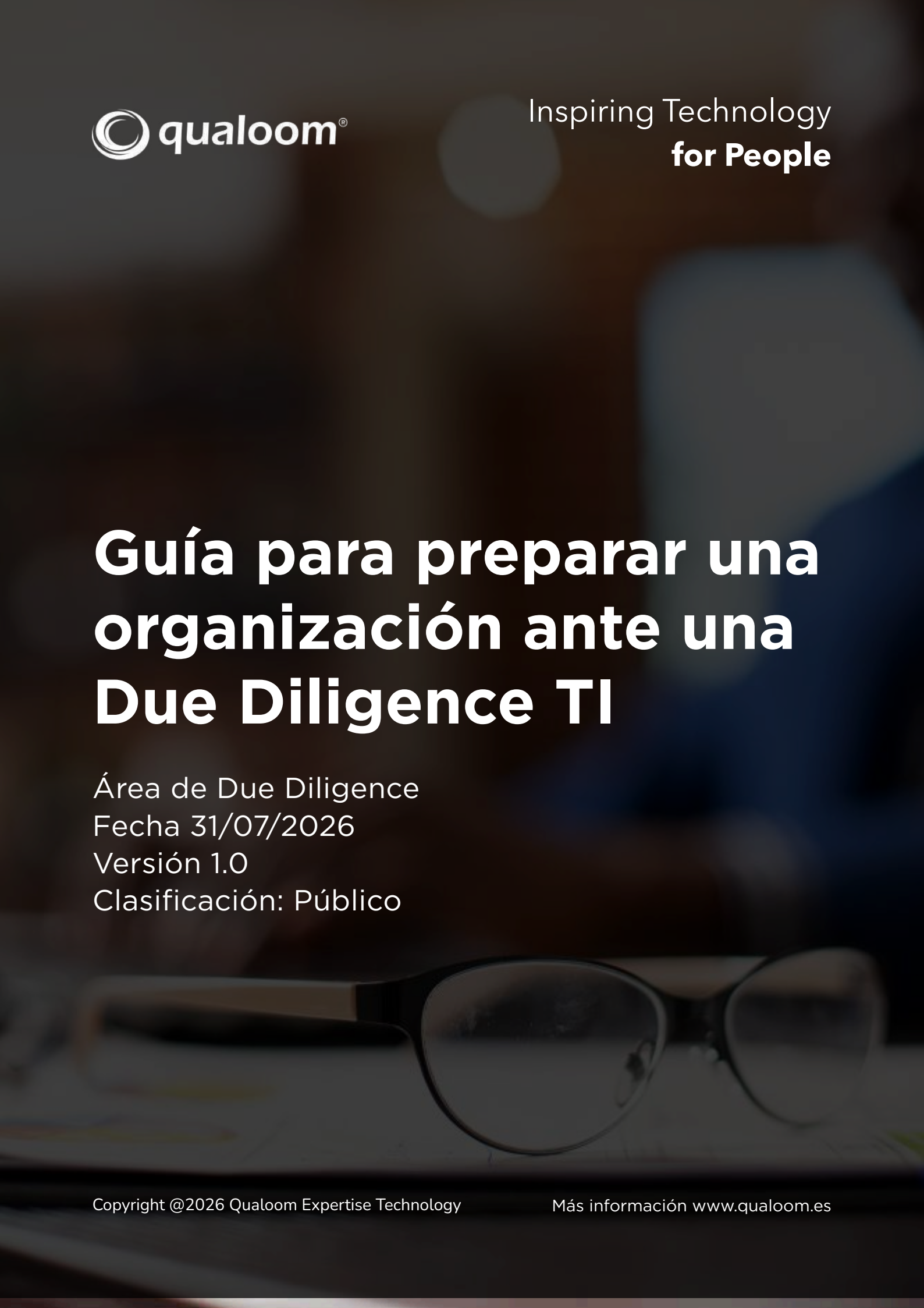
qualoom®

Inspiring Technology
for People

Guía para preparar una organización ante una Due Diligence TI

Área de Due Diligence
Fecha 31/07/2026
Versión 1.0
Clasificación: Público



Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

ÍNDICE

qualoom®

Inspiring Technology
for People

Introducción

Por qué prepararse ante una Due Diligence TI

Anticiparse a una Due Diligence TI es clave para garantizar que la infraestructura tecnológica de la organización esté **ordenada, segura y alineada con los objetivos** estratégicos. Una preparación adecuada permite **minimizar riesgos operativos y legales, aumentar la confianza de inversionistas y socios, y maximizar el valor de los activos tecnológicos.**

Beneficios de una preparación adecuada

Confianza

La claridad y organización de los activos tecnológicos proyecta profesionalismo y transparencia.

Reducción de riesgos

Identificar vulnerabilidades y pasivos permite implementar planes de mitigación antes de que se conviertan en problemas.

Incremento del valor percibido

Una infraestructura tecnológica organizada y segura se convierte en un activo estratégico para la empresa.

qualoom®

Inspiring Technology
for People

Introducción
Por qué prepararse ante una Due Diligence TI

Riesgos de no estar preparado

Integración compleja

Sistemas incompatibles o procesos duplicados pueden ralentizar fusiones y adquisiciones, generando costos adicionales.

Pasivos ocultos

La falta de control y transparencia puede disminuir la confianza de inversionistas, auditores y socios estratégicos.

Impacto reputacional

Vulnerabilidades de seguridad, licencias no regularizadas o contratos incumplidos pueden derivar en impactos financieros y legales.

qualoom®

Inspiring Technology
for People

Diagnóstico previo: conocerse a fondo

Antes de una Due Diligence TI, es esencial realizar un diagnóstico de la organización para identificar activos, riesgos y niveles de preparación tecnológica.

Inventario de activos TI

Hardware, software, licencias y servicios en la nube, asegurando control y regularización.

- Detectar activos obsoletos o subutilizados.
- Garantizar la correcta regularización de licencias y contratos.
- Identificar dependencias críticas que podrían afectar operaciones o integraciones futuras.

Arquitectura de sistemas

Diagramas de interdependencias y redundancias para evaluar resiliencia y facilitar integraciones.

- Evaluar la resiliencia y escalabilidad de los sistemas.
- Detectar posibles cuellos de botella o puntos críticos.
- Facilitar la integración de nuevos sistemas durante procesos de M&A o actualizaciones tecnológicas.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Diagnóstico previo: conocerse a fondo

Políticas y procedimientos internos

Seguridad, continuidad del negocio y cumplimiento normativo.

- Control efectivo sobre accesos y privilegios.
- Respuesta organizada ante incidentes de seguridad o fallos operativas.
- Cumplimiento de regulaciones legales y estándares internacionales aplicables.

Identificación de vulnerabilidades

Brechas de seguridad, dependencias críticas y riesgos tecnológicos que puedan afectar operaciones o integraciones.

- Revisiones de ciberseguridad y pruebas de penetración.
- Evaluación de dependencias de terceros y proveedores.
- Detección de riesgos que puedan impactar continuidad operativa o integridad de la información.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Organización documental: base para la transparencia

Contar con una **documentación organizada y completa** es un pilar fundamental en cualquier Due Diligence TI. La correcta gestión documental permite **demostrar transparencia, cumplimiento normativo y control de riesgos,** facilitando la evaluación de inversionistas, auditores o socios estratégicos.

Contratos con proveedores y licencias de software

Verificar la validez, vigencia y cobertura de todos los contratos garantiza que no existan **riesgos legales o incumplimientos** que puedan afectar la operación o la valoración del negocio.

Informes de auditorías y certificaciones

Documentación de auditorías previas y certificaciones como ISO, PCI DSS o cumplimiento de GDPR/LPD respalda la **madurez y confiabilidad del entorno TI.**

Manuales de operación y gestión de incidencias

Instrucciones claras sobre procedimientos internos y gestión de incidentes permiten **evaluar la capacidad de respuesta y continuidad operativa.**

Historial de incidentes y planes de mitigación

Registrar incidentes de seguridad, su impacto y las acciones correctivas aplicadas demuestra **gestión proactiva de riesgos y resiliencia tecnológica.**

qualoom®

Inspiring Technology
for People

Seguridad y compliance: el núcleo de la confianza

La **seguridad de la información y el cumplimiento normativo** son elementos críticos en cualquier Due Diligence TI.
Una gestión robusta en estas áreas **aseguran continuidad operativa y minimiza riesgos legales o reputacionales.**

Evaluación de ciberseguridad

Incluye la revisión de **infraestructura, sistemas y procesos** para identificar vulnerabilidades y amenazas potenciales. Esto abarca:

- Firewalls, antivirus y sistemas de detección de intrusiones.
- Monitoreo de red y análisis de logs para detectar comportamientos anómalos.
- Pruebas de penetración y simulaciones de ataque para evaluar la resiliencia de los sistemas.

Gestión de accesos y privilegios

La correcta administración de usuarios y permisos garantiza que solo el personal autorizado pueda acceder a información crítica:

- Implementación de controles internos y segregación de funciones.
- Políticas de autenticación robustas, como MFA
- Revisiones periódicas de permisos y registros de actividad para prevenir fraudes o errores.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Seguridad y compliance: el núcleo de la confianza

Cumplimiento normativo

La adherencia a regulaciones locales e internacionales asegura que la organización cumpla estándares de seguridad, privacidad y gobernanza:

- Normas ISO (ISO 27001, ISO 22301), GDPR, LOPD y SOX.
- Documentación de políticas internas y evidencia de auditorías previas.
- Monitoreo continuo de cambios regulatorios que puedan impactar procesos internos.

Planes de contingencia y recuperación ante desastres

Garantizar continuidad operativa frente a incidentes críticos es clave:

- Estrategias para recuperación de datos y restauración de servicios críticos.
- Simulaciones y pruebas periódicas de los planes de contingencia.
- Integración de estos planes dentro del marco general de gestión de riesgos de TI.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Eficiencia operativa y continuidad del negocio

Se analizan los procesos clave, métricas de rendimiento y planes de continuidad que permiten garantizar que la infraestructura TI funcione de manera eficiente y sin interrupciones

Procesos críticos

Los procesos TI deben estar **documentados, estandarizados y, en la medida de lo posible, automatizados,** para asegurar:

- Reducción de errores humanos y tiempos de respuesta más rápidos.
- Eficiencia operativa en tareas recurrentes y críticas.
- Transparencia en la gestión de incidentes y solicitudes de servicio.

Riesgos de Seguridad de la Información

Medir y monitorear indicadores clave permite evaluar la salud de la infraestructura y la efectividad de los procesos:

- Disponibilidad de sistemas y servicios críticos.
- Capacidad y uso eficiente de recursos tecnológicos.
- Tiempo de respuesta ante incidentes y resolución de problemas.
- Cumplimiento de SLA internos y externos.

Plan de transición y continuidad operativa

Especialmente relevante en fusiones, adquisiciones o integraciones de sistemas:

- Definición de pasos claros para la migración o consolidación de servicios.
- Identificación de dependencias críticas y mitigación de riesgos durante el cambio.
- Estrategias de contingencia para asegurar que los servicios críticos permanezcan operativos sin interrupciones significativas.

qualoom®

Inspiring Technology
for People

Presentar la organización de forma sólida

Preparar la presentación de la organización para una Due Diligence TI requiere **organizar la información clave, evidenciar la gestión de riesgos y mostrar la madurez operativa.** Una presentación estructurada facilita la comprensión de los auditores o inversionistas y transmite **confianza y transparencia**.

Resumen ejecutivo

Sintetiza los aspectos más relevantes de la organización TI:

- Estado de los activos y sistemas críticos.
- Principales riesgos identificados y medidas de mitigación implementadas.
- Información sobre procesos, políticas y continuidad operativa.

Evidencia de mitigación de riesgos

Proporciona soporte documental que demuestre que los riesgos han sido gestionados de manera efectiva:

- Controles de seguridad implementados.
- Resultados de auditorías internas o externas.
- Cumplimiento de normativas y certificaciones relevantes.

qualoom®

Inspiring Technology
for People

Presentar la organización de forma sólida

Cronograma de Due Diligence TI

Define de manera clara las fases del proceso, incluyendo:

- Actividades a realizar en cada fase.
- Responsables de cada tarea.
- Entregables esperados y fechas clave para su revisión.

Estrategia de comunicación

Coordina cómo se compartirá la información:

- Comunicación interna: mantener informados a los equipos sobre avances y hallazgos.
- Comunicación externa: presentación estructurada a inversionistas, auditores o socios estratégicos.
- Garantiza que la información sea clara, confiable y fácilmente verificable.

qualoom®

Inspiring Technology
for People

Valor agregado de una preparación efectiva

Una preparación adecuada frente a una Due Diligence TI genera **beneficios tangibles y estratégicos** para la organización. No se trata solo de cumplir con auditorías o evaluaciones externas, sino de fortalecer la infraestructura tecnológica, minimizar riesgos y aumentar la confianza de inversores y socios estratégicos.

Minimización de riesgos ocultos y mejora de la valoración empresarial

La identificación y mitigación anticipada de vulnerabilidades, pasivos tecnológicos y brechas de seguridad reduce la posibilidad de problemas posteriores, protege los activos críticos y mejora la percepción de valor de la organización ante inversores y potenciales compradores.

Incremento de confianza ante inversores y socios estratégicos

Una organización que presenta información clara, procesos documentados y evidencia de cumplimiento normativo transmite profesionalismo y transparencia, generando credibilidad y fortaleciendo relaciones estratégicas.

Fortalecimiento de la infraestructura TI y continuidad operativa

Documentar y optimizar procesos, mantener controles de seguridad y tener planes de contingencia claros garantiza la continuidad del negocio, reduce tiempos de respuesta ante incidentes y consolida la resiliencia tecnológica.

qualoom®

Inspiring Technology
for People

Impulsa la preparación de tu organización

CONTACTA CON NOSOTROS

www.qualoom.es

contacto@qualoom.es

(+34) 91 236 4808