



Esta traducción se facilita a título informativo. Solo la versión alemana es jurídicamente vinculante. [Ver la versión alemana](#)

Protección de datos para centros escolares en una página

Oferta escolar de secureIT · para delegados de protección de datos y titulares de centros · versión de 03.10.2026 (versión 1.0)

1. ¿Quién es el responsable?

El centro escolar es el responsable del tratamiento, en el sentido del RGPD, de los datos de su alumnado y de sus docentes. Decide si se utilizan cursos y cuáles. **secureIT UG (haftungsbeschränkt)** (Patrick Ihle, Breisgau) gestiona la plataforma y trata los datos exclusivamente por encargo del centro (art. 28 del RGPD). El contrato de encargo del tratamiento se perfecciona con el registro de la cuenta del centro y está disponible en PDF para archivarlo.

2. ¿Qué se guarda sobre el alumnado?

Lo menos posible. No hay **cuenta de alumno, ni aplicación, ni registro por correo electrónico**.

- **Para participar en clase:** el nombre de pila (de libre elección, también puede ser un apodo) y una cookie de reconocimiento en el propio dispositivo. Nada más. Las respuestas a las preguntas de cuestionario, las nubes de palabras y los juegos se asignan a la clase, no se califican y no se comunican al docente como resultado individual.
- **Formación en phishing solo en el curso «Autodefensa digital» y solo con consentimiento:** al final de este curso (de 8.º a 10.º curso), los alumnos pueden participar, con el consentimiento de sus padres (modelo en la carta a las familias), en el escenario de prueba de phishing de secureIT: tres intentos de fraude simulados por correo electrónico, elaborados de forma profesional, que muestran si se reconoce un intento de fraude preparado. Para ello se registra una dirección de correo electrónico; solo es visible en el Cockpit del docente, nunca en la vista del curso de la clase. El certificado acredita la participación satisfactoria en esta formación y solo se expide en caso de participación. Sin participación: participar en clase, sí; datos, ninguno; certificado, ninguno.
- **En la prueba de phishing:** solo se guarda si un correo se entregó, se abrió, se hizo clic en él o se notificó. **Las contraseñas introducidas nunca se guardan**, solo el hecho de que se introdujo algo. El resultado solo lo ve la propia persona; el docente no recibe ninguna lista de quién hizo clic.
- **Supresión:** los datos de los certificados se suprimen automáticamente al cabo de 60 días. Los datos del curso y de la prueba los suprime el propio centro en cualquier momento en el Cockpit o a petición dirigida a mí, sin formulario y sin plazo.

3. ¿Qué se guarda sobre los docentes?

- **Cockpit del centro:** nombre y dirección de correo electrónico profesional de la dirección del centro y de los docentes registrados, la contraseña solo como hash, y la fecha y hora del último inicio de sesión. Cada docente ve exclusivamente sus propios cursos.
- **Formación para el claustro (opcional):** nombre, dirección de correo electrónico profesional, finalización del curso con fecha, eventos de la simulación como se indica arriba. La dirección del centro ve la participación y la finalización del curso (para el justificante de formación), nunca el comportamiento de clic de personas concretas. Antes del inicio debe darse participación a la junta de personal (Personalrat, órgano de representación del personal docente); hay disponible un modelo de acuerdo de servicio (Dienstvereinbarung).

4. ¿Dónde están los datos?

En servidores de IONOS SE en Alemania (centro de datos con certificación ISO 27001). Todas las conexiones están cifradas con TLS. No hay **cesión a terceros**, ni publicidad, ni seguimiento, ni scripts ni fuentes externas cargados desde servidores ajenos. También los juegos didácticos se ejecutan íntegramente desde la plataforma. La estadística de visitas propia funciona sin cookies y sin referencia a personas.

5. Base jurídica

Para el centro escolar: cumplimiento de su misión educativa y formativa (art. 6.1.e) del RGPD en relación con la Ley de





Educación de Baden-Württemberg, Schulgesetz). Para la indicación voluntaria de una dirección de correo electrónico por parte del alumnado: consentimiento (art. 6.1.a) del RGPD); en el caso de menores, se recomienda informar a los padres; la carta a las familias para ello está disponible. Para los docentes: relación de servicio (§ 15 LDSG BW, Ley de Protección de Datos de Baden-Württemberg) y, en su caso, el acuerdo de servicio con la junta de personal.

6. Costes e intereses

Para los centros escolares todo es gratuito: cursos, Cockpit, juegos, certificados, formación para el claustro. No hay licencia, ni duración mínima, ni publicidad en clase, ni intención de venta frente al alumnado, las familias o los docentes. La oferta se financia a través de los clientes empresariales de secureIT.

7. Persona de contacto

Patrick Ihle, secureIT UG (haftungsbeschränkt), info@secureit-online.de, +49 157 58278025. Respondo directamente a las preguntas del delegado de protección de datos o del titular del centro (Schulträger), por lo general el mismo día.

8. Documentos para archivar

- Contrato de encargo del tratamiento (art. 28 del RGPD): <https://secureit.icu/es/auftragsverarbeitung.pdf>
- Modelo de acuerdo de servicio con la junta de personal: <https://secureit.icu/es/schulen/muster-dienstvereinbarung.pdf>
- Hoja informativa para el claustro: <https://secureit.icu/es/schulen/infoblatt-kollegium.pdf>
- Hoja informativa sobre el ponente y secureIT: <https://secureit.icu/es/schulen/infoblatt-secureit.pdf>
- Carta a las familias como modelo: <https://secureit.icu/es/schulen/elternbrief.pdf>
- Política de privacidad general: <https://secureit.icu/es/datenschutz>

Editor: secureIT UG (haftungsbeschränkt), Patrick Ihle. Esta hoja describe el tratamiento real en la plataforma secureit.icu y se actualiza cuando hay cambios; prevalece la versión vigente en secureit.icu/schulen/datenschutz.