

PRIVACIDAD Y SOBERANÍA DIGITAL

Qué entregamos cuando usamos internet y cómo
recuperar mayor control sobre nuestra vida digital



ENTIENDE
cómo funciona



USA
con criterio
y seguridad



AMPLÍA
tus capacidades



TRANSFORMA
Tu vida y tu trabajo

1. PAGAR CON DINERO NO ES LA ÚNICA FORMA DE PAGAR

Abres una aplicación gratuita.

1. Aceptas.
2. Navegas.
3. Buscas.
4. Compras.
5. Te desplazas.
6. Ves videos.
7. Das "me gusta".

Y durante todo ese proceso pueden generarse datos.

No significa que toda recopilación sea necesariamente abusiva.

Muchos datos permiten que los servicios funcionen.

La pregunta importante es: ¿Sabemos qué información entregamos, para qué se utiliza y qué capacidad tenemos para decidir sobre ella?

Ahí empieza la privacidad digital.

2. ¿QUÉ SON LOS DATOS PERSONALES?

No son solamente nombre, teléfono, dirección.

También pueden incluir, según el contexto, la ubicación, dirección IP, identificadores del dispositivo, compras, búsquedas, fotografías, voz, datos biométricos, comunicaciones, relaciones, patrones de comportamiento y existen datos especialmente sensibles que merecen mayores precauciones.

La privacidad empieza entendiendo que nuestra huella digital es mucho más amplia de lo que escribimos conscientemente en un formulario.

3. DATOS QUE DAS, DATOS QUE GENERAS Y DATOS QUE SE INFIEREN

Podemos pensar en tres niveles.

- **DATOS QUE ENTREGAS:** Nombre, correo, fotografía.
- **DATOS QUE GENERAS:** Clics, búsquedas, ubicaciones, horarios de conexión.
- **DATOS QUE PUEDEN INFERIRSE:** Intereses, hábitos, preferencias o determinados patrones.

Esta tercera categoría es especialmente importante.

A veces no necesitas decir explícitamente algo para que un sistema intente deducirlo de tu comportamiento.

4. ¿PARA QUÉ QUIEREN LOS DATOS

Los datos pueden utilizarse para prestar un servicio seguridad; personalización; estadísticas; recomendaciones; publicidad; desarrollo de productos; prevención de fraude.

Pero los modelos y prácticas varían enormemente entre servicios. Por eso evita dos extremos: “Todas las empresas venden absolutamente todos tus datos.” Y “Si no tengo nada que ocultar, da igual.”

La respuesta madura es: quiero saber qué se recopila, con qué finalidad y qué control tengo.

5. “NO TENGO NADA QUE OCULTAR”

Privacidad no significa necesariamente ocultar actividades incorrectas.

Cierras la puerta del baño. Proteges tus conversaciones. No publicas tu información bancaria. No permitirías que cualquiera revisara tu teléfono.

¿Por qué?

Porque privacidad significa también controlar qué partes de nuestra vida conoce cada persona o institución.

No tener nada que ocultar no significa tener todo que mostrar.

6. HAZ TU INVENTARIO DIGITAL

Escribe las principales cuentas que utilizas:

Servicio	Qué guarda	¿Lo necesito?	Prioridad
Correo	mensajes/contactos	Sí	Alta
Red social	publicaciones/datos	Sí/No	Media
App antigua	datos	No	Eliminar

Incluye correo, redes, nube, compras, aplicaciones, servicios laborales. Probablemente descubrirás cuentas que llevas años sin utilizar. Cada cuenta olvidada puede conservar información.

7. REVISA PERMISOS DEL TELÉFONO

Haz un ejercicio práctico.

Abre la configuración de privacidad de tu dispositivo.

Revisa qué aplicaciones acceden a ubicación, micrófono, cámara, contactos, archivos, calendario.

Para cada una pregunta:

¿Esta aplicación necesita realmente este permiso para la función que utilizo?

Si no: retíralo.

No tienes que borrar internet.

Empieza eliminando accesos innecesarios.

8. UBICACIÓN: UN DATO ESPECIALMENTE REVELADOR

Nuestra ubicación puede mostrar: dónde vivimos, dónde trabajamos, qué lugares frecuentamos, a qué horas nos movemos.

Revisa: qué aplicaciones acceden; si necesitan acceso permanente; historiales de ubicación; fotografías que puedan incorporar metadatos; publicaciones en tiempo real.

Compartir una fotografía de vacaciones después de abandonar un lugar puede ser diferente de anunciar públicamente que tu casa está vacía durante dos semanas.

Privacidad también es contexto.

9. COOKIES Y RASTREO: ¿QUÉ ESTÁ PASANDO?

Las cookies son pequeños datos almacenados por sitios web para distintas funciones.

Algunas pueden ser necesarias para mantener una sesión, recordar preferencias, guardar un carrito.

Otras pueden relacionarse con medición, personalización o publicidad.

Por eso no todas las cookies son iguales.

Cuando un sitio ofrece controles reales, revisa categorías en lugar de pulsar automáticamente: **“Aceptar todo”**.

10. PUBLICIDAD PERSONALIZADA

¿Alguna vez buscaste algo y después comenzaste a verlo repetidamente?

La publicidad digital puede utilizar diferentes señales y perfiles para intentar mostrar anuncios relevantes.

Puedes revisar, cuando las plataformas lo permitan: preferencias publicitarias; personalización; historial; actividad; conexiones con otros servicios.

No conseguirás necesariamente desaparecer del ecosistema publicitario.

Pero puedes entenderlo mejor y reducir determinados niveles de personalización o seguimiento.

11. LA NUBE NO ES UN LUGAR MÁGICO

Cuando guardamos algo “en la nube”, nuestros datos se almacenan y procesan mediante infraestructura administrada por determinados proveedores.

Pregunta:

- ¿qué estoy guardando?
- ¿quién ofrece el servicio?
- ¿qué seguridad proporciona?
- ¿cómo recupero mis datos?
- ¿puedo exportarlos?
- ¿qué ocurre si pierdo acceso a la cuenta?

La comodidad es valiosa.

Pero evita que toda tu vida digital dependa de un único punto que no

12. MINIMIZACIÓN: ENTREGA SOLO LO NECESARIO

Un principio extremadamente útil:

menos datos almacenados = menos datos potencialmente expuestos.

Antes de entregar información pregunta: ¿es necesaria?

Antes de conservarla: ¿todavía la necesito?

Antes de solicitarla a otra persona: ¿realmente necesitamos recopilarla?

Este principio sirve tanto para individuos como para organizaciones.

13. PRIVACIDAD PARA COLECTIVOS Y PEQUEÑAS ORGANIZACIONES

Imagina una asociación que guarda:

- Nombres
- Documentos
- Teléfonos
- Correos
- Fotografías
- Datos de participantes

Pregunta:

- ¿POR QUÉ LOS GUARDAMOS?
- ¿DÓNDE?
- ¿QUIÉN TIENE ACCESO?
- ¿DURANTE CUÁNTO TIEMPO?
- ¿QUÉ OCURRE SI SE FILTRAN?
- ¿NECESITAMOS TODOS ESOS DATOS?

Una hoja de cálculo olvidada también puede convertirse en un problema de privacidad.

14. SOBERANÍA DIGITAL: MÁS ALLÁ DE LA PRIVACIDAD

Privacidad pregunta: ¿quién puede acceder a mis datos?

Soberanía digital añade preguntas:

- ¿de quién dependen mis herramientas?
- ¿puedo llevarme mis datos?
- ¿puedo cambiar de proveedor?
- ¿entiendo las reglas fundamentales del servicio?
- ¿qué ocurre si mañana desaparece o cambia sus condiciones?

No significa rechazar grandes plataformas.

Significa evitar dependencias innecesarias y conservar capacidad de elección.

15. PORTABILIDAD: ¿PUEDES LLEVARTE TU VIDA DIGITAL?

Imagina que mañana quieres abandonar una plataforma.

¿Puedes descargar tus fotografías, documentos, contactos, publicaciones, archivos?

¿En un formato útil?

Si tus datos pueden entrar fácilmente pero salir es extremadamente difícil, existe una dependencia.

Por eso conviene conocer las opciones de:
exportación + copia + migración.

16. SOBERANÍA TAMBIÉN SIGNIFICA NO DEPENDER DE UN SOLO CANAL

Una organización construye una comunidad de 100.000 seguidores en una plataforma.

Un día pierde la cuenta.

Cambia el algoritmo. La plataforma reduce el alcance.

¿Qué queda?

Por eso es útil construir activos y canales complementarios:

- ☐ web
- ☐ correo
- ☐ comunidad
- ☐ distintos canales
- ☐ bases de contactos obtenidas y gestionadas legítimamente.

No construyas toda una comunidad sobre terreno prestado.

17. AUDITORÍA PERSONAL DE 30 MINUTOS

Revisa permisos.

5-10: Elimina aplicaciones innecesarias.

10-15: Revisa ubicación.

15-20: Comprueba cuentas antiguas.

20-25: Revisa privacidad y publicidad en servicios principales.

25-30: Comprueba que tus datos importantes tengan copia y puedan recuperarse.

Repite esta auditoría periódicamente.

18. EL SEMÁFORO DE DATOS

Antes de compartir información clasifícala.

VERDE

Información que no te preocupa hacer pública.

AMARILLO

Información que compartirías solo con determinados servicios o personas.

ROJO

Información sensible o de alto impacto.

Ejemplos: credenciales, información financiera, determinados documentos personales o información confidencial.

La clasificación concreta depende del contexto.

Lo importante es desarrollar el hábito: no todos los datos merecen el mismo nivel de exposición.

19. CHECKLIST DE SOBERANÍA DIGITAL

Sé qué aplicaciones utilizo.
Reviso sus permisos.
Elimino cuentas innecesarias.
Controlo razonablemente mi ubicación.
Reviso configuraciones de privacidad.
Tengo copias de información importante.
Sé cómo exportar mis datos principales.
No dependo de un único canal crítico.
Sé quién accede a datos de mi organización.
Evito recopilar información innecesaria.
Protejo especialmente los datos sensibles.
Reviso periódicamente mi huella digital.

No necesitas conseguir doce de doce inmediatamente.
Empieza por aquello que tenga mayor impacto.

20. DE LA SOBERANÍA PERSONAL A LA COMUNITARIA

Existe una dimensión todavía mayor.

Una comunidad puede depender completamente de herramientas digitales que:

- no controla
- no comprende
- no puede modificar
- no puede extraer fácilmente su información.

Por eso también podemos construir: alfabetización digital comunitaria; repositorios compartidos; protocolos de datos; formación tecnológica; copias descentralizadas; conocimiento sobre herramientas abiertas cuando sean adecuadas; capacidad local para administrar infraestructura.

La soberanía digital no significa que cada comunidad tenga que construir su propio internet.

Significa tener suficiente conocimiento y capacidad para elegir, migrar, protegerse y negociar sus dependencias tecnológicas.

21. EJERCICIO FINAL — TU PLAN DE SOBERANÍA DIGITAL

Completa:

MIS TRES CUENTAS MÁS IMPORTANTES

1. _____
2. _____
3. _____

- LOS DATOS QUE MÁS NECESITO PROTEGER: _____
- DOS PERMISOS QUE PUEDO REVISAR HOY: _____
- UNA CUENTA QUE YA NO NECESITO: _____
- INFORMACIÓN QUE NECESITO RESPALDAR: _____
- SERVICIO DEL QUE DEPENDO DEMASIADO: _____
- ALTERNATIVA O PLAN DE CONTINGENCIA: _____

Ahora ya no tienes solamente información.
Tienes acciones.

22. NUESTROS DATOS TAMBIÉN SON PARTE DE NUESTRA AUTONOMÍA

No necesitamos abandonar internet para proteger nuestra privacidad.
Necesitamos utilizarlo con mayor conciencia.

Preguntar:

- ¿Qué estoy entregando?
- ¿A quién?
- ¿Para qué?
- ¿Durante cuánto tiempo?
- ¿Puedo recuperarlo?
- ¿Puedo marcharme?

Y existe una dimensión colectiva.

Cuando comunidades, organizaciones y pequeños proyectos dependen completamente de infraestructuras que no comprenden, su autonomía también disminuye. por eso necesitamos redes comunitarias que compartan capacidades tecnológicas, formen a sus miembros y desarrollen alternativas cuando sean necesarias.

La Red Mundial Multitalentos puede servir también para conectar ese conocimiento: personas que saben de tecnología, comunicación, educación, economía, cultura o territorio ayudándose mutuamente a construir capacidades.

No se trata de controlar absolutamente todos nuestros datos.

Se trata de recuperar algo mucho más realista y valioso: mayor capacidad de decidir sobre nuestra vida digital.

Porque la tecnología debería ampliar nuestra autonomía.

No convertir nuestra dependencia en algo invisible.

De idea a impacto

INTELIGENCIA ARTIFICIAL

Una guía práctica para aprovechar el potencial de la IA sin perder lo más importante: tu criterio, tu autonomía y tu capacidad de decidir

Aprende a usar la IA como aliada para explicar, organizar, explorar, transformar, analizar y automatizar tareas en tu vida y tu trabajo.



SÍGUENOS EN NUESTRAS REDES SOCIALES



@librestaelflautista
@librestaJovenesTalentos

Conoce
más en:

WWW.LIBRESTA.ORG

LibreSta

El Flautista

