

TEMA DEL MES · GOBERNANZA DE LA INTELIGENCIA ARTIFICIAL

La IA ya no se prueba. Se gobierna.

Las obligaciones de transparencia del Reglamento Europeo de IA se aplican desde el 2 de agosto. ISO/IEC 42001 pone nombre a lo que hay que documentar. Y la pregunta que empiezan a hacer los auditores no es si el sistema funciona, sino quién decidió ponerlo en producción, con qué criterio y con qué evidencia.

FACTURA ELECTRÓNICA B2B

EN 16931, SPFE y VERI*FACTU: tres obligaciones que no son la misma

Por qué un XML técnicamente válido puede no ser una factura conforme.

PRUEBA ELECTRÓNICA

Deepfakes ante los tribunales

De «¿qué muestra este vídeo?» a «¿podemos demostrar que es auténtico?».

CONTROL HORARIO

Cuatro años de registros, y que se pueda demostrar quién los tocó

Biometría: la AEPD vuelve a abrir el debate con un nuevo borrador.

LEY ANTIFRAUDE

Quince meses para el 1 de enero de 2027

Lo que el software permite hacer pesa más que lo que dice el manual.

SAP

Vulnerabilidad con CVSS 10.0 en el kernel ABAP

CVE-2026-44756: qué revisar y qué dejar documentado.

TASACIÓN DE SOFTWARE

La deuda técnica no se ve en la cuenta de resultados

Cuándo la antigüedad tecnológica empieza a descontar valor.

CARTA DEL CEO

El software ya no falla solo. Ahora decide.

Una imagen repetida en las auditorías de septiembre: organizaciones que han metido IA en sus procesos sin que nadie haya firmado la decisión.

**Luis Vilanova**

CEO · LEGAL AUDITORS

Auditor CISA certificado por ISACA y perito judicial colaborador con la Administración de Justicia, entre otros.

Colegiado nº 498 — COIICV

En el número anterior escribí que las organizaciones no tienen un problema de normas, sino de evidencias. Un mes después he tenido que corregirme a la baja: en inteligencia artificial, muchas ni siquiera tienen el problema identificado.

Desde el 2 de agosto se aplican las obligaciones de transparencia del Reglamento Europeo de Inteligencia Artificial. No son obligaciones de dentro de dos años: son de ahora. Un usuario tiene derecho a saber que habla con una máquina; un contenido generado o alterado por IA tiene que poder identificarse como tal. Y aun siendo exigencias modestas comparadas con las que llegan en 2027 y 2028, en septiembre hemos encontrado **chatbots en producción sin una sola línea que advierta de que lo son**.

Lo interesante no es el incumplimiento: es el motivo. Casi nunca hay una decisión deliberada de no cumplir; hay una decisión que nadie tomó. El modelo entró dentro de una actualización del ERP y se puso a trabajar. Cuando preguntamos quién autorizó su uso para esa finalidad y quién supervisa sus salidas, la respuesta suele ser un silencio educado.

De eso trata ISO/IEC 42001, y por eso le dedicamos el tema central. Un sistema de IA puede estar impecablemente protegido frente a accesos no autorizados —ISO/IEC 27001 hace bien su trabajo— y estar, a la vez, **pésimamente gobernado**. Quien crea que su certificado de 27001 le cubre la IA se llevará una sorpresa el día que le pidan el expediente.

Hay un segundo frente más incómodo: la identidad. Los agentes de IA ya abren tickets, aprueban y escriben en sistemas de producción con credenciales que no siempre distinguen al agente de la persona en cuyo nombre actúa. Quien no pueda responder quién hizo la operación, en nombre de quién y con qué autorización, tiene un problema que no es tecnológico: es probatorio.

Y el calendario no se detiene: quince meses para el 1 de enero de 2027 de la Ley Antifraude, la factura B2B avanzando sobre EN 16931 y una inspección que ya no pregunta si fichas, sino si puedes demostrar que ese fichaje no se tocó después. La norma se lee en una tarde; el expediente se construye durante meses. Empecemos ya.

LUIS VILANOVA — Valencia, 1 de octubre de 2026

Lo que hemos publicado en septiembre, ordenado.

Los artículos publicados durante septiembre de 2026 en los blogs técnicos de Legal Auditors, con el enlace al original en cada bloque.

-
- 04** **TEMA DEL MES**
ISO/IEC 42001 e ISO/IEC 27001: qué comparten y qué debe auditarse por separado
Un sistema puede estar bien protegido y mal gobernado. Dos normas, dos alcances, un solo expediente.
-
- 05** **INTELIGENCIA ARTIFICIAL**
La identidad de los agentes de IA y quién decide si un modelo es seguro
Identidad, representación y autorización: la cadena que hay que poder reconstruir.
-
- 06** **AI ACT**
Las obligaciones de transparencia que ya se aplican desde agosto de 2026
Artículo 50: chatbots, contenido sintético y deepfakes. Y el calendario hasta 2028.
-
- 07** **AYUDAS Y FINANCIACIÓN**
Bono IA360: 600 millones y 25.000 empresas en el horizonte de 2027
Qué tiene que tener preparado un fabricante de software antes de la convocatoria.
-
- 08** **FACTURA ELECTRÓNICA B2B**
EN 16931 y SPFE: la norma europea y la solución pública
Por qué un XML válido no es necesariamente una factura conforme.
-
- 09** **LEY ANTIFRAUDE**
Cinco años auditando lo que el software realmente permite hacer
1 de enero de 2027 para sociedades. Y el artículo 201 bis LGT de fondo.
-
- 10** **CONTROL HORARIO**
Cuatro años de conservación y un borrador de la AEPD sobre biometría
Qué pide la inspección y qué hay que poder demostrar sobre cada modificación.
-
- 11** **PRUEBA ELECTRÓNICA**
Deepfakes, accesos no autorizados y proyectos «al 80 %»
Cadena de custodia, hash y metadatos: lo que convierte un archivo en prueba.
-
- 12** **SAP**
CVE-2026-44756, MASC y la cuenta atrás de SAP ECC hacia 2027
Documentación de proyecto, pruebas de aceptación y gestión de vulnerabilidades.
-
- 13** **TASACIÓN DE SOFTWARE**
Obsolescencia, deuda técnica y el valor de un software con IA
Qué descuenta valor de verdad y cómo se traduce en euros.
-

CÓMO LEER ESTE NÚMERO

Las fechas que aparecen junto a cada artículo son las de publicación original. Los enlaces al pie de cada bloque llevan al texto íntegro. Esta revista no sustituye al asesoramiento jurídico ni técnico particularizado: es una síntesis de criterio profesional sobre normativa en vigor a 1 de octubre de 2026.

TEMA DEL MES · GOBERNANZA DE LA IA

Un sistema de IA puede estar bien protegido y mal gobernado

ISO/IEC 27001 e ISO/IEC 42001 comparten estructura, comparten liderazgo y comparten el ciclo de mejora continua. No comparten alcance. Confundirlas es el error más caro que puede cometer hoy una organización que use inteligencia artificial.

ISO/IEC 27001:2022**Seguridad de la información**

- Confidencialidad, integridad y disponibilidad
- Control de accesos y cifrado
- Gestión de incidentes y continuidad
- Responde a: ¿está protegido?

ISO/IEC 42001:2023**Gobierno de sistemas de IA**

- Finalidad del sistema y uso previsto
- Calidad de datos y de resultados
- Impactos y supervisión humana
- Responde a: ¿está bien decidido?

Ambas normas siguen la estructura armonizada de ISO, de modo que una organización ya certificada en 27001 **puede reutilizar buena parte de su maquinaria**: el liderazgo, la gestión de riesgos, el programa de auditorías internas, la revisión por la dirección y el ciclo de mejora continua. Esa es la buena noticia, y explica por qué quien parte de un sistema de gestión maduro llega antes.

La mala es que la reutilización tiene un límite muy nítido. ISO/IEC 42001 introduce obligaciones que 27001 ni contempla ni pretende contemplar: evaluar para qué se usa el sistema, con qué datos, con qué calidad de resultado, qué impacto puede tener sobre las personas afectadas y cómo se articula la supervisión humana. Un modelo puede estar impecablemente cifrado, con doble factor y segregación de entornos, y estar tomando decisiones que nadie ha validado, sobre datos que nadie ha revisado y sin que exista un responsable identificado.

LO QUE HAY QUE HACER ANTES DE CERTIFICAR

- Un análisis de brechas específico de IA: no vale el de 27001 con otro título.
- Inventario de sistemas de IA en uso, incluidos los que entraron dentro del ERP, del CRM o de una actualización del proveedor.
- Identificación del rol jurídico de la organización en cada sistema (proveedor, responsable del despliegue, importador).
- Definición explícita de la supervisión humana: quién revisa, con qué frecuencia y qué puede revertir.

El enfoque razonable no es montar dos sistemas de gestión paralelos, sino **integrarlos sin duplicidades** y dejar documentado qué requisito responde a qué norma. Cuando llega una auditoría —o una reclamación— la pregunta no es si la organización tiene certificados, sino si puede señalar el documento concreto donde consta la decisión.

legalauditors.es/iso-iec-42001-e-iso-iec-27001-que-comparten-y-que-debe-auditarse-por-separado/ — publicado el 28/09/2026

INTELIGENCIA ARTIFICIAL · IDENTIDAD Y DECISIÓN

¿Quién está realmente detrás de cada operación?

Los agentes de IA ya ejecutan operaciones en sistemas de producción. La auditoría tiene que poder responder cuatro preguntas: quién la hizo, en nombre de quién, con qué autorización y qué quedó registrado.

AGENTES DE IA · 28/09/2026

Identidad, representación y autorización no son lo mismo

El artículo separa tres conceptos que en la práctica se mezclan: la **identidad** (qué agente es), la **representación** (en nombre de quién actúa) y la **autorización** (qué puede hacer). La cadena que debe poder reconstruirse es explícita: persona u organización → mandato → agente → credencial → autorización → operación → evidencia.

Sobre el terreno técnico, apunta a **eIDAS2** como marco para incorporar mecanismos de representación electrónica y a estándares como **SPIFFE** para dotar de identidad criptográfica a los procesos. Cada agente debe tener identidad única, credenciales diferenciadas y mínimo privilegio: compartir la cuenta de servicio entre varios agentes destruye la trazabilidad igual que compartir una cuenta de administrador entre varias personas.

legalauditors.es/la-identidad-de-los-agentes-de-ia-quien-esta-realmente-detras-de-cada-operacion/

GOBERNANZA · 28/09/2026

Data & AI Governance: gobernar es decidir, no solo documentar

Gobernar no consiste en acumular políticas, sino en tener criterio para decidir cuándo una solución está preparada para usarse, qué cambios exige y cuándo hay que retirarla. El texto insiste en que **la calidad del dato no se evalúa en abstracto**, sino contra una finalidad concreta, y sitúa la trazabilidad —poder reconstruir el recorrido desde el origen hasta el resultado— como requisito imprescindible, especialmente en arquitecturas RAG.

Como referencias, ISO/IEC 42001 y el marco del NIST (Govern, Map, Measure, Manage). La conclusión es incómoda y correcta: una solución válida hoy puede dejar de serlo mañana sin que nadie haya tocado una línea de código.

luisvilanova.es/data-ai-governance-como-saber-si-una-solucion-esta-realmente-preparada-para-utilizarse/

DEBATE · 28/09/2026

¿Quién debe decidir si un modelo de IA es suficientemente seguro?

La tesis es que la seguridad de los modelos avanzados no puede descansar solo en las evaluaciones internas de quien los desarrolla. Se han documentado casos de sistemas que sortearon restricciones durante pruebas de ciberseguridad, y la autorregulación, útil como primer filtro, carece de la independencia exigible para decisiones críticas.

Las propuestas van en cuatro direcciones: participación pública en la evaluación técnica de sistemas de frontera, organismos evaluadores independientes con criterios estandarizados, documentación de las pruebas con **valor probatorio** ante un incidente, y una línea roja explícita que determine cuándo un modelo sencillamente no puede desplegarse.

leyesytecnologia.com/quien-debe-decidir-si-un-modelo-de-ia-es-suficientemente-seguro/

AI ACT · OBLIGACIONES EN VIGOR

La transparencia dejó de ser voluntaria el 2 de agosto

El artículo 50 del Reglamento Europeo de Inteligencia Artificial ya se aplica. No es un calendario futuro: es una obligación presente que afecta a cualquier empresa con un chatbot, un asistente o contenido generado por IA.

02.08.2026

Obligaciones de transparencia del artículo 50. **Ya aplicables.**

02.12.2027

Sistemas de alto riesgo del Anexo III.

02.08.2028

Sistemas de IA integrados en productos ya regulados.

REGLAMENTO EUROPEO DE IA · 22/09/2026

Cuatro obligaciones que ya deben cumplirse

Primera: cuando una persona interactúa con un sistema de IA —chatbot, asistente virtual, voz automatizada— **debe saberlo**. Segunda: el contenido sintético, sea texto, imagen, audio o vídeo, tiene que poder identificarse técnicamente como generado o modificado por IA. Tercera: los deepfakes se etiquetan como contenido artificialmente manipulado. Cuarta: los textos publicados por sistemas de IA sobre asuntos de interés público exigen información clara al lector.

La recomendación práctica es la misma que venimos haciendo en auditoría: levantar un **inventario de sistemas de IA**, determinar el rol jurídico de la organización en cada uno dentro de la cadena de valor, y documentar las medidas adoptadas. Sin inventario no hay cumplimiento demostrable.

leyesytecnologia.com/ai-act-en-2026-las-nuevas-obligaciones-de-transparencia-que-ya-deben-cumplir-las-empresas/

RIESGO TECNOLÓGICO · 21/09/2026

Auditar la IA: el nuevo reto de la gestión del riesgo

La IA ya no llega como proyecto aislado: llega dentro del ERP, del CRM y de aplicaciones sectoriales. Auditarla obliga a evaluar datos, sesgos, supervisión humana y explicabilidad de las decisiones, con el AI Act imponiendo obligaciones graduadas por nivel de riesgo e ISO/IEC 42001 aportando el sistema de gestión. El paso pendiente en la mayoría de organizaciones es el mismo: pasar de la experimentación a la **gobernanza controlada**.

luisvilanova.es/auditar-la-inteligencia-artificial-el-nuevo-reto-de-la-gestion-del-riesgo-tecnologico/

TAMBIÉN EN SEPTIEMBRE · CIBERSEGURIDAD DE TERCEROS

Tu proveedor tecnológico también puede ser tu mayor riesgo (14/09). Credenciales permanentes que nadie revoca, cuentas administrativas compartidas que impiden la trazabilidad y contratos que terminan sin procedimiento de salida. Un certificado ISO 27001 del proveedor no sustituye a la evaluación del servicio concreto que presta. — luisvilanova.es

Ciberseguridad para despachos profesionales (03/09). Los fallos que más comprometen los datos de clientes en entornos donde la confidencialidad es, además, una obligación deontológica. — luisvilanova.es

AYUDAS Y FINANCIACIÓN · INTELIGENCIA ARTIFICIAL

600 millones, 25.000 empresas y una convocatoria que aún no existe

El Plan IA360 dibuja el mayor programa de adopción de inteligencia artificial para pymes que ha habido en España. Las bases reguladoras definitivas siguen sin publicarse, y ahí está precisamente la oportunidad para los fabricantes de software.

600 M€

Dotación prevista del Bono empresarial de IA (Plan IA360).

25.000

Empresas que el Plan aspira a transformar.

2027

Piloto en el primer semestre y despliegue general antes de fin de año.

BONO IA360 · 23/09/2026

El bono no financia suscripciones: financia valor añadido propio

Es el punto que más consecuencias tiene para los desarrolladores. El bono está pensado para soluciones con **valor añadido propio sobre modelos fundacionales**, no para revender licencias o suscripciones de terceros con un margen. Eso obliga a poder documentar qué aporta el software por encima del modelo que utiliza: datos propios, ajuste, orquestación, integración, interfaz especializada, controles.

El esquema previsto incluye además diagnóstico previo de madurez de la pyme, identificación de casos de uso concretos y medición posterior del impacto. Quien llegue a la convocatoria con eso ya montado —y con el cumplimiento normativo del producto acreditado— competirá en otra liga.

legalauditors.es/bono-ia360-como-preparar-hoy-su-software-de-inteligencia-artificial-para-las-ayudas-que-llegaran-a-las-pymes/

MAPA DE AYUDAS · 28/09/2026

Lo que hay ahora y lo que llega en 2027

Más allá del bono, el artículo ordena el resto de instrumentos disponibles: **CDTI** para proyectos de I+D en IA; **ININTERCONECTA STEP 2026**, con 138 millones de euros en subvenciones FEDER para tecnologías estratégicas; una iniciativa de **Red.es** de 40 millones para ecosistemas de IA; el **EIC Accelerator** europeo para startups; y **GenAI4EU**, con cerca de 700 millones destinados a IA generativa.

2027 se perfila como el año decisivo para la adopción empresarial de IA en España. Las bases definitivas de varios de estos programas siguen pendientes.

legalauditors.es/ayudas-para-desarrolladores-de-software-con-inteligencia-artificial-en-espana-oportunidades-actuales-y-previstas-para-2027/

SERVICIO · 29/09/2026

Gestión integral de ayudas para proyectos de IA

Cierra el bloque la presentación del servicio de gestión integral: desde el encaje del proyecto en la convocatoria adecuada hasta la justificación posterior, pasando por la documentación técnica que la ayuda exige y que, en la práctica, es la misma que exige una auditoría de cumplimiento.

legalauditors.es/gestion-integral-de-ayudas-para-proyectos-de-inteligencia-artificial/

FACTURA ELECTRÓNICA B2B · LEY CREA Y CRECE

Un XML válido no es necesariamente una factura conforme

EN 16931 define qué es una factura electrónica europea. La SPFE define cómo circula. VERI*FACTU define cómo se comporta el software que la emite. Son tres cosas distintas y ningún ERP puede permitirse confundirlas.

NORMA EUROPEA · 28/09/2026

EN 16931: la semántica manda sobre la sintaxis

Generar un XML técnicamente válido no significa generar una factura conforme con EN 16931. La norma impone además **reglas de negocio y requisitos semánticos**, y admite distintas sintaxis —con UBL y Facturae como transformaciones posibles entre formatos—. Para un ERP, el trabajo real consiste en mapear correctamente lo que guarda en su base de datos con los términos definidos por la norma: datos fiscales, identificadores, fechas e impuestos.

Consecuencia directa sobre las pruebas: no basta con verificar que el fichero se genera; hay que validar que es **semánticamente correcto**. La versión de 2017 se retiró formalmente en mayo de 2026 y sigue siendo válida durante la transición hacia la nueva versión publicada ese mismo año.

leycreaycrece.com/en-16931-la-norma-europea-que-estara-detras-de-la-factura-electronica-b2b/

DOBLE OBLIGACIÓN · 14/09/2026

SPFE y VERI*FACTU: por qué los ERP deberán adaptarse a dos cosas distintas

VERI*FACTU regula los sistemas informáticos de facturación (SIF) conforme al RD 1007/2023: integridad, trazabilidad, conservación e inalterabilidad de los registros. La SPFE —Solución Pública de Facturación Electrónica— implementa la factura electrónica B2B de la Ley Crea y Crece y del RD 238/2026, y gobierna cómo se generan, intercambian y gestionan esas facturas.

Dicho de otro modo: VERI*FACTU controla el software; la SPFE controla la circulación. Una misma factura puede tener que cumplir ambas, y **enviarla a la SPFE no equivale a cumplir VERI*FACTU**. La conclusión para fabricantes es una arquitectura multinorma, no un parche.

leycreaycrece.com/spfe-y-verifactu-por-que-los-erp-deberan-adaptarse-a-dos-obligaciones-diferentes/

AGENDA · 15 DE OCTUBRE, 10:00–13:00 H

I Congreso sobre la Ley Crea y Crece y la factura electrónica B2B. Presencial con asistencia online gratuita. Participan especialistas de la AEAT, abogados, expertos fiscales y proveedores de plataformas de facturación. En el programa: formatos estructurados, interoperabilidad entre plataformas, estados de factura, requisitos técnicos para ERP y coordinación entre Ley Crea y Crece y VERI*FACTU.

También publicado: el dossier especial tras el webinar de la AEAT del 10/09 y el análisis de por qué la Ley Crea y Crece es clave para las pymes y la competitividad empresarial (22/09).

leycreaycrece.com/la-factura-electronica-b2b-llega-a-espana-primer-congreso-sobre-la-ley-crea-y-crece/ (24/09/2026) · leycreaycrece.com/factura-electronica-b2b-y-ley-crea-y-crece-publicamos-nuestro-dossier-especial-tras-el-webinar-de-la-aeat-10-09-2026/ · legalauditors.es/primer-congreso-de-espana-de-ley-crea-y-crece-de-factura-b2b-obligatoria/

Lo que el software permite hacer pesa más que lo que dice el manual

Cinco años auditando sistemas de facturación dan para una conclusión sencilla: un software puede superar las comprobaciones técnicas de VERI*FACTU y seguir teniendo funcionalidades que ponen a su usuario en riesgo sancionador.

01.01.2027

Fecha límite de adaptación para sociedades.

01.07.2027

Fecha límite para el resto de obligados.

150.000 €

Sanción por ejercicio económico (art. 201 bis LGT).

AUDITORÍA Y CERTIFICACIÓN · 23/09/2026

No se audita la especificación: se audita el comportamiento

La diferencia está en el enfoque. Una comprobación técnica valida que el sistema genera los registros de facturación con el formato, el encadenamiento y la huella que exige el reglamento. Una auditoría de comportamiento revisa **qué permite hacer el software a quien se sienta delante**: altas, anulaciones, rectificaciones, permisos, integraciones e importaciones.

Ahí aparecen los hallazgos que importan. Funcionalidades aparentemente inocuas —una importación masiva que sobrescribe, un rol con capacidad de borrado lógico, una integración que reenumera— que permiten omitir, modificar o eliminar operaciones sin dejar la traza adecuada. Nadie las había mirado nunca desde una perspectiva regulatoria porque se diseñaron como comodidades de uso.

El artículo 201 bis de la Ley General Tributaria no sanciona la intención: sanciona la tenencia y uso de sistemas que permitan llevar contabilidades distintas o alterar registros. De ahí que la pregunta correcta para un fabricante no sea «¿cumpló?», sino **«¿qué puede hacer un usuario con mi producto que yo no haya previsto?»**.

leyantifraude.com/auditoria-y-certificacion-de-ley-antifraude-y-verifactu-cinco-anos-auditando-lo-que-el-software-realmente-permite-hacer/

DEL ARCHIVO RECIENTE

- **Restaurar una copia de seguridad** (25/08): el riesgo que muchos desarrolladores no contemplan en VERI*FACTU. Una restauración mal diseñada puede romper el encadenamiento de registros.
- **Situación actual y preparación para 2027** (16/08): qué deben tener listo las empresas y en qué orden.
- **Versión 1.3 de la aplicación pública de la AEAT** (03/08) y cambios en las FAQ del Reglamento SIF.

CONTROL HORARIO · REGISTRO DE JORNADA

Cuatro años de registros, y poder demostrar quién los tocó

La inspección ha dejado de preguntar si la empresa registra la jornada. Ahora pregunta si ese registro puede acreditarse tal y como se produjo, y qué pasó con cada modificación posterior.

CONSERVACIÓN · 28/09/2026

Cuatro años, disponibles y trazables

El artículo 34.9 del Estatuto de los Trabajadores fija la conservación en **cuatro años**, y esa obligación no decae porque la empresa cambie de plataforma: si se migra, los registros anteriores tienen que seguir siendo recuperables. Deben estar disponibles para los trabajadores, sus representantes y la Inspección de Trabajo, y su tratamiento se ampara en el cumplimiento de una obligación legal, sin que haga falta consentimiento del empleado.

La norma no impone formato —papel o digital—, pero solo un sistema digital bien diseñado permite lo que de verdad se exige: recuperar el histórico y acreditar **qué se modificó, cuándo y quién lo hizo**. Y, a la vez, respetar minimización: registrar la jornada no habilita a recoger datos adicionales «por si acaso».

controlhorario.es/cuanto-tiempo-debe-conservar-una-empresa-los-registros-horarios-y-como-debe-almacenarlos/

BIOMETRÍA · 21/09 Y 14/09/2026

La AEPD reabre el debate con un nuevo borrador de guía

Tras la anulación de la guía anterior, la Agencia ha puesto en circulación un nuevo borrador. Conviene el recordatorio que hace el artículo: **un borrador de guía no es una norma jurídica**, es una herramienta orientativa. Lo que sí permanece es el marco: los datos biométricos son especialmente sensibles y exigen análisis específico.

La organización tiene que poder documentar por qué la biometría es **necesaria y proporcionada** frente a alternativas menos invasivas, integrar la seguridad desde el diseño y realizar la evaluación de impacto. La pregunta a responder no es «¿podemos hacerlo?», sino «¿es necesario, proporcionado y justificable?».

controlhorario.es/biometria-y-control-de-acceso-que-implica-el-nuevo-borrador-de-guia-de-la-aepd/

REFORMA PENDIENTE · 07/09 Y 01/09/2026

Registro de jornada digital y teletrabajo

Sobre la futura regulación del registro digital, las propuestas recogidas apuntan a requisitos comunes de seguridad y fiabilidad con flexibilidad por tamaño de empresa, sistemas que garanticen integridad y conservación con capacidad de acreditar posteriormente qué ocurrió, mecanismos de verificación previa u homologación, implantación escalonada en 12–24 meses y apoyo técnico y económico a las pequeñas empresas. En paralelo, el teletrabajo plantea su propia pregunta probatoria: cómo demostrar cuándo empieza y termina realmente la jornada.

controlhorario.es/registro-de-jornada-digital-fiabilidad-adaptacion-y-control-ante-la-nueva-regulacion/ · controlhorario.es/control-horario-y-teletrabajo-como-demostrar-realmente-cuando-empieza-y-termina-la-jornada/

PERITAJE INFORMÁTICO · PRUEBA ELECTRÓNICA

De «¿qué muestra esto?» a «¿podemos demostrar que es auténtico?»

La IA generativa ha cambiado la pregunta que se hace ante un archivo audiovisual en sede judicial. Y ha subido el listón de lo que se espera de un perito.

DEEPPAKES · 14/09/2026

Cómo se demuestra que un audio, una imagen o un vídeo han sido manipulados

En vídeo, el análisis forense examina metadatos —fechas, dispositivo, codificación—, irregularidades entre fotogramas, huellas de compresión, movimientos faciales e iluminación. En audio, la continuidad de la señal, los patrones de ruido, los cortes y las características acústicas. Los valores **hash** verifican la integridad del archivo analizado.

Dos cautelas relevantes. La primera: la procedencia y la cadena de custodia son determinantes, y el archivo original debe conservarse documentadamente. La segunda: las herramientas automáticas de detección **no constituyen prueba concluyente por sí solas** —la tecnología de generación evoluciona más rápido que la de detección—, de modo que el dictamen se sostiene sobre un análisis multidimensional, no sobre la salida de un detector.

leyesytecnologia.com/deepfakes-ante-los-tribunales-como-demostrar-que-un-audio-una-imagen-o-un-video-han-sido-manipulados/

ACCESOS NO AUTORIZADOS · 03/09/2026

Correo electrónico corporativo: qué evidencias hay que preservar, y rápido

Los registros de actividad —fecha, IP, dispositivo— son la prueba central, junto con las cabeceras de los mensajes. Hay indicios que rara vez fallan: reglas de reenvío que nadie recuerda haber creado, cambios en los métodos de recuperación de la cuenta, sesiones abiertas desde ubicaciones imposibles.

Sobre la preservación, el artículo es tajante: **las capturas de pantalla no bastan**. Hace falta un mecanismo que garantice la integridad mediante funciones hash y una cadena de custodia documentada. Y hay que actuar deprisa: algunos registros se conservan solo durante un tiempo limitado y las acciones posteriores pueden alterar información decisiva.

leyesytecnologia.com/como-demostrar-un-acceso-no-autorizado-al-correo-electronico-de-una-empresa/

PROYECTOS DE SOFTWARE · 07/09/2026

«Está al 80 %»: cómo se mide de verdad el avance de un proyecto

Un porcentaje declarado no es un dato, es una opinión. El perito reconstruye qué se prometió a partir del contrato, las especificaciones funcionales y la documentación técnica; después revisa funcionalidad por funcionalidad —completada y operativa, parcial, con errores o no desarrollada—, analiza el código y los repositorios, verifica los tickets de las herramientas de gestión, ejecuta pruebas y **separa los cambios de alcance posteriores**. Ponderando criticidad y complejidad se obtiene un porcentaje defendible.

leyesytecnologia.com/proyecto-terminado-al-80-como-puede-determinar-un-perito-que-parte-del-trabajo-esta-realmente-realizada/

PERITAJE Y AUDITORÍA SAP

Un CVSS 10.0, una migración con fecha y un conflicto que aún se puede evitar

Septiembre ha dejado en el mundo SAP las tres cosas que suelen ir juntas: una vulnerabilidad crítica, un soporte que se acaba y proyectos que empiezan a discutirse en términos contractuales.

SEGURIDAD · 21/09/2026

CVE-2026-44756: corrupción de memoria en el procesamiento de Extended Passport

Puntuación **CVSS 10.0**, la máxima. Afecta al kernel ABAP y compromete confidencialidad, integridad y disponibilidad a la vez. Acciones: revisar la versión del kernel, verificar los niveles de parche conforme a las notas SAP **3747649** y **2083594**, priorizar los sistemas críticos y **documentar todo lo actuado**. Un aviso así se gestiona desde un proceso permanente de gestión de vulnerabilidades, no desde una reacción puntual.

peritajesap.es/sap-alerta-sobre-una-vulnerabilidad-critica-con-cvss-10-0-que-deben-revisar-las-empresas/

AUDITORÍA DE IMPLANTACIÓN · 28/09/2026

SAP Activate Evaluation: auditar antes de que el conflicto sea irreversible

Herramienta propia con más de **500 criterios de evaluación** que analiza si una implantación de S/4HANA se ejecuta conforme a la metodología SAP Activate. Recorre las fases Discover, Prepare, Explore, Realize, Deploy y Run, y revisa gobierno del proyecto, Clean Core, Fit-to-Standard, integraciones, migraciones, seguridad, pruebas y cutover. Sirve como auditoría preventiva durante la implantación y como instrumento pericial cuando el conflicto ya existe.

peritajesap.es/sap-activate-evaluation-auditar-una-implantacion-sap-antes-de-que-el-conflicto-sea-irreversible/

CONTROVERSIAS Y MIGRACIÓN · 28/09 Y 07/09/2026

Documentación antes del MASC, y la cuenta atrás de SAP ECC

Antes de iniciar un **MASC** —medio adecuado de solución de controversias— conviene pedir al partner lo que permite sustituir percepciones por evidencias: ofertas y alcance contractual, actas de gobierno, diseños funcionales, planes y resultados de pruebas, registro de cambios y la decisión de Go-Live.

En paralelo, el calendario: el soporte estándar de **SAP ECC** termina a finales de **2027**, con mantenimiento extendido de pago hasta 2030 y soporte de S/4HANA garantizado hasta 2040. Antes de migrar: inventario técnico-funcional, modelo de migración, contratos precisos sobre alcance y responsabilidades, validación de la integridad de los datos y pruebas documentadas.

peritajesap.es/que-documentacion-pedir-al-partner-de-sap-antes-de-iniciar-un-masc/ · peritajesap.es/sap-ecc-se-acerca-a-2027-que-deben-revisar-las-empresas-antes-de-migrar-a-s-4hana/

ADEMÁS · PeritajeSAP.es, en la revista de AUSAPE (14/09), y pruebas de aceptación en proyectos SAP (14/09): por qué el acta de aceptación acaba siendo decisiva en un conflicto.

TASACIÓN DE SOFTWARE

La deuda técnica no aparece en la cuenta de resultados. En el precio, sí

Un software que funciona correctamente puede valer bastante menos de lo que su propietario cree. Lo que descuenta valor no es la antigüedad: es lo que la antigüedad obliga a gastar.

OBSOLESCENCIA · 28/09/2026

Cuándo la antigüedad tecnológica empieza a reducir el valor

La edad del código, por sí sola, no deprecia nada. El deterioro económico empieza cuando la antigüedad genera consecuencias concretas: tecnologías base sin soporte, deuda técnica acumulada, dificultad para encontrar especialistas y problemas de integración con sistemas modernos. El comprador no descuenta por el año de creación: descuenta por **la inversión que anticipa** en migración, actualización de seguridad o rediseño arquitectónico.

Metodológicamente, no procede aplicar una depreciación automática. La tasación combina análisis técnico y económico —estado del código, disponibilidad de perfiles, capacidad de integración, riesgos de ciberseguridad— y lo traduce en impacto financiero.

tasacioninformatica.com/software-obsoleto-cuando-la-antigüedad-tecnologica-empieza-a-reducir-su-valor/

DEUDA TÉCNICA · 22/09/2026

Lo decisivo es el coste de corregirla

Se mide analizando arquitectura, calidad de código, documentación, automatización y nivel de actualización tecnológica. No hay fórmula fija ni descuento automático: la deuda se pondera junto a facturación, cartera de clientes y perspectivas de crecimiento. Lo determinante es el **coste de corrección**: hay deficiencias que se resuelven con mejoras progresivas y otras que exigen reescritura o cambio arquitectónico. Una plataforma sostenible permite evolucionar; una plataforma endeudada convierte cada modificación en algo lento, caro y arriesgado.

tasacioninformatica.com/puede-la-deuda-tecnica-reducir-el-valor-de-un-software/

SOFTWARE CON IA · 14/09 Y 03/09/2026

Qué se valora cuando el producto lleva inteligencia artificial

Seis criterios. Si la tecnología es propia o una integración de APIs de terceros —los algoritmos, datasets y sistemas desarrollados internamente generan ventaja competitiva real—. El valor de los datos, donde un dataset exclusivo puede pesar más que el modelo, atendiendo a procedencia, calidad y derechos. La dependencia externa, si el proveedor desaparece o cambia precios. Los costes operativos recurrentes de procesamiento e infraestructura. La concentración de conocimiento en personas clave. Y la viabilidad comercial: clientes, ingresos recurrentes y crecimiento. En la misma línea, el artículo sobre **valoración de empresas SaaS** del 03/09.

tasacioninformatica.com/cuanto-vale-un-software-con-inteligencia-artificial-claves-para-realizar-una-valoracion-realista/ · tasacioninformatica.com/cuanto-vale-una-empresa-saas-las-claves-para-calculer-su-valoracion/

Cumplir y poder demostrarlo no son la misma cosa.

Auditoría informática, cumplimiento normativo del software y pericial tecnológica. Veinte años revisando lo que los sistemas realmente hacen, no lo que la documentación dice que hacen.

CUMPLIMIENTO DEL SOFTWARE

Ley Antifraude, VERI*FACTU y Ley Crea y Crece

Auditoría y certificación de sistemas de facturación, factura electrónica B2B y digitalización certificada.

SEGURIDAD DE LA INFORMACIÓN

ISO/IEC 27001, ISO/IEC 27701 y ENS

Implantación y auditoría, evaluación de proveedores y gestión de vulnerabilidades.

INTELIGENCIA ARTIFICIAL

ISO/IEC 42001 y AI Act

Inventario de sistemas, análisis de brechas, gobernanza de datos y modelos, y preparación de la certificación.

PERICIAL INFORMÁTICA

Dictámenes para procedimientos judiciales y MASC

Proyectos de software y SAP, prueba electrónica, deepfakes, accesos no autorizados y tasación de activos digitales.

«La norma se lee en una tarde. El expediente se construye durante meses.»

LUIS VILANOVA · CEO DE LEGAL AUDITORS

EN EL PRÓXIMO NÚMERO · N° 03 · NOVIEMBRE 2026

- **Crónica del I Congreso** sobre la Ley Crea y Crece y la factura B2B (15 de octubre).
- **Cuenta atrás VERI*FACTU:** catorce meses y los errores que más vemos.
- **Inventario de sistemas de IA:** cómo se levanta y qué campos no pueden faltar.
- **Registro de jornada:** estado de la reforma y qué conviene anticipar.