

integra

soluciones técnicas industriales



Desde **INTEGRA sti, S.L.** ofrecemos soluciones de ingeniería a las empresas para que su organización, sus instalaciones o los productos que fabrican o comercializan cumplan de forma eficaz con los requisitos derivados, tanto de la legislación, como de la normativa aplicable.

Para ello, nuestro personal técnico busca siempre la mejor solución técnica, facilitando a las empresas el cumplimiento de los requisitos normativos y legales.

Nuestros proyectos de colaboración van dirigidos a empresas productivas y de servicios que precisan asistencia técnica o asesoramiento para dar respuesta a alguna de las siguientes necesidades:

- Fabricar y comercializar productos o equipos que cumplan con requisitos legales y de seguridad, recogidos en normas técnicas, Directivas, etc. (marcado CE, homologación de equipos, máquinas o vehículos,...).
- Legalizar las instalaciones a través de los correspondientes proyectos técnicos y su correspondiente Dirección de Obra (proyectos de baja tensión, distribución de agua sanitaria, instalaciones contra-incendios, climatización, energía solar, licencias de actividad,...).
- Implantar o mejorar sistemas de gestión, según requisitos contenidos en normas internacionales, en las áreas de calidad, medio ambiente y seguridad (ISO 9001, ISO 14001, ISO 22000, APPCC, ISO/TS 16949,...).
- Optimizar su gestión mediante la actualización de equipos y aplicaciones informáticas (venta, instalación y configuración de equipos, servidores, portátiles, redes de datos LAN, adecuación de ficheros a la LOPD,...).
- Mejorar la metodología de trabajo y optimizar su gestión interna mediante una eficaz distribución de equipos y medios de trabajo (análisis de procesos, distribución de puestos de trabajo e instalaciones en planta,...).

INTEGRA Soluciones Técnicas Industriales, S.L.
Parque Tecnológico Paterna, Ronda Narcís Monturiol, 3 Edif ABM B-8 46980 PATERNA (VALENCIA)
Telf. 96 193 55 12 - Fax 96 193 55 12
integra-sti@integra-sti.com
www.integra-sti.com

lenovo
Business Partner

integra

soluciones técnicas industriales



mercado CE y homologación de equipos

- mercado CE de productos, máquinas y equipos
- homologación de equipos y máquinas
- adecuación de máquinas a los requisitos de seguridad del R.D. 1215



proyectos de instalaciones y legalización

- legalización de equipos e instalaciones
- proyectos de instalaciones industriales y edificación
- direcciones técnicas de obra
- licencias medioambientales y legalizaciones de industria



soporte y sistemas informáticos



- legalización de ficheros con datos de carácter personal según la LOPD
- mantenimiento de sistemas informáticos y redes de datos
- suministro e instalación de hardware; asistencia técnica
- suministro y configuración de software
- consumibles de ofimática y antivirus
- TPV




organización industrial, calidad y medio ambiente

- sistemas de gestión de la calidad (UNE-EN ISO 9001)
- sistemas de gestión medioambiental (UNE-EN ISO 14001 y Reglamento EMAS)
- sistemas de gestión de la seguridad y prevención de riesgos laborales (OSHAS 18001)
- estándares sectoriales: automóvil (UNE-ISO/TS 16949), seguridad alimentaria en productores, distribuidores y manipuladores (UNE-EN ISO 22000), laboratorios clínicos (UNE-EN 15189), laboratorios de ensayo y calibración (UNE-EN ISO/IEC 17025)
- auditorías internas y de tercera parte
- mantenimiento y mejora de sistemas de gestión
- optimización y mejora de procesos. planificación de la producción
- distribución, optimización y automatización de almacenes
- distribución de equipos y maquinaria en planta
- manual de funciones y responsabilidades por áreas, departamentos o puestos de trabajo. análisis y optimización de funciones en puestos de trabajo
- análisis de productividad



homologación de vehículos

- homologación de vehículos
- adecuaciones, tuning y reformas de importancia
- homologaciones de tipo y homologaciones unitarias
- gestión de importaciones de vehículos

marcado  y homologación de equipos
proyectos de ingeniería y eficiencia energética
soporte y sistemas informáticos
organización industrial y sistemas de gestión
homologación de vehículos

integra

soluciones técnicas industriales

LOPD



REQUISITOS

Desde su entrada en vigor en el año 1999, la **Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD)** establece la obligatoriedad de que toda empresa, profesional autónomo u organización de cualquier tipo, que posea ficheros (automatizados o no) conteniendo datos de carácter personal sobre personas físicas, proceda a **registrarlos** en la Agencia Española de Protección de Datos. Si los ficheros están sometidos a tratamiento informático, también es obligado redactar un "**Documento de Seguridad**" en el que se establecen las medidas de seguridad que la empresa debe implantar para garantizar su integridad, impedir su pérdida o sustracción, detectar y registrar intentos de acceso no autorizados, etc. Además, deben establecerse las medidas necesarias para que en cada documento en el que se recopilan datos personales (por ejemplo, al cumplimentar una solicitud de empleo o al abrir una ficha a un cliente) se solicite el consentimiento para su tratamiento y se informe de la finalidad de esos datos.

Los ficheros con datos personales se clasifican en tres niveles de seguridad, que implican diferentes requisitos de seguridad, según se establece en el artículo 4 del **Reglamento de medidas de seguridad en ficheros que contienen datos personales (RD 994/1999)**.

En general, son ficheros de **nivel básico** los que contienen datos personales que identifican a las personas (nombre, dirección, DNI, cuenta bancaria, teléfono, dirección de correo-e, etc,...). Básicamente todas las empresas disponen ficheros de nivel básico referentes a empleados, clientes y proveedores. Si los ficheros contienen datos relativos a la comisión de infracciones administrativas o penales (por ejemplo, empresas que mantienen embargos de empleados o proveedores,...), Hacienda Pública o servicios financieros, deben cumplir con los requisitos previstos para el **nivel medio**. Si los ficheros contienen datos de ideología, afiliación sindical (por ejemplo, cuando las empresas retienen de la nómina de sus empleados la cuota sindical), religión, origen racial, salud (si se mantiene un registro de las causas de las bajas por enfermedad) o vida sexual deben cumplir con los requisitos previstos para el **nivel alto**.

SOLUCIONES

En **INTEGRA STI** ofrecemos asistencia técnica a las empresas para cumplir de manera sencilla con los requisitos previstos en la **LOPD**. Para ello, nuestras propuestas de colaboración incluyen:

- **Análisis previo** del fichero y de los requisitos que ha de cumplir según el tipo de información que se registra: generación de un informe con las adecuaciones propuestas para adecuar la aplicación informática a los requisitos, según el nivel de seguridad al que pertenezca el fichero.
- La **inscripción del fichero** en la Agencia Española de Protección de Datos, cumplimentando los registros de solicitud correspondientes, según el nivel de seguridad del fichero (nivel, bajo, medio alto).
- Desarrollar un **Documento de Seguridad** con las medidas de seguridad que cumple la aplicación informática que gestiona el fichero con datos personales (si el fichero está automatizado) con el fin de asegurar su confidencialidad e integridad; estos requisitos son distintos según el nivel de seguridad, y más estrictos cuanto más alto es el nivel.

En la hoja adjunta se resumen los requisitos que debe cumplir un fichero con datos de carácter personal en cada caso, según el nivel de seguridad asignado.

INTEGRA Soluciones Técnicas Industriales, S.L.

Parque Tecnológico Paterna, Ronda Narcís Monturiol, 3 Edif ABM B-8 46980 PATERNA (VALENCIA)

Telf. 96 193 55 12 - Fax 96 193 55 12

integra-sti@integra-sti.com

www.integra-sti.com

CUADRO RESUMEN MEDIDAS DE SEGURIDAD

Reglamento de medidas de seguridad de los ficheros que contengan datos de carácter personal (RD 994/1999)

Nivel básico: Ficheros que contengan datos de carácter personal.

Nivel medio: Ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y los que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia y crédito).

Nivel alto: Ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los recabados para fines policiales sin consentimiento de las personas afectadas.

	NIVEL BÁSICO	NIVEL MEDIO	NIVEL ALTO
DOCUMENTO DE SEGURIDAD	<ul style="list-style-type: none"> - Ambito de aplicación. - Medidas, normas, procedimientos reglas y estándares de seguridad. - Funciones y obligaciones del personal. - Estructura y descripción de ficheros y sistemas de información. - Procedimiento de notificación, gestión y respuesta ante incidencias. - Proced. realización copias de respaldo y recuperación de datos. 	<ul style="list-style-type: none"> - Identificación del responsable de seguridad. - Control periódico del cumplimiento del documento. - Medidas a adoptar en caso de reutilización o desecho de soportes. 	
PERSO NAL	<ul style="list-style-type: none"> - Funciones y obligaciones claramente definidas y documentadas. - Difusión entre el personal, de las normas que les afecten y de las consecuencias por incumplimiento. 		
INCIDEN CIAS	<ul style="list-style-type: none"> - Registrar tipo de incidencia, momento en que se ha producido, persona que la notifica, persona a la que se comunica y efectos derivados. 	<ul style="list-style-type: none"> - Registrar realización de procedimientos de recuperación de los datos, persona que lo ejecuta, datos restaurados y grabados manualmente. - Autorización por escrito del responsable del fichero para su recuperación. 	
IDENTIFICACIÓN Y AUTENTICACIÓN	<ul style="list-style-type: none"> - Relación actualizada de usuarios y accesos autorizados. - Procedimientos de identificación y autenticación. - Criterios de accesos. - Procedimientos de asignación y gestión de contraseñas y periodicidad con que se cambian. - Almacenamiento ininteligible de contraseñas activas. 	<ul style="list-style-type: none"> - Se establecerá el mecanismos que permita la identificación de forma inequívoca y personalizada de todo usuario y la verificación de que está autorizado. - Límite de intentos reiterados de acceso no autorizado. 	
CONTROL DE ACCESO	<ul style="list-style-type: none"> - Cada usuario accederá únicamente a los datos y recursos necesarios para el desarrollo de sus funciones. - Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. - Concesión de permisos de acceso sólo por personal autorizado. 	<ul style="list-style-type: none"> - Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información. 	
GESTIÓN DE SOPORTES	<ul style="list-style-type: none"> - Identificar el tipo de información que contienen. - Inventario. - Almacenamiento con acceso restringido. - Salida de soportes autorizada por el responsable del fichero. 	<ul style="list-style-type: none"> - Registro de entrada y salida de soportes. - Medidas para impedir la recuperación posterior de información de un soporte que vaya a ser desechado o reutilizado. - Medidas que impidan la recuperación indebida de la información almacenada en un soporte que vaya a salir como consecuencia de operaciones de mantenimiento. 	<ul style="list-style-type: none"> - Cifrado de datos en la distribución de soportes.
COPIAS DE RESPALDO	<ul style="list-style-type: none"> - Verificar la definición y aplicación de los procedimientos de copias y recuperación. - Garantizar la reconstrucción de los datos en el estado en que se encontraban en el momento de producirse la pérdida o destrucción. - Copia de respaldo, al menos semanal. 		<ul style="list-style-type: none"> - Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.
RESPON SABLE		<ul style="list-style-type: none"> - Uno o varios nombrados por el responsable del fichero. - Encargado de coordinar y controlar las medidas del documento. - No supone delegación de responsabilidad del responsable del fichero. 	
PRUE BAS		<ul style="list-style-type: none"> - Solo se realizarán si se asegura el nivel de seguridad correspondiente al tipo de fichero tratado. 	
AUDITORIA		<ul style="list-style-type: none"> - Al menos cada dos años, interna o externa. - Adecuación de las medidas y controles. - Deficiencias y propuestas correctoras. - Análisis del responsable de seguridad y conclusiones al responsable del fichero, - Adopción de las medidas correctoras adecuadas. 	
REGISTRO DE ACCESOS			<ul style="list-style-type: none"> - Registrar usuario, hora, fichero, tipo acceso y registro accedido. - Control del responsable de seguridad. Informe mensual. - Conservación 2 años.
TELE COMU NICACIONES			<ul style="list-style-type: none"> - Transmisión de datos cifrada.

- Los niveles son acumulativos y tienen la condición de mínimos exigibles.
- Los accesos a través de redes de telecomunicaciones deben garantizar un nivel de seguridad equivalente al de los accesos en modo local.
- La ejecución de trabajos fuera de los locales de la ubicación del fichero debe ser expresamente autorizada por el responsable del fichero y garantizar el nivel de seguridad.
- Los ficheros temporales deberán cumplir el nivel de seguridad correspondiente y serán borrados una vez que hayan dejado de ser necesarios.
- Los ficheros de nivel básico que contengan datos que permitan obtener una evaluación de la personalidad del individuo deberán garantizar, además de las medidas de nivel básico, las de nivel medio relativas a auditoria, identificación y autenticación, control de acceso físico y gestión de soportes.

marcado CE y homologación de equipos
proyectos de ingeniería y eficiencia energética
soporte y sistemas informáticos
organización industrial y sistemas de gestión
homologación de vehículos

integra

soluciones técnicas industriales

sistemas de seguridad
backup



METRORED
PARTNER

sage SP
PARTNER

lenovo
Business Partner

REQUISITOS

Seguridad en las comunicaciones

La creciente instalación de puntos de acceso WI-FI y la interconexión de las redes locales e intranets a internet proporcionan huecos de seguridad que hacen las comunicaciones vulnerables a ataque y pérdidas de datos.

Identificación de riesgos

Nunca estamos totalmente seguros de cuales son los riesgos en seguridad que asumimos al ampliar o conectar nuestras redes de información

Almacenamiento de la información

Optimizar las unidades de almacenamiento y servidores para garantizar la rapidez de acceso en condiciones seguras.

Gestion de desastres

Disponer de un respaldo ante una caída del sistema de información o una pérdida de datos que no implique dejar de trabajar un largo periodo de tiempo

Backup interno, externo y site to site

Tener la información sensible respaldada en nuestras propias instalaciones, en servidores externos seguros o replicada en otras sedes de la empresa para contar con la tranquilidad de no perder los datos incluso poder recuperarlos en otros equipos para seguir trabajando.

SOLUCIONES

Diseño de soluciones de seguridad aplicando Firewall por hardware para gestionar el trafico de nuestras redes, generar sistemas de identificación univoca para todos los dispositivos que acceden a nuestra información. Conexión de varias sedes mediante VPN y Firewall.

Analisis de riesgos estudiando pormenorizadamente la estructura de la red de comunicación y asesorando en las soluciones que garantizan el máximo nivel de seguridad.

Unidades de almacenamiento de réplica en servidores (Raid) y dispositivos de almacenamiento en red que unifican la rapidez de acceso con la seguridad. Sistemas totalmente escalables para crecer al ritmo de su negocio.

Recuperación de información en los mismos equipos que hayan sufrido la pérdida de datos, puesta en marcha de nuevos servidores con la configuración, programas y datos de su antiguo servidor o recuperación de su sistema de información en otra red donde poder continuar trabajando

Backup a la carta en dispositivos de copia en sus instalaciones, en espacios alquilados en servidores seguros, en su propio servidor alojados en Data Center, en dispositivos de almacenamiento en otras sedes de la misma empresa. Copia en Unidades de almacenamiento alojadas en régimen de custodia en instalaciones seguras.... Siempre hay un backup que se adapta a tu volumen de información.

INTEGRA Soluciones Técnicas Industriales, S.L.

Parc Tecnologic, Ronda Narcís Monturiol, 3. Edif. ABM. Torre B – 8º 46980 PATERNA (VALENCIA)

Telf. 96 193 55 12 - Fax 96 131 81 59 integra-sti@integra-sti.com

SONICWALL

ProCurve
Networking by HP

NETGEAR

BUFFALO

FUJITSU
COMPUTERS
SIEMENS

3COM