ANEXO IV MEDIDAS TÉCNICAS

Woffu es un software as a service que ofrece acceso a la Woffu Saas Platform, desarrollada utilizando todo el conocimiento y la experiencia adquirida con clientes con diferentes casuísticas durante los últimos años.

El servicio de hosting y conectividad de Woffu es Azure Cloud, un conjunto de servicios en la nube de la empresa Microsoft, que nos garantiza un almacenamiento y backup seguro y nos proporciona toda la accesibilidad de un entorno cloud.

Azure Cloud cuenta con Centros de Datos propios ubicados en Europa. En el caso de Woffu, todos los datos se replican y se respaldan entre dos regiones de Microsoft, al Norte (Irlanda) y al Este (Países Bajos). De esta forma aseguramos que ante una eventual caída de una región, desde Woffu podemos seguir ofreciendo servicio a nuestros clientes sin interrupciones.

Uno de los beneficios de que Woffu sea una SaaS nativa es que todos los datos de la empresa están ubicados en la nube, lo que hace que sea bastante fácil mantener las copias de seguridad actualizadas y escalar la plataforma cuando sea necesario.

Certificaciones ISO/IEC - Certificado de Privacidad en la Nube

Las certificaciones forman parte del día a día. En Woffu nos esforzamos arduamente para alcanzar los más altos estándares de seguridad para nuestros clientes. La Organización Internacional de Normalización (ISO) es una organización independiente y no gubernamental, y el desarrollador más grande del mundo de estándares internacionales voluntarios. Por otro lado, la Comisión Electrotécnica Internacional (IEC) es la organización líder del mundo en la preparación y publicación de normas internacionales acerca de tecnologías eléctricas, electrónicas y relacionadas.

Sabiendo la importancia y valor de estas organizaciones, hemos conseguido 3 certificaciones ISO/IEC que garantizan nuestro compromiso con la privacidad de datos y procesos.

ISO/IEC 27001. Certificación en la Gestión de la Seguridad de la Información.

La información de nuestros clientes es importante para nosotros por lo que es de vital importancia contar con un Sistema de Gestión de la Seguridad de la Información (SGSI) que nos permita la gestión y control de los riesgos de la seguridad de la información.

La certificación ISO/IEC 27001 nos permite contar con un SGSI basado en las mejores prácticas y para asegurarnos de tener control de dicho sistema en Woffu hemos implementado los 114 controles de la ISO/IEC 27002.

ISO/IEC 27018. Certificación en la Seguridad y Protección de información personal en la nube.

No todos los datos se tratan de la misma manera, dependiendo del tipo de dato que se maneja se deben de tener controles para protegerla.

La norma ISO/IEC 27018 nos permite tener un marco de privacidad enfocado a la seguridad de la información y proteger de la mejor manera la información de identificación personal (PII-Personally Identifiable Information) en un sistema en la nube como es Woffu.

ISO/IEC 27701. Certificación en la Protección de la información de Identificación Personal (PII-Personally Identifiable Information).

Dar cumplimiento al RGPD es de vital importancia para Woffu y por eso estamos certificados en ISO/IEC 27701 ya que esta norma es una integración de la norma 27001 y los requerimientos esenciales del RGPD.

Haber obtenido dichas certificaciones significa una apuesta por parte de Woffu por la seguridad de la información que ostenta. Es esencial proteger la información, principalmente la de Identificación Personal (PII)

en la nube de sus clientes y de sus empleados. La certificación convierte a Woffu en uno de los primeros SaaS especializado en RRHH de España en obtener los distintivos. De esta manera aportamos una mayor solvencia para nuestros clientes porque tienen la certeza de que su información y la de sus personas estará protegida.

Reglamento General de Protección de Datos (RGPD)

La confianza de nuestros clientes es vital para una buena relación y un buen desempeño de sus actividades diarias. No solo alcanzamos las certificaciones ISO/IEC, sino también cumplimos con el RGPD, la nueva legislación de carácter europeo de protección de datos de los clientes que se complementa con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Políticas, normas y medidas para el cumplimiento al Reglamento General de Protección de Datos

La Certificación ISO/IEC 27701 nos ha ayudado a mejorar los procesos de Protección de Datos de todos nuestros clientes y sus usuarios. A partir de aquí, en Woffu buscamos proteger el intercambio de información con terceras personas, estas son algunas de las políticas normas y medidas que hemos establecido para asegurar la integridad, disponibilidad y confidencialidad de los datos:

- Acuerdo de Confidencialidad con terceros para prevenir la divulgación no autorizada de la información.
- Compromiso de Confidencialidad y Secreto con todos los empleados para prevenir la divulgación no autorizada de la información.
- Solicitud y revisión de los antecedentes penales de las personas que tienen acceso a los datos personales.
- El acceso a los datos de los clientes es restringido y únicamente pueden acceder a ellos el personal autorizado y con la finalidad de dar soporte al cliente.
- Transferencia de datos con infraestructura:
  - Solo se permiten conexiones encriptadas a la base de datos SQL Azure.
  - Solo se permiten conexiones seguras a los servicios de almacenamiento y al servicio de caché.
  - La transferencia de archivos con terceros es cifrada mediante el protocolo SFTP.

Requisitos Generales de IT

Woffu es una aplicación web por lo que es imprescindible la conexión a la red. Para ordenadores de sobremesa o portátiles, Woffu está optimizado para las últimas versiones de Google Chrome (Versión 84 o superior), Firefox (Versión 79 o superior), y Edge (Versión 80 o superior) con versiones de Windows 7 o superior y Safari (Versión 12) con versiones de MacOS 10.12 o superior.

Para dispositivos portátiles, como móviles y tablets, la navegación es a través de sus navegadores web dada la versión responsive o con la aplicación móvil de Woffu disponible para iOS (Versión 11.0 o superior) y Android (Versión 5.0 o superior).

En Woffu estamos comprometidos en alcanzar los estándares más altos de seguridad para cuidar de la información de tu empresa y de tu gente. Por eso hemos alcanzado las 3 ISO/IEC siendo una de las primeras SaaS en España en obtenerlas.

Descripción de las medidas de seguridad técnicas y organizativas aplicadas por WOFFU JOB ORGANIZER SL

Con el fin de garantizar la seguridad de la información a la que accede, procesa, transmite y almacena Woffu Job Organizer SL., como encargado del tratamiento durante la prestación de servicios al responsable, Woffu garantizará, el cumplimiento de los siguientes requisitos de seguridad:

- Implementar una Política de Seguridad conforme a la normativa aplicable y a las internacionales como NIST o ISO 27001, cuyo alcance deberá abarcar a toda la empresa y, en todo caso, deberá cubrir el servicio objeto del contrato.

- Disponer de un Plan de Negocio actualizado, garantizando que se compruebe periódicamente y que cubra el alcance de los servicios prestados.
- Disponer de un Plan de Recuperación de Desastres actualizado, garantizando que se compruebe periódicamente y que cubra el alcance de los servicios prestados.
- Garantizar que los equipos cuenten con software antimalware con firmas actualizadas en todo momento.
- Garantizar que se dispone de elementos para proteger a los usuarios de correos electrónicos de suplantación de identidad, robo de identidad o programas maliciosos.
- Garantizar que se aplican parámetros de seguridad a los servidores o equipos que nos dan servicio.
- Garantizar que los empleados que van a dar servicio han participado en campañas de ciberseguridad durante el último año y también es deseable que hayan recibido formación.
- Garantizar que la aplicación o servicio objeto del contrato ha sido desarrollado siguiendo prácticas de programación seguras y que se han realizado Penetration Tests o ejercicios Red Team realizados.
- Disponer de un proceso de respuesta ante incidentes que garantice una adecuada gestión y coordinación de recursos para mitigar los efectos del incidente y favorezca la interrupción del servicio en caso de un incidente o la vuelta a la normalidad.
- Garantizar que la información tratada relativa al servicio se almacena y transmite cifrada.
- Garantizar que la Información Personal cumple con la normativa vigente.
- Implementar medidas sobre el Acceso físico y Lógico.
- Disponer de Controles de Separación de Datos a nivel de base de datos, indicando en cada registro a qué empresa pertenecen y estableciendo controles a nivel de lógica de negocio según el usuario autenticado usuario.
- Contar con un proceso de auditoría interna y que esta se realice anualmente.
- Contar con compromiso de Subprocesadores.
- Contar con una Política y Programa de protección de datos personales que le permita cumplir con la obligación exigida por la legislación aplicable.
- Disponer de un Programa de Gestión de Incidencias.

El Cliente podrá exigir, previo aviso, que se demuestre el cumplimiento con las obligaciones especificadas en este documento.