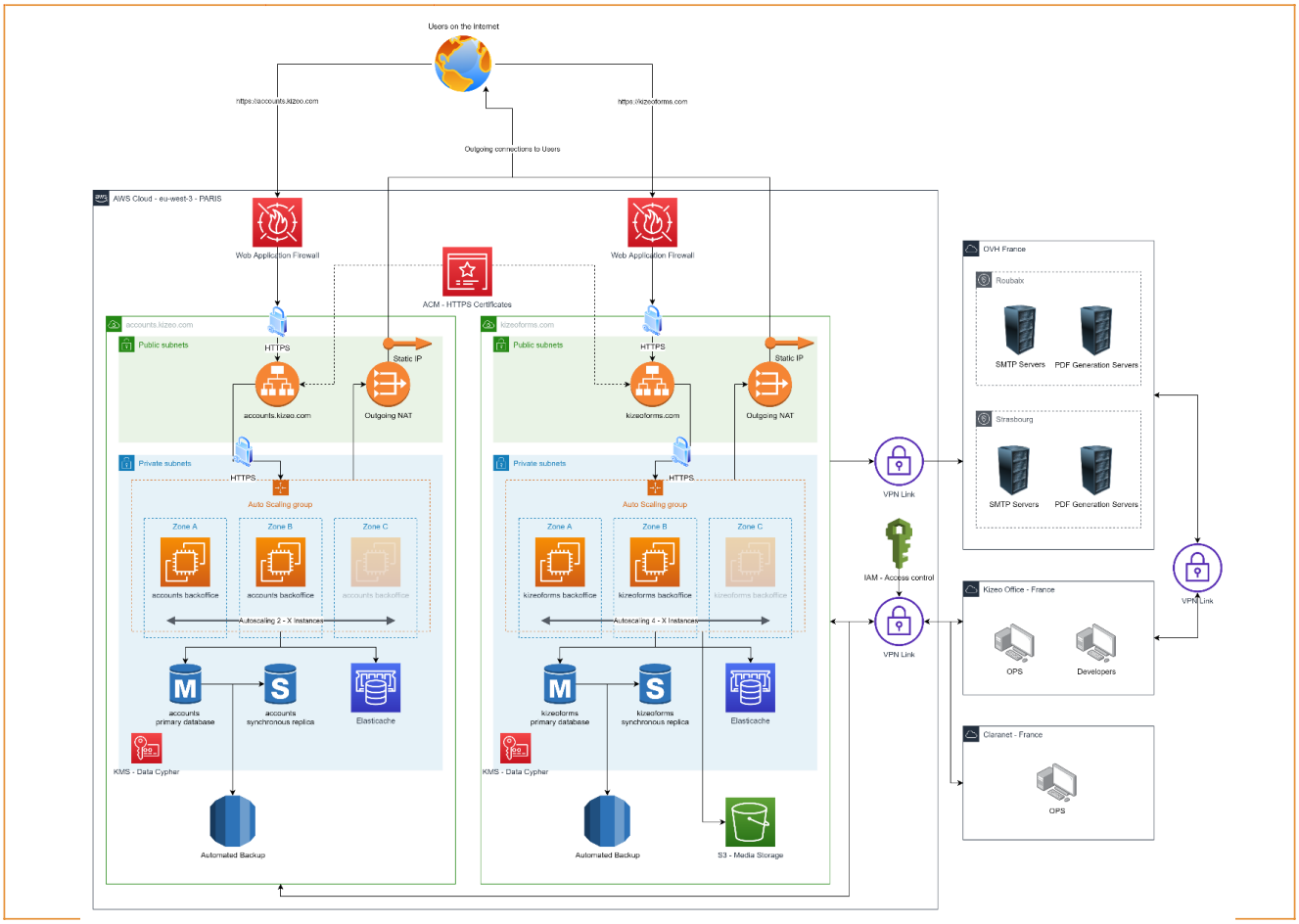
# Documento de seguridad Kizeo
# Producto: Kizeo Forms

| Puntos | Conforme | Notas complementarias / comentarios |
|---|---|---|
| **Seguridad organizacional** | | |
| **Nuestros empleados** | | |
| Responsables de seguridad | Si | Philippe Gellet (Presidente)<br>Vincent Demonchy (CTO) |
| Declaración de confidencialidad | Si | Todos nuestros empleados han firmado un acuerdo de confidencialidad y no divulgación. |
| Confidencialidad (externa) | Si | Sí, cualquier persona que trabaje para Kizeo y necesite tener acceso total o parcial a sus datos debe firmar un acuerdo de confidencialidad y no divulgación. |
| Acceso a los datos del cliente | Si | Para obtener asistencia tecnica, es posible que debamos acceder a sus datos. Por defecto, siempre le pediremos un acuerdo verbal o escrito. Sin embargo, usted puede solicitarnos un acuerdo por escrito. |
| **Certificaciones**<br>*Por el momento, Kizeo no planea obtener la certificación. Sin embargo, solo trabajamos con socios certificados por ISO / IEC 27001 cuando los datos de nuestros clientes están involucrados.* | | |
| Seguridad | No certificado | Nuestra infraestructura fue diseñada conforme con la certificación ISO/CEI 27001. |
| Organización | No | |
| **Alojamiento de datos** | | |
| **Localización**<br>*Todos nuestros datos se almaceman en tres centros ubicados en Francia. La transmisión de datos entre los diferentes sitios y con los dispositivos de nuestros clientes (móvil/computadora) están protegidos.* | | |
| Ubicación en Francia | Si | En centros de datos ubicados en Roubaix / Estrasburgo / Gravelines / París. |
| Ubicación fuera de Francia | - | Kizeo puede considerar esta solicitud dependiente de la situación. |
| Transferencias cifradas dentro del sistema Kizeo | Si | |
| Las transferencias dentro | Si | |
| Transferencia de datos cifrados con dispositivos del cliente | Si | TLS 1.2 por defecto. TLS1.0 sólo se utiliza con los dispositivos/navegadores más antiguos (Podría cambiar pronto). |
| Alojamiento | SAAS | Kizeo es una solución SaaS, esto significa que gestionamos el alojamiento de la solución para el cliente. |
| Servidores dedicados | | Sujetos a condiciones comerciales. |
| **Proveedores**<br>**Con el propósito de garantizar el mejor servicio, trabajamos con diferentes proveedores. Aquí están los implicados en el almacenamiento y seguridad de sus datos.** | | |
| **AWS** | | **Servicio de alojamiento (Hosting)** |
| ISO/CEI 27001: 2013 | Si | |
| ISO 27017 | Si | |
| ISO 27018 | Si | |
| SOC 1 | Si | |
| SOC 2 | Si | |
| SOC 3 | Si | |
| PCI DSS 1 | Si | |
| HDS | Si | |
| **OVH** | | **Servicio de alojamiento (Hosting)** |

| | | |
|---|---|---|
| ISO/CEI 27001: 2013 | Si | Dedicated cloud |
| SOC 1 type II (SSAE 16 et | Si | Private cloud |
| SOC 2 type II | Si | Private cloud |
| **Claranet** | | **Outsourcing y seguridad** |
| ISO/CEI 27001: 2013 | Si | Aplicado a todas las actividades de outsourcing. Directamente a Kizeo para garantizar:<br>- Garantizar la seguridad de los servicios, evitando violaciones de seguridad.<br>- Control sobre la confidencialidad, integridad y disponibilidad de la información.<br>- Un seguimiento de los incidentes de seguridad. |
| HDS | Si | https://www.claranet.fr/certification-hds |
| **Reversibilidad**<br>*A lo largo de los años, Kizeo desarrolló varias herramientas que garantizan la reversibilidad de los datos almacenados en nuestro servidor. Gracias a ellos, usted puede extraer sus datos en múltiples formatos.*<br><br>*Nuestra conformidad implica que nuestros clientes puedan extraer sus datos en muchos formatos sin requerir la contribución de Kizeo.* | | |
| Alojamiento de datos | Si | Los clientes pueden extraer datos solo en:<br>- Archivos (.pdf, .docx, .xlsx, .csv)<br>- Base de datos (Microsoft Access, MariaDB, PostgreSQL, Sql Server, Mysql)<br>- Sharepoint<br><br>También pueden extraer datos en formatos XML y JSON. |
| Medias | Si | Se pueden recuperar medias de nuestra aplicación web, de nuestro back office, Sharepoint, FTP o Dropbox. |
| Listas externas | Si | A través del servicio Web (formato de texto en bruto)<br>A través de la aplicación web (.xlsx) |
| Usuarios | Si | A través del servicio web (Cliente autónomo)<br>Formato .xlsx o .csv proporcionado por Kizeo |
| Grupos | Si | A través del servicio web (Cliente autónomo)<br>Formato .xlsx o .csv proporcionado por Kizeo |
| Formularios | Si | JSON formato (a través del Serviciovia Web) |
| **Informations utiles au SI pour votre bon fonctionnement**<br>*Voici les informations utiles pour vos SI, comprenant notamment les adresses IP succeptibles d'être demandées.* | | |
| Domaines à autoriser en HTTPS | | Strict minimum :<br>Tous les domaines *.kizeoforms.com<br>Le domaine accounts.kizeo.com |
| IP entrantes ? | | Kizeo communiquera toujours en HTTPS, même via Web Service, cela veut dire que nous maintenons un certificat à jour assurant notre identité lors des échanges.<br>Afin de garantir la meilleure qualité de service, Kizeo ne recommande pas de faire du filtrage IP en entrée, mais par noms de domaine.<br>En effet pour prévenir les pannes sur nos répartiteurs de charges, les adresses IP d'entrée peuvent changer. |
| **Infrastructure** | | |




| Gestión de datos sensibles (inc. RGPD) | | |
|---|---|---|
| **Datos sensibles recogidos por Kizeo** | | |
| Contraseña del usuario | Si | Solo impresión de contraseña (hash + salt) |
| Geolocalización | Si | Solo si es utilizado por el cliente en sus formularios. |
| Correo Electrónico | Si | Mantenemos los registros de correos electrónicos enviado por Kizeo Forms durante 3 días. |
| *Nota: De forma predeterminada, Kizeo no almacena datos personales confidenciales. Pero nuestros clientes pueden personalizar su aplicación de la forma que deseen lo que implica que pueden almacenar información personal que no podemos identificar si no nos notifican. Es deber del cliente declarar lo que es necesario y utilizar las herramientas que les proporcinamos para respetar y cumplir con las leyes de su área.* | | |
| *Nota (Listas externas): Las listas externas se crean para difundir una gran cantidad de información sobre un tema a sus usuarios, lo que simplifica la tarea de completar formularios. Sin embargo, tenga cuidado de no utilizarlos para almacenar y distribuir datos personales que no estén justificados por su ctividad profesional, ya que son necesidades legales (correo electrónico, geolocalización).* | | |
| **Cumplimiento de los datos médicos.**<br>*A pesar de que OVH tienes soluciones HealthCare que cumplen con HDSCP, cloud private y los servicios cloud no estan incluidos. Debido a que no son compatibles con HDSCP y no debe usar los Fomularios Kizeo para obtener información bajo este cumplimiento.* | | |
| Recolección por Kizeo | Ninguna | Kizeo no recopila datos médicos. |
| HDSCP (France/Europa) | No certificado | Kizeo no tiene la aprobación del HDS, pero nuestra infraestructura fue diseñada para serlo. |
| HIPAA (USA) | No certificado | Kizeo no tiene la aprobación del HIPAA, pero nuestra infraestructura fue diseñada para serlo. |
| **Política de contraseñas y seguridad de la cuenta** | | |
| Validez token | 1 día | |
| Complejidad configurable | Si | Bajo expresión regular |

| | | |
|---|---|---|
| Caducidad | No | |
| Doble autentificación | Si | |
| Azure Active Directory | Si | |
| SAMLv2 | No | |
| OpenId Connect | Si | |
| OAuth2 | Si | |
| LDAP (por medio de SSH) | No | Hemos desaprobado esta funcionalidad a favor del Azure AD, más comúnmente usado y |
| IP restriciones | No | No planificado |
| **Anonimización de datos**<br>*Kizeo no le impide anonimizar a sus usuarios si escriben información personal en nuestra aplicación.*<br>*Si recopila datos confidenciales de ciudadanos de la Unión Europea, debe asegurarse de que no puedan ser identificados.* | | |
| Posible | Si | |
| Cifrado de datos sensibles | Si | Todos los datos de Kizeo están encriptados (descanso + tránsito) |
| **Derechos** | | |
| Acceso | Si | El usuario que ingresa la información puede acceder a ella en cualquier momento durante |
| Editar/Corregir | Si | Se puede permitir la modificación de datos. |
| Derecho a ser olvidado | Si | Los datos pueden ser olvidados. |
| Borrado irreversible | Si | Vía Servicio Web. |
| Restricción | Si | Proporcionamos una configuración de derechos compleja para definir sus necesidades |
| Portabilidad | Si | Formatos : XLSX / CSV / XML / JSON / DOCX / PDF / XLSX / Base de datos<br>Vía : FTP / Dropbox / Servicio Web / HMI / Conector |
| **Trazabilidad**<br>*Mejoramos continuamente las herramientas de rastreo disponible para los administradores de nuestros clientes.* | | |
| Usuario: Conexión | Si | Solo para Kizeo (ret: 1 mes) |
| Usuario: Derechos de | Si | |
| Usuario: Edición | Si | |
| Usuario: Borrado | Si | |
| Datos: Acceso | Si | |
| Datos: Exportación | Si | |
| Datos: Edición | Si | |
| Datos: Eliminació (soft) | Si | |
| Datos: Eliminación (hard) | Si | Vía Servicio Web. |
| Formularios: Edición | Si | |
| Formularios: Suprimir | Si | |
| Formulario: Derechos de | Limitado | Se debe cambiar, pero aún no ha sido modificado. |
| Listas Externas: Edición | Si | |
| Listas Externas: Supresión | Si | |
| **Duración de la retención** | | |
| Copias de seguridad | 30 días | |
| Registros | 30 d a 3 meses | |
| Trazabilidad de registros | 1 mes a 5 años | |
| Datos (después de la finalización del contrato) | 2 años | Puede reducirse a 3 meses si se solicita.<br>Este tiempo de retención es para proteger la integridad de los clientes. |
| Datos (soft eliminación) | 6 meses | Para evitar eliminaciones no deseadas. |

## Seguridad física del local

**Impacto**
*Nuestras instalaciones no tienen impacto en la seguridad, no almacenamos los datos de los clientes en nuestras oficinas. Cada computadora está protegida con una contraseña y cualquier elemento clave que permita el acceso a los datos de nuestros clientes está encriptado.*

*En caso de robo, podemos revocar fácilmente el acceso a las claves utilizadas, ya que son personales y no se comparten. Además las computadoras con acceso están limitadas al requisimo mínimo.*

| | | |
|---|---|---|
| Acceso físico | Si | No almacenamos los datos de los clientes en nuestros dispositivos físicos. |
| Claves SSH cifradas | Si | Min. 2048 caracteres. |
| **Control de acceso** | | |
| Control de acceso global | Si | Sistema de acceso digital y alarmas. |
| Clave de acceso personal | Si | |
| Video vigilancia | Si | |
| Velocidd de intervención | Si | Menos de 30 minutos. |
| Identificación | Si | Clave de acceso personal. |

## Seguridad SI

**Copias de seguridad**
*"Cold" las copias de seguridad se almacenan en Estrasburgo (OVH). Su acceso está restringido solo a empleados técnicos calificados.*
*"Corto plazo" Las copias de seguridad a corto plazo, se almacenasn en la misma infraestructura que the cloud solution cuyo acceso está restringido a los empleados técnicos de Kizeo y a los equipos de outsourcing de Claranet (certificado ISO/CEI 27001).*

| | | |
|---|---|---|
| Geo-separación | Si | Tres sitios geográficamente distintos en Francia |
| Acceso | Si | Philippe Gellet (Presidente)<br>Vincent Demonchy (CTO) |
| Encriptado | Si | |
| **Cloud Solución**<br>*Nos beneficiamos de todas las soluciones disponibles para garantizar la estabilidad de nuestra red en AWS y OVH (incluidos los firewalls, VPN, sistemas anti-DDOS).*<br>*Claranet, como proveedor de servicios, nos garantiza una vigilancia permanente y una acción rápida en las acciones a realizar para mantener un nivel óptimo ante las fallas de seguridad.* | | |
| Anti-DDOS | Si | por AWS |
| Firewall | Si | |
| Anti-virus | Si | Windows Servers: Si<br>Linux: No, pero se aplica una política de seguridad estricta y las correcciones de seguridad son administradas por Claranet. |
| Intrusiones | Si | Restricción de IPs, Firewall, VPN |
| **S.I. Interno en Kizeo**<br>*Esta sección trata sobre las computadoras de nuestros empleados .* | | |
| Anti-DDOS | No | |
| Firewall | Si | |
| VPN | Si | |
| Antivirus | Si | En todos los dispositivos (Avast Business Edition). |
| Portátil | Si | |
| Constraseñas | Si | Rotación trimestral. |
| **Protección de acceso** | | |
| Claves SSH | Si | 2048 caracteres. |
| Claves cifradas | Si | |
| Restricción de acceso | Si | IT Equipo: Sin acceso.<br>IT Gerentes o técnicos de soporte sénior: Acceso (edición)<br>Claranet: Acceso (edición) |
| **Auditoría de seguridad** | | |
| Tests de penetración | Sí | Cada 6 meses |
| Publicación de resultados | Sí | Una vez al año |

| SLA | | |
|---|---|---|
| SLA Web App : Kizeo | 99.8% | Anual |

| Plan de continuidad del servicio | | |
|---|---|---|
| **3 sitios mínimo**<br>*En marzo de 2018, implementamos una nueva infraestructura basada en al menos très centros de datos. Gracias a esto, podríamos lidiar con una falla completa del centro de datos.* | | |
| Redundancia geográfica | Si | Al menos 3 centros de datos |