Anexo III: Condiciones de confidencialidad, protección de datos y seguridad de la información

CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES:

La Empresa se obliga a sí misma, sus funcionarios y demás empresas subcontratadas cumplir con la normativa vigente uruguaya en materia de datos personales (Ley Nº 18.331, de 11 de agosto de 2008 y Decreto Nº 414/2009, de 31 de agosto de 2009). Se considera dato personal la información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables, a modo enunciativo, cualquier información numérica, alfabética, gráfica, fotográfica, registro de voz e imagen, acústica o de cualquier otro tipo que refiera a ellas directa o indirectamente, conforme con lo dispuesto en el artículo 4 de la Ley Nº 18.331 y artículos 1 y 4 del Decreto Nº 414/009.

Fundación Ceibal/Centro Ceibal será el responsable de la base de datos y del tratamiento, siendo la Empresa y sus empresas subcontratadas, encargados de tratamiento, de acuerdo con lo dispuesto en los literales H) y K) del artículo 4 de la Ley Nº 18.331.

Asimismo, deberá:

A. Adoptar las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de los datos y evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información.
B. Proteger la información y datos creada, editada, borrada o accedida sin las autorizaciones correspondientes, en particular en cantidades masivas de datos.
C. Tomar las precauciones y controles necesarios para que la información y los datos personales no queden disponibles en navegadores, balanceadores de carga, copias temporales, cookies y otras estructuras donde no sea necesario.
D. Asegurar la confidencialidad de toda la información que se procese o utilice. La Información Confidencial comprende, entre otros y a vía de ejemplo, la siguiente información: toda estrategia, plan y procedimiento comercial, información propietaria, software, herramienta, proceso, imágenes, datos personales, metodología, información y secreto comercial, y demás información y material de Ceibal, así como de los alumnos, beneficiarios, docentes, centros de estudios, que pudiera ser obtenida de cualquier fuente o pudiera ser desarrollada. La Agencia deberá mantener la información confidencial en secreto y no la utilizará en beneficio propio o de terceros ni aún luego de finalizado el presente contrato.
E. Alojar los datos en territorio uruguayo, o en caso de transferencia internacional asegurar que el servidor se encuentre en países considerados con niveles adecuados de acuerdo con la Directiva 95/46/CE.

F. No utilizar la información / datos para una finalidad distinta a la contratada, ni en beneficio propio ya sea gratuito u oneroso, ni cederlos, comunicarlos o transferirlos a terceros.
G. Al término de este contrato, o ante la solicitud de Fundación Ceibal/Ceibal o del titular de la información, se obligan a devolver o suprimir de todos sus sistemas y archivos físicos y lógicos, sean propios o contratados a terceros, los datos personales accedidos, obtenidos o tratados en virtud de este contrato, así como los metadatos asociados, en caso de corresponder.

SEGURIDAD DE LA INFORMACIÓN:

La Empresa deberá cumplir con los "Requisitos de seguridad de la información y privacidad" definidos en la Política de seguridad de la información de Ceibal y su Manual de políticas de seguridad de la información, en lo que resulte aplicable, así como cumplir con la normativa interna vigente y de los organismos reguladores y de control.

Protección de la información:

En el caso que la información sea almacenada en servidores del proveedor ya sea en modalidad on premise o en nubes, se deberán extremar los cuidados. La Empresa deberá proteger la información en reposo, en tránsito o en uso tomando las medidas necesarias y desplegando los controles que aseguren la confidencialidad, integridad y disponibilidad de la información.

A modo de ejemplo se recomiendan:

- La encriptación a nivel de discos, dispositivos y/o base de datos.
- El uso de herramientas de DPL (data loss prevention) y CASB (cloud access security brokers).
- NO crear ni usar copias de la información, solamente en los casos que sean necesarios.
- La encriptación para los datos en tránsito.
- El uso de SFTP en el caso de compartir información a través de servidores o transferencia gestionada de archivos a través de links encriptados seguros (con cifrado cifrado SSL y TLS).
- El uso adecuado de sistemas de gestión de identidades que permitan una correcta autenticación de usuarios en los sistemas del proveedor que incluya por ejemplo: uso de políticas de contraseñas adecuadas, doble factor de autenticación para cuentas privilegiadas y otras medidas habituales para asegurar la identidad de los usuarios con acceso a la información.
- El uso de sistemas de autorización de usuarios adecuados que garanticen que los usuarios con los perfiles y roles correctos puedan acceder a la información para la cual tienen los privilegios necesarios.

- La aplicación de políticas, procesos y controles tecnológicos que garanticen la seguridad de la información en uso.
- Manejar esquemas y arquitecturas que tomen en cuenta la continuidad del servicio de manera de garantizar el SLA acordado, como por ejemplo implementar planes de recuperación ante desastres, contingencias, alta disponibilidad y respaldos adecuados.

Uso de la infraestructura de Centro Ceibal:

En el caso que el servicio a contratar incluya el uso, instalación, configuración y/o mantenimiento de infraestructura de Ceibal tanto lógica como física, se deberán estipular claramente las condiciones, responsabilidades y usos adecuados de la información afectada de manera de asegurar la confidencialidad, integridad y disponibilidad de la misma.

Se deberá:

- Realizar una gestión adecuada de los usuarios generados a la Empresa. Esto incluye información por parte de la Empresa de las altas, bajas y modificaciones de los funcionarios en tiempo y forma, incluyendo los perfiles y roles a ser generados, de manera de garantizar un acceso seguro a los recursos de Ceibal.
- Generar los usuarios de VPNs y demás componentes necesarios para un acceso seguro, usando los criterios de mínimos privilegios.

Incidentes:

En el caso de un incidente de ciberseguridad se deberá reportar inmediatamente al mail de csirt del Centro Ceibal csirt@ceibal.edu.uy detallando la mayor información posible, para una adecuada gestión del mismo. Se deberá reportar también al resto de las partes involucradas de acuerdo al incidente concreto.

Responsabilidad:

En el caso que el proveedor tenga responsabilidad frente a un incidente y el mismo genere consecuencias en la disponibilidad y/o integridad y/o confidencialidad de la información manejada por Fundación Ceibal/Centro Ceibal, este se reserva el derecho de iniciar las acciones legales que considere pertinentes.

Auditoría:

Fundación Ceibal/Centro Ceibal se reserva el derecho de auditar los procesos relacionados a la seguridad de la información y la privacidad de la Empresa con el objetivo de verificar que se cumpla lo estipulado entre las partes. En este contexto podrá solicitar a la Empresa la documentación respaldante que corresponda en cada caso.

Concientización y capacitación:

El personal de la Empresa deberá estar informado y concientizado con el objetivo de gestionar de manera segura la información que manejan del Centro Ceibal y Fundación Ceibal y dar un adecuado tratamiento a posibles incidentes de seguridad. Para ello se recomienda:

- Capacitar y concientizar al personal en temas relacionados a la seguridad de la información y la privacidad.
- Informar al personal de los canales y procesos adecuados para poder reportar eventos de seguridad en Ceibal.
- Concientizar al personal en la correcta aplicación de los procesos asociados a la seguridad de la información, como, por ejemplo: uso adecuado de contraseñas, uso seguro en entornos de teletrabajo, manejo responsable de dispositivos móviles y compartir información de manera segura.

Cadena de suministro

La empresa se obliga a trasladar estas mismas exigencias a todos sus subcontratistas, proveedores y terceros que participen directa o indirectamente en la prestación de los servicios objeto del presente contrato, garantizando que:

- Los subcontratistas implementen controles de seguridad equivalentes o superiores a los exigidos por este contrato.
- Se pueden realizar auditorías o evaluaciones a los subcontratistas sobre el cumplimiento de dichos controles.
- Se notifique de forma inmediata cualquier incidente de seguridad que afecte o pueda afectar la información o los sistemas de Centro Ceibal.
- Se mantiene un plan de respuesta a incidentes y continuidad del negocio que incluya a los subcontratistas.

Inteligencia Artificial generativa:

Para el caso en que el proveedor utilice modelos de inteligencia artificial generativa (IAG) propios o de terceros se deberán implementar los controles necesarios para proteger los datos garantizando la seguridad de la información. Para ello se deberán implementar controles y acuerdos que aseguren:

- Que la información enviada por parte de Fundación Ceibal/Centro Ceibal a los modelos no es usada para el entrenamiento de los mismos.
- Que los datos personales utilizados en el entrenamiento, validación o inferencia de los modelos han sido obtenidos legalmente y cuentan con las autorizaciones necesarias.

- Que se implementen medidas técnicas y organizativas adecuadas para proteger la confidencialidad, integridad y disponibilidad de la información procesada.
- Proporcionar documentación técnica que describa el funcionamiento del sistema, sus limitaciones y riesgos.
- Implementar controles de ciberseguridad que aseguren la protección frente a accesos no autorizados, manipulación de modelos, y vulnerabilidades en el ciclo de vida de la IAG.
- Mantener un registro de auditoría de eventos relevantes del sistema de IAG.
- Abstenerse de utilizar modelos de IAG para generar contenido falso, discriminatorio, ofensivo o que infrinja derechos de propiedad intelectual.
- Garantizar que los modelos utilizados han sido entrenados con datos que respetan los derechos de autor y no vulneran derechos de terceros

El Proveedor se obliga a trasladar estas exigencias a cualquier subcontratista o tercero que participe en el desarrollo, implementación o mantenimiento de los sistemas de IAG utilizados en el marco del presente contrato.