad de un modelo nacional.

Imagen sugerida: "2 - Creando Dataset.png"

6.3 Paso 1: Preparando el entorno y las herramientas

El primer paso fue preparar el entorno de trabajo.

- Se utilizó una PC de escritorio estándar, con Windows 10, 16GB de RAM y una GPU AMD RX570, perfectamente al alcance de miles de hogares uruguayos.
- Se creó un entorno virtual en Python y se instalaron las librerías necesarias: pandas, scikit-learn, joblib y torch.

Imagen sugerida: "1 - instalando las librerías.png"

¿Por qué es importante este paso? Porque demuestra que no hay barrera de hardware ni de software: todo es libre, abierto y accesible.

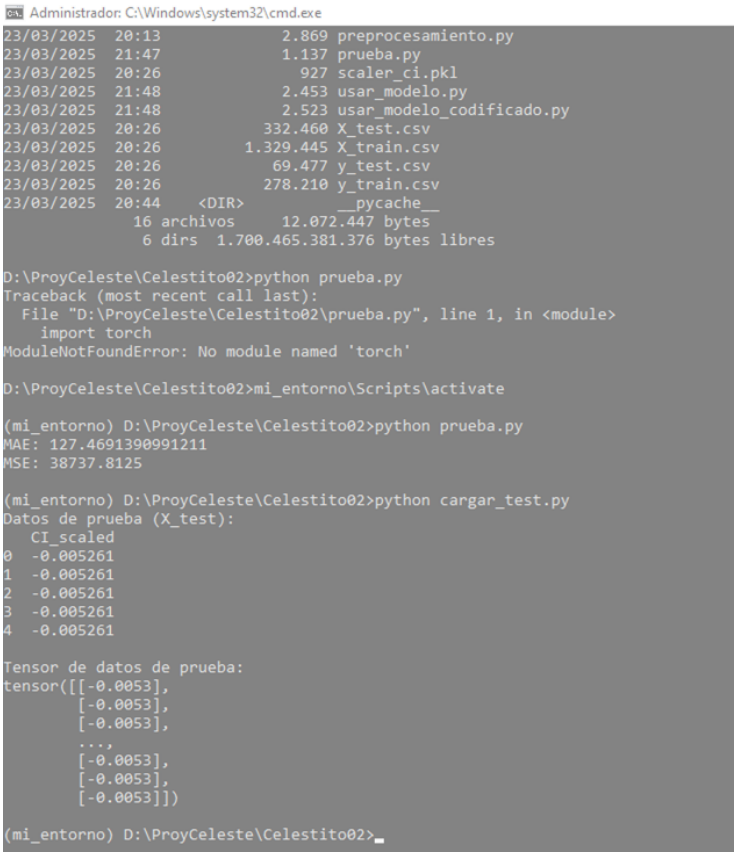
6.4 Paso 2: Generación del dataset sintético

No hay inteligencia artificial sin datos. Pero aquí no usamos datos sensibles ni información real de personas.

- Se generaron 70.000 filas de datos sintéticos, cada una simulando una persona:
    - Documento de identidad
    - Nombre y apellido
    - Localidad
    - Dirección

- Código postal
- Teléfono
- Y Otros campos simulados
- El objetivo era tener un dataset variado, estructurado y anonimizado al máximo, que sirviera para entrenar el modelo sin riesgos ni autorizaciones complejas.

6.5 Paso 3: Preprocesamiento y limpieza de datos



El siguiente paso fue limpiar el dataset:

- Se eliminaron duplicados, valores inconsistentes y espacios en blanco.
- Se normalizaron los datos numéricos y se codificaron las variables categóricas (ejemplo: localidades a códigos únicos).
- Se prepararon los archivos para entrenamiento y prueba, siguiendo buenas prácticas de ciencia de datos.

verificación de los datos preprocesados.

6.6 Paso 4: Arquitectura del modelo y entrenamiento

Con los datos prontos, llegó el momento de armar y entrenar la red neuronal.

- Se utilizó PyTorch, que es libre y gratuito.
- El modelo constó de varias capas densas, dropout y softmax en la salida para clasificación.
- Se usó un esquema de validación cruzada (K-fold), separando el 80% para entrenamiento y 20% para validación.
- La función de pérdida fue categorical cross-entropy y el optimizador, Adam.

Durante el entrenamiento se monitorearon las métricas (loss, accuracy) en tiempo real. El hardware respondió bien: ni calor extremo ni consumo desmedido de memoria.

Al final, el modelo fue guardado en formato .pth para ser usado cuando y donde se quiera, sin conexión a Internet.

6.7 Paso 5: Validación y prueba del modelo

Terminada la fase de entrenamiento, se evaluó el modelo:

- Se cargó el archivo de test y se probaron predicciones sobre nuevas identidades sintéticas.
- Se analizaron los errores y el rendimiento global.

El modelo arrojó resultados optimistas, permitiendo la asignación de cédulas a localidades con una precisión de acuerdo al modelo de prueba con fines educativos.

6.8 Paso 6: Uso práctico — ejecutando el modelo en la vida real

El script final, usar_modelo.py, permite a cualquier usuario ingresar una cédula (ficticia) y obtener, en segundos, la localidad sugerida.

Todo sucede en la propia PC, sin exponer datos al exterior ni depender de la nube.

Lección clave:

- No es necesario tener grandes presupuestos ni hardware fuera de serie.
- Usar datos sintéticos permite experimentar y aprender sin riesgos ni demoras burocráticas.
- Todo el proceso es 100% replicable, mejorable y auditable.

6.9 ¿Y ahora qué?

El desafío que sigue es que más liceos, clubes de ciencia, universidades y PyMEs se animen a probar, ajustar y mejorar estos procesos. La inteligencia artificial nacional no será una realidad si la miramos desde afuera. Hay que animarse a escribir el código, limpiar los datos, entrenar el modelo y compartir los logros, así como los errores.

Cada imagen, cada paso documentado, es testimonio de una idea sencilla: **la soberanía digital se construye también en la terminal** de la computadora de tu casa.

Capítulo 7

Ciberseguridad para todos los días: blindar la casa digital sin perder la calma

7.1 Por qué la seguridad informática ya no es asunto de "los de sistemas"

Durante décadas, la informática fue territorio de técnicos en guardapolvo o de "los muchachos de sistemas". Hoy, la frontera digital es la casa, la escuela, la chacra, la plaza. Cada persona, cada familia, cada grupo de trabajo, gestiona datos que pueden ser robados, manipulados o vendidos. La seguridad digital es tan transversal como el agua potable: si falta, todo se complica.

Hoy, cada uruguayo comparte información sin pensar: al enviar la receta médica por WhatsApp, al hacer una compra en línea, al compartir un meme. Confiamos en que nadie "malicioso" intercepte, replique o distorsione esos datos. Sin embargo, los riesgos no son ciencia ficción ni historias de grandes empresas: son cotidianos y, a menudo, invisibles hasta que producen daño.

La ciberseguridad cotidiana consiste en armar, reforzar y mantener pequeños muros digitales: nada más, y nada menos. No es paranoia, sino sentido común actualizado al siglo XXI.

7.2 El mapa de los peligros: ¿qué acecha tras la pantalla?

En Uruguay, la digitalización acelerada trajo oportunidades, pero también nuevos delitos. No hay que viajar lejos: los riesgos están en el correo, en el celular y en la nube donde guardamos fotos y documentos. Los ataques más frecuentes:

- **Phishing:** correos o mensajes que fingen ser del BPS, BROU o la DGI, pidiendo datos personales.
- **Ransomware:** archivos adjuntos que, al abrirse, cifran todo el disco y piden rescate.
- **Suplantación de identidad en redes:** perfiles falsos de amigos o familiares que piden ayuda urgente.
- **Ingeniería social telefónica:** llamadas fingiendo ser de una mutualista o empresa para sacar información privada.
- **Fraudes con QR:** stickers falsos sobre los originales, desvían el dinero al delincuente.
- **Desinformación viral:** audios o cadenas falsas sobre beneficios, vacunación o cambios en trámites, que se propagan rápido y confunden a miles.

Cada riesgo requiere un abordaje específico, pero la base de todas las defensas es la información y el criterio personal.
