

Ingeniesia Desarrollo Cloud S.L.

Actividad y necesidades.

Ingeniesia Desarrollo Cloud S.L. gestiona con sus propios medios y a través de servicios externos datos sensibles proporcionados por los clientes. Estos normalmente son del ámbito médico por lo que los datos gestionados son de especial tratamiento ya que de acuerdo con el RGPD 679/2016 y la LOPD-GDD 3/2018 tanto los datos sobre salud como biomédicos tiene la consideración de **datos especialmente protegidos**.

Ante este escenario se hace totalmente imprescindible contar con unos sistemas de seguridad y de respaldo que permitan tanto la salvaguarda de los datos, como la protección de los mismos sin perjudicar en la agilidad del acceso a ellos por parte de su propietario.

Las necesidades en este sentido son claras, ofuscación y cifrado de los datos personales de los pacientes punto a punto de manera que los mismos solo sean accesibles por el propietario y ante una eventual brecha de seguridad, estos no sean legibles por la persona atacante, garantizándose la confidencialidad de los datos en todo momento.

Garantizar tanto la integridad como la disponibilidad de los datos utilizando unos sistemas de tratamiento para tal fin que además permitan su restauración de manera ágil en el caso de una eventual caída de los sistemas por un fallo crítico de los mismos.

Plan de verificación, evaluación y valoración, resiliente y periódico en el tiempo que garantice el cumplimiento del compromiso acordado con nuestros clientes.

Sistemas internos.

La empresa cuenta con una serie de sistemas y protocolos internos para garantizar el funcionamiento, flujo y custodia de los datos de nuestros clientes, así como el certificado de cumplimiento de LOPD expedido por una empresa especializada cumpliendo con las medidas de seguridad exigidas en el R.D.1720/2007 de 21 de Diciembre (Reglamento de Medidas de Seguridad), velando por la seguridad e integridad de los datos y siendo titular de varios ficheros debidamente inscritos en la Agencia Española de Protección de Datos

Ingeniesia cuenta con una persona designada para ejercer las funciones de delegado de protección de datos, cuyos datos de contacto son los siguientes:

- **Dirección postal:** Edif. CETIC-UGR, C/ Periodista Fernando Gómez de la Cruz n.º 61, Planta Baja, Oficina 6, CP: 18014 - Granada.

Dirección electrónica de contacto: dpo@cliniccloud.es

INSTALACIONES DE DESARROLLO

La seguridad en este punto es primordial, por este motivo Ingeniesia Desarrollo Cloud S.L. dispone de un **departamento de desarrollo en una ubicación que garantiza el acceso controlado e identificado por medio de registro con tarjetas magnéticas** a las instalaciones.

Dentro de estas **personal debidamente formado en el cumplimiento de la LOPD-GDD** en cuanto a protección de datos se refiere y son plenamente conscientes de la sensibilidad de los datos que pueden llegar a manejar, es por esto que todo el personal ha aceptado y firmado un **contrato de confidencialidad con Ingeniesia Desarrollo Cloud S.L.** que impide que por medio de algún empleado pueda haber una filtración de cualquier dato sensible.

Los **equipos informáticos** en el departamento de desarrollo, como no puede ser de otra manera, cuentan con las **medidas de seguridad** necesarias para garantizar físicamente desde el primer momento la seguridad de los datos que se puedan utilizar para el desarrollo o mejora de las aplicaciones de Ingeniesia Desarrollo Cloud S.L. como son la **protección de los mismos por contraseñas que cumplen la fortaleza y complejidad exigidas por la Ley**, son conocidas únicamente por el usuario de cada equipo y son modificadas cada seis meses minimizando el peligro de filtración de las mismas.

SOFTWARE Y COPIAS DE SEGURIDAD

La utilización de software original en todos y cada uno de los equipos tanto para el funcionamiento de los mismos como para el desarrollo de las aplicaciones de Ingeniesia Desarrollo Cloud S.L. garantizando así la seguridad de los mismos por medio de actualizaciones periódicas de dicho software

Copias de seguridad periódicas de los datos contenidos en los equipos de desarrollo que son almacenadas en servidores de datos redundantes seguros que garantizan la continuidad de los trabajos desarrollo de manera ágil en una hipotética caída de alguno de los equipos.

PROTOCOLOS DE DESARROLLO

Protocolos de desarrollo con bases de datos especialmente diseñadas para tal fin, esto es, bases de datos que en su mayor parte no cuentan con los datos reales o completos de los pacientes de nuestros clientes ya que, en la mayoría de los casos, no es necesario que los datos sean los reales para el desarrollo y mejora de las aplicaciones de Ingeniesia Desarrollo Cloud S.L., además dichas bases de datos son destruidas de manera segura una vez finalizadas las labores de desarrollo.

Las aplicaciones de Ingeniesia Desarrollo Cloud S.L. se basan en la filosofía de **Cloud Computing o “datos en la nube”**, esto es, el cliente accede a sus datos almacenados en un centro de proceso de datos (CPD) de un tercero contratado por Ingeniesia Desarrollo Cloud S.L. que tiene la obligación y el compromiso de garantizar la salvaguarda e integridad de los mismos, por lo que el acceso a datos por parte del cliente se hace a través de la red. Para garantizar la seguridad del tráfico de los datos entre el cliente y el CPD todo el desarrollo de las aplicaciones de Ingeniesia Desarrollo Cloud S.L. se hace mediante el **protocolo HTTPS o navegación segura**, que encripta las comunicaciones punto a punto, por lo que es prácticamente imposible la interceptación de datos por parte de algún atacante.

Envío de contraseñas encriptadas a través de la red. Además del tráfico HTTPS, el protocolo de desarrollo de Ingeniesia Desarrollo Cloud S.L. incluye el envío de las **contraseñas de los usuarios encriptadas** desde el origen para que, ante un hipotético ataque, los datos sean totalmente inaccesibles por parte del atacante.

Sistemas externos.

Para mayor agilidad, potencia de proceso y escalabilidad Ingeniesia Desarrollo Cloud S.L. cuenta con los servicios externos de Trevenque S.L., empresa del sector de las T.I. y especializada en la gestión, custodia y salvaguarda de los datos digitales en sus CPDs. Estos servicios contratados cuentan con un Cluster redundante de datos compuesto por cuatro nodos no dependientes que garantizan el acceso continuo a los datos alojados en él.

Trevenque S.L. cuenta con las medidas de seguridad necesarias para garantizar los datos de La Empresa cumpliendo la normativa ISO 27001 para tal fin además de la normativa ISO 9001. En esta mejora continua por la seguridad, nuestro Partner, también posee la acreditación de nivel medio del Esquema nacional de Seguridad (E.N.S.).

Política de protección de datos de nuestro Partner

Sobre el RGPD, aquí pueden consultar la información de su proceso de adaptación: <https://www.trevenque.es/proteccion-de-datos/>

Plan de contingencias en caso de caída de servicios

Ante **la eventual caída de los servicios** en uno de los servidores físicos donde se encuentran almacenados los datos de Ingeniesia Cloud S.L. y **de manera automática se inician en otro** de los servidores físicos que componen el Cluster de alta disponibilidad.

A nivel de procesamiento, almacenamiento y red **TODOS** los elementos están redundados y **NO existe un punto único de fallo** para generar una eventual caída de servicios.

Adicionalmente, al tratarse de máquinas virtuales, en caso de desastre, podemos restaurar dichas máquinas virtuales en cualquier entorno virtualizado garantizando así la disponibilidad prácticamente inmediata de los datos de la Empresa.

Frecuencia de copias y plan de restauración

Copia diaria de todas las máquinas virtuales con retención de siete días de las mismas, esto es, la copias de seguridad se almacenan durante siete días antes de ser sobrescritas por otras más actualizadas y para garantizar la salvaguarda de los datos todo ello se realiza en el Data Center propiedad de nuestro Partner ubicado en Granada, además, existe una copia de seguridad de las bases de datos de Ingeniesia Cloud S.L. en otro Data Center redundante, propiedad también de nuestro Partner, ubicado en la Comunidad de Madrid

El **proceso de restauración** de las mismas, al ser máquinas virtuales es posible en un plazo no superior a treinta o cuarenta minutos desde la notificación de la incidencia.

Cifrado de los datos de Ingeniesia Cloud S.L.

Nuestro Partner cuenta con un sistema automático de cifrado de datos en nuestras BBDD, donde todas las tablas se encriptan de manera que, ante un eventual ataque con robo de datos, no podrán ser accesibles por el atacante. Este sistema se está terminando de implantar en todos los entornos.

Seguridad del firewall ante ataques externos

Nuestro Partner cuenta con varios niveles de cortafuegos de diferentes fabricantes, incluyendo cortafuegos de nueva generación, IDS\IPS, anti DDoS, además de tener contratado un servicio de black hole para derivar ataques DDoS con uno de sus operadores de comunicaciones.