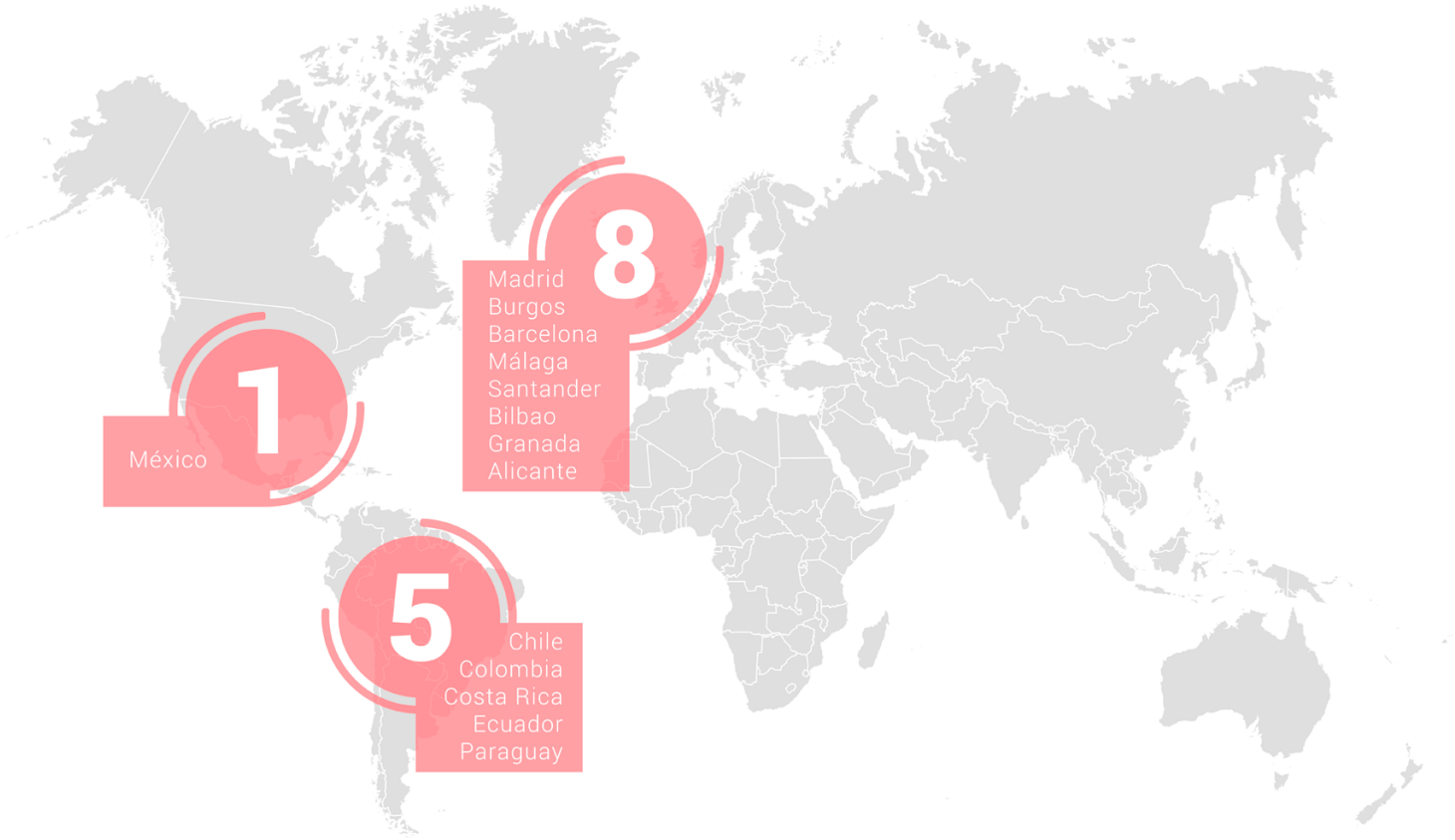
GrupoACMS
CONSULTORES

GRUPO ACMS Consultores

Caso real ISO 27001 aplicado a una empresa tecnológica



AENOR
ER
Empresa Registrada
ISO 9001

(ER-0772/2013)

Alcance ISO 9001

Diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión de la calidad, medioambiental, de la prevención de riesgos laborales, protección de datos, seguridad alimentaria y de la calidad y competencia técnica en laboratorios clínicos.

Alcance ISO 27001

Los sistemas de información que dan soporte a las actividades de diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión y el diseño, desarrollo y comercialización de software de sistemas de gestión de acuerdo con la declaración de aplicabilidad vigente.

AENOR
ER
Seguridad Información
ISO/IEC 27001

(SI-0021/2020)

Publicado el 06/02/2026

Caso real ISO 27001 aplicado a una empresa tecnológica

Las compañías tecnológicas dedicadas al desarrollo de software, apps o soluciones digitales personalizadas gestionan información de alto valor: código propio, datos personales, información confidencial de clientes y conocimiento estratégico.

Aun así, en muchos casos la protección de estos activos evoluciona de forma irregular, condicionada por la carga de trabajo y la capacidad técnica del equipo, sin un marco global que estructure y alinee la seguridad.

Con motivo del Día de Internet Seguro, presentamos el análisis de un caso real de una empresa tecnológica que optó por implantar y certificar ISO 27001.

Lo explicaremos con un enfoque totalmente práctico, alejado de la teoría o del mero cumplimiento documental: cómo era su punto de partida, por qué tomó la decisión, cómo se desarrolló la implantación y qué transformaciones se produjeron tras el proceso.

El objetivo de este análisis es aportar criterio a todas las empresas tecnológicas que se plantean si ISO 27001 tiene sentido para ellas? o no.

El contexto: empresas tecnológicas, innovación y riesgo

La empresa analizada es una compañía tecnológica de tamaño medio, especializada en el desarrollo de soluciones digitales a medida, aplicaciones móviles y plataformas software para distintos sectores. Trabaja por proyectos, con equipos multidisciplinares y un fuerte componente de innovación.

Como ocurre en muchas empresas de este perfil, el foco estaba en cumplir plazos y requisitos funcionales, la seguridad se abordaba desde el punto de vista técnico, no de gestión, y existía una alta dependencia de personas clave.

No había incidentes graves, pero sí una sensación creciente de que la seguridad de la información se sostenía más por la experiencia del equipo que por un enfoque estructurado.

Antes de ISO 27001: sensación de control, pero sin visión global

Antes de iniciar la implantación del sistema ISO 27001, la empresa contaba con medidas de seguridad razonables desde un punto de vista técnico, como el control de accesos a sistemas, uso de entornos cloud con proveedores reconocidos, copias de seguridad, buenas prácticas de desarrollo seguro...

Sin embargo, estas medidas no estaban integradas en un sistema de gestión. Cada proyecto, cada equipo y cada responsable aplicaba la seguridad ?a su manera?.

Algunas señales claras de esta situación eran que había ausencia de un análisis formal de riesgos de la información, decisiones de seguridad basadas en la urgencia del proyecto, documentación mínima o inexistente y dificultad para demostrar a terceros cómo se protegía la información.

La seguridad existía, pero no era demostrable ni homogénea.

El punto de inflexión: cuando los clientes empiezan a preguntar

El detonante no fue un ciberataque grave, fue algo mucho más habitual en empresas tecnológicas en crecimiento: los clientes empezaron a hacer preguntas incómodas.

En procesos de preventa y renovación de contratos comenzaron a aparecer cuestiones como:

- ¿Cómo gestionáis la seguridad de la información?

- ¿Tenéis un sistema formal?

- ¿Podéis demostrarlo?

- ¿Cumplís con estándares reconocidos?

Al principio, estas preguntas se respondían con explicaciones técnicas y documentos ad hoc. Pero el esfuerzo era cada vez mayor y la sensación interna era clara: se estaba improvisando.

La dirección entendió que el problema no era tecnológico, sino de enfoque. No bastaba con ?hacer las cosas bien?; había que ordenarlas, documentarlas y poder demostrarlas.

La decisión: por qué ISO 27001 y no soluciones aisladas

En ese contexto, la empresa valoró distintas opciones, como reforzar medidas técnicas puntuales, contratar auditorías de seguridad aisladas, o implantar un sistema de gestión de la seguridad de la información.

La elección de ISO 27001ciberseguridad no se basó en la certificación en sí, sino en varios factores clave, ya que ISO 27001 es un marco reconocido internacionalmente, permite hablar el mismo lenguaje que clientes y partners, es independiente de tecnologías concretas, y, sobre todo, obliga a analizar riesgos y tomar decisiones conscientes.

La certificación se planteó como una consecuencia natural del proceso, no como el objetivo principal.

La implantación: lo que realmente supone en una empresa tecnológica

Uno de los mayores miedos de nuestro cliente era que ISO 27001 supusiera burocracia, lentitud o freno a la innovación. La implantación demostró que el verdadero reto no estaba en la norma, sino en cómo se interpreta y se aplica.

Durante el proceso tuvimos que hacer frente a resistencias habituales, como por ejemplo, desarrolladores que veían la norma como ?papel?, responsables de proyecto preocupados por los plazos, dudas sobre cómo encajar ISO 27001 con metodologías ágiles.

La clave estuvo en adaptar el sistema a la realidad de la empresa, integrando la seguridad en los procesos existentes, definiendo responsabilidades claras, y priorizando controles en función del riesgo real, no del cumplimiento formal.

ISO 27001 no eliminó la flexibilidad, pero sí puso límites claros y criterios comunes.

Después de ISO 27001: cambios visibles y cambios silenciosos

Tras la certificación, los cambios más visibles fueron externos dado que:

- Obtuvieron mayor confianza en procesos de preventa.

- Se redujo el tiempo dedicado a responder cuestionarios de clientes.

- Se mejoró el posicionamiento frente a competidores similares,

- Y las auditorías de clientes fueron más fluidas.

Pero los cambios más importantes fueron internos y menos evidentes, como por ejemplo, las decisiones sobre seguridad dejaron de ser improvisadas, el conocimiento dejó de depender de personas concretas, los riesgos se analizaron antes de aceptar determinados proyectos, y la dirección ganó visibilidad real sobre la seguridad de la información.

La empresa no se volvió ?invulnerable?, pero sí más consciente, más ordenada y más previsible.

Qué enseña este caso a otras empresas tecnológicas

En base a nuestra experiencia, como expertos ISO y sobre todo como consultores ISO 27001, este caso real deja varios aprendizajes relevantes, que exponemos a continuación:

- ISO 27001 no es solo para grandes empresas.

- No sustituye al talento técnico ni a las herramientas de seguridad.

- No evita todos los incidentes, pero mejora la capacidad de respuesta.

- No todas las empresas necesitan certificarse de inmediato.

- Pero muchas sí necesitan trabajar como si fueran a certificarse.

La diferencia no está en tener el certificado, sino en adoptar el enfoque.

Cuándo tiene sentido plantearse ISO 27001

A la vista de este caso, podemos decir que ISO 27001 suele tener sentido cuando una empresa tecnológica gestiona información crítica de clientes, crece y necesita escalar sin perder control, participa en proyectos con requisitos de seguridad elevados, o quiere diferenciarse demostrando confianza, no solo prometiéndola.

En estos casos, la norma no es una carga, sino una herramienta de gestión.

Implantar el sistema ISO 27001 con criterio marca la diferencia

La experiencia demuestra que implantar el sistema ISO 27001 en empresas tecnológicas exige entender tanto la seguridad de la información como la realidad del negocio y del desarrollo tecnológico. Un enfoque excesivamente teórico o burocrático suele generar rechazo y poco valor real.

Desde una perspectiva práctica y basada en implantaciones reales, es posible integrar ISO 27001 sin frenar la innovación y convertirla en un apoyo para el crecimiento y la confianza del mercado.

Acompañamos a certificación ISO 27001 y ofrecemos apoyo técnico durante todo el proceso

Si estás pensando en obtener el certificado ISO 27001 en Grupo ACMS Consultores podemos asesorarte.

Consúltanos sin compromiso, explícanos en qué podemos ayudarte y cuáles son tus dudas. Para ello puedes, rellenar nuestro formulario de contacto o llamarnos por teléfono, lo que prefieras y nos pondremos en contacto con tu empresa.

Compromisos y garantías de Grupo ACMS Consultores

Aspecto

Ventaja líder

Experiencia

Más de 25 años de trayectoria en consultoría y formación. Fundado en 1998, con más de 1.000 proyectos implantados con éxito.

Certificados propios

Disponemos de los certificados ISO 9001, ISO 27001 y Marca Madrid Excelente en ACMS España.

Porfolio y diversificación

Amplia gama de servicios de consultoría en certificación (ISO 9001, ISO 14001, ISO 45001, etc.) y acreditación (ISO 15189, ISO 17025, ISO 17020, entre otras). Capacidad para abordar proyectos integrados y multisectoriales.

Precio

Presupuestos personalizados con condiciones de pago adaptadas a las necesidades de cada cliente.

Garantía

Compromiso de acompañamiento hasta la certificación o acreditación, asegurando resultados tangibles.

Desarrollo y soporte

Asesoramiento continuo durante todo el proceso de implantación, desde el diagnóstico inicial hasta la auditoría final.

Desarrollo de sistemas de gestión totalmente adaptados a cada organización evitando la burocratización del mismo.

Diseño de procedimientos documentados, flujogramas y cuadros de gestión de procesos de fácil comprensión.

Referencias

El GRUPO ACMS trabaja con pequeñas y grandes empresas tanto del sector público como privado. Conozca los testimonios de nuestros clientes .

Oficinas

Presencia nacional e internacional con sedes en Madrid, Barcelona, Burgos, México y Chile, lo que permite cercanía y atención personalizada.

Software propio

Plataforma ISOAPPWEB desarrollada internamente para el mantenimiento y control de la norma ISO 9001 que agiliza procesos, reduce costes y facilita el control documental.

Plataforma formación

Campus online con cursos especializados en diversas áreas donde ofrecemos asesoramiento. Incluye programas actualizados y accesibles en modalidad e-learning.

Grupo ACMS Consultores. Consultora especializada en diseño, implantación y mantenimiento de Sistemas de gestión

Nos definimos como una compañía consultora independiente cuyo objetivo fundamental es suministrar servicios de consultoría en las áreas de Gestión empresarial, que representen para el cliente una solución excelente, que satisfaga sus necesidades explícitas o implícitas, tenga en cuenta las regulaciones y normas aplicables, y cumpla los objetivos de plazo y coste establecidos.

Madrid

C/ Campezo 3, nave 5 28022 Madrid

Tfno.: (+34) 91 375 06 80

Burgos

Centro de Empresas, 73 09007 Burgos

Tfno.: (+34) 947 041 645

Barcelona

C/ Plaça Universitat 3 08007 Barcelona

Tfno.: (+34) 93 013 19 49

CDMX

José González Varela 15 14700 Tlalpan (Ciudad de México)

Tfno.: (+52) 5514 10 12 07

Santiago - Valparaiso - O´Higgins

Av. Pdte. Kennedy 7440, Oficina 701 7650618 Región Metro

Tfno.:

Veracruz

Avda 21 esquina calle 44 No.4402 Cordoba

Tfno.: (+52) 55 6576 8293

www.grupoacms.com
informacion@grupoacms.com