InterSystems Corporation
One Memorial Drive
Cambridge, MA 02142-1356
Principal: +1 617 621 0600
Soporte: +1 617 6210700
InterSystems.com

Documento técnico – Protección de datos, privacidad y seguridad

InterSystems apuesta por su programa Global Trust para proporcionar las medias de protección y salvaguarda adecuadas y necesarias que aseguren el uso legítimo, la divulgación adecuada y el contacto mínimo de cualquier información personal que, para InterSystems, esté recogida en las definiciones legales y reglamentarias relacionadas con los datos personales, ya sea InterSystems el responsable o el encargado del tratamiento de cualquier dato personal que (i) identifique o pueda ser utilizado para identificar, contactar o localizar a un individuo, o (ii) que se refiera a un individuo cuya identidad se pueda inferir de manera directa o indirecta, incluida cualquier información que esté vinculada o pueda vincularse a un individuo sin tener en cuenta cualquier atributo o estado de dicho individuo.

Nuestro programa Global Trust utiliza un marco de control basado en los requisitos de las normas ISO, HIPAA, NIST, APEC CBPR y los requisitos de los textos europeos DPD/RGPD. Con el objetivo de apoyar el programa Global Trust, en InterSystems (1) identificamos los fines específicos por lo que necesitamos recopilar, usar o divulgar información personal, (2) ponemos en funcionamiento medidas para proteger la información personal en lo relativo al derecho de privacidad de las personas, a la vez que garantizamos su disponibilidad para un uso y divulgación autorizados, (3) aplicamos medidas de salvaguarda para asegurar la confidencialidad, integridad y disponibilidad de la información personal en nuestros entornos, (4) abordamos la educación y concienciación mediante una iniciativa de formación integral sobre Global Trust, y (5) respondemos con rapidez ante cualquier sospecha o caso de amenaza o vulnerabilidad que afecte a la información personal.

Este documento informativo profundiza en nuestras prácticas sobre la protección de datos en lo que respecta a los productos y servicios de InterSystems.

Objetivos

Cualquier tratamiento de información personal por parte de InterSystems está directamente relacionado con los objetivos de los intereses legítimos perseguidos por el responsable del tratamiento, entre los que se incluyen:

- La investigación y la resolución de problemas relacionados con la información personal, incluidas las historias clínicas, en caso de que la organización de asistencia local no pudiera realizarlo por sí mismo o sin acceso a la información personal, como es el caso cuando un usuario ha completado una acción por error y desea retroceder la operación o rectificar el resultado o un usuario no puede completar una acción debido a un error en la aplicación.
- La implantación de un nuevo sistema o la actualización de un sistema ya existente para incluir una prueba de que el sistema está funcionando correctamente, dado que determinados comportamientos pueden deberse específicamente a datos existentes en lugar de a los nuevos datos añadidos.
- Los servicios de migración de datos, ya sea durante la implantación para la población de un nuevo entorno real con datos de un sistema anterior o para una actualización importante para la que la compatibilidad de la versión de la base de datos resulte un problema.
- Una prueba de interfaz en la que el sistema externo no tenga un entorno de prueba

con el que conectar.

- El soporte a las interfaces entre los sistemas clínicos y diferentes sistemas de soporte operativos con los datos de los pacientes.
- El soporte a la presentación de informes nacionales, por ejemplo, la puesta en servicio de bases de datos.

Protección de datos y privacidad

InterSystems incorpora y armoniza los requisitos de las legislaciones y reglamentos sobre privacidad y protección de datos en lo que se refiere a la recopilación, uso y divulgación de la información personal, todo ello mediante la implementación de los procedimientos y políticas de Global Trust, así como de su formación y asistencia en prácticas operativas, controles y medidas centradas en protecciones relevantes.

- **Responsable de la protección de datos - Ken Mortensen:** Con el objetivo de supervisar la responsabilidad de InterSystems en el cumplimiento de sus promesas sobre la protección de datos.

  InterSystems ha nombrado Responsable de la protección de datos de la empresa a un profesional en privacidad y seguridad con una formación en TI y derecho.

- **Procedimiento justo:** Con el objetivo de ayudar a los clientes a desarrollar su misión y objetivos mediante nuestra entrega, asistencia y mantenimiento de los sistemas y procesos de información que recopilan, usan y divulgan información personal.

  En InterSystems educamos a nuestros clientes sobre los diferentes momentos y escenarios en los que necesitamos información para garantizar que la información personal únicamente se trata en relación con nuestros servicios.

- **Objetivos lícitos:** con el objetivo de garantizar nuestra recopilación, uso y divulgación de enlaces de información personal para asistir a nuestros clientes en calidad de responsables del tratamiento.

  En InterSystems utilizamos contratos y procedimientos con nuestros clientes en los que cualquier tratamiento de información personal está relacionado los fines relevantes de los servicios o asistencia que ofrecemos.

- **Mínimo necesario:** con el objetivo de asegurarse de que InterSystems recopila, usa y divulga la información personal de manera apropiada, relevante y no excesiva.

  En InterSystems examinamos los datos entrantes con información personal para asegurarnos de que la información recibida es únicamente aquella necesaria, relevante y relacionada con los servicios o asistencia que ofrecemos.

- **Integridad de los datos:** con el objetivo de abordad la precisión de la información personal recopilada, usada y divulgada.

  En InterSystems utilizamos nuestra tecnología para asegurarnos de que los datos, incluyendo la información personal, conservan su integridad durante nuestro tratamiento mientras continuamos ofreciendo nuestros servicios o asistencia.

- **Conservación limitada:** con el objetivo de conservar la información personal únicamente durante el tiempo necesario para tratar las necesidades de nuestros clientes.

En InterSystems utilizamos constantemente procedimientos de supresión o destrucción de cualquier información personal una vez que esta ya no es necesaria para el desarrollo de nuestros servicios o asistencia.

- **Derechos de los interesados:** con el objetivo de coordinar con nuestros clientes cualquier respuesta o preocupación relacionada con el tratamiento de información personal, así como de establecer soluciones que permitan una accesibilidad y portabilidad eficientes de la información personal en nuestros productos.

  En InterSystems nos comunicamos con nuestros clientes para establecer enlaces con su personal de protección de datos y seguridad, a fin de conectar cualquier solicitud de datos con nuestros clientes en tiempo y forma.

- **Medidas técnicas y organizativas:** con el fin de establecer controles diseñados para proteger la privacidad y salvaguardar la información personal que InterSystems recopila, usa y divulga.

  En InterSystems establecemos controles para garantizar que contamos con las salvaguardas adecuadas y necesarias regidas por normas reconocidas, tales como la serie ISO 27000 y HITRUST, así como las mejores prácticas del sector.

- **Transferencia de datos:** con el objetivo de proporcionar las garantías adecuadas en lo referente a los requisitos de protección de datos relacionados con datos compartidos de forma interna o divulgados fuera del país de origen de la información personal.

  En InterSystems aplicamos un acuerdo internacional de transferencia de datos entre las entidades europeas y extra-europeas, tales como EE. UU. y Australia, para obligar a la totalidad de la organización a ajustarse a la legislación europea en materia de privacidad y seguridad.

Garantías de seguridad

InterSystems diseña y pone en práctica controles relevantes para garantizar la confidencialidad, integridad y disponibilidad de la información personal según la norma ISO 27001/2, a fin de asegurar que se cumplen los objetivos específicos sobre privacidad, seguridad y de negocio de InterSystems y de nuestros clientes. InterSystems examina de manera global y coordinada los riesgos para la privacidad y la seguridad con el objetivo de implementar un conjunto completo de controles y medidas en virtud del marco general de un sistema de gestión coherente.

- **Políticas y procedimientos:** Con el objetivo de garantizar la aplicación coherente y general de las medidas y de los controles apropiados y necesarios, InterSystems documenta sus procesos de privacidad y seguridad a través de políticas, procedimientos, normas, instrucciones de trabajo, directrices y de cualquier otro método.
- **Organización:** Con el objetivo de mantener el nivel de responsabilidad adecuado, InterSystems asigna roles tanto a su personal como a terceros para dar soporte a las tareas del Global Trust a través de actividades relativas a la privacidad y a la seguridad.
- **Recursos humanos** con el objetivo de promover el entendimiento entre los empleados de InterSystems y los contratistas que tienen acceso a los activos de

información de InterSystems, incluidos los datos de los clientes y la información personal, durante toda su vinculación a InterSystems en lo que se refiere a sus responsabilidades, así como a su idoneidad para desempeñar los puestos para los que los empleados de InterSystems y sus contratistas son propuestos.

- **Gestión de activos:** con el objetivo de que InterSystems identifique los activos organizativos y define las responsabilidades de protección adecuadas, así como la garantía de que la información recibe un nivel apropiado de protección de acuerdo con la importancia que tiene para InterSystems y para nuestros clientes.
- **Control de acceso:** con el objetivo de que el acceso a los activos de información sea únicamente el adecuado y necesario, mediante la gestión del acceso de los usuarios autorizados con responsabilidad sobre los empleados y contratistas de InterSystems, de manera que se evite un acceso no autorizado a los diferentes sistemas y servicios.
- **Criptografía:** con el objetivo de aplicar controles criptográficos que protejan la confidencialidad, la autenticidad y/o la integridad de la información.
- **Seguridad física y ambiental:** con el objetivo de definir áreas seguras para evitar el acceso físico no autorizado, el daño o la intromisión a la información y a las instalaciones de procesamiento de la información, así como de facilitar la protección de los activos frente a pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las operaciones.
- **Operaciones:** con el fin de que los sistemas y las instalaciones funcionen de manera segura, protegidos ante malware, con copias de seguridad de datos regulares para evitar la pérdida de datos, registros y seguimiento para guardar eventos y generar evidencias. Gestionar el software operativo para confirmar la integridad de los sistemas operativos, mitigar las vulnerabilidades técnicas que puedan descubrirse y revisar las normas de auditoría de los sistemas de información para minimizar el impacto de las actividades de auditoría en los sistemas operativos.
- **Comunicaciones y redes:** con el objetivo de gestionar la seguridad de las redes para proteger la información en estas y en las instalaciones de procesamiento de información de InterSystems, así como de mantener la seguridad de la información transferida tanto dentro de InterSystems como entre InterSystems, los clientes y terceros.
- **Adquisición, desarrollo y mantenimiento:** con el objetivo de implementar los requisitos de seguridad como una parte integral de los sistemas de información durante toda su vida útil, incluidos aquellos de los servicios en redes públicas y de nuestros procesos de desarrollo y soporte, a fin de diseñar dichos requisitos como parte de la vida útil de nuestros productos y sistemas.
- **Terceros:** con el objetivo de gestionar la seguridad de la información en nuestras relaciones con distribuidores, proveedores y otros terceros para la protección de los activos de información.
- **Respuesta ante incidentes:** Con el objetivo de responder ante incidentes de seguridad de la información de forma uniforme y efectiva para gestionar eventos de seguridad y vulnerabilidades, así como mitigar los riesgos para los activos de información, incluidos los datos de los clientes y la Información Personal, InterSystems mantiene un plan y un proceso de respuesta ante incidentes.
- **Continuidad de las operaciones comerciales:** con el objetivo de asegurar la

continuidad de las operaciones que garantizan una integridad y la disponibilidad efectiva de los activos de información.

- **Riesgo y cumplimiento:** con el objetivo de revisar el cumplimiento continuo para evitar infringir las obligaciones legales, normativas, reguladoras o contractuales mediante evaluaciones de la seguridad de la información de las políticas y procedimientos de InterSystems para los controles implementados y operativos, así como para las medidas de seguridad de la información.

Formación

- Todo el personal de InterSystems recibirá una formación sobre seguridad en forma de una revisión y confirmación de las políticas y procedimientos.
- Todo el personal de InterSystems debe revisar las políticas de al menos una vez al año.
- Todo el personal de InterSystems recibirá una formación sobre ITIL.

Respuesta ante incidentes de seguridad

Se entiende como incidente de seguridad cualquier violación identificada de acceso, tratamiento de datos o política de seguridad.
En caso de identificación de un incidente de seguridad, este se abordará con el grado de respuesta más elevado, utilizando todos los medios de forma continuada 24/7 hasta que el riesgo para los datos se haya subsanado.

- Todos los incidente de seguridad deberán comunicarse al departamento jurídico de InterSystems inmediatamente después de su detección. El departamento jurídico se encargará de coordinar la comunicación con el cliente.
- El vicepresidente de los servicios para clientes también deberá ser informado, siendo este el responsable en las comunicaciones con los altos directivos de InterSystems.
- Los incidente de seguridad NO quedarán registrados en WRC para evitar añadir riesgos adicionales a la seguridad de los datos.
- La difusión de incidentes de seguridad relacionados con los clientes de servicios gestionados no se hará pública a menos que el cliente lo autorice por escrito.
- Cualquier incidente que resulte en una violación de la seguridad de los datos seguirá el procedimiento de violación de datos estándar de InterSystems.
- En caso de cualquier incidente de seguridad, la prioridad de la respuesta la tendrá la protección de los datos. Los servicios gestionados evaluarán el riesgo y podrán dar prioridad a la seguridad de los datos sobre la disponibilidad del sistema.

Reglamento General de Protección de Datos

A pesar de que el programa Global Trust tiene como objetivo la protección de información personal mediante la aplicación de requisitos de privacidad y seguridad a nivel mundial, los controles de privacidad y seguridad de InterSystems están en conformidad con el Reglamento General de Protección de Datos (RGPD) de la UE. Tal y como se menciona anteriormente, nuestros controles actuales garantizan el cumplimiento de los principios de protección de datos existentes y se ajustan al RGPD y a las continuas actualizaciones de la legislación de los estados miembro europeos. InterSystems ha puesto en marcha diferentes medidas (algunas de ellas aún en curso) para hacer frente a los nuevos requisitos establecidos por el RGPD, en concreto:

1. Tal v como hemos mencionado con anterioridad, hemos nombrado un **Responsable de la protección de datos**.
2. Hemos realizado un análisis exhaustivo de nuestra información personal mediante la identificación, con la ayuda de nuestros clientes de cualquier información personal, si la hubiere, recopilada, usada o divulgada por nosotros.
3. Con la ayuda de nuestro Responsable de la protección de datos, hemos dado prioridad a medidas relevantes que incluyen una evaluación continua del ciclo de vida de la información personal, asegurándonos de que el diseño de nuestros procesos tiene en cuenta los riesgos asociados con la privacidad de las personas y con la seguridad de la información.
4. En los casos en que ha sido necesario, hemos aplicado procedimientos para realizar evaluaciones sobre el impacto de la protección de datos (DPIAs, por sus siglas en inglés) para entender si los riesgos existentes para los derechos de las personas se veían afectados por nuestro procedimiento y para identificar las reducciones necesarias para abordar los riesgos identificados.
5. Contamos con actividades organizativas en curso para organizar nuestros procesos internos, incluyendo las nuevas y actualizadas políticas sobre privacidad y seguridad, las evaluaciones en curso sobre los procesos operacionales para garantizar controles efectivos, las nuevas formaciones y campañas sobre la protección de datos por parte de los empleados, así como el impulso de nuestro programa de proveedores para los requisitos de la protección de datos.
6. Hemos puesto en marcha requisitos para documentar las decisiones tomadas en relación a la protección de datos, con el objetivo de que nuestras acciones y procedimientos se puedan explicar y entender de forma adecuada.

InterSystems utiliza su programa Global Trust para aumentar la protección de datos mediante la relación con nuestros clientes, incrementando la confianza que estos tienen en nosotros en la entrega de productos de calidad y de servicios efectivos.