

ANEXO III

Medidas técnicas y organizativas, incluidas las destinadas a garantizar la seguridad de los datos

Índice

Antecedentes y objetivos	1
Ámbito de aplicación	2
Descripción de las distintas medidas	3

Antecedentes y objetivos

Perseus Technologies GmbH («Perseus») adopta medidas técnicas y organizativas («MTO») adecuadas para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales, así como para asegurar la resiliencia de los sistemas. Por «adecuadas» se entiende que las medidas son adecuadas y proporcionadas en relación con los riesgos que deben controlarse.

A la hora de planificar, implementar y aplicar las medidas, Perseus tiene en cuenta el estado de la técnica, los costes de implementación, la naturaleza, el alcance, las circunstancias y los fines del tratamiento, así como la diferente probabilidad de que se produzca el riesgo y su gravedad para los derechos y libertades de las personas físicas. Estas medidas incluyen lo siguiente:

- la seudonimización y el cifrado de los datos personales;
- la capacidad de garantizar de forma permanente la confidencialidad, la integridad, la disponibilidad y la resiliencia de los sistemas y servicios relacionados con el tratamiento;

- la capacidad de restablecer rápidamente la disponibilidad de los datos personales y el acceso a los mismos en caso de incidente físico o técnico;
- un procedimiento para revisar, evaluar y valorar periódicamente la eficacia de las medidas técnicas y organizativas destinadas a garantizar la seguridad del tratamiento.

A la hora de evaluar el nivel adecuado de protección, Perseus tiene en cuenta, en particular, los riesgos asociados al tratamiento (por ejemplo, la destrucción, la pérdida, la alteración o la divulgación no autorizada de datos personales, así como el acceso no autorizado a los mismos).

Los requisitos se reflejan y documentan en las siguientes categorías de medidas técnicas y organizativas (TOM):

- Confidencialidad (art. 32, apartado 1, letra b) del RGPD)
- Integridad (art. 32, apartado 1, letra b) del RGPD)
- Disponibilidad y resiliencia (art. 32, apartado 1, letra b) del RGPD)
- Procedimientos de revisión, valoración y evaluación periódicas (art. 32, apartado 1, letra d) del RGPD; art. 25, apartado 1 del RGPD)

El presente documento sirve, en particular, para cumplir con la obligación de acreditación en materia de protección de datos de las partes contratantes.

Además de las medidas técnicas y organizativas (MTO) en el sentido de la legislación en materia de protección de datos, en particular de conformidad con el art. 32 del RGPD, Perseus ha implantado un sistema de gestión de la seguridad de la información (SGSI) que se basa en los requisitos de la norma internacional ISO/IEC 27001:2013.

Ámbito de aplicación y alcance

Perseus aplica las medidas de seguridad de datos tanto para sus propios tratamientos de datos como para los tratamientos de datos destinados a la prestación de los distintos servicios de ciberseguridad de Perseus. Para la prestación de sus servicios, Perseus recurre a encargados del tratamiento que, sobre la base de contratos acordados para el tratamiento por encargo (art. 28 del RGPD), llevan a cabo el tratamiento de datos personales por encargo siguiendo sus instrucciones. Estas relaciones de tratamiento por encargo y los acuerdos correspondientes constituyen relaciones de subcontratación a efectos del presente acuerdo. Los subencargados del tratamiento así designados cumplen, como mínimo, las normas de seguridad establecidas por Perseus. Las propias medidas técnicas y organizativas (TOM) de Perseus, así como las de los encargados del tratamiento, se complementan a la perfección en la prestación de los servicios y garantizan conjuntamente un nivel adecuado de seguridad de los datos.

El presente documento describe las medidas de seguridad de los datos que son relevantes para la prestación de los distintos servicios de ciberseguridad de Perseus.

Descripción de las medidas individuales

Confidencialidad (art. 32, apartado 1, letra b) del RGPD)

Control de acceso: protección contra el acceso no autorizado a las instalaciones de tratamiento de datos

Técnicas	Organizativo
• Sistema electrónico de control de acceso para las instalaciones utilizadas por Perseus (tarjetas con chip/transpondedores) • Cerraduras de seguridad mecánicas • Detectores de movimiento • Videovigilancia de los accesos • Medidas adecuadas en relación con	• definición de zonas de seguridad para las instalaciones utilizadas por Perseus • Asignación y gestión de derechos de acceso basadas en roles y documentadas («Role Based Access Control», RBAC) con proceso integrado de incorporación, traslado y baja • Normativa de visitantes para el acceso a las instalaciones de

Perseus subcontratistas de Perseus	instalaciones utilizadas por Perseus, en particular la asignación a un empleado de Perseus, el registro de la visita y la obligación de llevar tarjetas de visitante • servicio de seguridad • Medidas adecuadas en las instalaciones de los subencargados del tratamiento
---------------------------------------	--

Control de acceso: protección contra el uso no autorizado del sistema

Técnicas	Organizativo
• Autenticación con nombre de usuario + contraseña • Autenticación de dos factores • Cortafuegos • Red privada virtual (VPN) • Protección antivirus • Bloqueo automático de pantalla • medidas adecuadas en relación con los subcontratistas de tratamiento	• Asignación y gestión de derechos de acceso basadas en roles y documentadas («Role Based Access Control», RBAC) con un proceso integrado de incorporación, traslado y baja • Normativa sobre contraseñas y procedimientos de restablecimiento • Medidas adecuadas en relación con los subcontratistas

Control de acceso: protección contra la lectura, copia, modificación o eliminación no autorizadas de datos dentro de un sistema informático

Técnicas	Organizativo
• Registro de los accesos a las aplicaciones, especialmente en lo que respecta a la introducción, modificación y eliminación de datos • Cifrado de discos duros y dispositivos finales • Cifrado de soportes de datos • Uso de trituradoras de documentos	• Clasificación de la información (pública/interna/confidencial) • Concesión de autorizaciones según el principio de «necesidad de conocer» • Asignación y gestión de derechos de acceso basadas en roles y documentadas («Role Based

Medidas adecuadas en relación con los subcontratistas de Perseus	Control de acceso RBAC») con proceso integrado de incorporación, traslado y baja - Normativa sobre contraseñas y procedimiento de restablecimiento - Recurso a proveedores de servicios para la destrucción de expedientes y datos conforme a la norma DIN 66399 - Medidas adecuadas en relación con los subencargados del tratamiento
--	---

Principio de separación: tratamiento separado de los datos

Técnicas	Organizativo
- Separación de los entornos de desarrollo, pruebas y producción - Medidas adecuadas en los subencargados del tratamiento subcontratistas de Perseus	- Separación física o lógica de clientes - Medidas adecuadas en relación con los subencargados del tratamiento

Seudonimización —art. 32, apartado 1, letra a) del RGPD; art. 25, apartado 1 del RGPD—: sin recurrir a información adicional, los datos personales no pueden atribuirse a un interesado concreto

Técnicas	Organizativo
- Separación del fichero de asignación y su almacenamiento en un sistema informático independiente y seguro - Medidas adecuadas en relación con los subencargados del tratamiento	- Evaluación de todas las actividades de tratamiento para determinar si es posible un tratamiento de datos seudonimizados - Medidas adecuadas en relación con los subencargados del tratamiento