XUNTA DE GALICIA | CONSELLERÍA DE EDUCACIÓN, CIENCIA, UNIVERSIDADES E FORMACIÓN PROFESIONAL

L2501022 - Privacidade. Seguridade e benestar dixital

Nuria Campo Campo

Monforte de Lemos, 28 e 30 abril 2026

XUNTA DE GALICIA | CONSELLERÍA DE EDUCACIÓN, CIENCIA, UNIVERSIDADES E FORMACIÓN PROFESIONAL

Plan Integral de Benestar Dixital de Galicia
Xaneiro 2026

O plan busca garantir un uso saudable, seguro e responsable da tecnoloxía, especialmente en infancia e adolescencia, implicando escola, familias, administracións e sociedade.

A tecnoloxía non é o problema: o reto é como utilizala de forma consciente, ética e equilibrada.

Obxectivos clave

- **Protexer os dereitos fundamentais no ámbito dixital**
- **Promover o benestar emocional e hábitos saudables**
- **Fomentar o pensamento crítico e uso responsable**
- **Previr riscos como:**
  - **ciberacoso**
  - **adicción dixital**
  - **desinformación**
- **Crear unha cidadanía dixital responsable**

Dimensións do impacto tecnolóxico

O plan identifica 6 áreas principais:

1. **Dereitos e valores democráticos**
2. **Hábitos de vida**
3. **Convivencia familiar e escolar**
4. **Aprendizaxe e cognición**
5. **Socialización**
6. **Riscos e ciberseguridade**

Piares fundamentais

1. **Igualdade de acceso dixital**
2. **Contornas seguras**
3. **Participación da infancia**
4. **Coordinación institucional**

Estrutura do plan: 5 eixes

1. Sensibilización en dereitos dixitais
   - Educación sobre dereitos e riscos
   - Campañas, xogos educativos e actividades
2. Centros educativos saudables
   - Uso equilibrado da tecnoloxía
   - Benestar emocional (ex: “apagamento dixital”)
3. Uso seguro e responsable
   - Pensamento crítico e alfabetización mediática
   - Formación a alumnado, profesorado e familias

4. Coordinación institucional

- **Colaboración entre educación, sanidade e tecnoloxía**
- **Protocolos ante riscos dixitais**

5. Comunicación e participación

- **Difusión do plan**
- **Espazos de debate e participación social**

Seguimento e avaliación

- **Sistema de indicadores (si/non)**
- **Revisión anual**
- **Análise da participación e impacto**
- **Adaptación continua do plan**

Duración

- **Período: 2026–2030**

A protección da infancia no mundo dixital é unha responsabilidade compartida.
Só coa colaboración de todos se pode garantir un entorno dixital seguro, ético e saudable.

Seguridade e privacidade dixital

Creación de contidos dixitais

O profesorado pode crear diferentes tipos de recursos:

Presentacións, vídeos e podcasts educativos

Actividades interactivas (cuestionarios, xogos, simulacións)

Aulas virtuais/Agueiro

Materiais accesibles (con subtítulos, lectura fácil, etc.)

Boas prácticas:

- **Adaptar os contidos ao nivel do alumnado**
- **Empregar licenzas abertas como Creative Commons**
- **Fomentar a participación e o pensamento crítico**

Relación entre ambos aspectos

A creación de contidos dixitais debe integrar a seguridade desde o inicio:

- **Deseñar actividades que non requiran datos sensibles**
- **Empregar ferramentas que cumpran estándares de privacidade**
- **Avaliar riscos antes de publicar materiais**

Que é a seguridade dixital?

- **Protexer información persoal**
- **Evitar accesos non autorizados**
- **Previr fraudes e ataques**

Que é a privacidade dixital?

1. **Protexer os dispositivos.**
2. **Protexer os datos persoais.**
3. **Protexer a saúde e o benestar.**

Contorna dixital e solución de problemas

Coñecer a contorna, configurar os dispositivos tecnolóxicos e resolver problemas técnicos, identificar as necesidades de resposta tecnolóxica, usar as tecnoloxías de forma innovadora e creativa e identificar fallas nos coñecementos dixitais.

Riscos na contorna dixital:

⚠️ Principais ameazas:

- **Phishing (suplantación de identidade).**
- **Malware (virus).**
- **Roubo de contrasinais.**
- **Ciberacoso.**
- **Uso indebido de imaxes e ou vídeos.**

Casos reais:

- **Correos falsos que simulan ser de plataformas educativas.**
- **Suplantación en apps corporativas ou outras.**

Actividade práctica:

- **Analizar un correo falso e detectar sinais de fraude.**

Riscos na contorna dixital para alumnado e docentes

Riscos para o alumnado

Seguridade e privacidade

- Exposición de datos persoais (nome, ubicación, centro educativo)
- Uso de contrasinais débiles ou compartidas
- Roubo de contas

Interacción social

- Ciberacoso (insultos, ameazas, exclusión)
- Contacto con descoñecidos (grooming)
- Presión social en redes

Uso de contidos

Posible acceso a contidos inapropiados

Difusión de imaxes e ou vídeos sen consentimento

Pegada dixital negativa a longo prazo

Benestar dixital

Uso excesivo de pantallas

Dependencia de redes sociais

Impacto na autoestima

Cuadros de ansiedade/depresión

Riscos para docentes

🔐 Seguridade profesional

Suplantación de identidade

Roubo de credenciais de acceso a plataformas educativas

Ataques de phishing

Protección de datos

- **Manexo inadecuado de datos do alumnado**
- **Compartir información sensible sen protección**
- **Incumplimento do Reglamento Xeral de Protección de Datos**

Imaxe e reputación

- **Uso non autorizado da súa imaxe ou contidos**
- **Gravacións en clase difundidas sen permiso**
- **Confusión entre vida persoal e profesional nas redes**

Relación con alumnado e familias

- **Emprego de canles non oficiais (ex. WhatsApp)**
- **Malentendidos na comunicación dixital**
- **Falta de límites profesionais**

Riscos compartidos (centro educativo)

- **Uso inseguro de plataformas como Google Classroom o Moodle**
- **Fugas de información**
- **Accesos non autorizados a sistemas do centro**
- **Falta de protocolos de seguridade**

Claves para previr

- **Formación en seguridad dixital**
- **Uso de contrasinais seguras e 2FA**
- **Emprego de plataformas oficiais**
- **Educación en cidadanía digital**
- **Protocolos claros no centro**

Contrasinais e autenticación segura

Contidos:

- Creación de contrasinais robustas
- Uso de xestores de contrasinais
- Autenticación en dous factores (2FA)

Actividade práctica:

- Avaliar a seguridade de contrasinais con ferramentas online.

Privacidade na aula dixital:

Contidos:

- **Uso responsable de imaxes e vídeos do alumnado.**
- **Consentimento informado.**
- **Atención ao uso de redes sociais e exposición dixital.**

Actividade práctica:

- **Crear un protocolo de uso de uso de imaxes no centro.**

Dispositivos e redes seguras

Contidos:

- **Seguridade en dispositivos persoais e do centro.**
- **Redes WiFi seguras**
- **Actualizacións e antivirus**

Actividade práctica:

- **Checklist de seguridade para dispositivos docentes**

Cidadanía dixital e uso responsable:

Contidos:

- **Educación en ciberseguridad para o alumnado**
- **Prevención do ciberacoso**
- **Pegada dixital**

Actividade práctica:

- **Deseño dunha actividade para o alumnado sobre seguridade online.**

Seguridade en plataformas educativas

Contidos:

- **Uso seguro de plataformas educativas.**
- **Configuración da privacidade en contornas virtuais.**
- **Control de accesos e permisos.**

Actividade práctica:

- **Configurar correctamente unha aula virtual segura.**

Xestión de incidentes:

Contidos:

- **Que facer ante unha brecha de seguridade?**
- **Protocolos de actuación.**
- **Comunicación coa Administración e coas familias.**

Actividade práctica:

- **Simulación de incidente de seguridade dixital no centro.**

Checklist de Seguridade e Privacidade Dixital para Docentes

🔐 1. Contrasinais e accesos

- Uso contrasinais longos (mínimo 12 caracteres) e únicos para cada conta
- Non reutilizo contrasinais entre plataformas educativas e persoais
- Teño activada a verificación en dous pasos (2FA)
- Utilizo un xestor de contrasinais seguro
- Pecho sesión en dispositivos compartidos

2. Xestión de datos do alumnado

- **Só recollo os datos estritamente necesarios**
- **Almaceno a información en plataformas seguras**
- **Non comparto datos persoais por correo sen protección**
- **Anonimizo datos cando é posible**
- **Cumpro co Regulamento Xeral de Protección de Datos**

3. Uso de plataformas educativas

- **Configuro correctamente a privacidade na Aula virtual, Agueiro.**
- **Reviso os permisos de acceso do alumnado**
- **Evito compartir ligazóns públicas sen control**
- **Uso contas institucionais no canto de persoais**

4. Dispositivos seguros

- **Manteño actualizado o sistema operativo**
- **Teño instalado antivirus ou protección activa**
- **Bloqueo o dispositivo con contrasinal ou biometría**
- **Non instalo aplicacións de fontes descoñecidas**
- **Fago copias de seguridade periódicas**

5. Navegación e correo electrónico

- **Verifico remitentes antes de abrir correos ou ligazóns**
- **Non descargo arquivos sospeitosos**
- **Identifico intentos de phishing**
- **Uso conexións seguras (HTTPS)**

6. Uso de imaxes e contidos do alumnado

- **Teño consentimento para usar imaxes ou vídeos**
- **Non publico contido do alumnado en redes sen autorización**
- **Evito mostrar datos identificativos nas imaxes**
- **Uso plataformas pechadas para compartir contidos**

7. Interacción dixital co alumnado

- **Uso canles oficiais do centro educativo**
- **Manteño límites profesionais na comunicación**
- **Evito o uso de redes sociais persoais co alumnado**

8. Prevención e actuación ante incidentes

- **Sei como actuar ante un posible ciberataque ou fuga de datos**
- **Informo ao centro educativo de calquera incidente**
- **Cambio os contrasinais se detecto actividade sospeitosa**
- **Teño claro o protocolo de seguridade do centro**

9. Educación en cidadanía dixital

- **Ensino boas prácticas de seguridade ao alumnado**
- **Promovo o respecto e a privacidade en liña**
- **Traballo a prevención do ciberacoso**

Lista de verificación: Uso seguro dunha aplicación educativa

🔍 1. Avaliación inicial da aplicación

- Coñezo quen desenvolveu a aplicación (empresa ou organización responsable)
- Revisei as políticas de privacidade e uso de datos
- A aplicación cumpre co Regulamento Xeral de Protección de Datos
- Sei onde se almacenan os datos (UE / fóra da UE)
- A aplicación é adecuada para a idade do alumnado

2. Rexistro e acceso

- **Utilizo contas institucionais en lugar de persoais**
- **Evito rexistrar ao alumnado con datos innecesarios**
- **Configuro contrasinais seguros para o acceso**
- **Activo a verificación en dous pasos (se está dispoñible)**
- **Xestiono correctamente os permisos de acceso**

3. Configuración de privacidade

- **Reviso e configuro as opcións de privacidade antes de usala**
- **Limito a visibilidade dos perfís do alumnado**
- **Desactivo opcións públicas por defecto (perfís, publicacións, etc.)**
- **Controlo quen pode ver e compartir os contidos**

4. Uso na aula

- **Explico ao alumnado como usar a aplicación de forma segura**
- **Non comparto información persoal innecesaria**
- **Superviso a actividade do alumnado dentro da aplicación**
- **Evito o uso de chats ou interaccións non controladas (se é posible)**

5. Contidos e privacidade

- **Non subo imaxes ou vídeos do alumnado sen consentimento**
- **Evito publicar información identificativa**
- **Reviso os contidos antes de facelos visibles**
- **Uso contornos pechados ou restrinxidos**

6. Xestión de datos

- **Sei como eliminar contas e datos cando xa non se usan**
- **Evito almacenar información sensible innecesaria**
- **Fago revisións periódicas dos datos gardados**
- **Exporto ou borro datos ao finalizar o curso**

7. Seguridade e incidencias

- **Sei como actuar se hai unha brecha de seguridade**
- **Informo ao centro educativo ante calquera problema**
- **Actualizo a aplicación regularmente**
- **Cambio contrasinais ante actividade sospeitosa**

8. Educación e boas prácticas

- **Ensino ao alumnado normas de uso seguro da aplicación**
- **Promovo o respecto e a privacidade dixital**
- **Fomento o pensamento crítico sobre o uso das apps**

REDES SOCIALES >

Los adolescentes que crecieron sin ningún límite en las redes sociales: “Mis padres me dieron el móvil y, a partir de ahí, tiré sola”

Jóvenes que tuvieron su primer móvil a los 12 recuerdan una adolescencia sin normas digitales y reflexionan sobre el papel de los adultos

Texto completo

La falta de educación digital dispara los riesgos entre menores: normalizan invasiones de privacidad y el contacto con desconocidos

25. Marzo 2026

Texto completo

Un informe realizado en 60 centros educativos

Los datos del informe de ARAG se han obtenido a partir de 3.099 encuestas realizadas entre noviembre de 2024 y diciembre de 2025 al alumnado que participó en la formación gratuita “Los Peligros en la Red”. Esta charla forma parte del programa de RSC “Hechos y Derechos”, en el que abogados y abogadas de la aseguradora enseñan a los menores cómo defenderse cuando sus derechos son vulnerados, además de recordarles que sus propias acciones también pueden tener consecuencias legales.

Actualmente, el programa ofrece dos temáticas: “La Ley de Responsabilidad Penal de los Menores” y la ya mencionada “Los Peligros en la Red”.

Texto completo

Un 25% de los menores que juegan online ha vivido experiencias negativas

El 68% de los jóvenes encuestados participa habitualmente en videojuegos online y, entre ellos, uno de cada cuatro ha sufrido griefing: acoso dentro del propio juego o en sus chats, a través de mensajes insultantes o de contenido sexual.

“En los juegos online se reúnen jugadores de todo el mundo, y el riesgo está en que no siempre sabemos quién hay realmente detrás de la pantalla”, señala González. La solución, apunta, pasa por la educación: “Es fundamental informar a los menores sobre aquello que nunca deben hacer —como compartir datos personales— y sobre los peligros a los que pueden exponerse”.

Además del griefing, los menores deben aprender a identificar y reaccionar ante situaciones de ciberacoso o de grooming, cuando un adulto gana la confianza de un menor con fines sexuales.

Texto completo

Actividades prácticas:

1. **Pesquisar na rede sobre nós mesmos. Comprobar que datos aparecen e de onde poden proceder.**
2. **Propoñer como se podería evitar a súa aparición.**
3. **Avaliar a fortaleza das nosas contrasinais.**
4. **Protección de dispositivos.**
5. **Revisar un dos teus dispositivos e identificar tres melloras de seguridade (ex. permisos app, localización, etc.).**

6. **Revisar a páxina web do teu centro, identificar situacións relacionadas coa posible mellora da protección de datos.**
7. **Un/unha alumno/a solicita revisar todos os seus datos. A onde ten que dirixirse e cal é o procedemento?**
8. **A túa compañeira de nivel/departamento non está de acordo con que a reunión de Claustro sexa telemática e se grave?**
9. **Un compañeiro comparte nun grupo WhatsApp fotos dunha actividade nas que sae o docente e os demais compañeiros/as.**
10. **Unha empresa colaboradora pide datos do alumnado.**
11. **Analizar publicacións da rede (realidade vs. fakenews).**

12. **Auditar o teu teléfono móbil. Revisar os permisos das apps (ubicación, cámara, micrófono). Detectar apps con acceso innecesario. Ídem ordenador.**
13. **O teu centro vai trasladar á ANPA unha listaxe de alumnado interesado en participar nunha actividade. Pode facelo?**
14. **A orientadora do teu centro remitiu un informe dunha alumna ao EOE. A familia pon unha queixa na que manifesta que non se lle pediu permiso.**
15. **A parella do pai de Lucía solicita información académica da nena. A titora non sabe se pode facilitarlla.**

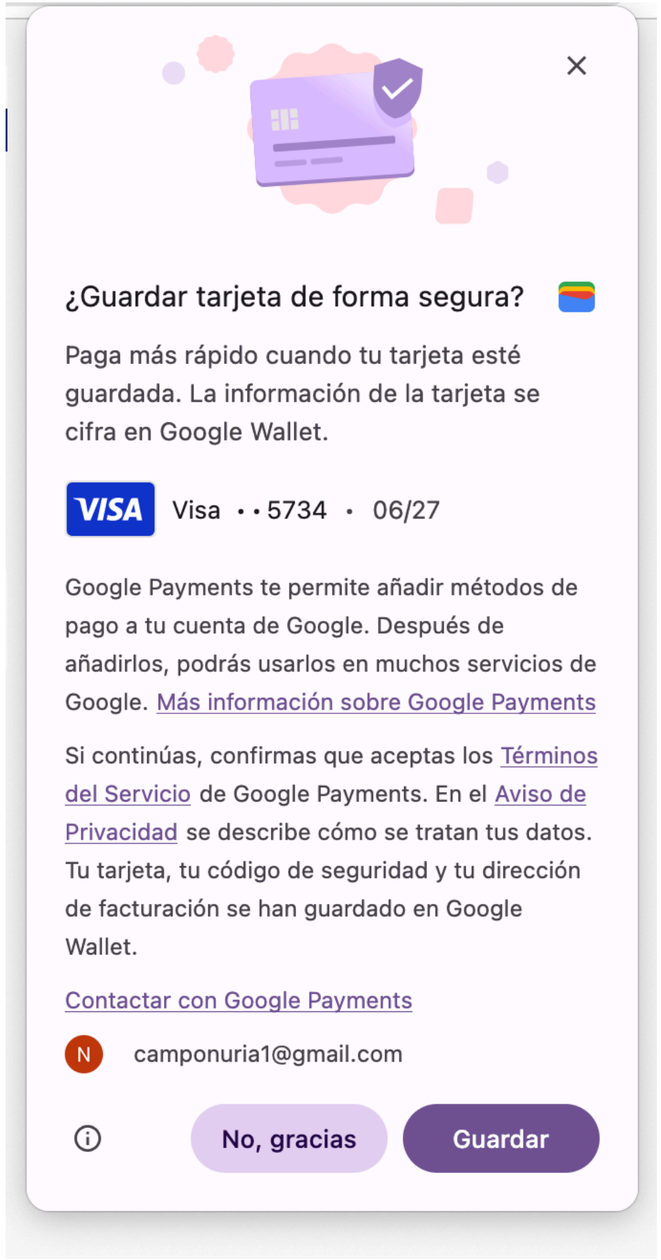
16. **Luis vai facer as prácticas nun taller de Monforte. O dono solicítalle ao IES que lle envíe os datos persoais do alumno. Pode facelo?**
17. **Os alumnos de 4º EP saen de excursión. A empresa de transporte solicítalle ao centro unha listaxe de alumnado e datos persoais para incorporar ao seguro de viaxes. Pode o centro envialos?**
18. **Un centro quere solicitar no formulario de matrícula información sobre a profesión dos proxenitores. Pode facelo?**

19. **Un alumno cambia de centro e o centro de orixe envía o seu expediente académico ao novo centro sen pedir permiso.**
20. **Un centro publica na súa web aberta ao público unha lista co nome completo e o DNI completo de alumnado admitido.**
21. **Un centro reutiliza datos do alumnado doutros cursos sen volver solicitalos.**
22. **O centro publica fotos do alumnado nunha rede social sen pedir autorización.**
23. **Un alumno de 15 anos consinte o uso da súa imaxe nun cartel escolar.**
24. **Un pai pide datos doutro alumno implicado nun conflito co seu fillo.**

Pautas fundamentais de seguridade dixital:

- **Bloqueo robusto: emprega PINs longos, contrasinais seguras ou biometría para evitar accesos non autorizados.**
- **Actualizacións automáticas: mantén o sistema operativo e as aplicación actualizadas para corrixir vulnerabilidades.**
- **Fontes oficiais: descarga aplicacións unicamente desde sitios oficiais.**
- **Seguridade en redes: evita redes Wi-Fi públicas. Desactiva Bluetoothe e Wi-Fi se non os estás empregando.**
- **Realiza copias periódicas dos teus arquivos.**
- **Autenticación en dous factores (2FA): engade capa extra de protección.**

- **Xestión de contrasinais: emprega contrasinais únicas para cada sitio e usa un xestor de contrasinais.**
- **Antivirus e Antimalware: instala solucións de seguridade fiables, tanto no ordenador como no móbil.**
- **Verificación de permisos: revisa e limita os permisos das aplicacións, especialmente o acceso á cámara, micrófono e contactos.**
- **Cifrado de datos: activa o cifrado na configuración do dispositivo para protexer a túa información.**
- **Coidado co Phishing: non fagas clic en ligazóns nin descargues arquivos de correos ou mensaxes sospeitosas.**


¿Guardar tarjeta de forma segura?
Paga más rápido cuando tu tarjeta esté guardada. La información de la tarjeta se cifra en Google Wallet.
VISA Visa ••5734 • 06/27
Google Payments te permite añadir métodos de pago a tu cuenta de Google. Después de añadirlos, podrás usarlos en muchos servicios de Google. Más información sobre Google Payments
Si continúas, confirmas que aceptas los Términos del Servicio de Google Payments. En el Aviso de Privacidad se describe cómo se tratan tus datos. Tu tarjeta, tu código de seguridad y tu dirección de facturación se han guardado en Google Wallet.
Contactar con Google Payments
N camponuria1@gmail.com
No, gracias
Guardar

Introduce la contraseña de permisos

SkAf*FM399t*RrQ

Enter permission password

Repite la contras

SkAf*FM399t*Rr

Re-enter permis

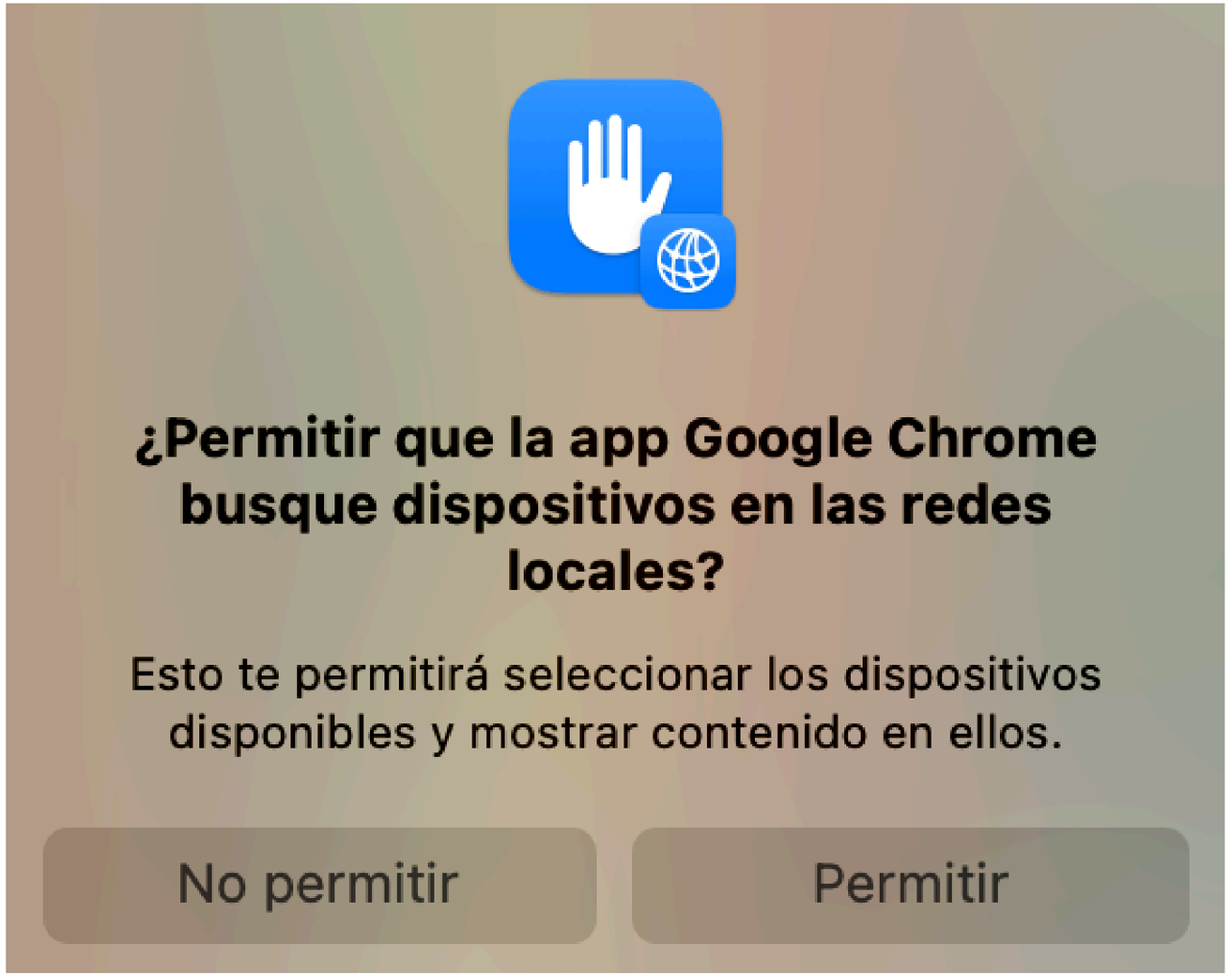
Gestor de contraseñas de Google ha creado una contraseña segura para este sitio web

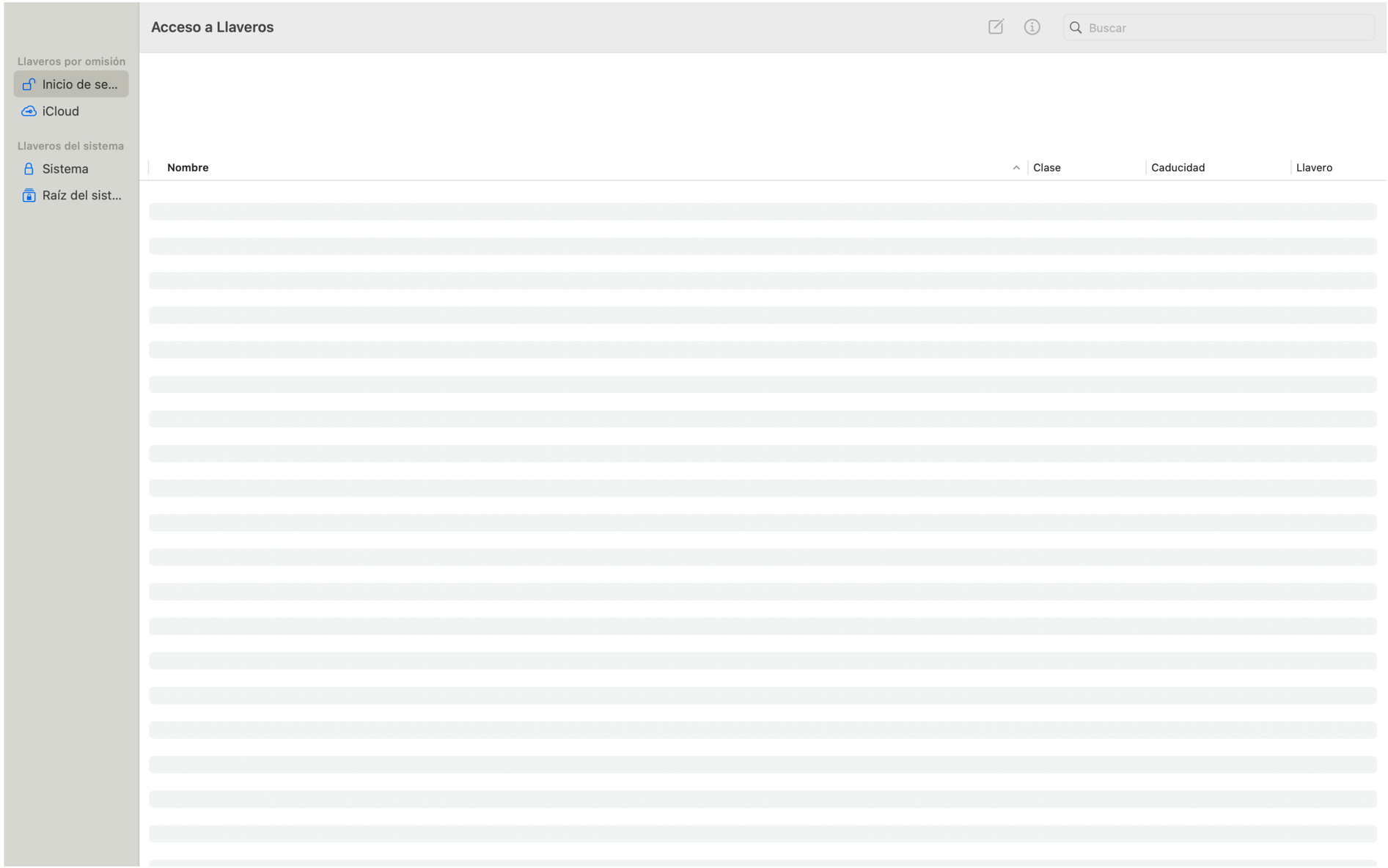
No tendrás que recordar esta contraseña. Se guardará en el Gestor de contraseñas de Google de camponuria1@gmail.com.

Elegir una personalizada

Usar contraseña segura

Ajustes opcionales


¿Permitir que la app Google Chrome busque dispositivos en las redes locales?
Esto te permitirá seleccionar los dispositivos disponibles y mostrar contenido en ellos.
No permitir
Permitir


Acceso a Llaveros
Buscar
Llaveros por omisión
Inicio de se...
iCloud
Llaveros del sistema
Sistema
Raíz del sist...
Nombre
Clase
Caducidad
Llavero

Como protexer unha carpeta?

Como limitar os permisos de edición dun pdf?

https://www.pdf2go.com/es/proteger-pdf