Apéndice: Cláusula DACHSER de Seguridad de la información

§ 1 Definiciones.

Los términos utilizados en mayúsculas tendrán el significado que se establece en esta Sección.

(1) "Proveedor" se refiere al proveedor real de un servicio en la nube, producto de software o cualquier otro servicio a DACHSER independiente de la operación real del servicio o producto.

(2) "Incidente de seguridad" se refiere a cualquier acto u omisión que comprometa materialmente la seguridad, confidencialidad o integridad de los datos o las salvaguardas físicas, técnicas, administrativas u organizativas establecidas por el Proveedor (o una persona autorizada) o DACHSER en caso de que DACHSER tenga acceso a los sistemas del Proveedor, en relación con la protección de la seguridad, confidencialidad o integridad de los datos personales, o la recepción de una queja relativa a las prácticas de privacidad y seguridad de datos del Proveedor (o una persona autorizada) o un incumplimiento o presunto incumplimiento del presente Acuerdo con respecto a dichas prácticas de privacidad y seguridad de datos.

§ 2 Disponibilidad / Gestión de la continuidad de las actividades

(1) **El proveedor** garantiza una disponibilidad anual del servicio de al menos el 99%, incluidas las ventanas de mantenimiento regulares y cualquier otro esfuerzo de mantenimiento planificado.

(2) **El proveedor** informará **a DACHSER** sin demora indebida mediante una declaración escrita (correo suficiente) de cualquier interrupción operativa que pueda afectar a la disponibilidad del servicio antes mencionada y acordada.

(3) **El proveedor** mantendrá planes de emergencia y contingencia para las instalaciones en las que se encuentren los sistemas de información del proveedor que procesen datos **de DACHSER**. El **proveedor** verificará periódicamente los controles de seguridad de la información y de continuidad de la actividad establecidos y aplicados. **El proveedor** facilitará estos planes a **DACHSER** a petición de **ésta**.

§ 3 Gestión del cambio

(1) **El proveedor** debe establecer un proceso de gestión de cambios definido y estructurado que cubra todo tipo de cambios en una aplicación o servicio sujeto a este acuerdo.

(2) El proceso de gestión de cambios incluirá, como mínimo, un análisis basado en el riesgo y la aprobación de todos los cambios, casos de prueba definidos, así como escenarios alternativos y soluciones. A petición de **DACHSER**, el **Proveedor** deberá facilitar información sobre los cambios fallidos que hayan dado lugar a interrupciones de la actividad de un servicio al presente acuerdo.

(3) Para evitar interrupciones, los cambios sólo se aplicarán durante las horas de mantenimiento definidas y acordadas. Cualquier cambio que pueda provocar interrupciones de los servicios prestados se comunicará **a DACHSER** antes de su aplicación. La información incluirá la ventana de tiempo prevista para la implementación, así como una justificación para la implementación fuera de la ventana de mantenimiento definida y acordada.

(4) **El vendedor** se asegurará de que los cambios no modificarán la naturaleza del servicio original.

§ 4 Gestión de parches y vulnerabilidades

(1) **El Proveedor**, sus empleados y contratistas están obligados a tomar nota e informar de cualquier vulnerabilidad (técnica) observada o sospechada que pueda afectar a los datos o sistemas de **DACHSER** en función de la criticidad de la vulnerabilidad. Los requisitos mencionados también se refieren a errores y fallos relacionados con el objeto de este acuerdo.

(2) Independientemente del requisito anterior, el **Proveedor** está obligado a proporcionar **a DACHSER** un informe sobre las vulnerabilidades que hayan surgido o de las que tenga conocimiento el Proveedor de forma periódica, pero al menos anualmente. El informe contendrá como mínimo una descripción de la vulnerabilidad, información sobre los efectos, una descripción cualificada del riesgo y las medidas aplicadas por el proveedor de servicios o las medidas necesarias que deba adoptar **DACHSER**.

(3) El **proveedor** deberá proporcionar parches de seguridad actualizados de forma periódica y sin solicitud previa por parte de **DACHSER**. En caso de vulnerabilidades, errores o fallos conocidos, tal como se especifica en la subsección (1) el **Proveedor** también proporcionará parches para mitigarlos sin demora indebida, en función de la criticidad.

§ 5 Incidentes relacionados con la Seguridad de la Información

(1) **El proveedor** establecerá procedimientos para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

(2) **El proveedor** deberá implantar procedimientos para que los incidentes de seguridad de la información se notifiquen a través de los canales de gestión adecuados lo antes posible. Todos los empleados y contratistas del **proveedor** deben ser conscientes de su responsabilidad de notificar los incidentes de seguridad de la información tan pronto como sea razonablemente posible.

(3) **El proveedor** está obligado a enviar **a DACHSER** un informe escrito sobre cualquier incidente de seguridad de la información que se produzca por su parte una vez que se haya mitigado. El informe deberá contener, como mínimo, una descripción cualificada del incidente de seguridad, medidas técnicas detalladas adoptadas para mitigar el incidente de seguridad y otras medidas técnicas y organizativas adoptadas durante el incidente de seguridad con el fin de prevenir futuros incidentes.

(4) **El proveedor** cooperará razonablemente con **DACHSER** en cualquier investigación posterior al incidente, reparación y esfuerzos de comunicación. Además, si procede teniendo en cuenta la naturaleza y el alcance del incidente el **proveedor** llevará a cabo una revisión forense de la seguridad y una auditoría en relación con cualquier incidente de seguridad de la información, y/o (ii) contratará a un auditor externo independiente para que lleve a cabo una auditoría o evaluación de los procedimientos, sistemas y red de seguridad de la información del vendedor, incluyendo: pruebas del sistema de controles; implementación de sistemas apropiados y análisis de vulnerabilidad y pruebas de penetración. En caso de que se identifique algún riesgo importante relacionado con la seguridad, el **proveedor** tomará las medidas correctivas oportunas basándose en las mejores prácticas del sector y en los resultados de dicha evaluación, auditoría o identificación de riesgos.

§ 5 Criptografía

(1) El **proveedor** tendrá una política sobre el uso de controles criptográficos basada en los riesgos evaluados.
(2) **El proveedor** evaluará y gestionará el ciclo de vida de los algoritmos criptográficos, algoritmos hash, etc., y eliminará y desautorizará el uso de débiles y longitudes de bits y bloques insuficientes.

(3) La política y los controles criptográficos del proveedor deberán abordar la selección adecuada de algoritmos, la gestión de claves y otras características fundamentales de las implementaciones criptográficas.

(4) El **proveedor** dispondrá de procedimientos para distribuir, almacenar, archivar y cambiar/actualizar claves; recuperar, revocar/destruir y tratar las claves comprometidas; y registrar todas las transacciones asociadas a dichas claves.

§ 6 Seguridad en la nube / Pruebas de penetración / Auditorías de proveedores

(1) El proveedor garantiza que tomará las medidas técnicas y organizativas necesarias para mantener la integridad de los datos de **DACHSER** procesados por el servicio en la nube **del vendedor**.

(2) A petición de **DACHSER**, el **proveedor** deberá informar **a DACHSER** sobre todas las medidas especificadas en el subapartado (1).

(3) El **proveedor** realizará pruebas de penetración periódicas en sus servicios utilizando herramientas de seguridad recomendadas por el sector para identificar información sobre vulnerabilidades. A petición de **DACHSER**, el **Proveedor** proporcionará un informe sobre la última prueba de penetración a nivel organizacional que podrá incluir un resumen ejecutivo de los resultados y no los detalles de los hallazgos.

(4) El **proveedor** responderá con prontitud y cooperará con las solicitudes razonables de **DACHSER** de evaluaciones de seguridad y otras actividades de auditoría, exploración, descubrimiento e informes de pruebas.

§ 7 Confidencialidad y seguridad de los datos

(1) El **proveedor** clasificará, categorizará y/o etiquetará los datos para ayudar a identificarlos y permitir que el acceso y el uso estén debidamente restringidos.

(2) Las partes se obligan a mantener en secreto toda la información y documentos que facilite la otra parte y a hacerlos accesibles únicamente a aquellos empleados, empresas afiliadas y subcontratistas que los necesiten absolutamente para utilizar el software contractual de conformidad con el acuerdo. En particular, las partes se comprometen a no divulgar la información obtenida a terceros sin autorización y únicamente en marco de la cooperación con la otra parte.

(3) Las partes están obligadas a mantener confidenciales todos los documentos y soportes de almacenamiento de datos entregados por la otra parte, del mismo modo que sus propios documentos sujetos a secreto.

(4) En caso de terminación de esta relación contractual las partes estarán obligadas a borrar o destruir la información, los documentos, el software contractual junto con todas las copias (permitidas o no permitidas), modificaciones y notas sobre el funcionamiento del software contractual y a entregar la descripción del programa a la otra parte respectiva. La prueba de la eliminación deberá presentarse inmediatamente a petición.

(5) Las obligaciones anteriores no se aplican a la información que ya estaba legalmente en posesión del destinatario antes de la celebración del acuerdo, o que se ha hecho accesible al público en general como resultado de publicaciones de terceros sin ninguna acción por parte del editor.

(6) Estas obligaciones permanecerán en vigor durante 5 años tras la finalización de la relación contractual.

§ 8 Seguridad de los RRHH

(1) **El proveedor** se asegurará de que su personal esté sujeto a un acuerdo de confidencialidad que incluya la protección de datos proporcionará formación adecuada sobre las políticas y procedimientos de privacidad y seguridad pertinentes. Además, **el proveedor** informará a su personal de las posibles consecuencias del incumplimiento de las políticas y procedimientos internos de seguridad, que deben incluir medidas disciplinarias, entre ellas el posible despido de sus empleados y la rescisión del contrato o de la misión para los contratistas y el personal temporal.

(2) Además de cualquier otra cláusula del acuerdo relacionada con este, el **proveedor** realizará comprobaciones de antecedentes penales y de otro tipo de su personal de conformidad con la legislación aplicable obligatoria.

29801672C JOSE MARIA SEGURA COTO (R: A78327350)

Firmado digitalmente por 29801672C JOSE MARIA SEGURA COTO (R: A78327350)
Fecha: 2025.04.25 12:08:07 +02'00'