



# nymiz

## ANONYMIZATOR

DOSSIER COMERCIAL Y TÉCNICO

*“Porque la información es el activo más valioso de una empresa”.*

Oscar Villanueva  
CEO  
Tf: 682611252  
Email: [oscar@nymiz.com](mailto:oscar@nymiz.com)  
Web: [www.nymiz.com](http://www.nymiz.com)

## ÍNDICE

1	COMPañÍA	3
1.1	Breve historia.	3
1.2	Nymiz.	3
2	¿ESTÁ MUERTO EL BIG DATA? MINIMIZACIÓN DE DATOS	4
3	POR QUÉ NYMIZ	5
4	SOLUCIÓN NYMIZ	7
4.1	Funcionalidades.	7
5	TECNOLOGÍA	8
5.1	Componentes	8
5.2	Arquitectura	8
5.3	Workflows	8
5.4	Plataformas	8
6	INTERFAZ DE USUARIO DE NYMIZ	9
6.1	Aplicación Nymiz en versión web (SaaS):	9
7	GO TO MARKET - ESTRATEGIA COMERCIAL	11
7.1	Mercado: Segmentación / Sectores	11
7.2	Tipos de servicio	11
7.3	Modalidades de servicio SaaS	12
8	CASOS DE USO	16

## 1 COMPAÑÍA

### 1.1 Breve historia.

NYMIZ es una nueva empresa de base tecnológica, recientemente constituida en el año 2020. El objetivo de NIMYZ es el desarrollo de soluciones de anonimización inteligente dirigidas a diferentes sectores.

### 1.2 Nymiz.

El proyecto NYMIZ tiene como objetivo desarrollar la herramienta de software más fiable y eficiente que permita a las empresas y administraciones públicas proteger la privacidad de los datos personales en sectores como el de salud, legal, bancario o de seguros. Para ese propósito, estamos integrando diferentes tecnologías que unen una base de aprendizaje durante años basada en reglas y diccionarios junto con algoritmos basados en Inteligencia Artificial y en Lenguaje Natural (PLN). Todo esto lo convierte en potente herramienta para la comprensión del texto en diferentes idiomas, como inglés y español.

El problema al que nos enfrentamos es global y está creciendo cada vez más en términos de entorno de regulación y seguridad, por lo que se hace imprescindible una solución que nos permita anonimizar para:

- Cumplir con los requerimientos regulatorios (RGPD en Europa, por ejemplo).
- Poder compartir información y documentos tanto internamente como con compañías externas, sin comprometer la confidencialidad.
- Obtención de información y datos de documentos y bases de datos para tratamiento estadístico.
- Para la Administración Pública, es necesario cumplir con el principio de transparencia, pudiendo compartir la información siempre que esté anonimizada.
- Por razones de seguridad, la anonimización es una capa más de servicio que permite mantener seguros los datos de los clientes, ya que, al estar anonimizados éstos no tienen valor en caso de ser sustraídos a través de una brecha de seguridad.

## 2 ¿ESTÁ MUERTO EL BIG DATA? MINIMIZACIÓN DE DATOS

*"Si bien se están dando algunos pasos hacia el cumplimiento de la ley, las empresas generalmente carecen de medidas organizativas y tecnológicas para satisfacer las nuevas normas regulatorias que exigen la minimización de los datos personales".*

Los datos personales, en su mayoría no estructurados en varios repositorios de datos locales y en la nube, representan un factor de riesgo importante para las empresas independientemente de su tamaño. Con regulaciones de privacidad cada vez más rigurosas como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, la Ley de Responsabilidad y Portabilidad del Seguro de Salud (HIPAA) y (vigente desde el 1 de enero de 2020) la Ley de Privacidad del Consumidor de California (CCPA), las empresas deben administrar adecuadamente toda la información con datos personales que contienen información sensible y confidencial.

Un elemento clave de este proceso de gestión es la **minimización de datos**, por el cual se retienen sólo los datos personales que son esenciales para el propósito comercial y en cumplimiento con varias regulaciones, directivas legales y mejores prácticas.

Sobre la base de una investigación realizada con 2.000 empresas en torno a la recopilación, almacenamiento y gobierno de datos personales, hemos obtenido las siguientes conclusiones:

- **La gestión de datos personales es clave.**  
Administrar los enormes y crecientes volúmenes de datos personales sensibles y confidenciales es esencial para las empresas que empiezan a ser conscientes de ellos.
- **Las empresas carecen de información sobre sus datos.**  
Los encargados de la toma de decisiones carecen de información sobre sus datos (particularmente información no estructurada), lo que significa que no están tomando las medidas adecuadas para proteger sus datos.
- **Las obligaciones regulatorias y de privacidad, no son impulsores clave.**  
Pocas empresas están abordando su gestión de datos personales de manera proactiva de conformidad con los requisitos a los que están sujetas.
- **Existe miedo a la pérdida de información.**  
Una de las razones por las que los datos personales no se minimizan de manera más efectiva parece ser el miedo a la pérdida de datos.

Limitar la retención de datos personales es esencial si las empresas quieren mitigar con éxito los riesgos y costes asociados con el robo de datos e infracciones regulatorias y legales. Sin embargo, un número considerable de ellas no está limitando su retención de datos personales, ni están utilizando tecnologías que serían útiles para mitigar riesgos. Dado el gran volumen de iniciativas reguladoras que están en el horizonte, esta situación tendrá que cambiar rápidamente.

### 3 POR QUÉ NYMIZ

*“Puedo cumplir la ley de protección de datos (RGPD) y al mismo tiempo mantener la riqueza analítica de mis datos”.*

Nymiz permite anonimizar y seudonimizar datos personales en cualquier contenido, tanto estructurado como no estructurado, como bases de datos o documentos de Word, pdf, txt, powerpoint y correos electrónicos (\*).

Cada vez hay más datos personales en la red con un crecimiento exponencial y, por lo tanto, existe el riesgo de que dichos datos estén expuestos y puedan ser robados para ser vendidos en la web oscura o solicitar un rescate a cambio. Esto está llevando a una mayor sensibilidad de los usuarios para dar estos datos y a la evolución de la ley que protege su protección, que, siendo tan relevante, tiene un alcance para toda la Unión Europea (UE), que se aplica a todos los estados miembros y otros países que tienen datos personales de clientes que residen en la propia UE. Por supuesto, estamos hablando del RGPD, que en 2018 se ha vuelto más exigente en todo su alcance.

¿Por qué necesito anonimizar la documentación o los archivos que tienen datos personales?  
Por 2 razones principales:

1. **Cumplimiento de RGPD.** La ley exige mantener los datos personales esenciales para proporcionar el servicio y eliminarlos una vez que el cliente deja de serlo, contemplando un período mínimo de mantenimiento por razones legales. Después de este período, la empresa debe eliminarlos o seudonimizarlos de forma irreversible. Esto significa que la empresa tiene que detectar los datos personales y eliminarlos, o elimina todo el documento o contenido que incluye esos datos personales. Si no, estará incumpliendo la ley. Y esto mismo se extiende a cualquier tipo de contenido. Es decir, podemos hablar de archivos de clientes, contratos, ficheros, correos electrónicos, registros en bases de datos, etc.

Este cumplimiento puede afectar a dos necesidades clave para las empresas:

- a. **Principio de transparencia y/o necesidad de compartir información.** Quiero compartir un documento internamente en la empresa o con una empresa del grupo o con un tercero. Pero tal vez no pueda si tiene datos personales. Por lo tanto, antes de compartirlo, tengo que eliminar esos datos personales para cumplir con el RGPD.
- b. **Valor de los datos.** Si tengo que eliminar datos personales, pierdo toda la riqueza analítica de los mismos y no podré extraer el valor que es intrínseco a ellos a través de herramientas de Big Data, machine learning, etc., porque los datos se eliminan. Y aquí Nymiz plantea la posibilidad de seudonimizarlos para que su valor no se pierda.

2. **Seguridad.** La mayoría de las compañías tienen medidas de seguridad para proteger sus datos, pero aun así, la mayoría de ellas han sufrido ataques con sus correspondientes violaciones de seguridad. Nymiz propone seudonimizar los datos más confidenciales, es decir, los datos personales para que se intercambian por otros datos que aparentemente no tienen sentido a través de una clave de conversión/cifrado sin la cual los datos no tienen valor. Por supuesto, la clave nunca estará con los datos seudonimizados, por lo que para hackearlos y obtener los datos originales, se deberían sustraer tanto los datos como la clave, lo que lo hace mucho más difícil y por tanto se convertirá en un factor esencial para disuadir al hacker.
3. **Cambio de titularidad del dato.** Si optamos por la opción disponible en Nymiz de seudonimizar, es decir, sustituir el dato personal o sensible por un código o token, automáticamente la titularidad de ese dato pasaría de ser del cliente a la empresa puesto que este token o código generado por Nymiz hace imposible identificar el dato personal y por tanto, identificar a la persona que hay detrás del dato personal haciendo que este nuevo dato generado por Nymiz no esté sujeto a la LOPDD o GDPR siempre y cuando esta seudonimización fuera irreversible (ante la LOPDD irreversible con la tecnología actual).

Esto es muy relevante porque permite a la empresa realizar analítica de datos avanzada sin perder el valor del dato personal, de tal manera que:

- la empresa no tendría que eliminar esa información del cliente una vez éste se diera de baja, y esto de manera indefinida en el tiempo
- podría hacer ofertas específicas y profiling para estudiar comportamiento de clientes y lanzar ofertas de repesca personalizadas
- usar estos datos para entrenar modelos de machine learning basados en algoritmos de inteligencia artificial
- incluso vender o realizar otras actividades económicas con esos datos

*“Nymiz nació por y para los datos personales. Nuestra misión es proteger los datos personales donde quiera que estén. Nuestra solución viene de la experiencia de grandes clientes y estamos comprometidos a ofrecer la solución más completa y fiable del mercado”.*

## 4 SOLUCIÓN NYMIZ

### 4.1 Funcionalidades.

Nymiz tiene las siguientes funcionalidades:

- Soporte para varios formatos de archivo: pdf, documentos de Word, texto plano y csv.
- La versión final agrega soporte para fuentes adicionales como correos electrónicos, bases de datos y detección de archivos en las carpetas compartidas de una red interna.
- Contempla varias formas de anonimato que consisten básicamente en:
  - Anonimización (eliminación irreversible de datos).
  - Seudonimización (reversible) y encriptación, de modo que pueda ser reversible o irreversible según la elección del cliente.
- Incorpora una estructura colaborativa con usuario administrador y grupo de usuarios para trabajar en equipo.
- Permite la revisión manual y visual de fuentes anónimas.
- Con gestión de usuarios, licencias y pasarela de pago.
- Diferentes modalidades de carga de archivos.
- Multilenguaje. Soporta Español e Inglés. Hay más idiomas en roadmap: francés, alemán, italiano, etc.
- Procesamiento de datos a través de algoritmos de patrones, diccionarios personalizables junto con procesamiento de lenguaje natural.
- Mantenimiento del formato y extensión de los documentos.

## 5 TECNOLOGÍA

### 5.1 Componentes

Las siguientes herramientas y marcos se utilizan en nuestra solución:

- Java / Spring.
- Angular.
- Bases de datos relacionales y NoSQL, incluida la caché distribuida.
- Servicios de cola de mensajes.
- Herramientas de control de versión descentralizadas.
- Containerización, para facilitar el proceso de implementación.
- Herramientas de CI / CD, para rastrear el estado y la calidad del código y tomar medidas correctivas cuando sea necesario.
- Herramientas de pruebas.

### 5.2 Arquitectura

Desde una perspectiva de arquitectura, la solución Nymiz es una aplicación web distribuida, con modelo SPA para construir la interfaz de usuario. Como backend, creamos un conjunto de API REST empresariales con un estilo de microservicios, respaldado por varios servicios de soporte para descubrimiento, service mesh, caché, gestión de tráfico y control de acceso. Elegimos dos tipos de bases de datos, para admitir la lógica comercial regular, almacenar datos estructurados y no estructurados y aumentar el rendimiento del sistema mediante el uso de caché distribuida.

En la hoja de ruta del producto, planeamos agregar tecnología blockchain para admitir casos de uso de datos anonimizados compartidos entre diferentes organizaciones o incluso agregar una capa de seguimiento y certificación cuando sea adecuado.

### 5.3 Workflows

Los diferentes flujos de trabajo del sistema implican procesamiento de datos no estructurados en tiempo real, basado en documentos y procesamiento por lotes. Además, estamos desarrollando la detección de datos en otros tipos de repositorios, que incluye un proceso asistido de configuración de las diferentes fuentes y su posterior búsqueda y procesamiento desatendido. Y Estos flujos de trabajo se pueden administrar a través de dos modalidades: interfaz gráfica de usuario u operación a través de una API pública.

### 5.4 Plataformas

El software Nymiz está diseñado para admitir tanto el modelo SaaS como las implementaciones locales. La clave para esto es la combinación de componentes en contenedores que se pueden ejecutar en plataformas en la nube y orquestadores privados (como Kubernetes, Openshift, etc.) y servicios y componentes de respaldo que se pueden encontrar en los proveedores de la nube e instalar en las instalaciones del cliente.



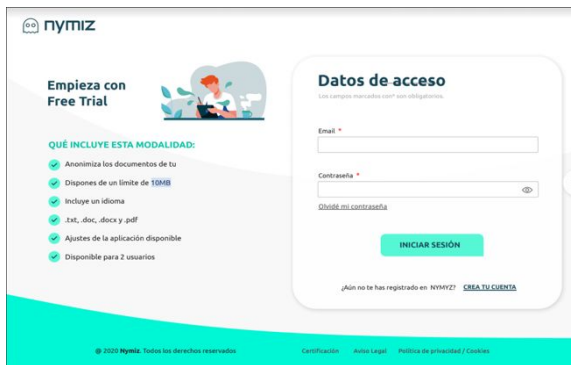
## 6 INTERFAZ DE USUARIO DE NYMIZ

### 6.1 Aplicación Nymiz en versión web (SaaS):

Vídeo Demo de la herramienta:

<https://youtu.be/1Ysj8-MldYI>

Algunas pantallas de la aplicación Nymiz son:



## 7 GO-TO-MARKET/ESTRATEGIA COMERCIAL

A continuación, se describe cuál es la estrategia comercial de Nymiz para llegar al mercado, con qué producto, a qué clientes, con qué canal, con qué marketing y, por último, describimos nuestro plan de despliegue internacional.

### 7.1 Mercado: Segmentación / Sectores

Nymiz se dirige a aquellas empresas que por su tamaño o actividad, dispongan de información que contengan datos personales tanto de empleados de la compañía, como de clientes o terceras empresas con las que colaboren. La RGPD obliga a cualquier empresa y/o persona física que tiene que cumplir una serie de requisitos a la hora de mantener esa información con datos personales.

Según la Agencia Española de Protección de Datos, hay dos tipos de obligaciones para empresas con respecto a la protección de datos: las que tienen poco riesgo y las que tienen alto riesgo. Las que aparecen a continuación están consideradas de alto riesgo y deben realizar un análisis de riesgos y tienen más “obligaciones”:

- **Sanidad.**
- Solvencia patrimonial y crédito.
- Generación y uso de perfiles.
- Actividades políticas, sindicales o religiosas.
- Servicios de telecomunicaciones.
- **Seguros.**
- **Entidades bancarias y financieras.**
- Actividades de servicios sociales.
- Publicidad.
- Videovigilancia masiva (Videovigilancia de grandes infraestructuras como estaciones de ferrocarril o centros comerciales).

Las que están indicadas en negrita junto con Sanidad, son los 4 sectores en los que Nymiz va a intentar posicionarse en una 1ª fase.

### 7.2 Tipos de servicio

Nymiz ofrece su servicio en 3 diferentes modalidades:

- **SaaS.** Mediante esta solución “Software as a Service”, el usuario puede conectarse a la solución que está en la Nube mediante un navegador y disfrutar de todas las funcionalidades de Nymiz en función de la opción elegida, transfiriendo los archivos originales y recibiendo los archivos anonimizados. Se facturará mediante modelo de suscripción.
- **API.** Mediante API (siglas de 'Application Programming Interface'), cualquier aplicación puede conectarse a Nymiz y aprovechar sus funcionalidades. Esta interfaz será especialmente utilizada por empresas y profesionales que se dedican a las áreas de protección de datos y que actualmente disponen ya de un software para realizar las

gestiones necesarias para el cumplimiento de RGPD, además de ser integrable con los principales repositorios documentales (Google Drive, Dropbox, etc.) y gestores documentales (Alfresco, Sharepoint, etc.) de forma que a través de esta API, puedan dotar a sus soluciones de la capacidad de anonimización de Nymiz. En este caso el servicio se facturará por volumen de datos anonimizados.

- **On Premise.** Para aquellas empresas o Administraciones Públicas que por tamaño, por decisión propia, por volumen de información y/o porque no puedan sacar fuera de su infraestructura la información sin anonimizar, podrán disponer de la solución de Nymiz instalada en sus infraestructura, con una capa de adaptación y customización del servicio de acuerdo a sus requerimientos. Esta capa será todo lo avanzada que el cliente requiera para asegurar que la anonimización es completa y sin fisuras. Adicionalmente, esta modalidad a su vez incluirá la anonimización en los emails, parte muy importante de las fuentes de información que suele albergar muchos datos personales. Se facturará con licencia y suscripción.

### 7.3 Modalidades de servicio SaaS

La solución en su modalidad SaaS se ofrece con 3 niveles de servicio más una modalidad Free Trial, que consisten en los siguiente:

1. **Free Trial.** El usuario dispone de 100 Mb/mes de documentos (.doc, .docx, .pdf, .txt y .csv) durante un período de 15 días para anonimizar sin coste. PRUÉBALO GRATIS pinchando aquí: <https://nymiz.com/registro/>
2. **Basic.** El usuario dispone de 1 Gb/mes de documentos para anonimizar (.doc, .docx, .pdf, .txt, .csv). No disponible de momento.
3. **Business.** El usuario dispone de 3Gb/mes de documentos para anonimizar (ídem que Básico más seudonimización y gestión de 3 usuarios). El precio es de 199€/mes\*.
4. **Enterprise.** El usuario dispone de 10Gb/mes de documentos para anonimizar (ídem que Business más BB.DD., emails). Contactar con Nymiz para precio.

\*NOTA: los precios son orientativos y sujetos a cambios.

## 8 CASOS DE USO

Existen multitud de casos de uso y a continuación tratamos de recoger algunos de los más significativos:

### 1. **SECTOR LEGAL/JURÍDICO:**

- Sentencias judiciales para poderlas hacer público y compartirlas entre despachos de abogados. Esto puede extenderse a cualquier tipo de información de cualquier sector que necesitamos compartir pero que no deberíamos hacerlo si no está anonimizada previamente.

### 2. **SECTOR SANITARIO:**

- Historias clínicas. De igual forma, es imprescindible anonimizar todos los datos personales y médicos de la persona para poder compartir y/o analizar para sacar información analítica o estadística.
- Otro tipo de información clínica donde hay que asociar los resultados clínicos al paciente y ésta debe ir anonimizada para que solo el personal médico autorizado pueda verla.
- Aplicaciones de seguimiento de Covid19 y también de detección de clientes en tiendas de retail. Nymiz es partner de un proveedor que luego puede ceder los datos a terceros para su análisis porque están anonimizados.

### 3. **SECTOR ASEGURADOR:**

- Información de clientes que hayan dejado de serlo en los últimos 5 años (este período puede variar según el sector). Legalmente pasado este tiempo habría que destruir toda la documentación o anonimizarla.
- Para datos personales que ya no podemos mantener y nos gustaría poder analizarlos con la tecnología actual de machine learning y Big Data, podríamos seudonimizar de forma irreversible y con ello cumplir la ley mientras podemos mantener en gran medida la riqueza analítica de esos datos.

### 4. **SECTOR FINANCIERO:**

- En grandes empresas se están desplegando “data lakes”, repositorios de información estructurada y no estructurada para cruzar la información y sacar “insights”. Pero esto legalmente no se puede hacer salvo que se tenga autorización expresa de los usuarios cuyos datos estamos considerando. Sí podemos hacerlo si los datos están seudonimizados.
- Todas las empresas han o están abordando, en su camino de digitalización, una migración de sus entornos a la Cloud. Sin duda, todos ellos buscan los beneficios que la Cloud aporta frente a los entornos monolito, etc, pero uno de los principales impedimentos que ven los CISOs, CIOs, etc, de migrar a los Cloud Providers, es el hecho de que la empresa pierde el control absoluto de su dato por dejarlo y fiarlo en un entorno nube. Es por ello que, cualquier pérdida del control del dato sensible de las empresas originada por cualquier mal uso, mala práctica, agujero de seguridad que estas Cloud tengan, no afectará al dato sensible de la empresa si éste está anonimizado.
- Fondos de pensiones

**5. SECTOR CONSULTORÍA:**

- Compartir casos de uso y conocimiento intra corporate.
- No eliminar proyectos para poder aprovechar los contenidos y proyectos para potenciales futuros clientes aprovechando el trabajo hecho previamente.
- Ofertar servicios llave en mano de anonimización

**6. SECTOR UTILITIES/ENERGÍA:**

- Compartir casos de uso y conocimiento intra corporate.
- Anonimización de datos en facturas, contratos con clientes
- Profiling de clientes por consumos, Business Intelligence
- Analítica avanzada e Inteligencia artificial
- Problemática con contadores inteligentes y smart meters en cuanto a manejo de datos personales
- Cloud y Data lakes, además de repositorios documentales

**7. ADMINISTRACIÓN PÚBLICA:**

- Para cumplir con la Ley de Transparencia en la Administración, tanto estatal como regional y local, tal y como:
  1. Portal del Ciudadano
  2. Ventanilla Única
  3. Datos de exposición pública
  4. Publicación de Juntas
  5. Hacienda, ticketing, información económica

**8. TRANSVERSAL A TODOS LOS SECTORES:**

- Seguridad. Por muchas soluciones de ciberseguridad, está demostrado que evitar la fuga de información puede ser casi imposible. Para ello Nymiz propone seudonimizar los datos sensibles y crear una llave de conversión que me permita volver al dato original.
- Cumplimiento de GDPR y LOPDD.