

SOLUCIONES

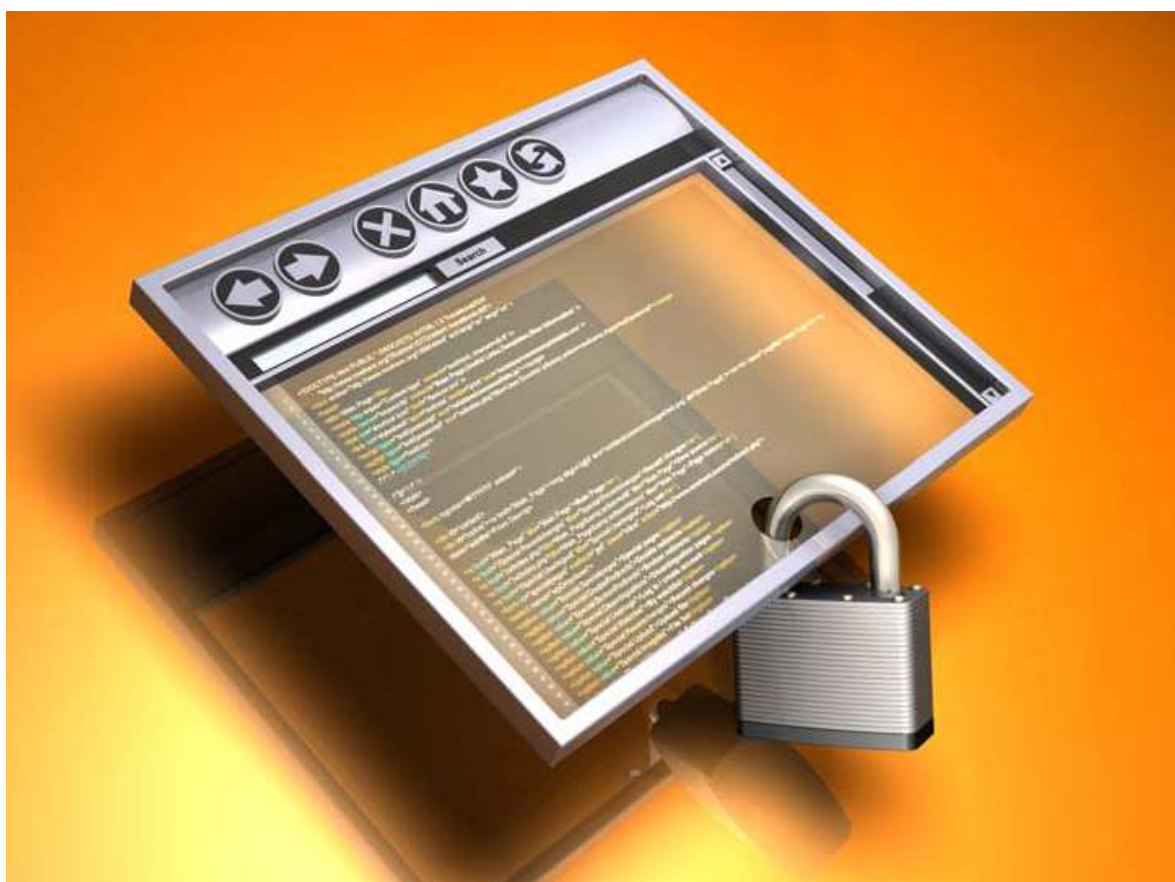
Backup remoto



Soluciones ArSeNet - backup remoto

## ArSeNet\_BackUP

*garantiza el cumplimiento de los requerimientos de la LOPD en relación a los procedimientos de Copias de Respaldo y Recuperación de Datos en los 3 niveles*





## Soluciones ArSeNet - backup remoto

### Obligaciones de la LOPD en materia de backup y recuperación de datos.

#### ¿Sabes si tu empresa está obligada a hacer backup remoto?

La LOPD<sup>1</sup> (Ley Orgánica de Protección de Datos) obliga a todas las organizaciones, empresas e instituciones a garantizar la seguridad de los datos de carácter personal *que tratan y almacenan* en sus sistemas de información y clasifica esos datos en 3 niveles de seguridad (básico, medio y alto). Para cada nivel impone una serie de obligaciones en materia de backup: desde garantizar la restauración de los datos al momento anterior de producirse la pérdida hasta disponer de backup remotos.

¿QUÉ TIPO DE INFORMACIÓN TRATAS Y ALMACENAS EN TU EMPRESA?	BASICO	MEDIO	ALTO
Ficheros de datos de carácter personal.	X		
Ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales.		X	
Ficheros que contengan datos sobre Hacienda Pública.		X	
Ficheros que contengan datos sobre Servicios Financieros.		X	
Ficheros que contengan datos sobre solvencia patrimonial y crédito.		X	
Ficheros que contengan datos relacionados con la ideología, origen racial, salud, creencias, filiación sindical, religión y sexo, principalmente.			X



## Soluciones ArSeNet - backup remoto

¿A QUÉ OBLIGA LA LOPD EN MATERIA DE BACKUP Y RECUPERACIÓN DE DATOS?	BASICO	MEDIO	ALTO	¿Que te aporta ArSeNet_Backup?
Deberán garantizar la restauración de los datos al momento anterior a producirse la pérdida.	X	X	X	<b>RESTAURACIÓN</b> Incluso, a momentos anteriores.
Realización de copias de backup al menos con una frecuencia semanal (art.14.3).	X	X	X	<b>COPIAS PROGRAMADAS</b> Sí, Backup automático. Programable con la frecuencia deseada.
Necesaria autorización para la ejecución de procedimientos de restauración de datos (art.21.2).		X	X	<b>SÓLO ACCESO AUTORIZADO</b> Las copias se almacenan encriptadas y es necesaria la clave (que sólo conoce el usuario) para recuperar cualquier información.
Almacenamiento externo de copias y procedimientos de restauración de datos (art.25).		X		<b>ALMACENAMIENTO EXTERNO SEGURO</b> En un CPD conforme a la normativa.

<sup>1</sup>Más información en

[https://www.agpd.es/upload/Canal\\_Documentacion/legislacion/Estatal/Ley%2015\\_99.pdf](https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/Ley%2015_99.pdf)

y en

[https://www.agpd.es/upload/Canal\\_Documentacion/legislacion/Estatal/A.8\)%20Real%20Decreto%200994-1999](https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/A.8)%20Real%20Decreto%200994-1999)



## Soluciones ArSeNet - backup remoto

Debes hacer Backup Remoto si...

Si tu empresa pertenece al sector de:	Si eres...	...gestionas y almacenas información de nivel alto como por ejemplo:
<b>FORMACION</b>	Centro de formación Colegio confesional	Información sobre el patrimonio familiar, IRPF, raza y religión para realizar las matriculaciones.
<b>SALUD</b>	Asociación de autoayuda Centro de médico: centro de estética, clínica odontológica, clínica de fertilidad,... Centro que realiza chequeos médicos (polideportivo, club deportivo, gimnasio, balneario...) Consulta Psicológica/Psiquiátrica Mutua Laboratorio hospitalario	<b>Historial médico</b> <i>Se entienden por 'datos de carácter personal relativos a la salud', 'las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo', pudiendo tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido. 'Estos datos comprenden igualmente las informaciones relativas al abuso del alcohol o al consumo de drogas'.</i>
<b>SERVICIOS</b>	Asesoría jurídica, laboral, contable,... Auditoria Banca Consultoría de estudios de mercado, estadísticas, tele-marketing... Correduría de seguros ETT o Consultora de RR.HH. Organización de inserción laboral de discapacitados	<b>Información facilitada por clientes relativa a:</b> - Ideología y creencias: donaciones a la Iglesia Católica, afiliación a partidos políticos, sindicatos.  -Salud: altas, bajas, minusvalías, historial médico. Partes de Enfermedad Profesional, partes de Accidentes de Trabajo, reconocimiento de discapacidad...
<b>SECTOR PUBLICO</b>	Órgano Administrativo o Entidad Pública: Ayuntamiento, Diputación, Gobierno Autónomo, INSS (Instituto Nacional de la SS), TGSS (tesorería General de la SS), INEM, etc.	-Expedientes de solicitud de ayudas y subvenciones que contengan datos relacionados con la ideología, origen racial, salud, creencias, filiación sindical, religión y sexo.
<b>OCIO</b>	Armería, Club deportivo Agencia matrimonial Hotel con servicios especiales para discapacitados.	Certificados de salud para obtener permisos de armas (exámenes psicológicos, físicos...) BBDD de clientes con datos sobre salud, raza, ideología y preferencias sexuales, minusvalías...
<b>OTROS</b>	Partido político Centro Religioso Sindicato	Datos de afiliación a agrupaciones que contienen información sobre ideología, religión y filiación sindical.



## Soluciones ArSeNet - backup remoto

¿Qué dice exactamente la normativa? Art 23, 24, 25 y 26 de LOPD

Cuadro resumen: adecuación ArSeNet_BackUP a la normativa	
Normativa	ArSeNet_BackUP
Art 23 Cifrado	Ok. 128 bits
Art 24 Registro de Accesos	Ok. El administrador del host no tiene acceso a los datos salvo autorización expresa del cliente en caso necesitar ejecutar una recuperación en el host. El usuario ha de proporcionarle la clave de seguridad. El acceso queda registrado.
Art. 25. Copias de respaldo en un lugar diferente a aquél en que se encuentran los equipos informáticos que los tratan	Ok. Es la funcionalidad principal de ArSeNet_BackUP. Copias de respaldo obligatorias para la protección de datos de alta nivel. Véase cuadro página 2.
Art. 26. Transmisión de datos por redes de Telecomunicaciones	Ok. Los datos se transmiten cifrados y se comunican bajo un protocolo de comunicación seguro SSH

### Las medidas de seguridad de nivel alto.

Para el tratamiento de datos de carácter personal de nivel alto se establecen medidas de seguridad específicas dada la especial relevancia de esta tipología de datos (salud, creencias, filiación sindical, religión y sexo, principalmente). Estas medidas podemos resumirlas en:

- La utilización de mecanismos de encriptación y cifrado de los datos.
- El registro, control y almacenamiento de logs de accesos a los ficheros.
- El almacenamiento de copia de seguridad en ubicación distinta.

#### - A) Distribución de soportes (art.23).

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

La finalidad perseguida por esta medida es evitar que, ante cualquier incidencia que pueda producirse en la distribución de los datos (o en el soporte que los contiene), terceros no autorizados puedan acceder a la datos; recomendándose la utilización de mecanismos de encriptación. Para la encriptación de los datos pueden utilizarse mecanismos de cifrado de 40, 56, 128 bits o más, siendo el más recomendable para esta tipología de datos el cifrado de 128 bits. El cifrado de los datos se realiza a través de algoritmos matemáticos. Actualmente, se están utilizando para la distribución de esta tipología de datos mecanismos de firma digital avanzada (claves públicas y claves privadas), que garantizan la autenticidad y confidencialidad de la información.



## Soluciones ArSeNet - backup remoto

### **B) Registro de Accesos (art.24).**

Esta medida impuesta por el Reglamento es la que conlleva más problemas técnicos y económicos para su implantación en las empresas, dado que han de configurarse las aplicaciones destinadas al tratamiento de los datos para que guarden y almacenen un gran volumen de datos.

Establece el Reglamento que, de cada acceso, se guardarán como mínimo:

- La identificación del usuario,
- Fecha y la hora en que se realizó el acceso,
- Fichero accedido,
- Tipo de acceso: autorizado o denegado,
- Y en el caso que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

Los mecanismos que permiten el registro de los datos detallados anteriormente estarán bajo el control directo del responsable de seguridad competente sin que se deba permitir, en ningún caso, la desactivación de los mismos. El período mínimo de conservación de los datos registrados será de dos años. Dado que el volumen de los datos a conservar puede ser muy alto, muchas empresas utilizan para cumplir con esta medida copias de seguridad específicas donde almacenan estos registros. Además, el Reglamento establece que el responsable de seguridad competente se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes. Estos informes deberán ser conservados junto con el Documento de Seguridad.

### **- C) Copias de respaldo y recuperación (art.25).**

El Reglamento establece para los ficheros de datos de nivel alto que deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente a aquél en que se encuentran los equipos informáticos que los tratan cumpliendo, en todo caso, las medidas de seguridad exigidas. El almacenamiento y conservación de juegos de copias de seguridad y de los procedimientos de restauración de datos fuera de la ubicación principal (por ejemplo, en cámaras de seguridad de bancos, que nos ofrecen altas medidas de seguridad) nos garantiza la continuidad de la actividad y la disponibilidad de la información ante cualquier incidencia grave o muy grave, sea física o lógica, que afecte a los equipos y servidores centrales (incendios, inundaciones, etc...).

### **- D) Transmisión de datos por redes de telecomunicaciones (art.26).**

El reglamento, finalmente, establece que la transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros. Habitualmente utilizamos para transmitir archivos redes de telecomunicaciones que son abiertas, es decir, que no cifran los datos mientras se transmiten entre dos puntos, permitiendo que puedan ser interceptados por terceras personas. Con la finalidad de evitar que en la transmisión de datos de nivel alto a través de redes puedan producirse intercepciones/manipulaciones de los datos, deben utilizarse mecanismos de cifrado de los datos o su transmisión a través de redes privadas, que garantizan que la comunicación entre los dos puntos es segura y no podrá ser interceptada/manipulada.