Política de Seguridad

<?xml encoding="utf-8" ?>

Política de Seguridad de la Aplicación Safety Software (SaaS)

ID: SE-2026-V2
Actualización: 2026-03-05

1. Finalidad y alcance

La presente Política de Seguridad define las normas de protección de la información y de los datos tratados en el marco de la aplicación Safety Software proporcionada en el modelo Software as a Service (SaaS).

El documento se refiere a la seguridad de los usuarios que utilizan la aplicación en el servicio Safety Software y constituye un complemento de los Términos y Condiciones y de la Política de Privacidad.

La Política tiene carácter informativo y describe las medidas técnicas y organizativas básicas aplicadas por Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Kraków, Polonia (en adelante: el «Administrador»).

2. Modelo de responsabilidad

El sistema opera bajo un modelo de responsabilidad compartida:

1. **Administrador (Safety Software)** es responsable de la seguridad del código de la aplicación, los mecanismos de inicio de sesión, autorización y sesión, la protección de datos en la capa de aplicación, la realización de copias de seguridad y la respuesta a incidentes de seguridad.

2. **Proveedores de infraestructura y servicios auxiliares** son responsables de la seguridad de los elementos que permanecen dentro del alcance de los servicios que prestan.

3. **Cliente** es responsable de la seguridad de sus dispositivos, contraseñas, identidades de usuario y de la gestión de los accesos dentro de su equipo.

3. Principios de seguridad de la aplicación

1. La transmisión de datos se realiza exclusivamente mediante cifrado TLS.

2. Las sesiones de usuario están protegidas mediante cookies con los atributos **HttpOnly**, **Secure** (para conexiones cifradas) y **SameSite**. Tras la autenticación se realiza la rotación del identificador de sesión.

3. Para las sesiones se aplican límites de inactividad y de duración máxima.

4. Las solicitudes que cambian el estado del sistema están protegidas con tokens CSRF verificados del lado del servidor.

5. La aplicación aplica una política de seguridad de contenidos restrictiva, incluidos mecanismos que limitan la ejecución de scripts no autorizados y los encabezados estándar de seguridad del navegador.

6. Se aplican mecanismos para limitar abusos, incluidos rate limiting y protección frente a intentos de inicio de sesión por fuerza bruta.

7. Cada operación se ejecuta en el contexto del usuario y de la organización; el acceso no autorizado se bloquea.

4. Cifrado y protección de datos

1. Las contraseñas de los usuarios se almacenan utilizando el algoritmo **bcrypt**.

2. Determinados datos sensibles almacenados en la base de datos se protegen mediante un modelo de cifrado de datos por envolvente. Las claves criptográficas se gestionan por separado en un sistema externo de gestión de claves.

3. Cuando está justificado, se aplican mecanismos que limitan la exposición de los datos manteniendo las funciones de búsqueda o identificación, sin necesidad de almacenar los valores completos en texto claro.

5. Copias de seguridad y recuperación (BCP/DR)

1. Aplicamos un enfoque por capas para las copias de seguridad: copias locales para una recuperación rápida y copias almacenadas fuera del entorno principal.

2. Las copias almacenadas fuera del entorno principal incluyen imágenes del entorno realizadas de forma incremental. Están cifradas, se validan periódicamente y están cubiertas por pruebas de recuperación.

3. La base de datos se protege mediante copias coherentes a nivel de aplicación. Además, se mantienen volcados locales de la base de datos que respaldan una recuperación rápida.

4. La integridad de las copias se verifica mediante mecanismos de control, incluidas sumas de verificación.

5. El proceso de realización de copias está automatizado, se ejecuta diariamente y está sujeto a monitorización del éxito y del fallo de las tareas.

6. Se realizan periódicamente pruebas de recuperación de datos, que incluyen al menos la recuperación de archivos seleccionados.

6. Monitorización y alertas

1. El sistema registra determinados eventos de seguridad y operaciones administrativas, en particular los relacionados con la autenticación, los intentos de acceso y el funcionamiento de procesos críticos.

2. Se aplican mecanismos de monitorización y alertas automáticas sobre el fallo de tareas, errores críticos y eventos que puedan indicar abuso o un incidente de seguridad.

3. El acceso a los logs y a la información operativa está limitado a las personas autorizadas.

7. Infraestructura y mantenimiento de la seguridad

1. El acceso administrativo está limitado a personas autorizadas y protegido mediante mecanismos de autenticación fuerte, incluida la autenticación mediante claves.

2. El inicio de sesión directo en una cuenta privilegiada está deshabilitado o limitado de acuerdo con el principio de mínimos privilegios.

3. Se aplican mecanismos de filtrado de tráfico, protección frente a intentos de acceso por fuerza bruta y monitorización de eventos de infraestructura.

4. Las actualizaciones de seguridad se implementan de forma regular.

5. Los servicios de correo utilizados para operar el sistema están protegidos mediante cifrado de la transmisión y mecanismos que limitan abusos.

8. Proveedores e integraciones

1. En la medida en que el sistema utilice servicios externos o integraciones auxiliares, la selección de soluciones tiene en cuenta la seguridad de los datos, el principio de minimización y el control del alcance de la información transmitida.

2. La comunicación con servicios externos se realiza mediante transmisión cifrada.

9. Notificación de incidentes

Las notificaciones relativas a la seguridad de la aplicación o sospechas de incidentes deben enviarse a la dirección:

office@safetysoftware.eu
Asunto del mensaje: SECURITY

Las notificaciones se analizan de acuerdo con el procedimiento interno de gestión de incidentes.

10. Conformidad y jurisdicción

1. Las medidas de seguridad se diseñan y mantienen teniendo en cuenta las disposiciones legales aplicables, incluidos los requisitos del **RGPD**, y las prácticas reconocidas de seguridad de la información.

2. La ley aplicable es la ley polaca.

3. En caso de discrepancias entre las versiones lingüísticas, prevalece la versión polaca.

11. Entrada en vigor

La presente versión de la Política de Seguridad está vigente a partir del día **2026-03-05**.

La versión actual del documento se publica en el servicio Safety Software.

Administrador de datos y propietario del sistema:
Safety Software Sp. z o.o.
ul. Półłanki 80
30-740 Cracovia, Polonia
Correo electrónico: **office@safetysoftware.eu**

Registro de cambios

Actualización: 2026-03-05

- se precisaron las copias de seguridad por capas y el proceso de restauración de datos (BCP/DR)
- se complementó la descripción del cifrado de datos con el modelo de sobre y la gestión externa de claves
- se amplió la descripción de la protección de la aplicación con sesiones, CSRF, CSP y mecanismos antiabuso
- se añadió una sección de monitorización y alertas y se simplificó la sección de integración con servicios externos